Extended Generalized Feistel Networks Using Matrix Representation

Thierry P. Berger[1], Marine Minier[2], and Gaël Thomas[1](✉)

[1] XLIM (UMR CNRS 7252), Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, France
{thierry.berger,gael.thomas}@unilim.fr
[2] CITI, INSA-Lyon, INRIA, Université de Lyon, F-69621 Villeurbanne, France
marine.minier@insa-lyon.fr

Abstract. While Generalized Feistel Networks have been widely studied in the literature as a building block of a block cipher, we propose in this paper a unified vision to easily represent them through a matrix representation. We then propose a new class of such schemes called Extended Generalized Feistel Networks well suited for cryptographic applications. We instantiate those proposals into two particular constructions and we finally analyze their security.

Keywords: Generalized feistel networks · Matrix representation · Scheme proposal · Security analysis

Introduction

While a classical Feistel network, such as DES [23] or Camellia [2], divides a plaintext into 2 n-bit-long halves, a Generalized Feistel Network (GFN) divides it into $k \geq 2$ n-bit-long subblocks. Various GFNs exist in the literature. This includes Source-Heavy (SH) as in RC2 [25] and SHA-1 [29]; Target-Heavy (TH) as in MARS [7]; Type-1 as in CAST-256 [1] and Lesamnta [11]; Type-2 as in RC6 [26], HIGHT [13] and CLEFIA [28]; Type-3 and Nyberg's GFNs [24]. Pseudo-randomness of these constructions is studied in [12,21,33] for Type-1, Type-2 and Type-3, in [12,22] for SH GFN and [12,21] for TH GFN. Figure 1 gives an example of Type-3 GFN. Usually GFNs perform a block-wise cyclic shift in their permutation layer.

In [30], Suzaki and Minematsu proposed to use a non-cyclic permutation instead and applied it to Type-2 GFNs. More precisely, they studied the maximum diffusion round. Roughly speaking, it is the minimum number of rounds such as every output block depends on every input block. They exhaustively searched all the optimum permutations for $k \leq 16$ and found that the diffusion in Type-2 GFNs can be improved. They also showed a lower bound on the

This work was partially supported by the French National Agency of Research: ANR-11-INS-011.

T. Lange, K. Lauter, and P. Lisoněk (Eds.): SAC 2013, LNCS 8282, pp. 289–305, 2014.
DOI: 10.1007/978-3-662-43414-7_15,

maximum diffusion round of Type-2 GFNs and when k is a power of 2, they gave a generic construction based on de Bruijn graphs whose maximum diffusion round is close to the lower bound they found. Besides, they studied the pseudorandomness of these GFNs and their resistance against classical attacks and showed that it is actually improved as well. One of these Type-2 GFNs is used in TWINE [31].

Following the work of [30], Yanagihara and Iwata [32] studied the case of Type-1, Type-3, SH and TH GFNs with non-cyclic permutation. For Type-1 and Type-3 GFNs, they showed that the maximum diffusion round can be improved by changing the permutation while for SH and TH GFNs it cannot. Besides, for Type-1 GFNs, they gave an optimum generic construction for any k and identified a necessary and sufficient condition for improved Type-3 to have a finite maximum diffusion round. They also evaluated the resistance of all those GFNs against classical attacks and showed that it can be improved in the Type-1 and Type-3 cases.

In this paper, we first investigate a unified vision of GFNs using a matrix representation and use it to further study the diffusion properties of GFNs. We then extend this matrix representation and propose a broader class of Feistel networks that we call Extended Generalized Feistel Networks (EGFNs). We finally propose one particular EGFN with good diffusion properties and study the security of this proposal.

This paper is organized as follows: Sect. 1 gives the matrix representation of a GFN, its link with diffusion and shows how each possible GFN could be represented using a particular matrix. Section 2 extends GFNs into EGFNs and contains a particular EGFN proposal with good diffusion properties. In Sect. 3 we present a complete security analysis concerning this proposal.

1 Matrix Representation of Feistel Networks

Before defining the matrix representation of a GFN, let us introduce a few notations.

