ON THE DIFFUSION OF THE IMPROVED GENERALIZED FEISTEL

TSONKA BAICHEVA
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria

SVETLANA TOPALOVA
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria

(Communicated by Subhamoy Maitra)

Abstract. We consider the Improved Generalized Feistel Structure (IGFS) suggested by Suzuki and Minematsu (LNCS, 2010). It is a generalization of the classical Feistel cipher. The message is divided into $k$ subblocks, a Feistel transformation is applied to each pair of successive subblocks, and then a permutation of the subblocks follows. This permutation affects the diffusion property of the cipher. IGFS with relatively big $k$ and good diffusion are of particular interest for light weight applications.

Suzuki and Minematsu (LNCS, 2010) study the case when one and the same permutation is applied at each round, while we consider IGFS with possibly different permutations at the different rounds. In this case we present permutation sequences yielding IGFS with the best known by now diffusion for all even $k \leq 2048$. For $k \leq 16$ they are found by a computer-aided search, while for $18 \leq k \leq 2048$ we first consider several recursive constructions of a permutation sequence for $k$ subblocks from two permutation sequences for $k_a < k$ and $k_b < k$ subblocks respectively. Using computer, we apply these constructions to obtain permutation sequences with good diffusion for each even $k \leq 2048$. Finally we obtain infinite families of permutation sequences for $k > 2048$.

1. Introduction

1.1. Block Ciphers. Block ciphers are important elementary components in the design of many cryptographic protocols. A block cipher is a deterministic algorithm operating on fixed-length groups of bits called blocks and using a transformation that is specified by a key. The modern design of block ciphers is based on the concept of an iterated product cipher. Product ciphers were suggested and analyzed by Claude Shannon in his seminal 1949 publication [7]. Iterated product ciphers carry out encryption in multiple rounds, and each round uses a different subkey derived from the original key.

There is no mathematical proof that product ciphers are completely secure. From practical point of view it is sufficient to demonstrate that the cipher looks highly random. Confusion and diffusion are two properties of the operation of a secure
cipher, which were identified by Shannon [7]. Confusion refers to making a relationship between the key and the ciphertext as complex and involved as possible. Diffusion is associated with dependency of bits of the output on bits of the input and of the key. In a cipher of good diffusion, flipping an input bit should change each output bit with a probability of one-half.

Many block ciphers are based on Feistel networks, and the structure and properties of Feistel ciphers have been extensively explored by cryptographers. Feistel networks were first seen commercially in IBM’s Lucifer cipher designed by Feistel and Coppersmith in 1973. A \( b \)-bit Feistel cipher consists of the repetition of \( r \) rounds of an identical structure. This repeated structure consists of a round function and a swap. The round function \( f \) maps a \( \frac{b}{2} \)-bit input to a \( \frac{b}{2} \)-bit output under the action of a set of round keys.

The Generalized Feistel Structure (GFS) is a generalization of the classical Feistel network [5], and it divides a plaintext into \( k \) subblocks for some \( k > 2 \). In [11] the so-called GFS of type 2 is suggested where the Feistel transformation is applied for each consecutive two subblocks and then a cyclic shift of the subblocks is applied.

GFS of type 2 can be easily implemented and examples of such ciphers are RC6 [6], HIGHT [4] and CLEFIA [8]. Unfortunately this type of a Feistel structure has low diffusion for large \( k \) and needs a large number of rounds.

1.2. The Improved Generalized Feistel Structure and known results about it. Suzaki and Minematsu [9] suggested the Improved Generalized Feistel Structure (IGFS) as a modification of the Generalized Feistel Structure of type 2. This modification allows improvement of the diffusion property. We briefly describe here how a block cipher based on IGFS works.

The block length is \( k.n \) (\( k \) is even) and the block has \( k \) parts of the same length (\( n \)-bits).

\[
p_1 \quad p_2 \quad p_3 \quad \cdots \quad p_k
\]

We shall denote by \( p_1, p_2, \ldots, p_k \) the subblocks of the input plain text block. The block is encrypted (decrypted) in \( R \) rounds (rounds 1, 2, \ldots, \( R \)). We denote the parts of the input block to round \( r \) by \( X_1^r, X_2^r, \ldots, X_k^r \), and those of the output block by \( Y_1^r, Y_2^r, \ldots, Y_k^r \), where \( X_1^1 = p_1 \) and \( X_i^r = Y_{i-1}^r \) for \( i = 1, 2, \ldots, k \) and \( r = 2, 3, \ldots, R \).

\[
\begin{array}{c}
X_1^r \downarrow \quad X_2^r \downarrow \quad X_3^r \downarrow \quad \cdots \quad X_k^r \downarrow \\
Y_1^r \downarrow \quad Y_2^r \downarrow \quad Y_3^r \downarrow \quad \cdots \quad Y_k^r \downarrow
\end{array}
\]

The subblocks are grouped two by two for the round transformation, namely \( X_i^r \) and \( X_{i+1}^r \) (for each odd \( i \)) are in one pair. The value of \( X_i^r \) remains unchanged, while the value of a nonlinear function \( f(X_i^r) \) is added bitwise to the value of \( X_{i+1}^r \). Then a permutation \( \pi_r \) is applied to the subblocks.
The inverse permutation $\pi_{r}^{-1}$ is used for the decryption. If the permutation applied at each round is the cyclic shift $(1, 2, \ldots, k)$, the GFS of type 2 is obtained.

Note that no permutation is applied at the last round, or if it is more convenient, we can think that the identity permutation $(1)(2)\ldots(k)$ is applied at this round.

Denote by $R_{en}$ ($R_{de}$) the smallest encryption (decryption) round after which each subblock depends on all input subblocks. We shall call the bigger of them **diffusion round** and will further denote it by $R_{d}$, namely

$$R_{d} = \max(R_{en}, R_{de}).$$

For the GFS of type 2 with $k$ subblocks $R_{d} = k$, while the diffusion round of IGFS depends on the permutations used at the different rounds.

Further investigations and new ideas on the Improved Generalized Feistel Structures are presented in [2], [3], [10], [12].

In [9] Suzaki and Minematsu construct for all even $k \leq 16$ all permutations $\pi$ which lead to the smallest $R_{d}$ if one and the same permutation $\pi$ is applied at each round. They notice that the permutations with smallest $R_{d}$ are even-odd ones, namely map odd to even subblocks and vice versa. They prove that for even-odd permutations the diffusion round

$$R_{d} \geq R_{D},$$

where $a_{R_{D}−1} < \frac{k}{2} \leq a_{R_{D}}$ and $a_{R_{D}}$ is the $R_{D}$-th element of the Fibonacci sequence (starting with 0, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots). For $k \leq 128$ the values of $R_{D}$ are

| k   | 2  | 4  | 6  | 8  | 10 | 12-16 | 18-26 | 28-42 | 44-68 | 70-110 | 112-128 |
|-----|----|----|----|----|----|-------|-------|-------|-------|--------|---------|
| $R_{D}$ | 2  | 4  | 5  | 6  | 7  | 8     | 9     | 10    | 11    | 12     |

The proof of the statement does not suppose the usage of one and the same permutation at each round. That is why this lower bound holds for any even-odd permutation sequence and we can use it in the multiple permutation case.

Suzaki and Minematsu [9] show by exhaustive computer search that the diffusion round can be $R_{d} = R_{D}$ for $k \leq 8$ and $R_{d} = R_{D} + 1$ for $10 \leq k \leq 16$ if one and the same permutation $\pi$ is applied at all rounds. They also construct IGFS with diffusion round $2t$ for all $k = 2^{t}$. In conclusion they point out that the consideration of a different permutation at each round might lead to structures with better diffusion.

To prove this conjecture for all even $4 \leq k \leq 16$ we find by a computer-aided search [1] sequences of even-odd permutations (possibly different for the different rounds) which lead to IGFS with diffusion round $R_{D}$. The applicability of big $k$ in lightweight cryptography and the better diffusion obtained for $k \leq 16$ in the
multiple permutation case, motivated us to look for constructions of permutation sequences with good diffusion for \( k > 16 \).

1.3. The Present Paper. Section 2 defines dependence matrices as a measure of the diffusion of the IGFS. Their usage is illustrated by several small examples which are further referred to in the next section.

In Section 3 we consider two permutation sequences for \( k_a \) and \( k_b \) subblocks respectively, and with diffusion rounds \( R_a \) and \( R_b \). We present several constructions which use them to make a permutation sequence for a greater number of subblocks. We prove that three of them always yield a sequence with a definite diffusion round. These are Construction 1 for \( 2k_a \) subblocks with diffusion round \( R_a + 2 \), the multiple construction for \( k_a k_b \) subblocks with diffusion round \( R_a + R_b \), and Construction 3 for \( k_a + k_b \) subblocks, where \( k_b = k_a + 2 \) with diffusion round \( \max(R_a, R_b) + 3 \). These constructions can be used to obtain infinite families.

