Type 1.x Generalized Feistel Structures

Shingo Yanagihara · Tetsu Iwata

Received: date / Accepted: date

Abstract We formalize the Type 1.x Generalized Feistel Structure (GFS) in order to fill the gap between Type 1 and Type 2 GFSs. This is a natural extension of Type 1 and Type 2 GFSs, and covers them as special cases. The diffusion property of GFS is known to vary depending on the permutation used in the round function. When we have two non-linear functions in one round, we propose a permutation that has a good diffusion property, and compare it with the structure that uses a sub-block-wise cyclic shift. We also present experimental results of exhaustively evaluating the diffusion properties of all permutations up to eight sub-blocks.

Keywords Blockcipher · Type 1.x generalized Feistel structure · permutation layer.

1 Introduction

Background. The Generalized Feistel Structure, which we write GFS, is one of the structures used in the design of blockciphers and hash functions. In the classical Feistel structure, the plaintext is divided into two sub-blocks, and these are encrypted through several round functions, while in GFS, the plaintext is divided into \( d \geq 3 \) sub-blocks. Compared to the SP network used in AES [4], GFS has an advantage in that computation of the nonlinear functions is the same in encryption and decryption. On the other hand, the diffusion property of GFS is generally poor and it requires many rounds to be secure.

There are several types of GFSs [12, 5]. For example, Type 1, Type 2, Type 3, Source-Heavy, Target-Heavy, Alternating, and Nyberg’s GFSs are known. We will focus on Type 1 and Type 2 GFSs, and the former is used for example in CAST-256 and Lesamnta, and the latter is used in RC6, HIGHT, and CLEFIA.
The security of these structures has been extensively evaluated. [5] shows the security of Nyberg’s GFS. The lower bounds on the number of active S-boxes for Type 1 and Type 2 GFSs with single SP-functions and single-round diffusion are shown in [10] and [6], respectively. [7] derives the lower bounds in the case of using multiple-round diffusions, and [1,3,2] analyze the security of Type 1 and Type 2 GFSs with double SP-functions.

In the round function, GFS generally uses the sub-block-wise cyclic shift over the sub-blocks, which we write \( \pi_s \), as the permutation. As stated above, the diffusion of GFS is generally slow and it requires many rounds to be secure. At FSE 2010, Suzuki and Minematsu proposed to use a non-cyclic shift in Type 2 GFS, and demonstrated that the diffusion property is improved by changing the permutation from \( \pi_s \) [8]. The result is incorporated into the design of a practical blockcipher called TWINE [9]. Following [8], Yanagihara and Iwata studied the diffusion properties of Type 1, Type 3, Source-Heavy, and Target-Heavy GFSs [11]. They showed that the diffusion properties of Type 1 and Type 3 GFSs can be improved by changing the permutation from \( \pi_s \).

In this paper, we abuse the definition of GFS and we use the term GFS to mean structures where their permutations are not restricted to the sub-block-wise cyclic shift. Now Type 1 GFS has one non-linear function in one round function, while Type 2 GFS has \( d/2 \) functions, where \( d \) is the number of sub-blocks which is even in Type 2 GFS. Then a natural question is to see structures where we have \( \eta \) non-linear functions in the round function, where \( 1 \leq \eta \leq d/2 \).

Our Contributions. In this paper, we formalize a type of GFS called Type 1.x GFS to fill the gap between Type 1 and Type 2 GFSs. Type 1.x GFS is characterized by two integers \( d \) and \( \eta \), where \( d \) is the number of sub-blocks which is not necessarily even, and \( \eta \) is the number of the non-linear functions in one round function. Type 1.x GFS covers Type 1 and 2 GFSs as special cases; they correspond to \( \eta = 1 \) and \( \eta = d/2 \), respectively. We note that Type 1.x GFS itself is not new. For example the key schedule of 80-bit key TWINE [9] can be seen as this structure with \( d = 20 \) and \( \eta = 2 \).

For \( \eta = 2 \), we propose a construction of a permutation, which we write \( \pi_p \), that has a good diffusion property. We also characterize the diffusion property of Type 1.x GFS when we use \( \pi_p \) as the permutation. We compare these two values to see that \( \pi_p \) indeed has a better diffusion property. We also present experimental results of exhaustively evaluating the diffusion properties of all permutations for parameters \( 3 \leq d \leq 8 \) and \( 1 \leq \eta \leq \lfloor d/2 \rfloor \), and confirm that the proposed construction is the optimum construction in terms of diffusion.