1.1 Definitions and Notations

A GFN divides its input into $k \geq 2$ blocks of n bits each. Let $x_0, \cdots, x_{k-1}$ denote the input blocks of a GFN round and $y_0, \cdots, y_{k-1}$ the corresponding output blocks. A GFN can be separated into two successive layers, as done in [30,32]: a round-function layer and a permutation layer, as on Fig. 1. The round-function layer is made of key-dependent functions whose inputs are some of the blocks and whose outputs are added (x-ored) to some other blocks. The permutation layer is a block-wise permutation of the k blocks. How the different round-functions are arranged depends on the type of GFN considered, while the permutation is usually the cyclic shift. We further denote by y_i^r the content of the i-th block after r rounds.

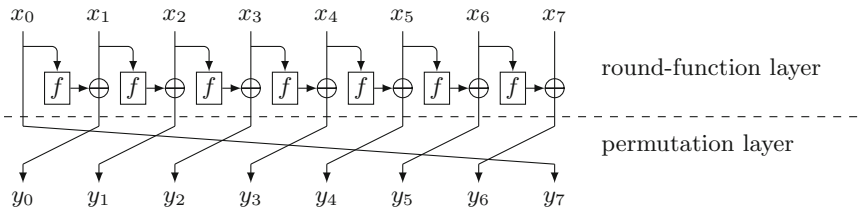


Fig. 1. One round of a Type-3 GFN with $k = 8$ blocks.

1.2 Diffusion Delay

We say input block x_i affects output block y_j^r if x_i effectively appears in the expression of y_j^r seen as a function of $x_0, \cdots, x_{k-1}$. We say x_i has diffused at round r if x_i affects every y_j^r for $0 \leq j \leq k-1$. If every input block x_i has diffused at round r, we say the GFN has reached full diffusion, that is every output block y_j^r depends on every input block x_i. We call full diffusion delay the minimum number of rounds required to reach full diffusion and denote it d^+. In fact, the notion of full diffusion delay is a general notion that can be applied to any automaton as done in [3]. In the particular case of GFNs, this is exactly the same notion as the maximum diffusion round introduced in [30].

Another way to see the full diffusion delay is from a graph point of view. For a k-block GFN, let us define the associated directed graph as the graph with vertex set $\{0, \cdots, k-1\}$ and such that (i, j) is an edge if the output y_j depends on the input x_i (directly or via a round-function). In other words, this is simply the usual Feistel schemes with outputs folded onto the input with same index. Knowing that, it is easy to see that the notion of *block* x_i *affecting block* y_j^r becomes *there exists a path of length exactly* r *going from* i *to* j. Thus the full diffusion delay d^+ can be alternately defined as the smallest integer r such that for all ordered pair of vertices (i, j) there exists a path of length exactly r going from i to j. Two things should now be noticed. First, if a GFN is in a full diffusion state at round r then it will remain so at round $r + 1$. Second, the full diffusion delay of a GFN depends solely on the structure of this graph and not on the round-functions used in the GFN.

Similarly, we can define full diffusion delay when considering decryption instead of encryption and denote it d^-. Following the work of [30], we consider the both-way full diffusion delay $d = \max(d^+, d^-)$. The both-way full diffusion delay d for the different classical GFNs is summed up in Table 1. For security reasons, it is necessary that d be finite.

1.3 Matrix Representation of Feistel Networks

Recall that a GFN is divided into two distinct transformations: first, the round-function layer and second, the permutation layer, represented by a permutation matrix $\mathcal{P}$. We call matrix representation of the round-function layer, the matrix denoted $\mathcal{F}$ with an all-one diagonal and with a parameter we call F at position

Table 1. Both-way full diffusion delay d for various GFNs with k blocks.

GFN Type	SH	TH	Type-1	Type-2	Type-3	Nyberg [32] Type-1	[30] Type-2
d	k	k	$(k-1)^2+1$	k	k	$k(k+2)/2-2$	$2\log_2 k$

(i, j) if and only if there is a round-function going from x_j to x_i. The parameter F is a formal parameter, meaning it merely indicates the presence of a round-function in the GFN, the same F is used for all the different round-functions used throughout the cipher. If one follows the matrix representation idea, one would define the matrix of the whole GFN as $\mathcal{M} = \mathcal{P} \times \mathcal{F}$.