We also present constructions which can only be applicable under definite conditions, or constructions which proved to be useful for some definite values of \( k_a \) and \( k_b \). Using them we obtain sequences for \( k_a + k_b \) subblocks, where \( k_b = k_a + 2 \) with diffusion round \( \max(R_a, R_b) + 2 \) (Constructions 4, 5, and 6), and sequences for \( k_a k_b \) subblocks with diffusion round \( R_a + R_b - 2 \) (Construction 2).

Each construction is followed by a relevant example. The dependence matrices for Examples 8 - 12 can be found in the files that are available online.

Section 4 is a summary of the properties of the permutation sequences with the best known diffusion which we construct for all even values of \( k \leq 2048 \). Section 5 shows how infinite series of permutation sequences can be derived for \( k > 2048 \).

2. Dependence Matrices

Consider an \( R \)-round IGFS with \( k \) subblocks. Denote by \( \pi_r \) the permutation at round \( r < R \). To simplify the notations, when it is clear from the context which round \( r \) is concerned, we use \( x_i \) instead of \( X_i^r \) and denote by \( y_i \) the \( i \)-th subblock after the Feistel transformation at round \( r \), but before applying \( \pi_r \).

We use a cyclic representation of the permutations. Namely, if \( \pi \) contains the cycle \((b_1, b_2, b_3, \ldots, b_f)\), then \( \pi \) moves the element which was in place \( b_1 \) to place \( b_2 \), the element which was in place \( b_2 \) to place \( b_3 \), \ldots, and the element which was in place \( b_f \) to place \( b_1 \). To express the same, we also use the notations \( \pi(b_1) = b_2, \pi(b_2) = b_3, \ldots, \pi(b_f) = b_1 \). The inverse permutation \( \pi^{-1} \) contains the cycle \((b_2, b_1, b_f, \ldots, b_3)\) and we write \( \pi^{-1}(b_2) = b_1, \pi^{-1}(b_1) = b_f, \ldots, \pi^{-1}(b_3) = b_2 \).

Example 1. Permutations and shuffles

Consider permutations of four elements. Let \( \pi_1 = (1, 2)(3, 4), \pi_2 = (1, 2, 3, 4), \pi_3 = (1, 4, 3, 2), \pi_4 = (1, 2, 3)(4) \). The corresponding shuffles are:

| perm | place | 1 | 2 | 3 | 4 |
|------|-------|---|---|---|---|
| \( \pi_1 \) | 2     | 1 | 4 | 3 |
| \( \pi_2 \) | 4     | 1 | 2 | 3 |
| \( \pi_3 \) | 2     | 3 | 4 | 1 |
| \( \pi_4 \) | 3     | 1 | 2 | 4 |

The inverse permutations are: \( \pi_1^{-1} = (1, 2)(3, 4), \pi_2^{-1} = (1, 4, 3, 2), \pi_3^{-1} = (1, 2, 3, 4), \pi_4^{-1} = (1, 3, 2)(4) \).
We denote by \(e_1, e_2, \ldots, e_k\) the encrypted subblocks after the last round \(R\), and by \(\rho_r\) the permutation at the \(r\)-th decryption round, where \(\rho_r = \pi^{-1}_{R-r}\) for \(r = 1, 2, \ldots, R - 1\) (the inverse permutations are used at decryption).

As a measure of the diffusion we consider the dependence matrix \(M = (m_{ij})_{k \times k}\), where \(m_{ij}\) is 1 if the value of the \(i\)-th subblock depends on the value of the \(j\)-th subblock of the plaintext, and 0 if not. In the following examples at encryption we denote by \(I_r\) the dependence matrix at the beginning of round \(r\), and by \(\Phi_r\) the dependence matrix after the Feistel transformation at round \(r\) (before applying \(\pi_r\)).

At decryption we use the notation \(\Gamma_r\) instead of \(I_r\), and \(\Phi_r\) instead of \(\Phi_r\).

For each odd \(i\) the value of the subblock \(x_i\) remains unchanged by the Feistel transformation, while the value of a nonlinear function \(f(x_i)\) is added bitwise to the value of \(x_{i+1}\). That is why after the Feistel transformation the subblock \(y_{i+1}\) starts depending on all subblocks on which \(x_i\) depends. Therefore the odd rows of \(\Phi_r\) are the same as those of \(I_r\), while the \(j\)-th element of the \(i\)-th row (for even \(i\)) of \(\Phi_r\) contains 1 if the \(j\)-th element of either the \(i\)-th, or the \(i-1\)-st row of \(I_r\) is 1, namely each odd row of \(I_r\) is added (elementwise and modulo 2) to the next even row to obtain the corresponding even row of \(\Phi_r\). The matrix \(I_{r+1}\) is obtained by applying \(\pi_r\) on the rows of \(\Phi_r\).

Note that at the diffusion round \(R_d\) the matrix \(\Phi_r\) is the all-one \(k \times k\) matrix. The decryption dependence matrices \(\Gamma_r\) and \(\Phi_r\) are related in the same way as \(I_r\) and \(\Phi_r\).

**Example 2. Permutations and dependence matrices for IGFS with \(k = 2\) and diffusion round 2**

Encryption/decryption permutation: \(\pi_1 = (1, 2)\).

\[
\begin{array}{c|cc}
I_1 & p_1 & p_2 \\
\hline
x_1 & 1 & 0 \\
x_2 & 0 & 1 \\
\end{array}
\quad
\begin{array}{c|cc}
F_1 & p_1 & p_2 \\
\hline
y_1 & 1 & 0 \\
y_2 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|cc}
I_2 & p_1 & p_2 \\
\hline
x_1 & 1 & 1 \\
x_2 & 0 & 1 \\
\end{array}
\quad
\begin{array}{c|cc}
F_2 & p_1 & p_2 \\
\hline
y_1 & 1 & 1 \\
y_2 & 1 & 1 \\
\end{array}
\]

By \(\pi_1: F_1 \rightarrow I_2\) as: \(y_1 (from F_1) \rightarrow x_2 (from I_2)\), \(y_2 (from F_1) \rightarrow x_1 (from I_2)\).

**Example 3. Permutations and dependence matrices for IGFS with \(k = 4\) and diffusion round 4**

\(\pi_1 = (1, 2)(3, 4), \pi_2 = (1)(2, 4)(3), \pi_3 = (1, 2)(3, 4).\) In this case the decryption sequence is the same.

Encryption

\[
\begin{array}{c|ccccc}
I_1 & p_1 & p_2 & p_3 & p_4 \\
\hline
x_1 & 1 & 0 & 0 & 0 \\
x_2 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 0 & 1 \\
x_4 & 0 & 0 & 0 & 1 \\
\end{array}
\quad
\begin{array}{c|ccccc}
F_1 & p_1 & p_2 & p_3 & p_4 \\
\hline
y_1 & 1 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 0 & 0 \\
y_3 & 0 & 0 & 1 & 0 \\
y_4 & 0 & 0 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|ccccc}
I_2 & p_1 & p_2 & p_3 & p_4 \\
\hline
x_1 & 1 & 1 & 0 & 0 \\
x_2 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 1 & 1 \\
x_4 & 0 & 0 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|ccccc}
F_2 & p_1 & p_2 & p_3 & p_4 \\
\hline
y_1 & 1 & 1 & 0 & 0 \\
y_2 & 0 & 0 & 0 & 0 \\
y_3 & 0 & 0 & 1 & 1 \\
y_4 & 0 & 0 & 1 & 1 \\
\end{array}
\]

\(\pi_1 = (1, 2)(3, 4): y_1 \rightarrow x_2, y_2 \rightarrow x_1, y_3 \rightarrow x_4, y_4 \rightarrow x_3.\)

\(\pi_2 = (1)(2, 4)(3): y_1 \rightarrow x_1, y_2 \rightarrow x_4, y_3 \rightarrow x_3, y_4 \rightarrow x_2.\)
\[ \pi_3 = (1, 2)(3, 4): y_1 \rightarrow x_2, y_2 \rightarrow x_1, y_3 \rightarrow x_4, y_4 \rightarrow x_3. \]

| \( \mathbf{I}_3 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) |
|---|---|---|---|---|
| \( \mathbf{F}_3 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) |
| \( x_1 \) | 1 | 1 | 0 | 0 |
| \( y_1 \) | 1 | 1 | 0 | 0 |
| \( x_2 \) | 0 | 0 | 1 | 1 |
| \( y_2 \) | 1 | 1 | 1 | 1 |
| \( x_3 \) | 0 | 0 | 1 | 1 |
| \( y_3 \) | 0 | 0 | 1 | 1 |
| \( x_4 \) | 1 | 1 | 0 | 0 |
| \( y_4 \) | 1 | 1 | 1 | 1 |