2 Preliminaries

We first introduce the Generalized Feistel Structure (GFS). Let \( n \) and \( d \) be integers, where \( n \) is the size of a sub-block in bits and \( d \) is the number of sub-blocks. Let \( x^0 = (x_0^0, x_1^0, \ldots, x_{d-1}^0) \in (\{0,1\}^n)^d \) be a \( dn \)-bit plaintext. GFS encrypts \( x^0 \) with a secret key by applying the round function for \( R \) times iteratively, and outputs a \( dn \)-bit ciphertext \( x^R = (x_0^R, x_1^R, \ldots, x_{d-1}^R) \in (\{0,1\}^n)^d \).

In Fig. 1, we show an example of the round function. The round function consists of \( F \)-Layer and \( H \)-Layer. \( F \)-Layer has key dependent \( F \) functions and the
xor operations. The structure of $\mathcal{F}$-Layer depends on the types of GFS. $\Pi$-Layer is a permutation $\pi$ over $d$ sub-blocks. We assume that in the final round, the round function consists of only $\mathcal{F}$-Layer so that both encryption and decryption start with $\mathcal{F}$-Layer. Similarly to encryption, decryption is done by using $\mathcal{F}^{-1}$-Layer and $\Pi^{-1}$-Layer instead of $\mathcal{F}$-Layer and $\Pi$-Layer.

As shown in Fig. 1, the $d$ sub-blocks are sequentially numbered from left to right as $0, 1, \ldots, d-1$ and $\pi$ is considered to be a permutation over $\{0, 1, \ldots, d-1\}$. We write $\pi(i)$ for the index of the sub-block after applying $\pi$ to the $i$-th sub-block. For example, in Fig. 1, we have $\pi(0) = 3, \pi(1) = 0, \pi(2) = 1$, and $\pi(3) = 0$, and we also write them as $\pi = (3, 0, 1, 2)$ collectively. For an integer $r \geq 1$, $\pi^r(i)$ is the index of the sub-block after applying $\pi$ to the $i$-th sub-block for $r$ times. Similarly, $\pi^{-r}(i)$ is the index of the sub-block after applying $\pi^{-1}$ to the $i$-th sub-block for $r$ times. We treat $\pi^0(i)$ as $i$. We define $\pi_s$ as $\pi_s = (d-1, 0, 1, \ldots, d-2)$, i.e. $\pi_s$ is the sub-block-wise left cyclic shift.

For encryption, let $x^r$ be the intermediate result after encrypting $r$ rounds, and $x^r_i$ be the $i$-th sub-block of $x^r$. We write $x^r = (x^r_0, \ldots, x^r_{d-1}) \in (\{0, 1\}^n)^d$. For decryption, we define $y^r$ and $y^r_i$ analogously. From these definitions, $x^0$ and $y^0$ correspond to the plaintext, and $y^R$ and $x^R$ correspond to the ciphertext.

Next, we introduce Type 1 and Type 2 GFSs.

**Type 1 GFS.** We write $E^{T1}(\pi)$ for Type 1 GFS that uses $\pi$ in $\Pi$-Layer. For $E^{T1}(\pi)$, $x^r_i$ is defined as

$$x^r_i = \begin{cases} F(x^r_{\pi^{-1}(i)} \oplus x^r_{i-1}) & \text{if } \pi^{-1}(i) = 1, \\ x^r_{\pi^{-1}(i)} & \text{otherwise}, \end{cases}$$

where $F: \{0, 1\}^n \rightarrow \{0, 1\}^n$. See Fig. 2 for an example of $E^{T1}(\pi_s)$ with $d = 6$. 

