Improving the Generalized Feistel

Tomoyasu Suzaki[1][2] and Kazuhiko Minematsu[1]

[1] NEC Corporation, 1753, Shimonumabe, Nakahara, Kawasaki 211-8666, Japan
{t-suzaki@pd, k-minematsu@ah}.jp.nec.com
[2] Chuo University, 1-13-27, Kasuga, Bunkyo, Tokyo 112-8551, Japan

Abstract. The generalized Feistel structure (GFS) is a generalized form of the classical Feistel cipher. A popular version of GFS, called Type-II, divides a message into $k > 2$ sub blocks and applies a (classical) Feistel transformation for every two sub blocks, and then performs a cyclic shift of k sub blocks. Type-II GFS has many desirable features for implementation. A drawback, however, is its low diffusion property with a large k. This weakness can be exploited by some attacks, such as impossible differential attack. To protect from them, Type-II GFS generally needs a large number of rounds.
In this paper, we improve the Type-II GFS's diffusion property by replacing the cyclic shift with a different permutation. Our proposal enables to reduce the number of rounds to attain a sufficient level of security. Thus, we improve the security-efficiency treading off of Type-II GFS. In particular, when k is a power of two, we obtain a significant improvement using a highly effective permutation based on the de Bruijn graph.

Key words: block cipher, generalized Feistel, diffusion, de Bruijn graph

1 Introduction

The generalized Feistel structure (GFS) is one of the basic structures of a block cipher. While basic Feistel ciphers divide a message into two sub blocks, GFS divides a message into k sub blocks for some $k > 2$, which is called the partition number. One popular form of GFS is so-called Type-II[3][28], where the output of a single round of Type-II GFS for input $(m_0, m_1, \dots, m_{k-1})$ is $(c_0, c_1, \dots, c_{k-1}) = (F_0(m_0) \oplus m_1, m_2, F_1(m_2) \oplus m_3, m_4, \dots, F_{k-2/2}(m_{k-2}) \oplus m_{k-1}, m_0)$, where F_is are round functions. As we can see, this operation is equivalent to applying Feistel transformation $(x, y) \rightarrow (x, F(x) \oplus y)$ for every two blocks and then performing a (left) cyclic shift of sub blocks. Recently, Type-II GFS receives a lot of attention for its simplicity and high parallelism. We have some modern Type-II-based block ciphers, e.g., CLEFIA [25] ($k = 4$), and HIGHT [11] ($k = 8$). When the length of message is fixed, the width (i.e., I/O lengths) of round function gets shorter as the partition number grows. Since the width of round function is a critical factor of the size of implementation, Type-II GFS with a large

[3] Zheng et al. [28] refers to this as the Type-II Feistel-Type Transformation. Some studies use the word GFS to mean Type-II GFS, e.g., [19].

partition number is considered to be suitable for small-scale implementations. Moreover, as well as the Feistel cipher, Type-II GFS's round function needs not be invertible. Thus, the implementation cost for decryption would be negligibly small when the encryption has been implemented. This can be an advantage over Substitution-Permutation Network (SPN) ciphers such as AES, if we focus on small-scale implementation while need decryption in its usage. This holds true for many block cipher modes such as CBC, OCB [24], and the most of storage encryption modes, e.g. EME [10]. However, Type-II GFS with a large k has one big drawback, namely its low diffusion. In order to diffuse the input difference to all output sub blocks, we need about k rounds (see Section 2.2 for details). If diffusion of input difference is imperfect, there will be some attacks, such as impossible differential attack [2] or saturation attack [7], etc. Hence, there is a treading off between efficiency (i.e. the number of rounds) and compactness (i.e. the partition number). This might be the reason why recent GFS ciphers have relatively small k to keep a balance of implementation size and speed.

To our knowledge, there has been no comprehensive study trying to improve Type-II GFS up to now. Nyberg [21] proposed a variant of Type-II GFS called Generalized Feistel Network (GFN), where a permutation of sub blocks (which we call block shuffle) different from the cyclic shift is used. She evaluated GFN's immunity against differential cryptanalysis (DC) and linear cryptanalysis (LC). However, the analysis of [21] can not be used to evaluate the goodness of diffusion. In this paper, we allow GFS to use an arbitrarily block shuffle (but identical for each round). Our goal is to find block shuffles having a better diffusion than the cyclic shift. For this purpose, we formally define a criterion for the goodness of diffusion called the maximum diffusion round, DRmax, which tells how many rounds are needed to achieve the full diffusion. Hence, a smaller DRmax would imply a faster, better diffusion. Moreover, we observe that DRmax is closely related to the security against impossible differential and saturation attacks, and the pseudorandomness analysis. This demonstrates the usefulness of our notion. We exhaustively searched the shuffles up to $k = 16$, using a computer. As a result, a better shuffle than the cyclic shift exists for $k \geq 6$. In addition, we present a family of highly diffusive shuffles when k is a power of two. This is based on the de Bruijn graph, and achieves DRmax being about $2 \log_2 k$. As DRmax of Type-II GFS is k, this means a significant improvement for a large k. To see the validity of our proposal, we also investigated our proposal's resistance against DC and LC, and experimentally confirmed that ours have the same resistance against these attacks as those provided by the cyclic shift. Our result enables us to build a secure GFS cipher having a fewer rounds than Type-II without increasing the implementation cost. From practical viewpoint, the primal application of our result would be the construction of small-scale block ciphers, where many ciphers are recently proposed in this category [4][11]. Additionally, it will also be useful to build large-block ciphers, such as 256 or 512-bit block. Applications of large-block ciphers are, e.g., storage encryption or block cipher-based hash functions, as mentioned by Junod and Macchetti [22].

2 Generalized Feistel Structure

2.1 Definition of GFS

First, let us make clear what GFS means in this paper. Let k be an even integer. A single round of k-partition GFS is a permutation over $(\{0,1\}^n)^k$ defined as

$$\begin{aligned}&(X_0, X_1, \ldots, X_{k-1})\\ &\to \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, \ldots, F_{(k-2)/2}(X_0) \oplus X_1),\end{aligned} \tag{1}$$

where $F_i : \{0,1\}^n \to \{0,1\}^n$ is a cryptographic keyed function called a round function, and $\pi : (\{0,1\}^n)^k \to (\{0,1\}^n)^k$ is a deterministic permutation. Here, we restrict π to be a block-wise permutation, i.e., a shuffle of k sub blocks. An encryption of a GFS cipher is done by iterating the above permutation for certain number of rounds, r, where the first input is the plaintext and the r-round output is the ciphertext. For the decryption, we perform an inversion of Eq. (1) using the inverse of π, denoted by π^{-1}. Throughout the paper, k denotes the partition number (the number of sub blocks) and n denotes the bit length of sub block. Thus a GFS cipher is always a kn-bit block cipher.

As mentioned, the most popular instance of GFS is Type-II proposed by Zheng et al.[28], which uses the left cyclic shift as π, i.e., $\pi(X_0, X_1, \ldots, X_{k-1}) = (X_1, X_2, \ldots, X_{k-1}, X_0)$, as shown by Fig. 1(Left). Another known instance of GFS is Nyberg's Generalized Feistel Network (GFN)[21]. It uses a different permutation π. A GFS using block shuffle π is denoted by GFS_π. Thus, if π is the (left) cyclic shift GFS_π is identical to Type-II GFS.

For convenience, we define the following notations. An input data to the $i+1$-th round for $i \geq 0$ is written as $X^i = (X^i_0, X^i_1, \cdots, X^i_{k-1})$, and the intermediate data is $Y^{i+1} = (Y^{i+1}_0, Y^{i+1}_1, \cdots, Y^{i+1}_{k-1})$, where $Y^{i+1}_j = X^i_j$ if j is even and $Y^{i+1}_j = X^i_j \oplus F^i_{(j-1)/2}(X^i_{j-1})$ if j is odd. Here F^i_h for $h = 0, 1, \ldots, m-1$ is the h-th (from left to right) F function in the i-th round. If underlying block shuffle is π, the output of $i+1$-th round (which is equivalent to the $i+2$-th round input) is $X^{i+1} = \pi(Y^{i+1})$. See Fig. 1 for reference.

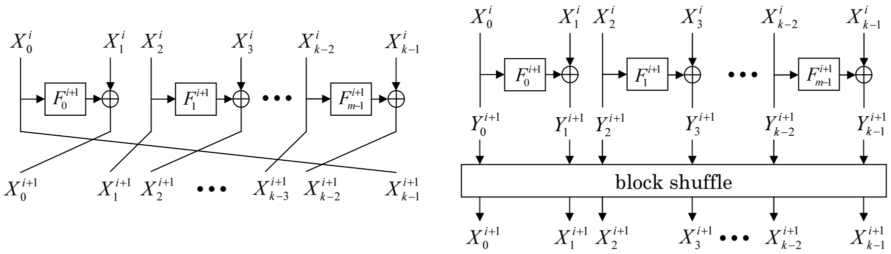

Fig. 1. Type-II GFS (Left) and Our generalization (Right)

2.2 Diffusion Property of Type-II GFS

In this section, we introduce a formal notion of the diffusion property of GFS. What we mean by 'diffusion' here is the state that a sub block input affects all of the sub blocks of output. More formally, if $X_j^{r_2}$ can be expressed by an equation containing $X_i^{r_1}$ for some i and $r_1 < r_2$, we say $X_j^{r_2}$ is affected by $X_i^{r_1}$. If all of the output sub blocks of the r_2-th round is affected by $X_i^{r_1}$, then we say $X_i^{r_1}$ has diffused to all of the sub-blocks in round r_2. For instance, in Type-II GFS, X_0^i can be expressed as $F_0^i(X_0^{i-1}) \oplus X_1^{i-1}$. Therefore X_0^i is affected by X_0^{i-1} and X_1^{i-1}. Note that the expression is allowed to include the target sub block in the raw or as an argument of F. Using this, we make the following definition.