Example 4. **Permutations and dependence matrices for IGFS with** \( k = 6 \) **and diffusion round 5**

\( \pi_1 = (1, 2)(3, 4)(5, 6), \pi_2 = (1, 6, 5, 4, 3, 2), \pi_3 = (1, 2, 5, 6, 3, 4), \pi_4 = (1, 6, 5, 2)(3, 4). \)

**Decryption sequence:** \( \rho_1 = \pi_4^{-1} = (1, 2, 5, 6)(3, 4), \rho_2 = \pi_3^{-1} = (1, 4, 3, 6, 5, 2), \rho_3 = \pi_2^{-1} = (1, 2, 3, 4, 5, 6), \rho_4 = \pi_1^{-1} = (1, 2)(3, 4)(5, 6). \)

**The encryption dependence matrices are:**

| \( \mathbf{I}_1 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
|---|---|---|---|---|---|---|
| \( \mathbf{F}_1 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
| \( x_1 \) | 1 | 0 | 0 | 0 | 0 | 0 |
| \( y_1 \) | 1 | 0 | 0 | 0 | 0 | 0 |
| \( x_2 \) | 0 | 1 | 0 | 0 | 0 | 0 |
| \( y_2 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( x_3 \) | 0 | 0 | 1 | 0 | 0 | 0 |
| \( y_3 \) | 0 | 0 | 1 | 0 | 0 | 0 |
| \( x_4 \) | 0 | 0 | 0 | 1 | 0 | 0 |
| \( y_4 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( x_5 \) | 0 | 0 | 0 | 0 | 1 | 0 |
| \( y_5 \) | 0 | 0 | 0 | 0 | 1 | 0 |
| \( x_6 \) | 0 | 0 | 0 | 0 | 0 | 1 |
| \( y_6 \) | 0 | 0 | 0 | 0 | 1 | 1 |

\( \pi_1 = (1, 2)(3, 4)(5, 6). \)

| \( \mathbf{I}_2 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
|---|---|---|---|---|---|---|
| \( \mathbf{F}_2 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
| \( x_1 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( y_1 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( x_2 \) | 1 | 0 | 0 | 0 | 0 | 0 |
| \( y_2 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( x_3 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( y_3 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( x_4 \) | 0 | 0 | 1 | 0 | 0 | 0 |
| \( y_4 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( x_5 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( y_5 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( x_6 \) | 0 | 0 | 0 | 0 | 1 | 0 |
| \( y_6 \) | 0 | 0 | 0 | 0 | 1 | 1 |

\( \pi_2 = (1, 6, 5, 4, 3, 2). \)

| \( \mathbf{I}_3 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
|---|---|---|---|---|---|---|
| \( \mathbf{F}_3 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
| \( x_1 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( y_1 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( x_2 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( y_2 \) | 1 | 1 | 1 | 1 | 0 | 0 |
| \( x_3 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( y_3 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( x_4 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( y_4 \) | 0 | 0 | 1 | 1 | 1 | 1 |
| \( x_5 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( y_5 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( x_6 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( y_6 \) | 1 | 1 | 0 | 0 | 1 | 1 |

\( \pi_3 = (1, 2, 5, 6, 3, 4). \)

| \( \mathbf{I}_4 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
|---|---|---|---|---|---|---|
| \( \mathbf{F}_4 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) |
| \( x_1 \) | 0 | 0 | 1 | 1 | 1 | 1 |
| \( y_1 \) | 0 | 0 | 1 | 1 | 1 | 1 |
| \( x_2 \) | 1 | 1 | 0 | 0 | 0 | 0 |
| \( y_2 \) | 1 | 1 | 1 | 1 | 1 | 1 |
| \( x_3 \) | 1 | 1 | 0 | 0 | 1 | 1 |
| \( y_3 \) | 1 | 1 | 0 | 0 | 1 | 1 |
| \( x_4 \) | 0 | 0 | 1 | 1 | 0 | 0 |
| \( y_4 \) | 1 | 1 | 1 | 1 | 1 | 1 |
| \( x_5 \) | 1 | 1 | 1 | 1 | 0 | 0 |
| \( y_5 \) | 1 | 1 | 1 | 1 | 0 | 0 |
| \( x_6 \) | 0 | 0 | 0 | 0 | 1 | 1 |
| \( y_6 \) | 1 | 1 | 1 | 1 | 1 | 1 |
The diffusion round depends on the permutation sequence. This is illustrated in the following example.

**Example 5. Permutations and dependence matrices for IGFS with $k = 6$ and diffusion round 6**

Consider Example 4, but let $\pi_4 = (1, 5)(2, 4)(3, 6)$. Then:

\[
\begin{array}{cccccccc}
  x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
  x_2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_4 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
  x_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

With this $\pi_4$ round 5 is not the diffusion round ($F_5$ is not an all-one matrix). The diffusion round can be 6 if we further choose a suitable $\pi_5$. Let $\pi_5 = (1, 2)(3, 4)(5, 6)$. Then:

\[
\begin{array}{cccccccc}
  x_1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
  x_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

### 3. Recursive constructions

#### 3.1. A double construction. **Construction 1.**

Suppose there is a permutation sequence $\alpha_1, \alpha_2, \ldots, \alpha_{ra}$ for $ka$ subblocks with diffusion round $Ra = ra + 1$. Define a permutation sequence $\pi_1, \pi_2, \ldots, \pi_{ra+2}$ for $k = 2ka$ subblocks in the following way:

1. **At round** $r = ra$ we apply the permutation $\pi_r$ to the first $ka$ rows, and simultaneously to the subsequent $ka$ rows:
   - $\pi_r(j) = \alpha_r(j)$ for $j \leq ka$.
   - $\pi_r(j) = \alpha_r(j - ka) + ka$ for $j > ka$.

2. **At round** $r = ra + 1$:
   - $\pi_{ra+1} = (1)(2, ka+2)(3)(4, ka+4) \ldots (ka-1)(ka, k)(ka+1)(ka+3)(ka+5) \ldots (k-1)$.

3. **At round** $r = ra + 2$:
   - $\pi_{ra+2} = (1, 2)(3, 4) \ldots (k-1, k)$.

Construction 1 yields a sequence with diffusion round $Ra + 2$ (Theorem 3.1).
Example 6. Construction 1 for $k = 2, k_a = 8$ subblocks

From the permutation sequence for 4 subblocks from Example 3 we obtain a permutation sequence for 8 subblocks with diffusion round 6. The first three encryption rounds lead to $\mathbf{F}_4$ containing two $4 \times 4$ all-one submatrices:

\[
\pi_4 = (1)(2,6)(3)(4,8)(5)(7)
\]

\[
\begin{array}{c|cccccccc}
I_4 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_3 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_4 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_6 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
x_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_8 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|cccccccc}
F_4 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_3 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_4 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_6 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_8 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{array}
\]

\[
\pi_5 = (1,2)(3,4)(5,6)(7,8)
\]

\[
\begin{array}{c|cccccccc}
I_5 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_3 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_4 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_6 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
x_8 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\end{array}
\quad
\begin{array}{c|cccccccc}
F_5 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_3 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_4 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
y_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_6 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
y_8 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{array}
\]

Decryption

\[
\rho_1 = \pi_5^{-1} = \pi_5 = (1,2)(3,4)(5,6)(7,8)
\]

\[
\begin{array}{c|cccccccc}
\Gamma_1 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
x_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
x_6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
x_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\hline
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{array}
\quad
\begin{array}{c|cccccccc}
\Phi_1 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
y_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
y_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
y_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

\[
\begin{array}{c|cccccccc}
\Gamma_2 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
x_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
x_4 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
x_5 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
x_6 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
x_7 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\hline
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|cccccccc}
\Phi_2 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
y_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
y_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
y_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
y_8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]
On the diffusion of the Improved Generalized Feistel

\[ \rho_2 = \pi_4^{-1} = \pi_4 = (1)(2,6)(3)(4,8)(5)(7) \]

\[
\begin{array}{c|cccccccc}
\Gamma_3 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
x_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
x_5 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_6 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
x_8 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
\end{array}
\]

\[
\Phi_3 | e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
y_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
y_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
y_5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y_6 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
y_7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
y_8 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
\end{array}
\]

For all odd \( j \), the \( j \)-th and \( j + 1 \)-st columns of \( \Gamma_3 \) are the same, so rearranging the columns as follows, we see that \( \Gamma_3 \) is made of four submatrices of dimension \( 4 \times 4 \) that contain one 1 in each row and column.

\[
\begin{array}{c|cccccccc}
\Gamma_3 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
\hline
x_1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
x_2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
x_4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
x_5 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
x_6 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{array}
\]

That is why the next application of \( \pi_3^{-1}, \pi_2^{-1} \), and \( \pi_1^{-1} \) will lead to an all-one matrix.