---

**Type 1.x GFS** ((d, η) = (6, 2))

---

**Fig. 1 Round Function**

**Fig. 2 Type 1 GFS (d = 6)**

**Fig. 3 Type 2 GFS (d = 6)**

**Fig. 4 Type 1.x GFS ((d, η) = (6, 2))**
Type 2 GFS. We write $E^{T2}(\pi)$ for Type 2 GFS that uses $\pi$ in $\Pi$-Layer. For $E^{T2}(\pi)$, $x'_i$ is defined as

$$x'_i = \begin{cases} F(x_{\pi^{-1}(i)-1}) \oplus x_{\pi^{-1}(i)}^{-1} & \text{if } \pi^{-1}(i) \mod 2 = 1, \\ x_{\pi^{-1}(i)}^{-1} & \text{otherwise}, \end{cases}$$

where $F : \{0,1\}^n \to \{0,1\}^n$. Type 2 GFS is not defined when $d$ is odd. See Fig. 3 for an example of $E^{T2}(\pi)$ with $d = 6$.

Type 3 [12], Source-Heavy, Target-Heavy, and Alternating are also known as other types of GFS. We note that as we allow any permutation in $\Pi$-Layer, Nyberg’s GFS can be seen as a special case of Type 2 GFS.

3 Type 1.x GFS

Definition of Type 1.x GFS. In this section, we formalize a type of GFS which we call Type 1.x GFS.

Definition 1 Let $d$ and $\eta$ be integers such that $d \geq 3$ and $1 \leq \eta \leq \lfloor d/2 \rfloor$. In Type 1.x GFS, $x'_i$ is defined as

$$x'_i = \begin{cases} F(x_{\pi^{-1}(i)-1}) \oplus x_{\pi^{-1}(i)}^{-1} & \text{if } \pi^{-1}(i) \mod 2 = 1 \text{ and } \pi^{-1}(i) \leq 2\eta - 1, \\ x_{\pi^{-1}(i)}^{-1} & \text{otherwise}, \end{cases}$$

where $F : \{0,1\}^n \to \{0,1\}^n$. We write $E^{(d,\eta)}(\pi)$ for Type 1.x GFS that uses $\pi$ in $\Pi$-Layer.

Figure 4 shows $E^{(6,2)}(\pi_s)$. We see that $E^{T1}(\pi)$ with $d$ sub-blocks is equivalent to $E^{(d,1)}(\pi)$, and $E^{T2}(\pi)$ with $d$ sub-blocks is equivalent to $E^{(d,d/2)}(\pi)$ where $d$ is even. For example, Fig. 2 is $E^{(6,1)}(\pi_s)$ and Fig. 3 is $E^{(6,3)}(\pi_s)$. The integer, $\eta$, denotes the number of $F$ functions in one round, which is equivalent to the number of xor operations in one round.

Equivalence of Type 1.x GFS. We next define the equivalence of Type 1.x GFS. Intuitively, if $E^{(d,\eta)}(\pi')$ is obtained by exchanging several sub-blocks in $E^{(d,\eta)}(\pi)$, then we say that these two structures are equivalent.

More precisely, we say that $E^{(d,\eta)}(\pi)$ and $E^{(d,\eta)}(\pi')$ are equivalent if there exists $\pi^* = (a_0, \ldots, a_{d-1})$ such that $\pi' = \pi^* \circ \pi \circ (\pi^*)^{-1}$, where

$$\{a_0, a_2, \ldots, a_{2\eta-2}\} = \{0, 2, \ldots, 2\eta - 2\},$$

$$a_1 = a_0 + 1, a_3 = a_2 + 1, \ldots, a_{2\eta-1} = a_{2\eta-2} + 1, \text{and}$$

$$\{a_{2\eta}, a_{2\eta+1}, \ldots, a_{d-1}\} = \{2\eta, 2\eta + 1, \ldots, d - 1\}.$$

We note that $g \circ f(x)$ is $g(f(x))$. That is, $E^{(d,\eta)}(\pi)$ and $E^{(d,\eta)}(\pi')$ are equivalent if $\pi'$ permutes the elements within $\{(0,1), (2,3), \ldots, (2\eta - 2, 2\eta - 1)\}$ and $\{2\eta, 2\eta + 1, \ldots, d - 1\}$. It can be verified that $E^{(d,\eta)}(\pi') = \pi^* \circ E^{(d,\eta)}(\pi) \circ (\pi^*)^{-1}$. Therefore, $E^{(d,\eta)}(\pi)$ and $E^{(d,\eta)}(\pi')$ are the same structures except that the orders of the input and the output are different.
4 Diffusion Property

In this section, following [8], we introduce the notion of $\text{DRmax}^{(d, \eta)}(\pi)$ to evaluate the diffusion property of Type 1.x GFS.