In other words, for a GFN with k blocks, let $\mathcal{M}$ be the $k \times k$ matrix over $\mathbb{Z}[F]$ defined as follows: for indices $0 \leq i, j \leq k-1$, coefficient at row i and column j of $\mathcal{M}$ is either a 1 if output y_i directly depends on x_j, that is without going through a round-function, or a formal parameter F, if y_i depends on x_j via a round-function, or 0 otherwise. This corresponds to the definition of Encryption Characteristic Matrix given in [14]. E.g. Fig. 2 gives the matrices $\mathcal{M}$, $\mathcal{P}$ and $\mathcal{F}$ of the GFN on Fig. 1.

$$\mathcal{M} = \begin{pmatrix} F & 1 & & & & & & \\ & F & 1 & & & & & \\ & & F & 1 & & & & \\ & & & F & 1 & & & \\ & & & & F & 1 & & \\ & & & & & F & 1 & \\ & & & & & & F & 1 \\ 1 & & & & & & & \end{pmatrix} \quad \mathcal{P} = \begin{pmatrix} & & & & & & & 1 \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & & & 1 & & & \\ & & & 1 & & & & \\ & & 1 & & & & & \\ & 1 & & & & & & \\ 1 & & & & & & & \end{pmatrix} \quad \mathcal{F} = \begin{pmatrix} 1 & & & & & & & \\ F & 1 & & & & & & \\ & F & 1 & & & & & \\ & & F & 1 & & & & \\ & & & F & 1 & & & \\ & & & & F & 1 & & \\ & & & & & F & 1 & \\ & & & & & & F & 1 \end{pmatrix}$$

Fig. 2. Decomposition of the transition matrix of the Type-2 GFN given on Fig. 1

As round-functions in a GFN are unlikely to be linear, such a matrix is not an exact representation. However it still retains enough information to evaluate diffusion; namely which output block y_i is influenced by which input block x_j and whether this done directly or via a round-function.

An important feature of GFNs is to transform a set of non-invertible round-functions into an invertible permutation. Hence the matrix of the GFN in decryption mode $\mathcal{M}^{-1}$ should not contain inverses of expressions containing a F. This translates into $\det(\mathcal{M})$ is independent of F, or equivalently $\det(\mathcal{F}) = \pm 1$, as $\mathcal{P}$ is a permutation matrix. This is the case for all of the classical GFNs (SH, TH,...) including those of [30,32] because the matrix $\mathcal{F}$ is lower triangular with an all-one diagonal.

An other feature of many GFNs is quasi-involutiveness, that is encryption/decryption is roughly the same process, up to using the direct/inverse permutation layer $\mathcal{P}$. To ensure that, one asks that the round-function layer be

quasi-involutive. Except the Type-3 GFNs where the round-functions must be evaluated sequentially, all GFNs round-function layers are quasi-involutive. We choose to focus on GFNs that satisfy this property:

Definition 1. *A matrix $\mathcal{M}$ with coefficients in $\{0, 1, F\} \subset \mathbb{Z}[F]$ is a GFN matrix if it can be written as $\mathcal{M} = \mathcal{P}\mathcal{F}$ such that $\mathcal{P}$ is a permutation matrix and the matrix $\mathcal{F}$ satisfies the following conditions:*

1. *the main diagonal is filled with 1,*
2. *the off-diagonal coefficients are either 0 or F,*
3. *for each index i, row i and column i cannot both have an F coefficient.*

In other words, the blocks of the GFN can be partitioned into three categories: blocks that emit (through a round-function), blocks that receive and blocks that do not emit nor receive. This definition encompasses most of the known GFNs, with the exception of the Type-3. The property of quasi-involutiveness comes from the following theorem.

Theorem 1. *Let $\mathcal{M} = \mathcal{P}\mathcal{F}$ be a GFN according to Definition 1. Then $\mathcal{F}$ is invertible and $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$, where $\mathcal{I}$ stands for the identity matrix.*

Proof. To prove $\mathcal{F}$ is invertible, we compute $\det(\mathcal{F})$. Because of Condition 3 of Definition 1, for each index i either row i or column i is all-zero except for the diagonal coefficient. Thus by successively expanding the determinant along either row i or column i, $\det(\mathcal{F}) = 1$.