The construction is well illustrated by Example 3 too, where the presented permutation sequence for 4 subblocks can be considered as obtained by Construction 1 using the permutation sequence for 2 subblocks from Example 2. Namely:

\[ \alpha_1 = (1,2) \] and therefore \( \pi_1 = (1,2)(3,4) \), \( \pi_2 = (1)(2,4)(3) \), \( \pi_3 = (1,2)(3,4) \).

**Theorem 3.1.** If there exists a permutation sequence \( \alpha_1, \alpha_2, \ldots, \alpha_r \) for \( 2k_a \) subblocks with diffusion round \( R_a = r_a + 1 \), then there exists a permutation sequence \( \pi_1, \pi_2, \ldots, \pi_{r_a+2} \) for \( 2k_a \) subblocks with diffusion round \( R_a + 2 \).

**Proof.** We will show that Construction 1 yields a permutation sequence with diffusion round \( R_a + 2 \). At the first \( r_a \) rounds the subblocks are partitioned in two groups (first group: \( 1, 2, \ldots, k_a \) and second group: \( k_a + 1, k_a + 2, \ldots, 2k_a \)) and the permutations move blocks within their group. Therefore after the first \( r_a \) rounds the 1-s in the dependence matrix are grouped in two all-one submatrices of dimension \( k_a \times k_a \) (see \( F_2 \) of example 3 or \( F_1 \) of example 6). By permutation \( \pi_{r_a+1} \) each of the even subblocks moves next to an odd subblock of the other group. The even subblock in a Feistel pair depends now on all elements on which the odd subblock does not, and vice versa. That is why two rounds are needed to share dependencies by the Feistel transformation. The last permutation \( \pi_{r_a+2} \) permutes the two blocks within each pair of subblocks and this way the all-one matrix is obtained after round \( \pi_{r_a+2} \). The encryption diffusion round is \( R_a + 2 \).

The first two decryption rounds lead to \( \Gamma_2 \) and \( \Gamma_3 \) whose \( j \)-th and \( j+1 \)-st columns are the same for all odd \( j \) and therefore the columns of \( \Gamma_3 \) can be permuted in such a way that the odd columns precede the even ones. The resulting matrix is made of four submatrices of dimension \( k_a \times k_a \) containing one 1 in each row and column (see \( \Gamma_3 \) of example 6). The dependence matrix before round 1 of an IGFS for \( k_a \)
subblocks is a matrix of dimension $k_a \times k_a$ that contains one 1 in each row and column. The application of $\alpha_{r_a}^{-1}, \alpha_{r_a-1}^{-1}, \ldots \alpha_{1}^{-1}$ turns such a matrix to an all-one matrix. That is why the next application of the permutations $\alpha_{r_a}^{-1}, \alpha_{r_a-1}^{-1}, \ldots \alpha_{1}^{-1}$ both to the first, and to the second $k_a$ subblocks will result in an all-one dependence matrix (made of four $k_a \times k_a$ all-one submatrices), i.e. the decryption diffusion round is $R_a + 2$ too.

3.2. The Multiple Construction. Suppose that there exist two permutation sequences:

- $\alpha_1, \alpha_2, \ldots \alpha_r$, for $k_a$ subblocks with diffusion round $R_a = r_a + 1$
- $\beta_1, \beta_2, \ldots \beta_{r_b}$ for $k_b$ subblocks with diffusion round $R_b = r_b + 1$.

Define a permutation sequence $\pi_1, \pi_2, \ldots \pi_{r_a+r_b+1}$ for $k = k_a k_b$ subblocks as follows:

1. **At round** $r \leq r_a$: We partition the subblocks to $k_a$ groups of size $k_a$ and apply $\alpha_r$ to each group.

$$\pi_r(j + (l-1)k_a) = \alpha_r(j) + (l-1)k_a, \text{ where } j = 1, 2, \ldots, k_a, \ l = 1, 2, \ldots, k_b.$$ 

2. **At round** $r = R_a$: We rearrange the subblocks in $k_a$ groups of size $k_b$, such that each group contains one subblock from each former group of size $k_a$.

$$\pi_{R_a}(j + (l-1)k_b) = l + (j-1)k_b, \text{ where } j = 1, 2, \ldots, k_a, \ l = 1, 2, \ldots, k_b.$$ 

3. **At round** $r > R_a$: We apply $\beta_r$ to each of the successive groups of size $k_b$.

$$\pi_r(l + (j-1)k_b) = \beta_r(l) + (j-1)k_b, \text{ where } j = 1, 2, \ldots, k_a, \ l = 1, 2, \ldots, k_b.$$ 

The construction results in a permutation sequence for $k_a k_b$ subblocks with diffusion round $R_a + R_b$ (Theorem 3.2). The next example illustrates how it works.

**Example 7. The multiple construction for $k = k_a k_b = 24 = 8$ subblocks**

Let $k_a = 2$ and $k_b = 4$ and use the permutation sequences from Examples 2 and 3. A permutation sequence for $k = 8$ subblocks with diffusion round 6 is obtained.

**Encryption**

\[
\begin{array}{c|cccccccc|cccccccc}
I_1 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & F_1 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & y_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & y_3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
x_4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & y_4 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & y_5 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
x_6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & y_6 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & y_7 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & y_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\]

The first permutation $\pi_1$ is obtained by applying the permutation $\alpha_1$ to the successive groups of size $k_a = 2$, i.e. $\alpha_1 = (1, 2) \Rightarrow \pi_1 = (1, 2)(3, 4)(5, 6)(7, 8)$

\[
\begin{array}{c|cccccccc|cccccccc}
I_2 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & F_2 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & y_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & y_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & y_3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & y_4 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_5 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & y_5 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
x_6 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & y_6 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & y_7 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & y_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\]

The matrix $F_2$ has all-one $2 \times 2$ ($k_a \times k_a$) matrices along the main diagonal and zeros elsewhere. The next permutation $\pi_2$ will rearrange the subblocks in successive groups of size $k_b = 4$, such that each group contains one subblock from each former group of size $k_a = 2$. 
\( \pi_2 = (1)(2, 5, 3)(4, 6, 7)(8) \)

\[
\begin{array}{c|cccccccc}
I_3 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
x_5 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_6 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
x_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\quad \begin{array}{c|cccccccc}
F_3 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_3 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
y_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y_5 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
y_6 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
y_7 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
y_8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\]

\( \beta_1 = (1, 2)(3, 4) \Rightarrow \pi_3 = (1, 2)(3, 4)(5, 6)(7, 8) \)

\[
\begin{array}{c|cccccccc}
I_4 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
x_4 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_5 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_6 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_8 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\quad \begin{array}{c|cccccccc}
F_4 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y_5 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
y_6 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y_8 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\]

\( \beta_2 = (1, 4, 3, 2) \Rightarrow \pi_4 = (1, 4, 3, 2)(5, 8, 7, 6) \)

\[
\begin{array}{c|cccccccc}
I_5 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_3 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
x_4 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_5 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
x_6 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
x_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
x_8 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
\end{array}
\quad \begin{array}{c|cccccccc}
F_5 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
y_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y_4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
y_5 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
y_6 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
y_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y_8 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
\end{array}
\]

\( \beta_3 = (1, 2)(3, 4) \Rightarrow \pi_5 = (1, 2)(3, 4)(5, 6)(7, 8) \)

\[
\begin{array}{c|cccccccc}
I_6 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
x_1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_4 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_6 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_8 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{array}
\quad \begin{array}{c|cccccccc}
F_6 & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\
\hline
y_1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

Decryption
\( \rho_1 = \pi_5^{-1} = (1, 2)(3, 4)(5, 6)(7, 8) \), \( \rho_2 = \pi_4^{-1} = (1, 2, 3, 4)(5, 6, 7, 8) \), \( \rho_3 = \pi_3^{-1} = (1, 2)(3, 4)(5, 6)(7, 8) \). The successive application of \( \rho_1 \), \( \rho_2 \) and \( \rho_3 \) at the first three decryption rounds results in all-one \( 4 \times 4 \) \((k_b \times k_b)\) matrices along the main diagonal of \( \Phi_4 \) and zeros elsewhere.
The permutation \( \rho_4 \) rearranges the subblocks in groups of size \( k_a = 2 \), such that each group contains one subblock from each former group of size \( k_b = 4 \). If we apply the same permutation to the blocks of \( \Gamma_5 \), the matrix \( \Gamma_5' \) is obtained.