**Data Dependent Variables.** We first introduce the *data dependent variables* of Type 1.x GFS, which we write $X^r$ and $Y^r$. For encryption, if we consider the diffusion of the $i$-th sub-block of the plaintext, we let $X^0 = (X^0_0, X^0_1, \ldots, X^0_{d-1}) \in \{0, 1\}^d$, where $X^0_i = 1$ and $X^0_i = 0$ for $\forall i \neq i$. Intuitively, if the $i$-th input sub-block diffuses to the $j$-th sub-block after encrypting $r$ rounds, then we let $X^r_j = 1$, and $X^r_j = 0$ otherwise. We write $X^r = (X^r_0, X^r_1, \ldots, X^r_{d-1})$. Similarly, the data dependent variable $Y^r = (Y^r_0, Y^r_1, \ldots, Y^r_{d-1}) \in \{0, 1\}^d$ is defined for decryption. If $Y^0_i = 1$ and $Y^r_j$ depends on $Y^0_i$, then we let $Y^r_j = 1$, and $Y^r_j = 0$ otherwise.

Let $j = \pi^{-1}(i)$. If $j \text{ mod } 2 = 1$ and $j \leq 2\eta - 1$, then the $i$-th sub-block of the $r$-th round depends on the $(j - 1)$-st sub-block through the $F$ function and the $j$-th sub-block of the $(r - 1)$-st round. Otherwise, the $i$-th sub-block of the $r$-th round depends on the $j$-th sub-block of the $(r - 1)$-st round. Therefore, given $X^0 = (X^0_0, X^0_1, \ldots, X^0_{d-1}) \in \{0, 1\}^d$, $X^r$ for $r \geq 1$ is successively defined as follows.

\[
X^r = \begin{cases} 
X^{r-1}_{\pi^{-1}(i)} \vee X^{r-1}_{\pi^{-1}(i)} & \text{if } \pi^{-1}(i) \text{ mod } 2 = 1 \text{ and } \pi^{-1}(i) \leq 2\eta - 1, \\
X^{r-1}_{\pi^{-1}(i)} & \text{otherwise}.
\end{cases}
\]

We note that $a \vee b$ is the or operation of $a$ and $b$. Similarly, for decryption, given $Y^0 = (Y^0_0, Y^0_1, \ldots, Y^0_{d-1}) \in \{0, 1\}^d$, $Y^r$ for $r \geq 1$ is defined as follows.

\[
Y^r = \begin{cases} 
Y^{r-1}_{\pi(i)} \vee Y^{r-1}_{\pi(i)} & \text{if } \pi(i) \text{ mod } 2 = 1 \text{ and } \pi(i) \leq 2\eta - 1, \\
Y^{r-1}_{\pi(i)} & \text{otherwise}.
\end{cases}
\]

Let $|X^r|$ be the number of bit “1” in $X^r$. If $X^r_i = 1$, then we say that the $i$-th sub-block is active. If there exists $r \geq 0$ such that $|X^r| = d$, then we say that the input $X^0$ achieves FD (Full Diffusion). If all $X^0$ such that $|X^0| = 1$ achieve FD, then we say that the GFS achieves FD.

**Definition of $\text{DRmax}^{(d, \eta)}(\pi)$ [8].** Next, we define $\text{DRmax}^{(d, \eta)}(\pi)$, which is used to characterize the diffusion property of Type 1.x GFS using $\pi$ in $H$-layer. This value is defined as the minimum number of round so that every sub-block depends on all the input sub-blocks.