Definition 1. *For* GFS_π, *let* $\mathrm{DR}_i(\pi)$ *be the minimum number of rounds such that the i-th sub input block of the first round,* X_i^0, *is diffused to all sub output blocks. Then, the maximum diffusion rounds for* GFS_π, *denoted by* $\mathrm{DRmax}(\pi)$, *is defined as* $\mathrm{DRmax}(\pi) \overset{\mathrm{def}}{=} \max_{0 \le i \le k-1} \mathrm{DR}_i(\pi)$. *If π is clear from the context, we simply write* DR_i *or* DRmax.

It is trivial to see that X_i^0 is diffused to all sub output blocks after any round greater than $\mathrm{DR}_i(\pi)$. Thus, for any GFS_π, any sub output block is affected by any sub input block after $\mathrm{DRmax}(\pi)$ rounds. We call this state the *full diffusion*. As we will see, if full diffusion has not been attained a certain attack is possible. Hence, any GFS_π cipher needs at least $\mathrm{DRmax}(\pi)$ rounds for its security[4], implying that a block shuffle π with a small $\mathrm{DRmax}(\pi)$ is desirable.

To understand the property of DRmax, Fig. 2 shows traces of the paths that represents how X_7^0 diffuses to all sub blocks in Type-II GFS with $k = 8$. The thick solid line is the data path that does not pass through any F function and the thick dotted lines are data paths that pass through at least one F function. The implications of these paths can be explained as follows. Let two distinct inputs be $X^0 = (X_0^0, \ldots, X_7^0)$ and $\widetilde{X}^0 = (\widetilde{X}_0^0, \ldots, \widetilde{X}_7^0)$ with $X_i^0 = \widetilde{X}_i^0$ for $i \le 6$, and $X_7^0 \oplus \widetilde{X}_7^0 = \delta$ for some $\delta \neq 0$. Then, the thick solid path indicates that $X_7^7 \oplus \widetilde{X}_7^7 = \delta$ holds with probability 1, as XORs on the path bring no difference to the initial difference, δ. In contrast, dotted paths indicate that $X_i^7 \oplus \widetilde{X}_i^7$ for all $i = 0, \ldots, 6$ is close to random due to the randomness of round functions.

As Fig. 2 suggests, for a k-partition Type-II GFS, it is easy to prove that $\mathrm{DRmax} = k$. Then, how we can improve this? Note that $X_4^3 (= X_7^0)$ affects X_5^3 via F_2^4, but X_5^3 is also affected by X_7^0 and therefore a collision of paths occur. Such collisions continue to occur in round 5 and subsequent rounds. Intuitively, what we have to do is to reduce such collisions, as frequent collisions may imply a large DRmax. For example, the above-mentioned collision can be avoided if Y_5^3 and Y_6^3 are given to F_i^4 for some $0 \le i \le 2$ and F_j^4 for some $i \neq j$, $0 \le j \le 2$.

Table 1 shows the number of collisions and its proportion to the number of XORs for DRmax rounds. As k increases, the number and the proportion of collisions also increase. This exhibits the low diffusion property of Type-II GFS.

[4] In fact, we have to take care of chosen plaintext and ciphertext attacks, thus roughly need $\mathrm{DRmax}(\pi) + \mathrm{DRmax}(\pi^{-1})$ rounds. See Section 5.2.

Table 1. Collision of data paths for k-partition Type-II GFS.

Partition number k	2	4	6	8	10	12	14	16
Number of collision	0	1	4	9	16	25	36	49
Proportion (%)	0	12.5	22.2	28.1	32.0	34.7	36.7	38.3

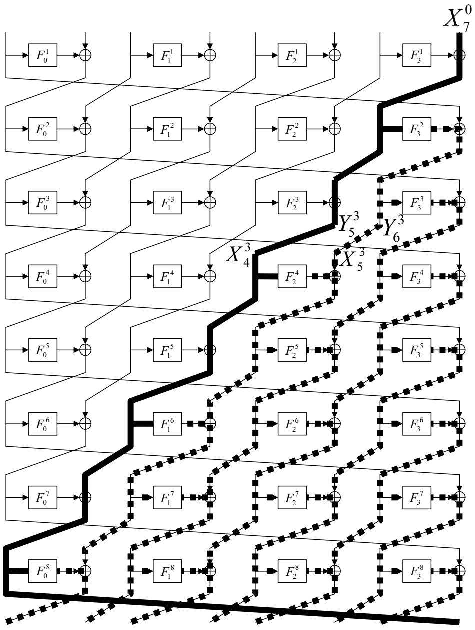

Fig. 2. Diffusion path of Type-II GFS.

3 Exhaustive Search for Optimum Shuffles

For each $4 \leq k \leq 16$, we investigated DRmax(π) for all shuffles with a computer program. Let $\varPi_k$ be the set of all shuffles of k sub blocks. Note that $|\varPi_k| = k!$. As we think the securities of encryption and decryption are equally important, we focus on finding shuffle π that has a small

$$\mathrm{DRmax}^{\pm}(\pi) \overset{\mathrm{def}}{=} \max\{\mathrm{DRmax}(\pi), \mathrm{DRmax}(\pi^{-1})\}.$$

Thus the optimum shuffle is one that provides

$$\mathrm{DRmax}^{*}_{k} \overset{\mathrm{def}}{=} \min_{\pi \in \varPi_k} \{\mathrm{DRmax}^{\pm}(\pi)\}.$$

We denote the optimum shuffle for a given k by π^*_k. Note that π^*_k may not be unique. The results are presented in Table 2 (also, see Appendix A for the specific values of block shuffles). Interestingly, π^*_k always fulfills $\mathrm{DRmax}(\pi^*_k) =$

Table 2. Search result.

Partition number k	4	6	8	10	12	14	16
DRmax_k^*	4	5	6	7	8	8	8

$\mathrm{DRmax}((\pi_k^*)^{-1})$. For example, for $k = 8$, there was a block shuffle π having $\mathrm{DRmax}(\pi) = 5$ and $\mathrm{DRmax}(\pi^{-1}) = 7$, which is not optimal in our sense. As well as DRmax, it is easy to prove $\mathrm{DRmax}^{\pm} = k$ for the cyclic shift. Thus Table 2 shows that the gain of optimum shuffle from the cyclic shift is obtained from $k = 6$ and gradually increasing. We also include Nyberg's GFN in our investigation (See [21] for the exact definition of shuffle). When $k = 4$, we have no gain, as there are only three valid shuffles: right and left cyclic shifts and Nyberg's GFN and they have $\mathrm{DRmax} = 4$. For k up to 16, the DRmax of Nyberg's GFN was the same as for Type-II GFS (we did not prove this for arbitrary k, however we think the proof is easy.). As far as we searched, any optimum block shuffle π_k^* has the property that any even-number input block is mapped to an odd-number output block, and vice versa. We refer to such shuffles as *even-odd* shuffles. From this fact, we hereafter focus on even-odd block shuffles, and we generally use the word "shuffle" to mean an even-odd shuffle. An example of π_8^* is shown in Fig. 3 (corresponding to Table 4, $k = 8$, No.1 of Appendix A). The diffusion path is represented in the same way as in Fig. 2. The collision that occurred in the fourth round of Fig. 2 is avoided, and the number of collisions is reduced from nine to four. Note that if we use different shuffles for each round, we could attain the same improvement. Since this approach will increase the implementation cost, we only consider using the same shuffle for every round.

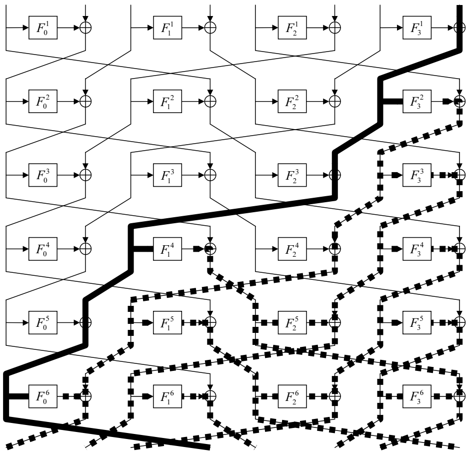

Fig. 3. GFS with an optimum shuffle for $k = 8$.

Lower Bound. A lower bound of DRmax* for even-odd shuffles can be derived as follows. For a fixed one block input difference, let N_i^o (N_i^e) be the number of odd-number (even-number) sub blocks in the i-th round output affected by that input block. Initially we have $N_0^e = 0$ and $N_0^o = 1$. If the shuffle works ideally, we have $N_i^e = N_{i-1}^e + N_{i-1}^o$, and $N_i^o = N_{i-1}^e$, thus $N_{i+2}^e = N_i^e + N_{i+1}^e$ holds true. Hence N_i^e is Fibonacci sequence. For a GFS with an even-odd shuffle, if a certain number of rounds is sufficient to achieve the diffusion to all even output blocks, the full diffusion is achieved by one more round. Therefore, if i is the smallest integer that satisfies $N_i^e \geq k/2$, $i+1$ is the lower bound of DRmax for all even-odd shuffles for k blocks (not necessarily achievable). As i-th term of Fibonacci sequence is about $\tau^i/\sqrt{5}$, where τ is the golden ratio, this lower bound is roughly $\log_\tau \sqrt{5}k/2 \simeq \log_2 1.44k$. In our search, we found block shuffles that attain the lower bound described above for all $k \leq 8$ (see Fig. 4).

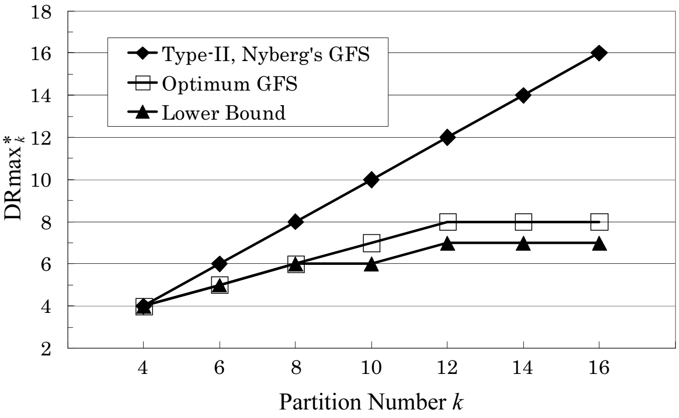

Fig. 4. Search result and lower bound for $k \leq 16$.