\[
\rho_4 = \pi_2^{-1} = (1)(2, 3, 5)(4, 7, 6)(8)
\]

\[
\begin{array}{c|cccccccc}
\Phi_4 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \\
y_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_3 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_4 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y_6 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y_8 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{array}
\]

\[
\begin{array}{c|cccccccc}
\Phi_5 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \\
x_1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_4 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_5 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_6 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
x_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_8 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\end{array}
\]

\[
\begin{array}{c|cccccccc}
\Phi_6 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \\
y_1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_5 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
y_8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

**Theorem 3.2.** If there exist two permutation sequences: \( \alpha_1, \alpha_2, \ldots, \alpha_{a_i} \) for \( k_a \) subblocks with diffusion round \( R_a = r_a + 1 \), and \( \beta_1, \beta_2, \ldots, \beta_{b_i} \) for \( k_b \) subblocks with diffusion round \( R_b = r_b + 1 \), then there exists a permutation sequence \( \pi_1, \pi_2, \ldots, \pi_{R-1} \) for \( k_a k_b \) subblocks with diffusion round \( R = R_a + R_b \).

**Proof.** We will prove that the multiple construction yields a permutation sequence with diffusion round \( R_a + R_b \). At the first \( r_a \) rounds the subblocks are partitioned to \( k_b \) groups of size \( k_a \). Let subblock \( x_i \) be the \( j \)-th subblock in the \( l \)-th group. Then \( i = j + (l-1)k_a \). The permutations at rounds \( r \leq r_a \) move blocks within their group by \( \alpha_a \). If we consider IGFS with \( k_a \) subblocks, the successive application of the permutations \( \alpha_1, \alpha_2, \ldots, \alpha_{a_i} \) transforms the \( k_a \times k_a \) identity matrix (the dependence matrix at round 1) to a \( k_a \times k_a \) all-one matrix (the dependence matrix at round \( R_a \)). Therefore, after the first \( r_a \) rounds of the multiple construction, the \( 1 \)-s in the dependence matrix are grouped in \( k_b \) all-one submatrices of dimension \( k_a \times k_a \) along the main diagonal (see \( F_2 \) of example 7).

By the permutation at round \( R_a \) the subblocks are rearranged in \( k_a \) groups of size \( k_b \), such that each group contains one subblock from each former group of size \( k_a \). Since permutations of the columns of the dependence matrix do not affect the diffusion round, to better explain the effect of \( \pi_{R_a} \), we can apply it to the
columns of the dependence matrix too. This will turn it to a matrix made of \(k_b \times k_b\) submatrices containing exactly one 1 in each row or column (see \(\Gamma_5^k\) in example 7). At the rounds bigger than \(R_b\) the permutations \(\beta_1, \beta_2, \ldots, \beta_{r_b}\) are applied to each such \(k_b \times k_b\) submatrix, thus transforming it to an all-one submatrix (because each \(k_b \times k_b\) matrix with one 1 in each row and column can be the round 1 dependence matrix of an IGFS with \(k_b\) subblocks). That is why the encryption diffusion round is \(R_a + R_b\).

Decryption works in just the same way, but it starts with applying the decryption sequence for \(k_b\) subblocks, then rearranges the blocks to groups of size \(k_a\), and goes on with the decryption sequence for \(k_a\) subblocks. Thus the decryption diffusion round is \(R_a + R_b\) too.

Since there exists a permutation sequence for two subblocks with diffusion round 2, Theorem 3.1 can also be proved using Theorem 3.2.

3.3. Construction 2. This is a modification of the multiple construction. Suppose that there exist two permutation sequences:

- \(\alpha_1, \alpha_2, \ldots, \alpha_{r_a}\) for \(2k_a\) subblocks with diffusion round \(R_a = r_a + 1\)
- \(\beta_1, \beta_2, \ldots, \beta_{r_b}\) for \(2k_b\) subblocks with diffusion round \(R_b = r_b + 1\), where
  \[\beta_1 = (1, 2)(3, 4)\ldots(2k_b - 1, 2k_b)\].

Define a permutation sequence \(\pi_1, \pi_2, \ldots, \pi_{R-1}\) for \(k = 2k_a k_b\) subblocks as follows:

1. **At round** \(r \leq r_a\): We partition the subblocks to successive groups of size \(2k_a\) and apply \(\alpha_r\) to each group, namely
   \[\pi_r(j + 2l k_a) = \alpha_r(j) + 2l k_a,\]  
   where \(j = 1, 2, \ldots, 2k_a, l = 0, 1, \ldots, k_a - 1\).

2. **At round** \(r = R_a\): The permutation \(\psi\) rearranges the subblocks in successive groups of size \(2k_b\) and such that each group contains 2 subblocks from each former group of size \(2k_a\).
   \[\psi((j - 1)k_a + l + 1) = j + 2l k_b,\]  
   where \(j = 1, 2, \ldots, 2k_b, l = 0, 1, \ldots, k_a - 1\).

   We intend to go on applying the permutations of the second sequence at the next rounds. The specific choice of \(\beta_1\), however, allows us to skip the two rounds corresponding to the first two permutations, because with this \(\beta_1\) they do not add any new dependencies. But to go on, we need the same arrangement of the subblocks. That is why skipping the two rounds, we must apply the corresponding to them permutations at round \(R_a\), namely: \(\pi_{R_a} = \varphi_2 \varphi_1 \psi\), where the permutations \(\varphi_1\) and \(\varphi_2\) are obtained by applying \(\beta_1\) and \(\beta_2\) to the \(k_a\) successive groups of size \(2k_b\), i.e.
   \[\varphi_1(j + 2l k_b) = \beta_1(j) + 2l k_b,\]  
   for \(j = 1, 2, \ldots, 2k_b, l = 0, 1, \ldots, k_a - 1\).

3. **At round** \(r > R_a\) we apply \(\beta_3, \beta_4, \ldots, \beta_{r_b}\) to each of the successive groups of size \(2k_b\). More precisely:
   \[\pi_r(j + 2l k_b) = \beta_r(j - R_a + 2)(j) + 2l k_b,\]  
   for \(j = 1, 2, \ldots, 2k_b, l = 0, 1, \ldots, k_a - 1\).

   The encryption diffusion round is \(R = R_a + R_b - 2\). In all cases when we used the construction with \(k \leq 2048\) the decryption diffusion round was \(R_a + R_b - 2\) too.

**Example 8. Construction 2 for** \(k = 2k_a k_b = 2.3.3 = 18\) **subblocks**

A permutation sequence for 18 subblocks with diffusion round 8 is constructed from the permutation sequence \(\alpha_1 = \beta_1, \ldots, \alpha_4 = \beta_4\) for 6 subblocks with diffusion round 5 from example 4. The first 4 permutations \(\pi_1, \ldots, \pi_4\) are obtained from \(\alpha_1, \ldots, \alpha_4:\)

- \(\alpha_1 = (1, 2)(3, 4)(5, 6) \Rightarrow \pi_1 = (1, 2)(3, 4)\ldots(17, 18)\)
- \(\alpha_2 = (1, 6, 5, 4, 3, 2) \Rightarrow \pi_2 = (1, 6, 5, 4, 3, 2)\ldots(13, 18, 17, 16, 15, 14)\)
- \(\alpha_3 = (1, 2, 5, 6, 3, 4) \Rightarrow \pi_3 = (1, 2, 5, 6, 3, 4)\ldots(13, 14, 17, 18, 15, 16)\)
- \(\alpha_4 = (1, 6, 5, 2)(3, 4) \Rightarrow \pi_4 = (1, 6, 5, 2)(3, 4)\ldots(13, 18, 17, 14)(15, 16)\)
Applying them at the first 4 rounds leads to the following dependence matrix $F_5$ which consists of all-one submatrices of dimension $6 \times 6$ along the main diagonal and zeroes elsewhere. The subblocks are then rearranged in new groups of size 6 by the permutation $\psi = (1)(2, 7, 3, 13, 5, 8, 9, 15, 17, 12, 16, 6, 14, 11, 10, 4)(18)$. Each new group contains 2 subblocks from each old group.

$$
\begin{align*}
F_5 & = \\
\psi F_5 & = \\
\end{align*}
$$

We can check that the columns of the matrix $\psi F_5$ can be permuted in such a way that the resultant matrix consists of 9 copies of the matrix:

$$
\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 
\end{bmatrix}
$$

This is the matrix $F_2$ from Example 4. That is why applying $\pi_1$ at the next round will not lead to new dependencies. So we set $\pi_5 = \pi_2 \pi_1 \psi$, $\pi_6 = \pi_3$ and $\pi_7 = \pi_4$.