More precisely, it is defined as follows:

\[
\text{DRmax}^{(d, \eta)}(\pi) \overset{\text{def}}{=} \max\{\text{DRmax}_{E}^{(d, \eta)}(\pi), \text{DRmax}_{D}^{(d, \eta)}(\pi)\}
\]

First, we define $\text{DRmax}^{(d, \eta)}_{E}(\pi)$ by using $\text{DRmax}^{(d, \eta)}_{E,i}(\pi)$. $\text{DRmax}^{(d, \eta)}_{E,i}(\pi)$ is the minimum number of round such that the $i$-th input sub-block diffuses to all the sub-blocks in the encryption direction. Therefore, $\text{DRmax}^{(d, \eta)}_{E,i}(\pi)$ is defined as

\[
\text{DRmax}^{(d, \eta)}_{E,i}(\pi) \overset{\text{def}}{=} \min\{r \mid \forall i' \neq i, X^0_{i'} = 0, X^0_i = 1, |X^r| = d\}. 
\]
Then $\text{DRmax}^{(d, \eta)}_E(\pi)$ is defined as the maximum of $\text{DRmax}^{(d, \eta)}_{E,i}(\pi)$ over all $0 \leq i \leq d - 1$ as follows:

$$
\text{DRmax}^{(d, \eta)}_E(\pi) \overset{\text{def}}{=} \max\{\text{DRmax}^{(d, \eta)}_{E,i}(\pi) | 0 \leq i \leq d - 1\}
$$

Similarly, $\text{DRmax}^{(d, \eta)}_{D,i}(\pi)$ and $\text{DRmax}^{(d, \eta)}_{D}(\pi)$ are defined for decryption. We let $\text{DRmax}^{(d, \eta)}_{D,i}(\pi) \overset{\text{def}}{=} \min\{|r | \forall d' \neq i, Y^0_{r'} = 0, Y^0_{i'} = 1, |Y^r_{d'}| = d\}$ and $\text{DRmax}^{(d, \eta)}_D(\pi) \overset{\text{def}}{=} \max(\text{DRmax}^{(d, \eta)}_{D,i}(\pi) | 0 \leq i \leq d - 1)$. We note that the optimum $\pi$ may not be unique.

We also note that this paper focuses on the diffusion property of a construction and we use $\text{DRmax}^{(d, \eta)}(\pi)$ to characterize the diffusion property. We expect that a better diffusion property implies better resistance against various cryptographic attacks, e.g., [8] shows, under a certain condition on the permutation, the relation between $\text{DRmax}^{(d,d/2)}(\pi)$ and the number of rounds of the impossible differential path and saturation path. However, $\text{DRmax}^{(d, \eta)}(\pi)$ may or may not directly reflect the security against, for example, differential or linear attacks, and hence the security against these attacks has to be evaluated independently.

5 Proposed Construction $\pi_p$

In this section, we focus on $\eta = 2$ and present our proposed construction which we call $\pi_p$. We also derive a value of $\text{DRmax}^{(d,2)}(\pi_p)$.

First, we present our construction of $\pi_p$.

**Definition 2** Let $d \geq 5$, and $a$ be an integer such that $1 \leq a \leq d - 3$. We define $\pi_p$ as follows:

$$
\pi_p = \begin{cases} 
(1, 3, 4, 2, 5, 6, \ldots, d - 1, 0) & \text{if } a = 1 \\
(1, 4, 0, 2, 5, 6, \ldots, d - 1, 3) & \text{if } a = d - 3 \\
(1, 4, a + 3, 2, 5, 6, \ldots, a + 2, 3, a + 4, a + 5, \ldots, d - 1, 0) & \text{otherwise}
\end{cases}
$$

For example, we have the following $\pi_p$'s when $d = 9$:

$$
\pi_p = \begin{cases} 
(1, 3, 4, 2, 5, 6, 7, 8, 0) & \text{if } a = 1 \\
(1, 4, 5, 2, 3, 6, 7, 8, 0) & \text{if } a = 2 \\
(1, 4, 6, 2, 5, 3, 7, 8, 0) & \text{if } a = 3 \\
(1, 4, 7, 2, 5, 6, 3, 8, 0) & \text{if } a = 4 \\
(1, 4, 8, 2, 5, 6, 7, 3, 0) & \text{if } a = 5 \\
(1, 4, 0, 2, 5, 6, 7, 8, 3) & \text{if } a = 6
\end{cases}
$$
See Fig. 6 for an example of Type 1.x GFS with $\pi_p$ when $(d, \eta) = (9, 2)$ and $a = 1$.