4 A Shuffle Family with Good Diffusion

4.1 Graphical Interpretation of Diffusion Rounds

The search result of previous section reveals optimum shuffles up to $k = 16$. Since the cost of exhaustive search exponentially grows with k, a different approach is certainly required to find a shuffle with a good diffusion for larger k. In this section we introduce a graph-theoretic interpretation of the DRmax evaluation problem for even-odd shuffles, and propose an even-odd shuffle family having much better DRmax than that of cyclic shift, for k being a power of two. For any shuffle of order k, π, let $\overline{\pi}[*] : \{0, \ldots, k-1\} \rightarrow \{0, \ldots, k-1\}$ denote the corresponding index mapping (i.e., $\pi(x_0, \ldots, x_{k-1}) = (x_{\overline{\pi}[0]}, \ldots, x_{\overline{\pi}[k-1]})$).

For any even-odd shuffle π, there is an equivalent, compact directed graph.

Definition 2. *For any even-odd shuffle π of even order k, the corresponding graph of π, denoted by $G[\pi]$, is a directed graph with order $m = k/2$. The vertices of $G[\pi]$ are labeled with $\{0, 1, \ldots, m-1\}$. Every arc (a directed edge) of $G[\pi]$ is colored red or blue, and is determined as*

- *if $\overline{\pi}[i] = j$ for even i and odd j, there is an arc colored red from node $i/2$ to node $(j-1)/2$*
- *if $\overline{\pi}[i'] = j'$ for odd i' and even j', there is an arc colored blue from node $(i-1)/2$ to node $j/2$.*

For example, the graph of the cyclic shift is in Fig, 5, where red arcs are written as thin lines and blue ones are written as thick ones.

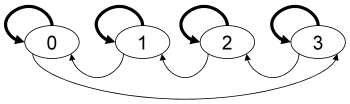

Fig. 5. Graph for the cyclic shift with $k = 8$.

For two vertices x, x' of $G[\pi]$, we write $x \xrightarrow{r} x'$ ($x \xrightarrow{b} x'$) if there is a red (blue) arc from x to x'. Clearly, the in- and out-degrees of $G[\pi]$ are 2. Every node of $G[\pi]$ has one outgoing red arc and one outgoing blue arc (i.e. one arc is red and the other is blue) and has one incoming red arc and one incoming blue arc. This condition is known as the arc-coloring of the second type [27]. If we have a path (a sequence of connected arcs) between any two vertices of a directed graph G, we say G is strongly connected. Moreover, if G has in- and out-degrees being 2, and has an arc-coloring of the second type, we say G is a *proper shuffle graph.* For any proper shuffle graph G of order N, we have a corresponding even-odd shuffle for $2N$ elements.

The following definition plays a crucial role in evaluation of DRmax.

Definition 3. *Let G be a proper shuffle graph. A directed path between two vertices of G is appropriate if its first and last arcs are blue-colored and there are no successive red arcs. If there always exists an appropriate path of length L between any two (possibly the same) vertices, G is said to be L-appropriately-reachable. The minimum of such L is defined as the sufficient distance (SD) of G, and denoted by $SD(G)$. In addition, if there always exists a path (not necessarily be appropriate) of length L between any two vertices, G is said to be L-reachable [27] and the minimum of such L is defined as the weak sufficient distance (WSD) of G, denoted by $WSD(G)$.*

Note that WSD can be defined for directed graphs with single-colored arcs. For any proper shuffle graph G with $SD(G) = L$, G is $(L+i)$-appropriately-reachable for any $i \geq 0$ and $Diam(G) \leq WSD(G) \leq SD(G)$, where $Diam(G)$ is the diameter of G, i.e., the maximum distance of any two vertices.

Proposition 1. *If $SD(G[\pi]) = L$ for even-odd shuffle π,* $\mathrm{DRmax}(\pi) \leq L + 1$.

This proposition is easy to verify. From the definition of SD, for any sub input block, X_i^0, we have a connected data path from X_i^0 to X_j^L for any even j. As underlying shuffle is even-odd, this means that there are a connected data path from X_i^0 to X_h^{L+1}, for any odd h. Also, we have a connected data path from X_j^L to $X_{h'}^{L+1}$ for any even j and h', by going through an F function. Thus, we have a connected path from X_i^0 to X_j^{L+1} for any j.

4.2 Colored de Bruijn Graph

Proposition 1 implies that if shuffle π has a small DRmax, $G[\pi]$ will also have a small SD. Then, how we can build such a graph? We answer this question by using the well-known de Bruijn graph.

Definition 4. *The binary de Bruijn graph, denoted by* $\mathrm{dB}(s) = (V_s, E_s)$*, is a directed graph of order* $N = 2^s$ *for non-negative integer* s*. Its vertex set* V_s *is* $\{0,1\}^s$*, or corresponding integer set* $\{0,\ldots,N-1\}$ *(we interchangeably use). The arc set,* $E_s \subseteq V_s \times V_s$*, is defined as* $E_s = \{(u,u') : u = (u_1,u_2,\ldots u_{s-1},u_s), u' = (u_2,u_3,\ldots,u_s,w), w \in \{0,1\}\}$.

It is obvious that in- and out-degrees of $\mathrm{dB}(s)$ are two. Also, it is well-known that $Diam(\mathrm{dB}(s)) = s$ and it is even s-reachable, since we can move to any node u by choosing s successive arcs according to the bits of u in descending order. The diameter of $\mathrm{dB}(s)$ is minimal for all directed graphs with order 2^s and maximum degree 2. Now, our task is to color the arcs of $\mathrm{dB}(s)$ so that it has an arc-coloring of the second type. Our coloring function is quite simple, which is as follows.

Definition 5. *For any* $s \geq 2$*, let* $\mathsf{CF} : E_s \to \{0,1\}$ *be the coloring function of arcs of* $\mathrm{dB}(s)$*, where* 0 *and* 1 *denote red and blue. For* $u = (u_1,u_2,\ldots u_{s-1},u_s)$ *and* $v = (v_1,v_2,\ldots v_{s-1},v_s)$*, it is defined as*

$$\mathsf{CF}(u,v) = \begin{cases} v_s & \text{if } u_1 = u_s, \\ v_s + 1 & \text{if } u_1 \neq u_s, \end{cases}$$

where v_s+1 *denotes the complement of* v_s*. The colored de Bruijn graph,* $\mathrm{CdB}(s)$*, is defined as the binary de Bruijn with* CF *arc-coloring. Formally,* $\mathrm{CdB}(s) = (V_s, E'_s)$ *with* $E'_s = (u, v, \mathsf{CF}(u,v))$ *for all* (u,v) *in* E_s *of* $\mathrm{dB}(s)$*. That is, if* $(u,v) \in E_s$*,* $\mathrm{CdB}(s)$ *has an arc* $u \xrightarrow{c(\mathsf{CF}(u,v))} v$ *with mapping* $c(0) = r$ *and* $c(1) = b$.

Fig. 6 depicts CdB(3) and CdB(4), where a thick line denotes a blue arc and a thin line denotes a red arc. Note that, if $u \xrightarrow{r} u'$ in $\mathrm{CdB}(s)$, we have

$$u'_1 = u_2, u'_2 = u_3, \ldots, u'_{s-1} = u_s, u'_s = u_1 + u_s \tag{2}$$

and if $u \xrightarrow{b} u'$ in CdB(s) we have

$$u'_1 = u_2, u'_2 = u_3, \ldots, u'_{s-1} = u_s, u'_s = u_1 + u_s + 1. \tag{3}$$

It is easy to see that CdB(s) for $s \geq 2$ has an arc-coloring of second type[5], thus CdB(s) is a proper shuffle graph of order 2^s and we have a corresponding even-odd shuffle for 2^{s+1} elements, for $s \geq 2$. For concrete representations of block shuffles built from CdB(s), see Appendix A. As Fig. 6 shows, the graph is symmetric including the arc-coloring, thus the corresponding shuffles are also symmetric. This property will be beneficial for implementation.

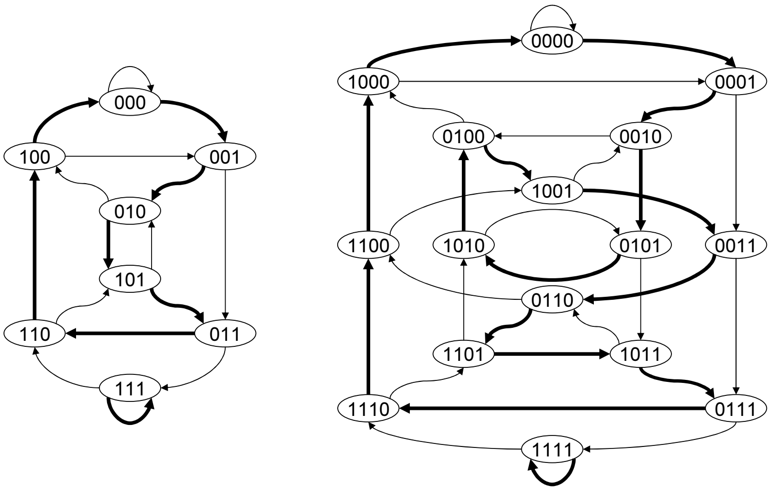

Fig. 6. Colored de Bruijn Graphs CdB(3) (Left), and CdB(4) (Right).

4.3 Sufficient Distance of Colored de Bruijn Graph

We want to know (a bound of) SD(CdB(s)). It can be expected to be small from the minimality of dB(s)'s diameter, however, this expectation has to be theoretically verified. To do this, we focus on the successive arc pairs of CdB(s).

Definition 6. *Let $G = (V, E)$ be a proper shuffle graph of order N, where $E \subseteq V \times V \times \{r, b\}$. Its double-path graph, denoted by $\widetilde{G} = (V, \widetilde{E})$, is a directed graph with the same vertex set as G, and $\widetilde{E} \subseteq V \times V \times \{rb, bb\}$. For any $(u, w, v) \in V^3$ with $(u, w, b), (w, v, b) \in E$, we have $(u, v, bb) \in \widetilde{E}$ and for any $(u', w', v') \in V^3$ with $(u', w', r), (w', v', b) \in E$, we have $(u', v', rb) \in \widetilde{E}$.*

[5] This does not hold true when $s = 1$. The valid colorings for dB(1) are ones that implement the left and right cyclic shifts. Also, CF is not the unique solution to provide an arc-coloring of the second type.