To prove $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$, we equivalently prove $(\mathcal{F} - \mathcal{I})^2 = 0$. Let $f_{i,j}$ (resp. $f'_{i,j}$) denote the coefficient of $\mathcal{F} - \mathcal{I}$ (resp. $(\mathcal{F} - \mathcal{I})^2$) at row i and column j. By definition of the matrix product, for all i and j, we have $f'_{i,j} = f_{i,i}f_{i,j} + f_{i,j}f_{j,j} + \sum_{\substack{\ell \neq i \\ \ell \neq j}} f_{i,\ell}f_{\ell,j} = \sum_{\substack{\ell \neq i \\ \ell \neq j}} f_{i,\ell}f_{\ell,j}$. In the sum, consider one term $f_{i,\ell}f_{\ell,j}$. As $\ell \neq i$, $f_{i,\ell}$ can either be zero or F. But, if $f_{i,\ell}$ is non-zero then the ℓ-th column of $\mathcal{F}$ contains an F thus, by Condition 3 the ℓ-th row must not contain any F, implying $f_{\ell,j} = 0$ for all $j \neq \ell$. Thus, each term $f_{i,\ell}f_{\ell,j}$ is zero, so $f'_{i,j} = 0$. □

Notice that in the case where the outputs of round-functions are xored with other blocks, then matrix $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$ is simply $\mathcal{F}$ itself. Besides, we can characterize the matrices $\mathcal{F}$ for which $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$ holds.

Theorem 2. *Let $\mathcal{F}$ be a matrix that verifies Conditions 1 and 2 of Definition 1. If $(\mathcal{F} - \mathcal{I})^2 = 0$ then $\mathcal{F}$ also verifies Condition 3.*

Proof. Let $f_{i,j}$ be the coefficient of $\mathcal{F} - \mathcal{I}$ at row i and column j. For all i and j, we have $0 = \sum_{\ell=0}^{k-1} f_{i,\ell}f_{\ell,j} = \sum_{\ell \neq i,j} f_{i,\ell}f_{\ell,j}$. All the coefficients $f_{i,\ell}$ and $f_{\ell,j}$ in the previous equation are off-diagonal, thus are either F or 0. Hence the sum can be zero only if all its terms are zero. For each index ℓ, we need to prove that row ℓ and column ℓ cannot both have an F coefficient. Suppose column ℓ has an F coefficient, say $f_{i,\ell}$ with $i \neq \ell$. This implies that for all $j \neq \ell$, $f_{\ell,j} = 0$. Thus row ℓ has no F coefficient. By transposing, the same goes when considering rows instead of columns. □

In other words, the GFNs round-function layer matrices $\mathcal{F}$ which are quasi-involutive are exactly those where Condition 3 of Definition 1 holds.

Recall that the full diffusion delay can be expressed in term of distance in a directed graph. In fact, if one evaluates the matrix $\mathcal{M}$ of the GFN in $F = 1$, we obtain the adjacency matrix of this graph. The full diffusion delay d^+ is then the smallest integer such that $\mathcal{M}^{d^+}$ has no zero coefficient. The same goes for the decryption full diffusion delay d^-, using $\mathcal{M}^{-d^-}$.

1.4 Matrix Equivalences

Now that we have matrices representing GFNs, we define an equivalence relations on them that will help us to find GFNs.

Definition 2. *Two GFNs matrices $\mathcal{M}$ and $\mathcal{M}'$ are equivalent if there exists a permutation (matrix) π of the k blocks such that $\pi\mathcal{M}\pi^{-1} = \mathcal{M}'$.*

In other words, two GFNs are equivalent if they are the same up to block reindexation and thus share the same properties, such as a common full diffusion delay. We then have the property of "equivalent decompositions":

Theorem 3. *Let $\mathcal{M} = \mathcal{P}\mathcal{F}$ and $\mathcal{M}' = \mathcal{P}'\mathcal{F}'$ be two GFNs according to Definition 1 and equivalent under Definition 2. Let also be π such that $\pi\mathcal{M}\pi^{-1} = \mathcal{M}'$. Then $\pi\mathcal{P}\pi^{-1} = \mathcal{P}'$ and $\pi\mathcal{F}\pi^{-1} = \mathcal{F}'$.*