We next introduce $r_{ij}$ and $SB_{ij}$ which are used to compute $DR_{\max}^{(d, 2)}(\pi_p)$.

**Definition 3** For any $\pi$, let $r_{ij}$ be the smallest integer $r \geq 1$ such that $\pi^r(i) = j$, and a set $SB_{ij}$ be $SB_{ij} = \{k | \pi^r(i) = k, 0 < r \leq r_{ij}\}$.

Intuitively, $r_{ij}$ is the smallest number of applications of $\pi$ so that the $i$-th sub-block propagates to the $j$-th sub-block, and $SB_{ij}$ is the set of sub-blocks which are passed in the process.

Figure 6 shows the propagation of the left four sub-blocks of Type 1.x GFS with $\pi_p$. The 0th sub-block propagates to the 1st sub-block, and the 3rd sub-block propagates to the 2nd sub-block in one round. The 1st sub-block propagates to the 3rd sub-block in $a$ rounds, and the 3rd sub-block propagates to the 2nd sub-block in $(d - 2 - a)$ rounds. By using the notation of $r_{ij}$ and $SB_{ij}$, we have

$$
\begin{align*}
&\begin{cases} 
  r_{01} = r_{32} = 1, r_{13} = a, r_{20} = d - 2 - a, \\
  0, 2 \notin SB_{13}, 1 \notin SB_{20}, SB_{13} \cap SB_{20} = \emptyset, \text{ and} \\
  SB_{13} \cup SB_{20} \cup \{1, 2\} = \{0, 1, \ldots, d - 1\},
\end{cases} \\
\end{align*}
$$

(1)

since $SB_{13} = \{3, 4, 5, \ldots, a + 1, a + 2\}$ and $SB_{20} = \{0, a + 3, a + 4, \ldots, d - 1\}$.

Intuitively, $\pi_p$ is designed so that if the 2nd sub-block of $E^{(d, 2)}(\pi_p)$ is active in the encryption direction, then all the subsequent 2nd sub-blocks remain active as well. Similarly, if the 1st sub-block is active in the decryption direction, then all the 1st sub-blocks in the following rounds are active. The right $(d - 2\eta)$ sub-blocks are used as the propagation from the 1st and 2nd sub-blocks to the 3rd and 0th sub-blocks, respectively.

The next lemma shows the value of $DR_{\max}^{(d, 2)}(\pi_p)$.

**Lemma 1** Let $d \geq 5$. Then we have $DR_{\max}^{(d, 2)}(\pi_p) = 2d - 4$.  

For decryption, we have \( \text{DR}_{\pi_0}^{(d,2)}(\pi_p) \) for all \( 0 \leq i \leq d - 1 \). By using (1), it can be shown that \( \text{DR}_{\pi_0}^{(d,2)}(\pi_p) = 2(r_{13} + r_{20}) = 2d - 4 \) is larger than other \( \text{DR}_{\pi_0}^{(d,2)}(\pi_p) \)'s. For decryption, we have \( \text{DR}_{\pi_0}^{(d,2)}(\pi_p) = \text{DR}_{\pi_0}^{(d,2)}(\pi_p) \) since \( E^{(d,2)}(\pi_p) \) and \( E^{(d,2)}(\pi_p^{-1}) \) are equivalent, and the lemma follows.

Lemma 2 covers \( d \geq 5 \). For \( d = 4 \), we can define \( \pi_p = (1, 3, 0, 2) \). Then we have \( r_{10} = r_{32} = r_{13} = r_{20} = 1 \). Since \( SB_{13} = \{3\} \) and \( SB_{20} = \{0\} \), we also have \( 0, 2 \notin SB_{13}, 1 \notin SB_{20}, SB_{13} \cap SB_{20} = \emptyset, \) and \( SB_{13} \cup SB_{20} \cup \{1, 2\} = \{0, 1, 2, 3\} \). Since these properties are equivalent to (1) and the proof of Lemma 1 works with these properties, we have \( \text{DR}_{\pi_0}^{(d,2)}(\pi_p) = 2 \times 4 - 4 = 4 \).

### 6 Analysis of \( E^{(d,\eta)}(\pi_s) \)

In this section, we analyze the diffusion property of \( E^{(d,\eta)}(\pi_s) \).