In other words, if G has $u\xrightarrow{b}w\xrightarrow{b}v$ for some w, $\widetilde{G}$ has $u\xrightarrow{bb}v$, and if G has $u\xrightarrow{r}w'\xrightarrow{b}v$ for some w', $\widetilde{G}$ has $u\xrightarrow{rb}v$. Note that we did not use all pair of arcs (such as br and rr), and $\widetilde{G}$ may not be strongly connected.

For the double-path graph of $\mathrm{CdB}(s)$, we have the following.

Lemma 1. *The double-path graph of the colored de Bruijn graph,* $\widetilde{\mathrm{CdB}}(s)$*, is isomorphic to* $\mathrm{CdB}(s)$ *itself under the arc-label mapping* $r \to rb$ *and* $b \to bb$*.*

Proof. If x is an s-bit value, we write x_i to denote its i-th bit, i.e., $x = (x_1, \ldots, x_s)$. Let u, u', v, v' be vertices of the double-path graph of $\mathrm{CdB}(s)$, $\widetilde{\mathrm{CdB}(s)}$. From Equations (2) and (3), when $u \xrightarrow{rb} v$ and $u' \xrightarrow{bb} v'$, we have

$$\begin{aligned} v &= (u_3, u_4, \ldots, u_s, u_1 + u_s, u_1 + u_2 + u_s + 1), \\ v' &= (u'_3, u'_4, \ldots, u'_s, u'_1 + u'_s + 1, u'_1 + u'_2 + u'_s). \end{aligned} \tag{4}$$

To prove the lemma, we do separate analyses for even and odd s. First, assume s is even. Let $t = s/2 + 1$. We define the mapping $f : \{0,1\}^s \to \{0,1\}^s$. For $f(x) = y$, $x, y \in \{0,1\}^s$, f is defined as

$$y_i = \begin{cases} x_{\frac{i}{2}+t-1} & \text{if } i \text{ is even} \\ x_{\frac{i-1}{2}+1} + x_{\frac{i-1}{2}+t} + 1 & \text{if } i \text{ is odd,} \end{cases} \tag{5}$$

for $i = 1, \ldots, s$. Note that f is invertible; to obtain x from y, we first get $x_t, \ldots, x_s$ as corresponding y's even bits, and add them to the odd bits of y. What we shall prove is that f is an isomorphism from $\mathrm{CdB}(s)$ to $\widetilde{\mathrm{CdB}}(s)$ with an arc-label mapping defined as r → rb and b → bb. To prove this, we need to show (1) iff $x \xrightarrow{r} x'$ in $\mathrm{CdB}(s)$ then $f(x) \xrightarrow{rb} f(x')$ in $\widetilde{\mathrm{CdB}}(s)$, and (2) iff $x \xrightarrow{b} x'$ in $\mathrm{CdB}(s)$ then $f(x) \xrightarrow{bb} f(x')$ in $\widetilde{\mathrm{CdB}}(s)$. Let us assume $x \xrightarrow{r} x'$ in $\mathrm{CdB}(s)$, and let $y = f(x)$ and $y' = f(x')$. Since $x'_i = x_{i+1}$ for $i = 1, \ldots, s-2$, we have

$$\begin{aligned} y'_i &= x'_{\frac{i}{2}+t-1} = x_{\frac{i}{2}+t-1+1} = x_{\frac{i+2}{2}+t-1} = y_{i+2}, \\ y'_j &= x'_{\frac{j-1}{2}+1} + x'_{\frac{j-1}{2}+t} + 1 = x_{\frac{(j+2)-1}{2}+1} + x_{\frac{(j+2)-1}{2}+t+1} + 1 = y_{j+2}, \end{aligned} \tag{6}$$

for all even $2 \le i \le s-2$ and all odd $1 \le j \le s-3$. For y'_{s-1}, we have

$$y'_{s-1} = x'_{\frac{s-2}{2}+1} + x'_{\frac{s-2}{2}+t} + 1 = x'_{t-1} + x'_s + 1 = x_t + (x_1 + x_s) + 1 = y_1 + y_s,$$

from Eq. (2). For y'_s, we have $y'_s = x'_s = x_1 + x_s = y_1 + y_2 + y_s + 1$. Hence $y' = (y_3, y_4, \ldots, y_s, y_1 + y_s, y_1 + y_2 + y_s + 1)$, which means $y \xrightarrow{rb} y'$ from Eq. (4).

Next, we assume $\hat{x} \xrightarrow{b} \hat{x}'$ in $\mathrm{CdB}(s)$ and let $\hat{y} = f(\hat{x})$ and $\hat{y}' = f(\hat{x}')$. The first $s-2$ bits of $\hat{y}'$ are the same as Eq. (6), and

$$\hat{y}'_{s-1} = \hat{x}'_{t-1} + \hat{x}'_s + 1 = \hat{x}_t + (\hat{x}_1 + \hat{x}_s + 1) + 1 = \hat{y}_1 + \hat{y}_s + 1,$$

from Eq. (3). Also $\hat{y}'_s = \hat{x}'_s = \hat{x}_1 + \hat{x}_s + 1 = \hat{y}_1 + \hat{y}_2 + \hat{y}_s$. Thus $\hat{y}' = (\hat{y}_3, \hat{y}_4, \ldots, \hat{y}_s, \hat{y}_1 + \hat{y}_s + 1, \hat{y}_1 + \hat{y}_2 + \hat{y}_s)$, which means the walk $\hat{y} \xrightarrow{bb} \hat{y}'$ from Eq. (4). This proves the direct part of the lemma for even s. The converse (i.e., if $x \overset{r}{\not\to} x'$ in $\mathrm{CdB}(s)$ then $f(x) \overset{rb}{\not\longrightarrow} f(x')$ in $\widetilde{\mathrm{CdB}}(s)$ and if $x \overset{b}{\not\to} x'$ in $\mathrm{CdB}(s)$ then $f(x) \overset{bb}{\not\longrightarrow} f(x')$ in $\widetilde{\mathrm{CdB}}(s)$) is easy. For odd s, we use a slight different isomorphism. Since the proof is almost the same, we omit it here.

Let us consider to build an appropriate path from u to v, for two (possibly the same) vertices u, v of $\mathrm{CdB}(s)$. We assume $u \xrightarrow{b} w$. From Lemma 1 and that $\widetilde{\mathrm{CdB}}(s)$ is s-reachable, there always exists a path of length $2s$ from w to v in $\mathrm{CdB}(s)$, where the last arc is colored blue. This implies the existence of appropriate path of length $2s + 1$ from u to v in $\mathrm{CdB}(s)$. Thus we have proved the following.

Lemma 2. *$SD(\mathrm{CdB}(s)) \leq 2s + 1$.*

Using Lemma 2 and Proposition 1, we can build a block shuffle of $k = 2^{s+1}$ (for any $s \geq 2$) whose DRmax is at most $2s + 2 = 2\log_2 k$. As mentioned in Section 3, the lower bound of DRmax is about $1.44 \log_2 k$, derived from Fibonacci sequence. Hence, the diffusion property of $\mathrm{CdB}(s)$ is close to the optimum.

Related Work. Massey [15] also proposed a graphical representation of block shuffles. However the meaning of arc-coloring is different, i.e., a thick (thin) line denotes a mapping from even (odd) input to even (odd) output block. He combined a block shuffle, called Armenian Shuffle, with a two-block linear operation called PHT to form a diffusion layer of an Substitution-Permutation Network (SPN) block cipher, SAFER+. His notion of diffusion (for the diffusion layer, not for the block shuffle itself) is different from us, which is close to the branch number. Armenian Shuffle is based on dB(3). However, it is not even-odd. No arc-coloring rule of the second type (and the idea of SD) was presented in [15]. Hence, even though the basic methodology of us and [15] have some similarities, our proposal has many important differences.

5 Security

5.1 Pseudorandomness

For a new block cipher structure, it is typical to ask its pseudorandomness in the idealized setting. This kind of analysis is needed to see if there is a structural flaw in the proposal, as mentioned by [20]. For this, we have to prove the maximum prp-advantage and sprp-advantage in an idealized setting, defined as

$$\mathtt{Adv}^{\mathtt{prp}}_{\mathsf{C}}(q) \overset{\text{def}}{=} \max_{\mathcal{A}:q-\text{CPA}} |\Pr[\mathcal{A}^{\mathsf{C}} = 1] - \Pr[\mathcal{A}^{\mathsf{P}_n} = 1]|, \text{ and },$$

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathsf{C}}(q) \overset{\text{def}}{=} \max_{\mathcal{A}:q-\text{CCA}} |\Pr[\mathcal{A}^{\mathsf{C},\mathsf{C}^{-1}} = 1] - \Pr[\mathcal{A}^{\mathsf{P}_n,\mathsf{P}_n^{-1}} = 1]|. \tag{7}$$

Here, C is the encryption function of an n-bit block cipher with some idealized functions as internal modules. P_n is an n-bit uniform random permutation (URP), which is distributed uniformly over all n-bit permutations. Their inversions are written as C^{-1} and P_n^{-1}. The adversary, $\mathcal{A}$, tries to distinguish C from P_n using q encryption queries, i.e., chosen-plaintext attack (CPA), or $(\mathsf{C}, \mathsf{C}^{-1})$ from $(\mathsf{P}_n, \mathsf{P}_n^{-1})$ using q encryption and decryption queries, i.e., chosen-ciphertext attack (CCA). The final guess of $\mathcal{A}$ is either 0 or 1, and the probability that $\mathcal{A}$'s guess is 1 when $\mathcal{A}$ queries C is written as $\Pr[\mathcal{A}^{\mathsf{C}} = 1]$, where probability is defined by the randomness of $\mathcal{A}$ and C. The maximums in Eq. (7) are taken for all adversaries with q queries without computational restriction. For example, the seminal Luby-Rackoff's result [14] proved that $\mathtt{Adv}^{\mathtt{prp}}_{\Phi_3}$ and $\mathtt{Adv}^{\mathtt{sprp}}_{\Phi_4}$ are $O(q^2/2^n)$, where Φ_r is the r-round, $2n$-bit block Feistel structure with round functions being n-bit uniform random functions (URFs). This also means that 3-round Feistel is a pseudorandom permutation (PRP) and 4-round one is a strong PRP (SPRP), if round functions are pseudorandom functions (PRFs). These results are considered as a theoretical justification of basic Feistel ciphers. Similar analysis was done for other structures, e.g., Misty structure [9][12].