3.4. ADDITIVE CONSTRUCTIONS. Construction 1 (the double construction) can be used to find a permutation sequence for $k$ subblocks from a permutation sequence for $k/2$ subblocks if $k$ is divisible by 4. The following additive constructions are similar to it, but they can be used if $k$ is not divisible by 4.

Let $k = k_a + k_b$, where $k_b = k_a + 2$. Suppose that there exist two permutation sequences:

- $\alpha_1, \alpha_2, \ldots, \alpha_{r_a}$ for $k_a$ subblocks with diffusion round $R_a = r_a + 1$
- $\beta_1, \beta_2, \ldots, \beta_{r_b}$ for $k_b$ subblocks with diffusion round $R_b = r_b + 1$.

We define a permutation sequence $\pi_1, \pi_2, \ldots, \pi_{R_a - 1}$ for $k_a + k_b$ subblocks in the following way:

1. At round $r \leq \min(r_a, r_b)$: We apply $\alpha_r$ to the first $k_a$ subblocks and $\beta_r$ to the remaining $k_b$ subblocks.

At the next (usually 3 or 4) rounds: The permutations are different for the different additive constructions we use.

3.4.1. Construction 3. At the next rounds:

2. If $r_a \neq r_b$ then at round $r > \min(r_a, r_b)$ and $r \leq \max(r_a, r_b)$:

   If $r_a < r_b$ we do not permute the first $k_a$ subblocks and apply $\beta_r$ to the remaining $k_b$ subblocks.
If \( r_a > r_b \) we apply \( \alpha_r \) to the first \( k_a \) subblocks and do not permute the remaining \( k_b \) subblocks.

3. At round \( r = \max(r_a, r_b) + 1 \): the odd subblocks do not move, while each even subblock \( j < k_b \) interchanges with the even subblock \( j + k_a \):

\[
\pi_{\max(r_a, r_b) + 1} = (1)(2, k_a + 2)(3)(4, k_a + 4) \ldots (k_a - 1)(k_a, k - 2)(k_a + 1)(k_a + 3)(k_a + 5) \ldots (k - 1).
\]

4. At round \( r = \max(r_a, r_b) + 2 \) we apply a cyclic shift:

\[
\pi_{\max(r_a, r_b) + 2} = (1, 2, \ldots, k - 1, k).
\]

5. At round \( r = \max(r_a, r_b) + 3 \): \( \pi_{\max(r_a, r_b) + 3} = (1, 2, 3, 4) \ldots (k - 1, k) \).

The result is a permutation sequence with diffusion round \( \max(R_a, R_b) + 3 \) (proved in Theorem 3.3).

Example 9. Construction 3 for \( k = k_a + k_b = 12 + 14 = 26 \) subblocks

A permutation sequence for 26 subblocks and diffusion round 10 is obtained from two sequences for 12 and 14 subblocks respectively, and both with diffusion round 7. The permutations of the two sequences are applied at the first six rounds, and the remaining 3 permutations are: \( \pi_7 = (1)(2, 14)(3)(4, 16) \ldots (11)(12, 24)(13)(15)(26) \), \( \pi_8 = (1, 2, \ldots, 26) \), \( \pi_9 = (1, 2)(3, 4) \ldots (25, 26) \).

Theorem 3.3. If there exists a permutation sequence \( \alpha_1, \alpha_2, \ldots, \alpha_{r_a} \) for \( k_a \) subblocks with diffusion round \( R_a = r_a + 1 \), and a permutation sequence \( \beta_1, \beta_2, \ldots, \beta_{r_b} \) for \( R_b = r_b + 1 \), then there exists a permutation sequence \( \pi_1, \pi_2, \ldots, \pi_{R-1} \) for \( k_a + k_b \) subblocks with diffusion round \( R = \max(R_a, R_b) + 3 \).

Proof. We will show that Construction 3 yields a permutation sequence for IGFS with diffusion round \( \max(R_a, R_b) + 3 \). At the first \( r_a \) rounds the subblocks are partitioned in two groups (first group: 1, 2, \ldots, \( k_a \) and second group: \( k_a + 1 \), \( k_a + 2 \), \ldots, \( k_a + k_b \)) and the permutations move blocks within their group. Therefore after the first \( \max(r_a, r_b) \) rounds the 1-s in the dependence matrix are grouped in two all-one submatrices (along the main diagonal) of dimensions \( k_a \times k_a \) and \( k_b \times k_b \) respectively (one can see, for instance, the available online file with dependence matrices for 26 subblocks).

By permutation \( \pi_{\max(r_a, r_b) + 1} \) each of the even subblocks, except the last one, moves next to an odd subblock of the other group. The even subblock in each Feistel pair, except the last pair, depends now on all elements on which the odd subblock does not, and vice versa. After the next Feistel transformation all even blocks, except the last one, contain only 1-s. The last odd subblock becomes first after the next cyclic shift. Now the odd subblock of the first Feistel pair depends on all elements on which the even subblock does not, while the odd subblocks of the other pairs contain only 1s. One more round is needed to share dependencies within the first Feistel pair. This way the all-one matrix is obtained after round \( \max(R_a, R_b) + 3 \), which is the encryption diffusion round.

The first three decryption rounds lead to dependence matrix \( \Gamma_4 \) which consists of two submatrices \( \Gamma_{4a} \) and \( \Gamma_{4b} \) of dimensions \( k_a \times (k_a + k_b) \) and \( k_b \times (k_a + k_b) \) respectively, and each of these submatrices has at least one 1 in each row and column. That is why the application of \( \alpha_{r_a}^{-1}, \alpha_{r_a}^{-1}, \ldots, \alpha_{r_a}^{-1} \) on the first \( k_a \) subblocks and \( \beta_{r_b}^{-1}, \beta_{r_b}^{-1}, \ldots, \beta_{r_b}^{-1} \) on the remaining \( k_b \) subblocks, turns \( \Gamma_{4a} \) and \( \Gamma_{4b} \) to all-one matrices. Therefore the decryption diffusion round is \( \max(R_a, R_b) + 3 \).
For some values of $k$ the following three additive constructions lead to permutation sequences with diffusion round $\max(R_a, R_b) + 2$, i.e. one round better than Construction 3. Constructions 4, 5 and 6, however, do not work for each even $k$.

3.4.2. **Construction 4.** It is a modification of Construction 3 leading to a permutation sequence with diffusion round $\max(R_a, R_b) + 2$ if $r_a < r_b$.

2. **At round** $r > r_a$ and $r < r_b$: we do not permute the first $k_a$ subblocks and apply $\beta_r$ to the remaining $k_b$ subblocks.

3. **At round** $r = r_b$ the odd subblocks do not move, while each even subblock $j < k_b$ interchanges with the even subblock $j + k_a$:

$$\pi_{r_b} = (1)(2, k_a + 2)(3, k_a + 4) \ldots (k_a - 1)(k_a, k - 2)(k_a + 1)(k_a + 3)(k_a + 5) \ldots (k - 1)k_a.$$  

4. **At round** $r = r_b + 1$ a cyclic shift is applied: $\pi_{r_b + 1} = (1, 2, \ldots, k - 1, k)$.

5. **At round** $r = r_b + 2$: $\pi_{r_b + 2} = (1, 2)(3, 4) \ldots (k - 1, k)$.

**Example 10. Construction 4 for** $k = k_a + k_b = 16 + 18 = 34$ **subblocks**

A permutation sequence for 34 subblocks and diffusion round 10 is constructed from two sequences for 16 and 18 subblocks, and with diffusion rounds 7 and 8 respectively. The permutations of the two sequences are applied at the first six rounds, and the remaining three permutations are:

$$\pi_7 = (1)(2, 18)(3)(4, 20) \ldots (15)(16, 32)(17)(19) \ldots (31)(33)(34), \pi_8 = (1, 2, \ldots, 34), \pi_9 = (1, 2)(3, 4) \ldots (33, 34).$$

3.4.3. **Construction 5.** Similarly to Construction 4 we suppose $r_a < r_b$.

2. **At round** $r > r_a$ and $r < r_b$: we do not permute the first $k_a$ subblocks and apply $\beta_r$ to the remaining $k_b$ subblocks.