**Lemma 2** For any \( d \geq 3 \) and \( 1 \leq \eta \leq \lfloor d/2 \rfloor \), we have \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) = \max\{\text{DR}_{\pi_0}^{(d,\eta)}(\pi_s), \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s)\} \), where

\[
\text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) = \begin{cases} 
\left\lfloor \frac{d - 2}{\eta} \right\rfloor (d - \eta) + 2 & \text{if } (d - 2) \mod \eta = 0 \\
\left\lceil \frac{d - 2 - 2\eta}{\eta} \right\rceil (d - 2\eta) + 2(d - \eta) & \text{otherwise}
\end{cases}
\]

(2)

\[
\text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) = \begin{cases} 
\left\lfloor \frac{d - 1}{\eta} \right\rfloor (d - \eta) + 1 & \text{if } (d - 1) \mod \eta = 0 \\
\left\lceil \frac{d - 2 - 2\eta}{\eta} \right\rceil (d - 2\eta) + 2(d - \eta) & \text{otherwise}
\end{cases}
\]

(3)

We show a brief overview of the proof. First, we compare \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) for all \( 0 \leq i \leq d - 1 \), and show that \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) = 2d - 2\eta \) is the largest. Similarly, we analyze the decryption direction, and we have (2) and (3). Then we show that \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) and \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) are the candidates for the largest \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) value. Finally, we compare these three values to show \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \geq \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) and \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \geq \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \), and we have the lemma.

**Discussions.** We summarize the comparison between Lemma 1 and Lemma 2 for \( 3 \leq d \leq 16 \) in Fig. 7. From the figure, we see that \( E^{(d,2)}(\pi_p) \) is better than \( E^{(d,2)}(\pi_s) \) in terms of the diffusion property for \( 3 \leq d \leq 16 \), that is, we have \( \text{DR}_{\pi_0}^{(d,2)}(\pi_s) \geq 2(d - 2) = 2d - 4 = \text{DR}_{\pi_0}^{(d,2)}(\pi_p) \). We note that we have experimentally verified the result.

### 7 Experimental Results

In this section, we present our experimental results on computing \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \). We compute \( \text{DR}_{\pi_0}^{(d,\eta)}(\pi_s) \) for all \( 3 \leq d \leq 8 \) and \( 1 \leq \eta \leq \lfloor d/2 \rfloor \). In Tables 1–4,
we list \( \pi_s \) and all optimum \( \pi \)'s, i.e., \( \text{DRmax}^{\langle d, \eta \rangle}(\pi) \) is the minimum among all permutations for given \( d \) and \( \eta \). Only the lexicographically first permutations in the equivalent classes are presented in the tables. Table 1 shows the results for \( \eta = 1 \). Similarly, Tables 2, 3, and 4 show results for \( \eta = 2, 3, \) and 4, respectively.

In the tables, permutations with \( s \) are equivalent to \( \pi_s \). In Table 2 (for \( \eta = 2 \)), the superscript in permutations with \( p \) indicates a value of \( a \) in Definition 2.

Table 1 corresponds to Type 1 GFS, and we see that the result is the same as the result in [11]. Also, we can verify that when \( d = 6 \), the permutation \( \pi = (1, 2, 5, 0, 3, 4) \) in Table 3 is equivalent to the inverse of “No. 1” in [8, p. 38, \( k = 6 \)]. Similarly, when \( d = 8 \), \( \pi = (3, 0, 1, 4, 7, 2, 5, 6) \) and \( \pi = (1, 2, 5, 0, 3, 6, 7, 4) \) in Table 4 are equivalent to “No. 1” and its inverse in [8, p. 38, \( k = 8 \)], respectively.

Furthermore, \( \pi = (1, 2, 5, 6, 7, 4, 3, 0) \) is equivalent to both “No. 2” and its inverse in [8, p. 38, \( k = 8 \)].

We summarize observations from these tables as follows:

- In many cases, there exist optimum permutations \( \pi \) such that \( \text{DRmax}^{\langle d, \eta \rangle}(\pi) < \text{DRmax}^{\langle d, \eta \rangle}(\pi_s) \), i.e., the diffusion property of Type 1.x GFS can be improved by changing the permutation from \( \pi_s \).
- For \( 4 \leq d \leq 8 \) and \( \eta = 2 \), the proposed construction \( \pi_p \) is the optimum permutation in terms of diffusion.