For the pseudorandomness of Type-II GFS, the following result is known.

Lemma 3. *(by [28][20]) Let* $\mathrm{TypeII}_{r,k}$ *be the r-round, kn-bit Type-II GFS with partition number k and round functions being n-bit URFs. Then we have*

$$\mathtt{Adv}^{\mathtt{prp}}_{\mathrm{TypeII}_{k+1,k}}(q) \le \frac{k^2q^2}{2^n}, \text{ and } \mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{TypeII}_{2k,k}}(q) \le \frac{k^2q^2}{2^n}.$$

Using the idea of Mitsuda and Iwata [19], the pseudorandomness of any GFS with an even-odd shuffle π can be evaluated via its sufficient distance.

Theorem 1. *Let π be an even-odd shuffle of order k, and let* $\mathrm{GFS}_{r,k}$ *denote the r-round GFS with shuffle π. Its block size is kn bits, partition number is k, and all round functions are independent n-bit URFs. Then we have*

$$\mathtt{Adv}^{\mathtt{prp}}_{\mathrm{GFS}_{L+2,k}}(q) \le \frac{kL}{2^{n+1}}q^2 \quad \text{if } SD(G[\pi]) \le L, \text{ and}$$
$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{GFS}_{2L+2,k}}(q) \le \frac{kL}{2^{n}}q^2 \quad \text{if } \max\{SD(G[\pi]), SD(G[\pi^{-1}])\} \le L.$$

Proof. For $\mathbf{x} = (x_0, \ldots, x_{k-1}) \in (\{0,1\}^n)^k$, let $\mathbf{x}_{[i]} = x_i$. Following [19], if keyed permutation over $(\{0,1\}^n)^k$, H, satisfies

$$\max_{\mathbf{x}\neq\mathbf{x}'} \Pr[H(\mathbf{x})_{[i]} = H(\mathbf{x}')_{[i]} \text{ for some even } i \in \{0,\ldots,k-1\}] \le \epsilon, \text{ and}$$
$$\max_{\mathbf{x}\neq\mathbf{x}'} \Pr[H(\mathbf{x})_{[i]} = H(\mathbf{x}')_{[i]} \text{ for some odd } i \in \{0,\ldots,k-1\}] \le \epsilon,$$

then H is called ϵ-AU$_e$ and ϵ-AU$_o$, respectively [19]. Then we obtain

$$\mathtt{Adv}^{\mathtt{prp}}_{\mathrm{GFS}_{2,k}\circ H_1}(q) \le \left(\epsilon + \frac{k}{2^{n+1}}\right) \cdot \binom{q}{2} \qquad (8)$$

by extending the lemma 9 and theorem 7 of Maurer [17] (We omit the proof here. This slightly improves the constant of the result of [19] for Type-II GFS.). For any two distinct $\mathbf{x}$ and $\mathbf{x}'$, we have

$$\Pr[\mathrm{GFS}_{L,k}(\mathbf{x})_{[i]} = \mathrm{GFS}_{L,k}(\mathbf{x}')_{[i]}] \le \frac{L}{2^n}, \text{ for any even } i \in \{0, \ldots, k-1\}. \quad (9)$$

Eq. (9) is easily proved as follows. W.l.o.g. we assume $(x_0, x_1) \neq (x'_0, x'_1)$ and estimate the probability of $\mathrm{GFS}_{L,k}(\mathbf{x})_{[0]} = \mathrm{GFS}_{L,k}(\mathbf{x}')_{[0]}$. From the assumption, there is an appropriate path of length L in $G[\pi]$, whose start and goal are vertex 0. For $h = 1, \ldots, L$, we can define a sequence of internal outputs, $Z_h = \mathrm{GFS}_{h,k}(\mathbf{x})_{[s(h)]}$, with $s(h)$ following that appropriate path (e.g. $s(1) = \overline{\pi}[1]$ and $s(L) = 0$). Obviously we have $\Pr[Z_1 = Z'_1] = \Pr[F(x_0) \oplus x_1 = F(x'_0) \oplus x'_1] \le 1/2^n$, when F is URF. Moreover, using the independence of all round functions, we have $\Pr[Z_j = Z'_j | Z_{j-1} \neq Z'_{j-1}] \le 1/2^n$ for any $j = 2, \ldots, L$. Therefore, $\Pr[Z_L = Z'_L]$ is at most $\sum_{j=2}^{L} \Pr[Z_j = Z'_j | Z_{j-1} \neq Z'_{j-1}] + \Pr[Z_1 = Z'_1] \le L/2^n$. This indicates that Eq. (9) is true, and thus $\mathrm{GFS}_{L,k}$ is $\frac{k \cdot L}{2^{n+1}}$-$\mathrm{AU}_e$ from the union bound. From this and Eq. (8), prp-advantage of $\mathrm{GFS}_{L+2,k}$ is at most $(\frac{k \cdot L}{2^{n+1}} + \frac{k}{2^{n+1}})\binom{q}{2} \le \frac{k \cdot L}{2^{n+1}} q^2$. This proves the first claim of Theorem 1. To prove the second, we consider two independently-keyed permutations over $(\{0,1\}^n)^k$, H_1 and H_2. We assume H_1 is ϵ_1-AU_e and H_2 is ϵ_2-AU_o. Then we have

$$\mathtt{Adv}^{\mathtt{sprp}}_{H_2^{-1} \circ \mathrm{GFS}_{2,k} \circ H_1}(q) \le \left(\epsilon_1 + \epsilon_2 + \frac{1}{2^{kn}}\right)\binom{q}{2} \le (\epsilon_1 + \epsilon_2)\, q^2 \quad (10)$$

using similar arguments as those of [17][19][18].

Let $\overline{\mathrm{GFS}}_{r,k}$ be $\mathrm{GFS}^{-1}_{r,k}$ without the final shuffle (i.e. $\mathrm{GFS}^{-1}_{r,k} = \pi_k^{-1} \circ \overline{\mathrm{GFS}}_{r,k}$). As $SD(G[\pi^{-1}]) \le L$, $\mathrm{GFS}^{-1}_{L,k}$ is $\frac{k \cdot L}{2^{n+1}}$-$\mathrm{AU}_e$. As π is even-odd, π_k^{-1} is also even-odd. Hence $\overline{\mathrm{GFS}}_{L,k}$ is $\frac{k \cdot L}{2^{n+1}}$-$\mathrm{AU}_o$, and the sprp-advantage of $(\overline{\mathrm{GFS}}_{L,k})^{-1} \circ \mathrm{GFS}_{2,k} \circ \mathrm{GFS}_{L,k} = \pi^{-1} \circ \mathrm{GFS}_{2L+2,k}$ is at most $2\frac{k \cdot L}{2^{n+1}} q^2 = \frac{k \cdot L}{2^n} q^2$ from Eq. (10). Of course the last application of π^{-1} has no impact on security, hence this bound also holds for $\mathrm{GFS}_{2L+2,k}$. This proves the second claim.

Combining Lemma 2 and Theorem 1, we obtain the pseudorandomness result for GFS with shuffle derived from $\mathrm{CdB}(s)$, when $k = 2^{s+1}$.

Corollary 1. *Let $\Omega_{r,k}$ be the kn-bit GFS with shuffle from $\mathrm{CdB}(s)$ for $k = 2^{s+1}$ for $s \ge 2$, where all round functions are independent n-bit URFs. Then we have*

$$\mathtt{Adv}^{\mathtt{prp}}_{\Omega_{2\log k+1,k}}(q) \le \frac{2k \log k}{2^n} q^2, \text{ and } \mathtt{Adv}^{\mathtt{sprp}}_{\Omega_{4\log k,k}}(q) \le \frac{4k \log k}{2^n} q^2,$$

where the base of logarithm is 2.

Corollary 1 demonstrates the power of colored de Bruijn: $\mathrm{TypeII}_{r,k}$ needs $k \sim 2k$ rounds, while $\Omega_{r,k}$ needs only $2\log k \sim 4\log k$ rounds. The gain is obtained for any $k \ge 8$ being a power of two.

If k is not a power of two, we cannot use $\mathrm{CdB}(s)$. In such a case, we have to search a proper shuffle graph of order $2k$ having a small SD. The search result of Section 3 implies the existence of a graph with SD about $2\log k$ for any k, but proving this is an open problem.

5.2 Evaluation of Security against Cryptanalysis

We also evaluate the security against the known cryptanalysis. In particular, we consider impossible differential attack, saturation attack and differential/linear cryptanalysis and evaluate the security of GFS with the optimum block shuffles found by the search. In the evaluation, we treat the round function as an arbitrary bijective function and assume that there is no pair of nonzero input and output differential that holds with probability 1. Each evaluation is carried out to derive the number of rounds for characteristic we focus. Specific numbers of round for characteristic are provided in Appendix A.