Proof. By hypothesis, we have $\pi\mathcal{P}\mathcal{F}\pi^{-1} = \mathcal{P}'\mathcal{F}'$. Also by definition, $\mathcal{F}$ and $\mathcal{F}'$ have an all-one diagonal and either F or zero elsewhere. Hence $\mathcal{F}$ and $\mathcal{F}'$ both evaluate to the identity matrix $\mathcal{I}$ in $F = 0$. Thus, specifying the above equation in zero, we obtain $\pi\mathcal{P}\pi^{-1} = \mathcal{P}'$, which implies $\pi\mathcal{F}\pi^{-1} = \mathcal{F}'$. □

In other words, two GFNs are equivalent if and only if both layers are equivalent with same conjugating element. For example, if one studies a class of GFNs with a fixed $\mathcal{F}$ matrix, as done in [30,32], Theorem 3 allows to define an equivalence relation on the permutation layer.

1.5 Exhaustive Search of Feistel Networks

We investigated all the GFNs according to Definition 1 with $k = 8$ blocks up to equivalence. We consider three parameters:

- the full diffusion delay d,
- the number of round-functions per round s,
- the cost for full diffusion, i.e the total number of round-functions required for full diffusion, $c = d \times s$.

We found there is no GFN with cost $c < 24$. However, there are cases where the number of rounds d is a more important criterion than the total cost c. For each possible value of $d \leq 12$, Table 2 gives the minimum number of round-functions s required for an 8-block GFN to fully diffuse in d rounds. It also gives

Table 2. Minimum number s of functions per round required to have a full diffusion in d rounds and corresponding total cost $c = s \times d$. For each case, the number of different $\mathcal{F}$ matrices ($\#\mathcal{F}$) and the total number of GFNs ($\#\mathcal{M}$) are also given up to equivalence.

d	1,2	3	4	5	6	7	8	9	10	11	12
s	∞	16	7	6	4	4	4	3	3	3	2
c	∞	48	28	30	24	28	32	27	30	33	24
$\#\mathcal{F}$	0	1	1	8	3	13	13	1	6	6	1
$\#\mathcal{M}$	0	5	3	26	9	101	652	18	100	56	5

the number of GFNs that achieve such diffusion, splitted into the number of different $\mathcal{F}$ matrices (row $\#\mathcal{F}$) and the total number of GFNs (row $\#\mathcal{M}$), up to equivalence.

Note that among the GFNs that fully diffuse in $d = 6$, with $s = 4$ round-functions, are the Type-2 GFNs with non-cyclic permutation given in [30], which are then diffusion-optimum among the GFNs of Definition 1.

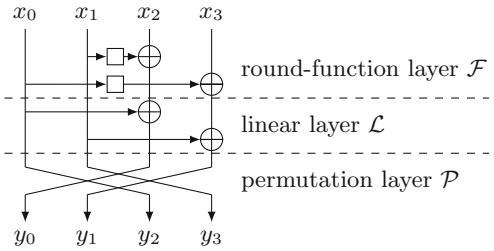
2 New Feistel Network Proposals

2.1 Extended Generalized Feistel Networks

For a GFN $\mathcal{M} = \mathcal{P}\mathcal{F}$, to achieve quicker diffusion, one can increase the number of round-functions in $\mathcal{F}$. However, this also makes costlier GFNs. The other possibility is to look at the permutation layer $\mathcal{P}$. Definition 1 already allows for block-wise permutations. A possible generalization is to use a linear mapping instead, thus looking for GFNs $\mathcal{M} = \mathcal{G}\mathcal{F}$ with $\mathcal{G}$ an invertible $k \times k$ matrix. This is however much costlier than a simple block-wise permutation and besides it loses the quasi-involutive property. What we propose is to have a $\mathcal{G}$ which is itself a GFN but with the identity mapping as round-functions. In other words, we write $\mathcal{G} = \mathcal{P}\mathcal{L}$ where $\mathcal{P}$ is a permutation matrix and $\mathcal{L}$ is matrix similar to $\mathcal{F}$ but with I off-diagonal non-zero coefficients instead of F. We call this matrix $\mathcal{L}$ the linear layer. In that case, the whole Feistel network matrix becomes $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$, e.g. Fig. 3. Because matrices $\mathcal{L}$ and $\mathcal{F}$ have common structure, we regroup them into a single matrix $\mathcal{N} = \mathcal{L}\mathcal{F}$, and write $\mathcal{M} = \mathcal{P}\mathcal{N}$. The matrix $\mathcal{N}$ is the new round-function part of the Feistel network but now has two formal parameters: F for non-linear round-functions to provide cryptographic security and I for identity round-functions to provide quick diffusion. We call these new schemes Extended Generalized Feistel Networks (EGFNs).