For given \( d \) and \( \eta \), Tables 1–4 are useful to know a permutation with a good diffusion property. However, suppose that \( (d, \eta) \neq (d', \eta') \) and we want to compare the diffusion properties of \( E^{\langle d, \eta \rangle}(\pi) \) and \( E^{\langle d', \eta' \rangle}(\pi') \). In this case, the value of \( \text{DRmax} \) may not be suitable for this purpose, and one possible option to make a comparison is to consider the value \( \eta \text{DRmax}^{\langle d, \eta \rangle}(\pi)/d \), which can be easily derived from Tables 1–4.
hence the structures obtained from Tables 1–4 do not imply that they can be used as a good diffusion property. Also, we have focused on the diffusion property and GFS with $\text{DR}_{\text{max}}$.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>$\text{DR}_{\text{max}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$(2, 0, 1)_p$</td>
<td>$\frac{6}{7}$</td>
</tr>
<tr>
<td>5</td>
<td>$(2, 0, 3, 4, 1)_p$</td>
<td>$\frac{14}{17}$</td>
</tr>
<tr>
<td>6</td>
<td>$(2, 0, 3, 4, 5, 1)_p$</td>
<td>$\frac{26}{29}$</td>
</tr>
<tr>
<td>7</td>
<td>$(2, 0, 3, 4, 5, 6, 1)_p$</td>
<td>$\frac{37}{40}$</td>
</tr>
<tr>
<td>8</td>
<td>$(2, 0, 3, 4, 5, 6, 7, 1)_p$</td>
<td>$\frac{50}{53}$</td>
</tr>
<tr>
<td></td>
<td>$(1, 1, 3, 3, 0, 1, 1, 1)_p$</td>
<td>$\frac{38}{41}$</td>
</tr>
<tr>
<td></td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{38}{41}$</td>
</tr>
</tbody>
</table>

Table 2: $\text{DR}_{\text{max}}$ for $4 \leq d \leq 8$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>$\text{DR}_{\text{max}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{8}{11}$</td>
</tr>
<tr>
<td>5</td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{8}{11}$</td>
</tr>
<tr>
<td>6</td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{12}{15}$</td>
</tr>
<tr>
<td>7</td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{12}{15}$</td>
</tr>
<tr>
<td>8</td>
<td>$(1, 1, 3, 3, 4, 0, 1, 1)_p$</td>
<td>$\frac{12}{15}$</td>
</tr>
</tbody>
</table>

Table 3: $\text{DR}_{\text{max}}$ for $6 \leq d \leq 8$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>$\text{DR}_{\text{max}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
<tr>
<td>7</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
<tr>
<td>8</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
</tbody>
</table>

Table 4: $\text{DR}_{\text{max}}$ for $d = 8$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>$\text{DR}_{\text{max}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
<tr>
<td>7</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
<tr>
<td>8</td>
<td>$(1, 2, 5, 0, 4, 4)_p$</td>
<td>$\frac{6}{11}$</td>
</tr>
</tbody>
</table>

8 Conclusions

In this paper, we formalized Type 1.x GFS, which covers Type 1 and Type 2 GFSs as special cases. We also proposed a construction $\pi_p$ for $q = 2$ and derived $\text{DR}_{\text{max}}(d, 2)(\pi_p)$. We then derived $\text{DR}_{\text{max}}(d, 0)(\pi_p)$, and we showed that Type 1.x GFS with $\pi_p$ is better than the one with $\pi_s$ in terms of diffusion. Finally, we presented our experimental results for $3 \leq d \leq 8$ and $1 \leq q \leq \lfloor d/2 \rfloor$.

As future work, it would be interesting to see constructions for $q > 2$ with a good diffusion property. Also, we have focused on the diffusion property and hence the structures obtained from Tables 1–4 do not imply that they can be used...
in practice with the suggested number of rounds. The security against various cryptographic attacks remains to be evaluated.

Acknowledgements The authors would like to thank the reviewers for useful comments. This work was supported in part by MEXT KAKENHI, Grant-in-Aid for Young Scientists (A), 22680001.

References