Impossible Differential Attack. An impossible differential attack [2] uses the differential characteristic of probability zero (impossible differential characteristic, IDC) to eliminate wrong key candidates. Here, IDC is represented as a pair of input and output differences, e.g., $(\alpha \nrightarrow \beta), \alpha, \beta \in (\{0,1\}^n)^k$ for a k-partition cipher E with $Pr[E(x) + E(x + \alpha) = \beta] = 0$ for any x. To find an IDC, we use the $\mathcal{U}$-method of Kim et al. [13]. $\mathcal{U}$-method can efficiently search for IDCs using a truncated difference in sub block units classified by five types: zero difference, nonzero unfixed difference, nonzero fixed difference, exclusive-or of nonzero fixed and unfixed differences, and unfixed difference. These types are denoted by 0, δ, γ, $\delta + \gamma$, and R, respectively. For $r \geq 1$, $\alpha^r = (\alpha_0^r, \alpha_1^r, \ldots, \alpha_{k-1}^r)$ denotes the output difference after r-round and α^0 denotes the input difference. Each coordinate of α^r is classified into one of the five types described above. Note that α^0 always consists of types 0 and γ. For decryption, the output difference is denoted by β^r. If there is a contradiction between α_i^{r1} and β_i^{r2} $(0 \leq i \leq k-1)$, the path from α to β is impossible, i.e., $(\alpha \nrightarrow \beta)$ is an IDC of $(r1 + r2)$ rounds. We can determine the number of round for IDC from DRmax, which is as follows. After DRmax(π) rounds, we have two cases :
Case 1 **:** If $\alpha_i^{\mathrm{DRmax}}$ for some odd i has type γ, there exists a data path, P, that does not pass through any F (i.e., the equation corresponding to that path does not contain X_i^0 as a part of arguments of F). If $\alpha_{i-1}^{\mathrm{DRmax}}$ has type δ, then $\alpha_j^{\mathrm{DRmax}+1}$ with $j = \overline{\pi}[i]$ has type $\gamma \oplus \delta$. Here, if β_j^{DRmax} has type γ, it is an IDC for $2\mathrm{DRmax} + 1$ rounds.
Case 2 **:** If all data paths pass through at least one F function, Both α^{DRmax} and β^{DRmax} do not contain type γ. From the definition of DRmax, DRmax-1 rounds does not achieve full diffusion. Thus α^{DRmax} must contain type 0. This implies that we can detect a contradiction involving difference of type 0 and difference δ or γ. Accordingly, the number of round for IDC is at most $2\mathrm{DRmax} - 1$.

To see the tightness of above analysis, we also perform $\mathcal{U}$-method. As a result, the number of round for IDC for any GFS with optimum shuffle is one of $2\mathrm{DRmax} - 2$, $2\mathrm{DRmax} - 1$, and $2\mathrm{DRmax} + 1$.

Saturation Attack. Saturation Attack [7] works for block ciphers using permutations over a small space, hence it is a strong attack on GFS with invertible round functions. This attack exploits the fact that the output sum of a permutation is zero when all inputs are given to determine whether the guessed key is correct. We define the following four states for a set of 2^n n-bit inputs:

Constant (C) : if $\forall i, j \;\; x_i = x_j$ **All** (A) : if $\forall i, j \;\; i \neq j \Leftrightarrow x_i \neq x_j$
Balance (B) : if $\bigoplus_i^{2^n-1} x_i = 0$ **Unknown** (U) : Other

The saturation characteristics (SC) is of form $(\alpha \rightarrow \beta), \alpha \in \{C, A\}^k, \beta \in \{C, A, B, U\}^k$, where the input state α contains at least one A and the output state β is not all Us. We investigated the maximum number of rounds for which an SC exists, for all optimum shuffles. For this purpose, we used a method developed by the evaluation report of CLEFIA [26]. Here we briefly describe the method. See [26] for details. To apply the method of [26], we can use DRmax, as well as the case of IDC. Note that, in case of IDC we only need to focus on a data path not passing through F, while in case of SC we also have to consider data paths passing through F, as input state A (to some F) implies output state A.

We first search an SC, $(\alpha \rightarrow \beta)$, such that α consists of one A for an even sub block and $k-1$ Cs. From the definition of DRmax, the state after DRmax encryption rounds does not contain C. Let us assume that the state after DRmax contains two As for i-th and $i+1$-th blocks for some even i. By adding one more round, the state of j-th($j = \overline{\pi}[i+1]$) sub block is $B(= F(A) \oplus A)$. After another round, the state of s-th($s = \overline{\pi}[j+1]$) sub block is $U(= F(B) \oplus \mathit{any})$ and that of t-th($t = \overline{\pi}[j]$) sub block is B. Then, in the next round, the states of all sub blocks become $U(= F(U) \oplus \mathit{any})$. Therefore, an SC (containing one A and $k-1$ Cs) exists for at most DRmax + 2 rounds. For other cases, it is easy to confirm that such an SC exists for at most DRmax + 1 rounds. Next, the SC $(\alpha \rightarrow \beta)$ we found in the above is used to find another SC, $(\alpha' \rightarrow \alpha \rightarrow \beta)$, where α is an intermediate state and α' is not all As (as this means the attack using all plaintexts). Following [26], this can be done by adding rounds to the input state α. Using the fact that α contains only one A, we can add at most DRmax − 2 rounds to obtain a valid SC. Therefore, the maximum number of rounds for SC is at most DRmax + 2 + DRmax − 2 = 2DRmax. In fact, we confirmed that the maximum number of rounds for SC was either 2DRmax or 2DRmax − 1 for all optimum shuffles we searched.

Differential / Linear Cryptanalysis. Differential cryptanalysis (DC) and linear cryptanalysis (LC) are the most basic attacks on block ciphers. Because it is generally difficult to obtain a strict maximum differential/linear probability, we usually count the number of active S-boxes instead [25][1]. If the maximum differential probability of S-box is p and the number of active S-boxes is N, p^N is the maximum differential characteristic probability ($\mathrm{DCP}_{\max}$), which serves as one index of security against DC. For sufficient security, $\mathrm{DCP}_{\max} \leq 2^{-kn}$ is required. Similarly, by counting the minimum number of active S-boxes with respect to linear masking, we can derive the maximum linear characteristic probability ($\mathrm{LCP}_{\max}$), which works as an index of security against LC. For each GFS with an optimum shuffle, we evaluate the minimum numbers of active S-boxes for DC and LC, denoted by AS_D and AS_L, for 20 rounds. The result is in Appendix A. The number of active S-boxes is different for individual shuffles, even

Table 3. Number of active S-boxes of every round (Differential and Linear).

	Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
k=8	Type-II	0	1	2	3	4	6	7	9	10	13	15	17	18	19	20	21	22	24	25	27
	No.2	0	1	2	3	4	6	8	10	12	12	14	16	16	18	20	20	22	24	24	26
$k = 16$	Type-II	0	1	2	3	4	6	7	9	10	13	15	17	19	22	24	26	28	32	35	39
	No.1	0	1	2	3	4	6	8	11	14	19	21	24	25	27	30	31	33	36	37	39

if their DRmax are the same; some are better than the Type-II and others are worse. From this result, we expect that the security against DC/LC of GFS_π with optimum π is the same level as Type-II GFS.

A typical construction of F is of the form $F(x) = S(K \oplus x)$, where K is the key and $S : \{0,1\}^n \rightarrow \{0,1\}^n$ is S-box. Following AES, if S-box is based on the field inversion over $GF(2^n)$, its $\mathrm{DP}_{\max}$ ($\mathrm{LP}_{\max}$) is 2^{-n+2} if n is even and 2^{-n+1} if n is odd. Assuming such F for $n = 8$ (thus $\mathrm{DP}_{\max}$ and $\mathrm{LP}_{\max}$ are 2^{-6}), we derive the number of rounds for differential/linear characteristics. Here we focus on Type-II and an optimum GFS using CdB(s). For these two structures, Table. 3 shows AS_D and AS_L for every round up to 20. Due to their duality the figures of AS_D and AS_L are basically the same. Let us assume $k = 8$, i.e., a 64-bit block cipher. In this case, if AS_D is less than 11 there is an exploitable differential characteristic as $(2^{-6})^{10} > 2^{-64}$. Thus, Type-II GFS has 9-round differential characteristic while optimum GFS has 8-round one. Similarly, if we set $k = 16$ (i.e., 128-bit block), AS_D must be less than 22 to have an exploitable differential characteristic. Table 3 shows the existences of 13-round characteristics for Type-II GFS and 11-round one for optimum GFS. The same results hold true for LC. From these analyses, we think our proposal slightly improves the security against DC/LC, or at least provides the same level of security as that of Type-II GFS.

6 Concluding Remarks

We have shown that the diffusion property of Type-II GFS can be improved by only changing the internal block shuffle from the cyclic shift. Based on a concrete notion of diffusion, we have searched all optimum shuffles up to partition number $k \leq 16$. We also proposed a block shuffle family based on a de Bruijn graph for k being a power of two, and proved that their diffusion property is close to the best possible. We then confirmed that such block shuffles can be used to improve the resistance of GFS against some cryptanalysis, such as impossible differential attack and saturation attack, and improve the efficiency with respect to pseudorandomness. While known instances of Type-II GFS ciphers have relatively small partition number to keep a balance of speed and implementation size, our results enables to build a fast, secure GFS cipher having a large partition number.

One might think of using different shuffles for each round to achieve a better (or at least comparable) diffusion than ours in return for a larger implementation cost. For example, we can alternately use a two block-wise swap (i.e. $(a, b, c, d) \rightarrow$

(b, a, d, c), two-round classical Feistel), which offers a local diffusion, and another global shuffle. For some small k we observed that this two-round Feistel-based scheme can offer a diffusion property as good as our optimum ones. However, it is open if multiple shuffles can contribute to a smaller DRmax than ours.