As done in Sect. 1.3 for GFNs, to be considered an EGFN we require that matrix $\mathcal{M} = \mathcal{P}\mathcal{N}$ is invertible and that $\det(\mathcal{M})$ does not depend on F nor I, which translates into $\det(\mathcal{N}) = \pm 1$. Again, we choose to focus on EGFNs that are quasi-involutive. Hence the following definition.

Definition 3. *A matrix $\mathcal{M}$ with coefficients in $\{0, 1, F, I\} \subset \mathbb{Z}[F, I]$ is an Extended Generalized Feistel Network (EGFN) matrix if it can be written as*



$$\mathcal{M} = \begin{pmatrix} I & F & 1 & \\ F & I & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \quad \mathcal{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

$$\mathcal{L} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ I & & 1 & \\ & I & & 1 \end{pmatrix} \quad \mathcal{F} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & F & 1 \\ F & & & \end{pmatrix}$$

Fig. 3. Overview of an EGFN three layers and corresponding matrices (right).

$\mathcal{M} = \mathcal{P}\mathcal{N}$ such that $\mathcal{P}$ is a permutation matrix and the matrix $\mathcal{N}$ satisfies the following conditions:

1. *the main diagonal is filled with* 1,
2. *the off-diagonal coefficients are either* 0, F *or* I,
3. *for each index i, row i and column i cannot both contain a non-zero coefficient other than on the diagonal,*
4. *for each index i, if row i contains an I then it also contains an F.*

As in Sect. 1.3, Condition 3 allows to partition the blocks into emitters and receivers. Condition 4 ensures that the pseudorandomness evaluation of EGFNs can be computed (see Sect. 3.1). Because Definition 3 is essentially the same as Definition 1, the following theorem on quasi-involutiveness is straightforward.

Theorem 4. *Let $\mathcal{M} = \mathcal{P}\mathcal{N}$ be an EGFN according to Definition 3. Then* $\det(\mathcal{N}) = 1$ *and* $\mathcal{N}^{-1} = 2\mathcal{I} - \mathcal{N}$.

Proof. Same as Theorem 1, since Conditions 1, 2 and 3 of Definition 3 are essentially the same as in Definition 1. □

Besides, define matrices $\mathcal{L}$ and $\mathcal{F}$ for the EGFNs of Definition 3.

Definition 4. *Let $\mathcal{M} = \mathcal{P}\mathcal{N}$ be a EGFN according to Definition 3. Then define matrix $\mathcal{F} \in \mathbb{Z}[F]$ as the evaluation of $\mathcal{N}$ in $I = 0$ and similarly matrix $\mathcal{L} \in \mathbb{Z}[I]$ as the evaluation of $\mathcal{N}$ in $F = 0$.*

Theorem 5 verifies this definition works as intended, that is $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$.

Theorem 5. *Let $\mathcal{N}$, $\mathcal{F}$ and $\mathcal{L}$ be defined as in Definition 4, then $\mathcal{N} = \mathcal{L} + \mathcal{F} - \mathcal{I}$ and $\mathcal{N} = \mathcal{L} \times \mathcal{F} = \mathcal{F} \times \mathcal{L}$.*

Proof. The first equation is a straightforward consequence of the definition of $\mathcal{N}$, $\mathcal{L}$ and $\mathcal{F}$. As for the second, let $a_{i,j}$ be the coefficient at row i and column j of matrix $\mathcal{L}\mathcal{F}$ and show that $a_{i,i} = 1$ and $a_{i,j} = \mathcal{L}_{i,j} + \mathcal{F}_{i,j}$ otherwise (with obvious notations). Write $a_{i,i} = \mathcal{L}_{i,i}\mathcal{F}_{i,i} + \sum_{\ell \neq i} \mathcal{L}_{i,\ell}\mathcal{F}_{\ell,i}$. Then $a_{i,i} = \mathcal{L}_{i,i}\mathcal{F}_{i,i} = 1$ because all terms in the rightmost sum are 0 as a consequence of Condition 3 of Definition 3. For the same reason, if $i \neq j$, $a_{i,j} = \mathcal{L}_{i,i}\mathcal{F}_{i,j} + \mathcal{L}_{i,j}\mathcal{F}_{j,j} + \sum_{\substack{\ell \neq i \\ \ell \neq j}} \mathcal{L}_{i,\ell}\mathcal{F}_{\ell,j}$ and then $a_{i,j} = \mathcal{L}_{i,j} + \mathcal{F}_{i,j}$. □