3. **At round** $r = r_b$: $k - 1$ and $k$ change places, the odd subblocks which are smaller than $k - 1$ do not move, while each even subblock $j < k_b$ interchanges with the even subblock $j + k_a$:

$$\pi_{r_b} = (1)(2, k_a + 2)(3, k_a + 4) \ldots (k_a - 1)(k_a, k - 2)(k_a + 1)(k_a + 3) \ldots (k - 3)(k - 1, k).$$

4. **At round** $r = r_b + 1$ a cyclic shift is applied: $\pi_{r_b + 1} = (1, 2, \ldots, k - 1, k)$.

5. **At round** $r = r_b + 2$:

$$\pi_{r_b + 2} = (1, 2)(2, k_a + 1)(3, k_a + 3)(5) \ldots (k_a - 1)(k_a, k - 3)(k_b, k - 1)(k_b + 2)(k_b + 4) \ldots (k - 2).$$

**Example 11. Construction 5 for** $k = k_a + k_b = 10 + 12 = 22$ **subblocks**

A permutation sequence for 22 subblocks and diffusion round 9 is constructed from two sequences for 10 and 12 subblocks, and with diffusion rounds 6 and 7 respectively. The permutations of the two sequences are applied at the first five rounds. The remaining permutations are:

$$\pi_6 = (1)(2, 12)(3)(4, 14)(5)(6, 16)(7)(8, 18)(9)(10, 20) (11)(13)(15)(17)(19)(21, 22), \pi_7 = (1, 2, \ldots, 22),$$

$$\pi_8 = (1, 22)(2, 11)(3)(4, 13)(5)(6, 15)(7)(8, 17)(9)(10, 19)(12, 21)(14)(16)(18)(20).$$

3.4.4. **Construction 6.** We suppose $r_a > r_b$.

2. **At round** $r > r_b$ and $r < r_a$: we apply $\alpha_r$ to the the first $k_a$ subblocks and do not permute the remaining $k_b$ subblocks.

3. **At round** $r = r_a$:

$$\pi_{r_a} = (1, k_a + 1, k, k_a, k_a - 2, k_a - 4, \ldots, 2, k - 1, k_a - 1, k - 3, k_a - 3, k - 2, k_a - 5, \ldots k - (k_a - 3), 3, k - (k_a - 1))(k_b, k_b + 2, \ldots, k - 2).$$

4. **At round** $r = r_a + 1$ we apply a cyclic shift: $\pi_{r_a + 1} = (1, 2, \ldots, k - 1, k)$. 
5. At round $r = r_a + 2$: $\pi_{r_a+2} = (1)(2,k-1)(3)(4,k_b+1)(5)(6,k_b+3)\ldots(k_a-1)(k_a,2k_a-1)(k_a+1,k)(k_b,k_b+2,k_b+4\ldots k-2)$.

**Example 12. Construction 5 for $k = k_a + k_b = 46 + 48 = 94$ subblocks**

A permutation sequence for 94 subblocks and diffusion round 14 is constructed from two sequences for 46 and 48 subblocks, and with diffusion rounds 12 and 10 respectively. The permutations of the two sequences are applied at the first ten rounds, and the remaining three permutations are:

- $\pi_{11} = (1,47,94,46,44,\ldots,2,93,45,91,43,\ldots,51,3,49)$ (48, 50, 52, \ldots, 92),
- $\pi_{12} = (1,2,3,\ldots,93,94),$
- $\pi_{13} = (1)(2,93)(3)(4,49)(5)(6,51)\ldots(45)(46,91)(47,94)$ (48, 50, 52, \ldots, 92).

4. Permutation sequences with the best known diffusion

We construct permutation sequences with the best known by now diffusion for all even values of $k \leq 2048$. We say that an IGFS with a definite permutation sequence has optimal diffusion if its diffusion round $R_d$ attains the lower bound $R_D$ for even-odd permutations. We found the permutation sequences with optimal diffusion for 2, 4, 6, 8, 10, 12, 14 and 16 subblocks by a computer search method presented in [1]. All the remaining permutation sequences for $18 \leq k \leq 2048$ were obtained from them by a computer-aided application of different recursive constructions. Our software processed the even values of $k$ in ascending order making use of the already found permutation sequences for smaller $k$.

A summary of the results for $k \leq 128$ is presented in Table 1. Following the notations above, the diffusion round is denoted by $R_d$, and the even-odd lower bound by $R_D$. The table shows how the corresponding dependence sequence is obtained, namely the construction number is given in column $C$ and the parameters of the ingredient sequences are presented in the $Rem$ark column. If Suzuki and Minematsu have a result for this $k$, the diffusion round obtained by them is given in column $R_{SM}$. The permutation sequences with optimal diffusion are marked by a star. We obtain 19 optimal sequences (all with $k \leq 128$) and 54 with $R_d = R_D + 1$. The sequences with $R_d = R_D + 1$ for $k > 128$ are presented in Table 2.

5. Infinite families

For $t > 2$ Suzuki and Minematsu [9] construct an infinite family of IGFS with $2^t$ subblocks and with diffusion round $2t$. Although IGFS with more than 2048 subblocks do not seem to be of practical interest, we want to note that infinite families based on some of the presented constructions can be defined for big $k$.

**Theorem 5.1.** If there exists an IGFS for $m.2^t$ subblocks with diffusion round $R$, then for each integer $t \geq s$ there exists an IGFS for $m.2^t$ subblocks with diffusion round $R + 2(t - s)$

**Proof.** The statement can be proved by induction. Suppose there exists a dependence sequence with $m.2^{t-1}$ subblocks with diffusion round $R + 2(t - 1 - s)$. By Theorem 3.1 using Construction 1 we can obtain a dependence sequence for $m.2^{t-1}2 = m.2^t$ subblocks with diffusion round $R + 2(t - 1 - s) + 2 = R + 2(t - s)$. Since there is a dependence sequence for $m.2^s$ subblocks with diffusion round $R$, the assertion is true for $t = s$, and this way the statement is proved.

**Corollary 1.** There exists an IGFS with:

- $2^t$ subblocks and diffusion round $2t - 3$ for $t \geq 10$. 

Table 1. IGFS with $k \leq 128$ subblocks

| $k$ | $R_d$ | $R_D$ | $C$ | $R_{SM}$ | $k$ | $R_d$ | $R_D$ | $C$ | $R_{SM}$ |
|-----|-------|-------|-----|---------|-----|-------|-------|-----|---------|
| * 2 | 2     | 2     | c   | -       | 2   | 66    | 12    | 10  | 2       |
| * 4 | 4     | 4     | c   | -       | 4   | 68    | 12    | 10  | 1       |
| * 6 | 5     | 5     | c   | -       | 5   | 70    | 11    | 11  | 2       |
| * 8 | 6     | 6     | c   | -       | 6   | 72    | 12    | 11  | 1       |
| * 10| 6     | 6     | c   | -       | 7   | 74    | 13    | 11  | 4       |
| * 12| 7     | 7     | c   | -       | 8   | 76    | 13    | 11  | 1       |
| * 14| 7     | 7     | c   | -       | 8   | 78    | 13    | 11  | 2       |
| * 16| 7     | 7     | c   | -       | 8   | 80    | 11    | 11  | 2       |
| * 18| 8     | 8     | 2   | 2.3.3   | -   | 82    | 13    | 11  | 3       |
| * 20| 8     | 8     | 1   | 2.10    | -   | 84    | 12    | 11  | 1       |
| 22  | 9     | 8     | 5   | 10+12   | -   | 86    | 13    | 11  | 5       |
| 24  | 9     | 8     | 1   | 2.12    | -   | 88    | 13    | 11  | 1       |
| 26  | 10    | 8     | 3   | 12+14   | -   | 90    | 11    | 11  | 2       |
| * 28| 9     | 9     | 1   | 2.14    | -   | 92    | 14    | 11  | 1       |
| * 30| 9     | 9     | 2   | 2.3.5   | -   | 94    | 14    | 11  | 6       |
| * 32| 9     | 9     | 1   | 2.16    | 10  | 96    | 12    | 11  | 1       |
| 34  | 10    | 9     | 4   | 16+18   | -   | 98    | 12    | 11  | 2       |
| 36  | 10    | 9     | 1   | 2.18    | -   | 100   | 12    | 11  | 1       |
| 38  | 11    | 9     | 3   | 18+20   | -   | 102   | 13    | 11  | 2       |
| 40  | 10    | 9     | 1   | 2.20    | -   | 104   | 14    | 11  | 1       |
| 42  | 10    | 9     | 2   | 2.3.7   | -   | 106   | 15    | 11  | 3       |
| 44  | 11    | 10    | 1   | 2.22    | -   | 108   | 13    | 11  | 1       |
| 46  | 12    | 10    | 3   | 22+24   | -   | 110   | 13    | 11  | 2       |
| * 48| 10    | 10    | 2   | 2.3.8   | -   | 112   | 12    | 12  | 2       |
| * 50| 10    | 10    | 2   | 2.5.5   | -   | 114   | 14    | 12  | 2       |
| 52  | 12    | 10    | 1   | 2.26    | -   | 116   | 14    | 12  | 1       |
| 54  | 11    | 10    | 2   | 2.3.9   | -   | 118   | 14    | 12  | 6       |
| 56  | 11    | 10    | 1   | 2.28    | -   | 120   | 13    | 12  | 1       |
| 58  | 12    | 10    | 3   | 28+30   | -   | 122   | 14    | 12  | 4       |
| 60  | 11    | 10    | 1   | 2.30    | -   | 124   | 14    | 12  | 1       |
| 62  | 12    | 10    | 3   | 30+32   | -   | 126   | 13    | 12  | 2       |
| 64  | 11    | 10    | 1   | 2.32    | 12  | 128   | 12    | 12  | 2       |

- $3.2^t$ subblocks and diffusion round $2t + 1$ for $t \geq 7$.
- $5.2^t$ subblocks and diffusion round $2t + 2$ for $t \geq 7$.
- $7.2^t$ subblocks and diffusion round $2t + 3$ for $t \geq 7$.