Acknowledgments

We would like to thank Yukiyasu Tsunoo, Norifumi Kamiya, Toshihiko Okamura, Hiroyasu Kubo, Maki Shigeri, Teruo Saito, Takeshi Kawabata, Hirokatsu Nakagawa, Jinhui Chao and anonymous referees for helpful comments.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-bit block cipher suitable for multiple platforms." in Proceedings of Selected Areas in Cryptography - SAC '00, LNCS 2012, pp. 41-54, 2001.
2. E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossbile differentials." *Advances in Cryptology* - EUROCRYPT '99, LNCS 1592, pp.12-23, 1999.
3. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems." CRYPTO '90, LNCS 537, pp.2-21, Springer-Verlag, 1991.
4. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", CHES 2007, LNCS 4727, pp. 450-466, 2007.
5. L. Carter and M. Wegman. "Universal Classes of Hash Functions." *Journal of Computer and System Science*, Vol. 18, pp. 143-154, 1979.
6. P. Crowley. "Mercy: A Fast Large Block Cipher for Disk Sector Encryption.", *Fast Software Encryption*- FSE'00, LNCS 1978, pp. 49-63, 2000.
7. J. Daemen, L. R. Knudsen, and V. Rijmen, "The block cipher SQUARE." *Fast Software Encryption*-FSE'97, LNCS 1267, pp.149-165, 1997.
8. M. A. Fiol, I. Alegre, J. L. A. Yebra, J. Fábrega. "Digraphs with walks of equal length between vertices." in *Graph Theory with Applications to Algorithms and Computer Science.*, John Wiley and Sons, Inc., 1985.
9. H. Gilbert and M. Minier. "New Results on the Pseudorandomness of Some Blockcipher Constructions." *Fast Software Encryption*-FSE'01, LNCS 2355, pp. 248-266.
10. S. Halevi and P. Rogaway. "A Parallelizable Enciphering Mode." *Topics in Cryptology*- CT-RSA'04, LNCS 2964, pp. 292-304, 2004.
11. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim and S. Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device." CHES 2006, LNCS 4249, pp. 46-59, 2006.
12. T. Iwata, T. Yoshino, T. Yuasa and K. Kurosawa. "Round Security and Super-Pseudorandomness of MISTY Type Structure." *Fast Software Encryption*-FSE'01, LNCS 2355, pp. 233-247.
13. J. Kim, S. Hong, J. Sung, C. Lee and S. Lee, "Impossible Differential Cryptanalysis for Block Cipher Structures." INDOCRYPT 2003, LNCS 2904, pp.82-96, 2003.
14. M. Luby and C. Rackoff. "How to Construct Pseudo-random Permutations from Pseudo-random functions." *SIAM J. Computing*, Vol. 17, No. 2, pp. 373-386, 1988.

15. J. Massey. "On the Optimality of SAFER+ Diffusion." *Second AES Candidate Conference*, National Institute of Standards and Technology, 1999.
16. M. Matsui, "Linear cryptanalysis of the data encryption standard." EUROCRYPT'93, LNCS 765, pp.386-397, Springer-Verlag, 1994.
17. U. Maurer. "Indistinguishability of Random Systems." *Advances in Cryptology-* EUROCRYPT'02, LNCS 2332, pp. 110-132, 2002.
18. K. Minematsu. "Tweakable Enciphering Schemes from Hash-Sum-Expansion." *Progress in Cryptology-* INDOCRYPT'07, LNCS 4859, pp. 252-267, 2007.
19. A. Mitsuda and T. Iwata. "Tweakable Pseudorandom Permutation from Generalized Feistel Structure." *Provable Security* - ProvSec'08, LNCS 5324, 2008.
20. S. Moriai and S. Vaudenay. "On the Pseudorandomness of Top-Level Schemes of Block Ciphers." *Advances in Cryptology* - ASIACRYPT '00, LNCS 1976, pp.289-302.
21. K. Nyberg, "Generalized Feistel Networks." ASIACRYPT '96, pp.90-104.
22. P. Junod and M. Macchetti. "Revisiting the IDEA Philosophy.", *Fast Software Encryption-* FSE'09, LNCS 5665, pp. 277-295, 2009.
23. R.L. Rivest, M.J.B. Robshaw, R. Sidney and Y.L. Yin, "The RC6 block cipher." v1.1, August 20, 1998. Available at http://people.csail.mit.edu/rivest/Rc6.pdf.
24. P. Rogaway, M. Bellare, J. Black, and T. Krovetz. "OCB: a block-cipher mode of operation for efficient authenticated encryption."*ACM Conference on Computer and Communications Security* ACM CCS'01, pp. 196-205, 2001.
25. T. Shirai, K. Shibutani, T. Akishita, S. Moriai and T. Iwata, "The 128-bit Blockcipher CLEFIA." *Fast Software Encryption-*FSE'07, LNCS 4593, pp. 181-195, 2007.
26. Sony Corporation, "The 128-bit Blockcipher CLEFIA Security and Performance Evaluations", Revision 1.0, June 1, 2007. Available at http://www.sony.co.jp/Products/cryptography/clefia/technical/data/clefia-eval-1.0.pdf
27. D. B. West. "Introduction to Graph Theory.", Prentice Hall N. J., 1996.
28. Y. Zheng, T. Matsumoto, and H. Imai. "On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses." *Advances in Cryptology* - CRYPTO '89, LNCS 435, pp. 461-480, 1989.

A Optimum Block Shuffles

Table 4,5 and 6 show the optimum shuffles found in the search and their security evaluation. We eliminate isomorphic shuffles. Type-II and Nyberg's GFN are also evaluated. Shuffles based on de Bruijn graph is indicated by $*$. A shuffle is presented in list: $\pi = \{3, 0, 1, 4, 5, 2\}$ means that the first input sub block is mapped to the third sub block of output, etc. Here, D denotes DRmax. IDC and SC denote the maximum numbers of rounds for impossible differential characteristics and saturation characteristics. AS_D and AS_L are as defined by Section 5.2. We evaluated both π and π^{-1}. If SC (or AS_D, AS_L) is written as x/y, x is for π and y is for π^{-1}. Otherwise the evaluations were the same for π and π^{-1}.

Table 4. Result of security evaluation for k=6,8,10 and 12

$k = 6$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{5,0,1,2,3,4}	{1,2,3,4,5,0}	6	13	12	25	25
Nyberg	{2,0,4,1,5,3}	{1,3,0,5,2,4}	6	11	12	18	18
No.1	{3,0,1,4,5,2}	{1,2,5,0,3,4}	5	9	10	25	25

$k = 8$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{7,0,1,2,3,4,5,6}	{1,2,3,4,5,6,7,0}	8	17	16	27	27
Nyberg	{2,0,4,1,6,3,7,5}	{1,3,0,5,2,7,4,6}	8	14	15	18	18
No.1	{3,0,1,4,7,2,5,6}	{1,2,5,0,3,6,7,4}	6	11	11	30	30
No.2$*$	{3,0,7,4,5,6,1,2}	{1,6,7,0,3,4,5,2}	6	10	11	26	26

$k = 10$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{9,0,1,2,3,4,5,6,7,8}	{1,2,3,4,5,6,7,8,9,0}	10	21	20	32	32
Nyberg	{2,0,4,1,6,3,8,5,9,7}	{1,3,0,5,2,7,4,9,6,8}	10	17	18	20	20
No.1	{5,0,7,2,9,6,3,8,1,4}	{1,8,3,6,9,0,5,2,7,4}	7	12	13	34	34
No.2	{3,0,1,4,7,2,5,8,9,6}	{1,2,5,0,3,6,9,4,7,8}	7	13	13	33	33
No.3	{3,0,7,4,1,6,5,8,9,2}	{1,4,9,0,3,6,5,2,7,8}	7	12	13	35	35

$k = 12$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{11,0,1,2,3,4,5,6,7,8,9,10}	{1,2,3,4,5,6,7,8,9,10,11,0}	12	25	24	37	37
Nyberg	{2,0,4,1,6,3,8,5,10,7,11,9}	{1,3,0,5,2,7,4,9,6,11,8,10}	12	20	21	16	16
No.1	{3,0,7,2,9,4,11,8,5,10,1,6}	{1,10,3,0,5,8,11,2,7,4,9,6}	8	15	15	34	34
No.2	{3,0,7,2,11,4,1,8,5,10,9,6}	{1,6,3,0,5,8,11,2,7,10,9,4}	8	15	16	33	33
No.3	{7,0,9,2,11,4,1,8,5,10,3,6}	{1,6,3,10,5,8,11,0,7,2,9,4}	8	14	15	36	36
No.4	{5,0,9,2,1,6,11,4,3,10,7,8}	{1,4,3,8,7,0,5,10,11,2,9,6}	8	15	15	37	37
No.5	{5,0,7,2,1,6,11,8,3,10,9,4}	{1,4,3,8,11,0,5,2,7,10,9,6}	8	14	15	35	35
No.6	{5,0,7,2,3,6,11,8,1,10,9,4}	{1,8,3,4,11,0,5,2,7,10,9,6}	8	14	15	35	35
No.7	{5,0,7,2,3,6,11,8,9,10,1,4}	{1,10,3,4,11,0,5,2,7,8,9,6}	8	15	15	35	35
No.8	{5,0,7,2,9,6,11,8,3,10,1,4}	{1,10,3,8,11,0,5,2,7,4,9,6}	8	15	15	33	33
No.9	{5,0,9,2,1,6,11,8,7,10,3,4}	{1,4,3,10,11,0,5,8,7,2,9,6}	8	14	15	35	35
No.10	{5,0,9,2,3,6,11,8,1,10,7,4}	{1,8,3,4,11,0,5,10,7,2,9,6}	8	15	15	30	30
No.11	{5,0,9,2,3,6,11,8,7,10,1,4}	{1,10,3,4,11,0,5,8,7,2,9,6}	8	15	15	35	35
No.12	{3,0,1,4,7,2,9,8,5,10,11,6}	{1,2,5,0,3,8,11,4,7,6,9,10}	8	15	15/16	33	33
No.13	{3,0,1,4,7,2,11,8,9,10,5,6}	{1,2,5,0,3,10,11,4,7,8,9,6}	8	14	15	37	37
No.14	{3,0,7,4,9,2,11,8,1,10,5,6}	{1,8,5,0,3,10,11,2,7,4,9,6}	8	14	15	34	33
No.15	{3,0,7,4,11,2,1,8,9,10,5,6}	{1,6,5,0,3,10,11,2,7,8,9,4}	8	14	14/15	28	28
No.16	{3,0,7,4,11,2,5,8,1,10,9,6}	{1,8,5,0,3,6,11,2,7,10,9,4}	8	14	15	35	35
No.17	{7,0,1,4,9,2,11,8,3,10,5,6}	{1,2,5,8,3,10,11,0,7,4,9,6}	8	14	15	35	35
No.18	{7,0,1,4,11,2,5,8,3,10,9,6}	{1,2,5,8,3,6,11,0,7,10,9,4}	8	14	15	33	34
No.19	{7,0,3,4,11,2,1,8,5,10,9,6}	{1,6,5,2,3,8,11,0,7,10,9,4}	8	14	15	37	37
No.20	{7,0,9,4,11,2,5,8,3,10,1,6}	{1,10,5,8,3,6,11,0,7,2,9,4}	8	14	15	34	34
No.21	{3,0,7,4,1,6,11,8,5,10,9,2}	{1,4,11,0,3,8,5,2,7,10,9,6}	8	14	15	35	34
No.22	{3,0,7,4,5,6,11,8,1,10,9,2}	{1,8,11,0,3,4,5,2,7,10,9,6}	8	14	14	36	34
No.23	{3,0,7,4,9,6,5,8,1,10,11,2}	{1,8,11,0,3,6,5,2,7,4,9,10}	8	14	15	34	35
No.24	{3,0,7,4,9,6,11,8,5,10,1,2}	{1,10,11,0,3,8,5,2,7,4,9,6}	8	17	16/15	35	35
No.25	{3,0,7,4,11,6,1,8,5,10,9,2}	{1,6,11,0,3,8,5,2,7,10,9,4}	8	14	15	36	36
No.26	{3,0,7,4,11,6,5,8,9,10,1,2}	{1,10,11,0,3,6,5,2,7,8,9,4}	8	14	15/14	34	36
No.27	{3,0,9,4,1,6,5,8,7,10,11,2}	{1,4,11,0,3,6,5,8,7,2,9,10}	8	14	15	33	33
No.28	{3,0,9,4,1,6,11,8,7,10,5,2}	{1,4,11,0,3,10,5,8,7,2,9,6}	8	14	15	34	35
No.29	{3,0,9,4,11,6,1,8,7,10,5,2}	{1,6,11,0,3,10,5,8,7,2,9,4}	8	15	15	33	34
No.30	{3,0,9,4,11,6,5,8,7,10,1,2}	{1,10,11,0,3,6,5,8,7,2,9,4}	8	15	15	33	33
No.31	{3,0,11,4,1,6,5,8,9,10,7,2}	{1,4,11,0,3,6,5,10,7,8,9,2}	8	14	15	35	35
No.32	{3,0,11,4,9,6,1,8,5,10,7,2}	{1,6,11,0,3,8,5,10,7,4,9,2}	8	14	15	34	33