Proof. The statements follow from Theorem 5.1 and the existence of dependence sequences for $1024 = 2^{10}$ subblocks with diffusion round 17, for $384 = 3.2^7$ subblocks with diffusion round 15, for $640 = 5.2^7$ subblocks with diffusion round 16, and for $896 = 7.2^7$ subblocks with diffusion round 17 (Table 2). □

Theorem 5.2. If there exists an IGFS for $k$ subblocks with diffusion round $R$, then for each integer $t \geq 1$ there exists an IGFS for $k^t$ subblocks with diffusion round $R_t$.

Proof. We will prove the statement by induction. Suppose there exists a dependence sequence for $k^{t-1}$ subblocks with diffusion round $R(t-1)$. We can use this sequence and the sequence for $k$ subblocks with diffusion round $R$ with the multiple Construction. The result will be a dependence sequence for $k^{t-1}k = k^t$ subblocks.
with diffusion round \( R(t - 1) + R = R.t \) (Theorem 3.2). Since there is a dependence sequence for \( k \) subblocks with diffusion round \( R \), the assertion holds for \( t = 1 \), and the statement is proved.

All previously known results for \( k > 2048 \) come from Suzuki and Minematsu's infinite family of IGFS with \( 2^t \) subblocks with diffusion round \( 2t \). Corollary 1 shows that there exist IGFS with \( 2^t \) subblocks with diffusion round \( 2t - 3 \) for each \( t \geq 10 \). The four infinite families of permutation sequences presented in Corollary 1, are obviously not all infinite families that can be obtained by Theorem 5.1. In a similar way new infinite families can be obtained using the sequences for \( k \leq 2048 \) subblocks and Theorem 5.2.

### Table 2. IGFS with \( 128 < k \leq 2048 \) subblocks and diffusion round \( R_d = R_D + 1 \)

| \( k \) | \( R_d \) | \( R_D \) | \( C \) | \( \text{Remark} \) | \( R_{SM} \) |
|---|---|---|---|---|---|
| 140 | 13 | 12 | 1 | 2.70 | - |
| 144 | 13 | 12 | 2 | 2.3.24 | - |
| 150 | 13 | 12 | 2 | 2.3.25 | - |
| 160 | 13 | 12 | 1 | 2.80 | - |
| 180 | 14 | 13 | 1 | 2.90 | - |
| 192 | 14 | 13 | 1 | 2.96 | - |
| 196 | 14 | 13 | 1 | 2.98 | - |
| 200 | 14 | 13 | 1 | 2.100 | - |
| 210 | 14 | 13 | 2 | 2.3.35 | - |
| 224 | 14 | 13 | 1 | 2.112 | - |
| 240 | 14 | 13 | 2 | 2.3.40 | - |
| 250 | 14 | 13 | 2 | 2.5.25 | - |
| 256 | 14 | 13 | 1 | 2.128 | 16 |
| 294 | 15 | 14 | 2 | 2.3.49 | - |
| 300 | 15 | 14 | 1 | 2.150 | - |
| 320 | 15 | 14 | 1 | 2.160 | - |
| 336 | 15 | 14 | 2 | 2.3.56 | - |
| 350 | 15 | 14 | 2 | 2.5.35 | - |

6. Concluding remarks and open problems

The presented recursive constructions lead to examples of permutation sequences for IGFS with the best known diffusion for even \( k \leq 2048 \) subblocks. For \( k > 16 \) previous examples exist only if \( k \) is a power of 2. We stop at 2048 because bigger \( k \) presently seem to be of no practical importance. There is, however, no problem to go on with \( k > 2048 \), because for each even \( k \) Construction 1 can be applied if \( k \) is divisible by 4, and Construction 3 if it is not.

Suzuki and Minematsu [9] establish that for \( k \leq 16 \) and when one and the same permutation is used at all rounds, the best diffusion is achieved by even-odd permutations. The optimal permutation sequences which we construct for \( k > 16 \) contain some permutations that are not even-odd, but these sequences meet the even-odd lower bound on the diffusion round. It is an open question, however, whether sequences with permutations that might not be even-odd can lead to a diffusion round which is smaller than the even-odd lower bound.
The results we obtain show that IGFS with different permutations at the different rounds can offer effective solutions with respect to the diffusion property. The implementation cost is certainly expected to be higher than that in the one-permutation case, but the recursive way in which the sequences are constructed make them contain multiple copies of some parts of the permutations. This might be beneficial to achieve a reasonable implementation cost.

Files with the constructed permutation sequences and the corresponding to them encryption and decryption dependence matrices can be freely downloaded from http://www.moi.math.bas.bg/~svetlana/IGFeistel.htm. There is a separate file for each even $k \leq 2048$. One can find among them the files corresponding to the sequences constructed in examples 8–12 which are not fully presented here. A text file with $k_{RD}R_D$ in its name contains the dependence matrices of a sequence for $k$ subblocks with diffusion round $R_d$, where $R_D$ is the even-odd lower bound for this $k$. All the sequences can further be used by anyone who is interested in implementing them in IGFS ciphers. We have only established that their usage leads to good diffusion. Those who might want to apply some of them, should further find out how they affect other aspects of the cipher’s security, such as pseudorandomness and security against cryptanalysis.

References

[1] T. Baicheva and S. Topalova, On the diffusion property of the Improved Generalized Feistel with different permutations for each round, in Algebraic Informatics, CAI 2019 (eds. M. Ćirić, M. Droste and J.É. Pin), Lecture Notes in Computer Science, 11545 (2019), 38–49.

[2] T. Berger, M. Minier and G. Thomas, Extended generalized Feistel networks using matrix representation, Selected Areas in Cryptography–SAC 2013, Lecture Notes in Comput. Sci., Springer, Heidelberg, 8282 (2014), 289–305.

[3] T. Berger, J. Francq, M. Minier and G. Thomas, Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput, IEEE Transactions on Computers, 65 (2016), 2074–2089.

[4] 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, Lecture Notes in Computer Science - CHES, 4249 (2006), 46–59.

[5] K. Nyberg, Generalized Feistel networks, in Advances in Cryptology - ASIACRYPT '96 (eds. K. Kim and T. Matsumoto), Lecture Notes in Computer Science, 1163 (1996), 90–104.

[6] R. L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, The RC6 block cipher, August 1998. Available from: http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf.

[7] C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal, 28 (1949), 656–715.

[8] T. Shiromi, K. Shibutani, T. Akishita, S. Moriai and T. Iwata, The 128-bit block cipher CLEFIA (Extended abstract), Lecture Notes in Computer Science–FSE, 4593 (2007), 181–195.

[9] T. Suzuki and K. Minematsu, Improving the generalized Feistel, Lecture Notes in Computer Science–FSE, 6147 (2010), 19–39.

[10] L. Zhang and W. Wu, Analysis of permutation choices for enhanced generalized Feistel structure with SP-type round function, IET Information Security, 11 (2017), 121–128.

[11] Y. Zheng, T. Matsumoto and H. Imai, On the construction of block ciphers provably secure and not relying on any unproved hypothesis, Advances in Cryptology - CRYPTO'89, Lecture Notes in Computer Science, 435 (1990), 461–480.

[12] Y. Wang and W. Wu, New criterion for diffusion property and applications to improved GFS and EGFN, Designs Codes and Cryptography, 81 (2016), 393–412.

Received October 2019; revised February 2020.

E-mail address: tsonka@math.bas.bg
E-mail address: svetlana@math.bas.bg