Table 5. Result of security evaluation for k=14

$k = 14$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{13,0,1,2,3,4,5,6,7,8,9,10,11,12}	{1,2,3,4,5,6,7,8,9,10,11,12,13,0}	14	29	28	39	39
Nyberg	{2,0,4,1,6,3,8,5,10,7,12,9,13,11}	{1,3,0,5,2,7,4,9,6,11,8,13,10,12}	14	23	24	15	15
No.1	{1,2,9,4,3,6,13,8,7,10,11,12,5,0}	{13,0,1,4,3,12,5,8,7,2,9,10,11,6}	8	15	15	39	39
No.2	{1,2,9,4,13,6,7,8,5,10,3,12,11,0}	{13,0,1,10,3,8,5,6,7,2,9,12,11,4}	8	14	15	40	40
No.3	{1,2,11,4,3,6,13,8,9,10,7,12,5,0}	{13,0,1,4,3,12,5,10,7,8,9,2,11,6}	8	14	15	40	40
No.4	{5,2,1,4,11,6,3,8,13,10,9,12,7,0}	{13,2,1,6,3,0,5,12,7,10,9,4,11,8}	8	15	16	39	40/39
No.5	{5,2,9,4,1,6,13,8,7,10,3,12,11,0}	{13,4,1,10,3,0,5,8,7,2,9,12,11,6}	8	15	15/16	37	37
No.6	{5,2,13,4,11,6,3,8,1,10,9,12,7,0}	{13,8,1,6,3,0,5,12,7,10,9,4,11,2}	8	15	15	37	37
No.7	{1,2,7,4,3,6,13,8,5,12,9,10,11,0}	{13,0,1,4,3,8,5,2,7,10,11,12,9,6}	8	15	15	39	39
No.8	{1,2,7,4,5,6,11,8,3,12,13,10,9,0}	{13,0,1,8,3,4,5,2,7,12,11,6,9,10}	8	15	15	37/38	39
No.9	{1,2,7,4,11,6,13,8,5,12,3,10,9,0}	{13,0,1,10,3,8,5,2,7,12,11,4,9,6}	8	15	15/16	39	39
No.10	{1,2,9,4,3,6,7,8,11,12,13,10,5,0}	{13,0,1,4,3,12,5,6,7,2,11,8,9,10}	8	15	16	39	39
No.11	{1,2,9,4,5,6,11,8,7,12,13,10,3,0}	{13,0,1,12,3,4,5,8,7,2,11,6,9,10}	8	15	15	39	37
No.12	{1,2,9,4,11,6,7,8,5,12,13,10,3,0}	{13,0,1,12,3,8,5,6,7,2,11,4,9,10}	8	14	15	38	40
No.13	{1,2,11,4,9,6,3,8,7,12,13,10,5,0}	{13,0,1,6,3,12,5,8,7,4,11,2,9,10}	8	14	15	33	33
No.14	{1,2,11,4,13,6,7,8,5,12,9,10,3,0}	{13,0,1,12,3,8,5,6,7,10,11,2,9,4}	8	14	15	40	38
No.15	{5,2,1,4,11,6,9,10,7,8,13,0,3,12}	{11,2,1,12,3,0,5,8,9,6,7,4,13,10}	8	15	15	38	38
No.16	{5,2,9,4,1,6,13,10,11,8,7,0,3,12}	{11,4,1,12,3,0,5,10,9,2,7,8,13,6}	8	15	15/16	39	39
No.17	{5,2,9,4,3,6,1,10,7,8,13,0,11,12}	{11,6,1,4,3,0,5,8,9,2,7,12,13,10}	8	15	15	38	38
No.18	{5,2,9,4,11,6,3,10,7,8,13,0,1,12}	{11,12,1,6,3,0,5,8,9,2,7,4,13,10}	8	14	15	39	39
No.19	{7,2,1,4,9,6,3,10,11,8,13,0,5,12}	{11,2,1,6,3,12,5,0,9,4,7,8,13,10}	8	15	15	39	39
No.20	{7,2,1,4,9,6,5,10,3,12,13,0,11,8}	{11,2,1,8,3,6,5,0,13,4,7,12,9,10}	8	14	15	40	40
No.21	{1,2,11,4,3,8,5,6,13,0,7,12,9,10}	{9,0,1,4,3,6,7,10,5,12,13,2,11,8}	8	14	15	38	38
No.22	{1,2,9,6,3,4,13,0,5,10,7,12,11,8}	{7,0,1,4,5,8,3,10,13,2,9,12,11,6}	8	14	15	41	41
No.23	{1,2,9,6,13,4,3,0,7,10,5,12,11,8}	{7,0,1,6,5,10,3,8,13,2,9,12,11,4}	8	15	16	36	36

Table 6. Result of security evaluation for k=16

$k = 16$	block shuffle π	block shuffle π^{-1}	D	IDC	SC	AS$_D$	AS$_L$
TypeII	{15,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14}	{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,0}	16	33	32	39	39
Nyberg	{2,0,4,1,6,3,8,5,10,7,12,9,14,11,15,13}	{1,3,0,5,2,7,4,9,6,11,8,13,10,15,12,14}	16	26	27	16	16
No.1∗	{1,2,9,4,15,6,5,8,13,10,7,14,11,12,3,0}	{15,0,1,14,3,6,5,10,7,2,9,12,13,8,11,4}	8	15	16	39	39
No.2	{1,2,11,4,9,6,7,8,15,12,5,10,3,0,13,14}	{13,0,1,12,3,10,5,6,7,4,11,2,9,14,15,8}	8	15	15	35	36
No.3	{1,2,11,4,9,6,15,8,5,12,7,10,3,0,13,14}	{13,0,1,12,3,8,5,10,7,4,11,2,9,14,15,6}	8	15	15	38	38
No.4	{5,2,9,4,1,6,11,8,15,12,3,10,7,0,13,14}	{13,4,1,10,3,0,5,12,7,2,11,6,9,14,15,8}	8	15	15	39	26
No.5	{5,2,9,4,11,6,15,8,3,12,1,10,7,0,13,14}	{13,10,1,8,3,0,5,12,7,2,11,4,9,14,15,6}	8	14	15	41	41
No.6	{5,2,11,4,1,6,15,8,3,12,13,10,7,0,9,14}	{13,4,1,8,3,0,5,12,7,14,11,2,9,10,15,6}	8	15	15	26	39
No.7	{1,2,11,4,3,6,7,8,15,12,5,14,9,0,13,10}	{13,0,1,4,3,10,5,6,7,12,15,2,9,14,11,8}	8	14	15	40	40
No.8	{1,2,11,4,9,6,7,8,15,12,13,14,3,0,5,10}	{13,0,1,12,3,14,5,6,7,4,15,2,9,10,11,8}	8	15	15	26	26
No.9	{1,2,11,4,9,6,15,8,5,12,7,14,3,0,13,10}	{13,0,1,12,3,8,5,10,7,4,15,2,9,14,11,6}	8	15	16/15	42	42
No.10	{7,2,13,4,11,8,3,6,15,0,9,10,1,14,5,12}	{9,12,1,6,3,14,7,0,5,10,11,4,15,2,13,8}	8	14	15	44	44
No.11	{7,2,13,4,11,8,9,6,15,0,3,10,5,14,1,12}	{9,14,1,10,3,12,7,0,5,6,11,4,15,2,13,8}	8	15	16	38	38
No.12	{1,2,11,4,15,8,3,6,7,0,9,12,5,14,13,10}	{9,0,1,6,3,12,7,8,5,10,15,2,11,14,13,4}	8	15	16	42	42
No.13	{5,2,11,6,13,8,15,0,3,4,9,12,1,14,7,10}	{7,12,1,8,9,0,3,14,5,10,15,2,11,4,13,6}	8	15	15	35	35