Finally, the last thing to update to EGFNs is the equivalence relation. The definition of two equivalent EGFNs $\mathcal{M}$ and $\mathcal{M}'$ is the same as for GFNs, the only difference being that $\mathcal{M}$ and $\mathcal{M}'$ now also have I coefficients. In other words, a conjugating element π of $\mathcal{M}$ and $\mathcal{M}'$ exchanges the positions of F's, as well as the positions of I's but it cannot exchange an F and an I. The analogous of Theorem 3 is straightforward.

Theorem 6. *Let $\mathcal{M} = \mathcal{PLF}$ and $\mathcal{M}' = \mathcal{P}'\mathcal{L}'\mathcal{F}'$ be two equivalent EGFNs defined by Definition 3. Let also π be such that $\pi\mathcal{M}\pi^{-1} = \mathcal{M}'$. Then $\pi\mathcal{P}\pi^{-1} = \mathcal{P}'$, $\pi\mathcal{L}\pi^{-1} = \mathcal{L}'$ and $\pi\mathcal{F}\pi^{-1} = \mathcal{F}'$.*

Proof. Same as Theorem 3 by evaluating I, F or both in 0. □

2.2 An Efficient Example

We give here a particular case of EGFN with good full diffusion delay and cheap cost. This EGFN with k blocks is depicted on Figs. 4 and 5. Its diffusion is issued in Theorem 7. Besides Sect. 3 studies the security of this EGFN.

$$\mathcal{M} = \begin{pmatrix}
 & & & & F & 1 & & \\
 & (0) & & F & I & & 1 & \\
 & & \iddots & & I & & & \ddots \\
 & F & & (0) & \vdots & & & 1 \\
F & I & I & \cdots & I & & & & 1 \\
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & \ddots & & & & (0) & \\
 & & & 1 & & & & \\
 & & & & 1 & & &
\end{pmatrix}$$

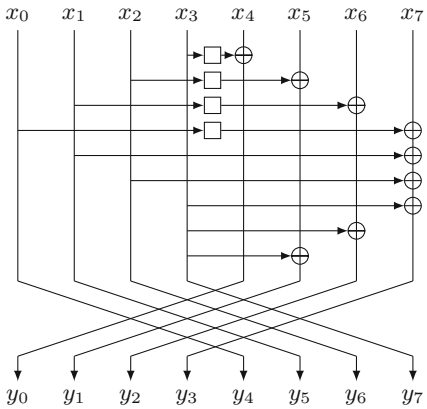


Fig. 4. EGFN matrix $\mathcal{M}$ (left) with $s = \frac{k}{2}$ round-functions with the corresponding diagram (right) that reaches full diffusion in $d = 4$ rounds.

Theorem 7. *For an even integer k, let $\mathcal{M}$ be the k-block EGFN defined on Fig. 4 and let d be its full diffusion delay. Then if $k = 2$ then $d = 2$ and if $k \geq 4$ then $d = 4$.*

Proof. Write $\mathcal{M} = \left(\begin{smallmatrix} \mathcal{A} & \mathcal{I} \\ \mathcal{I} & 0 \end{smallmatrix}\right) \in \mathbb{Z}[F, I]$ where $\mathcal{I}$ stands for the $\frac{k}{2} \times \frac{k}{2}$ identity matrix and the upper left quarter of $\mathcal{M}$ is $\mathcal{M}$ is $\mathcal{A} = \begin{pmatrix} & & & F & I \\ (0) & & F & I & \\ & \iddots & & I & \\ & & F & \vdots & \\ F & I & I & \cdots & I \end{pmatrix}$. Note

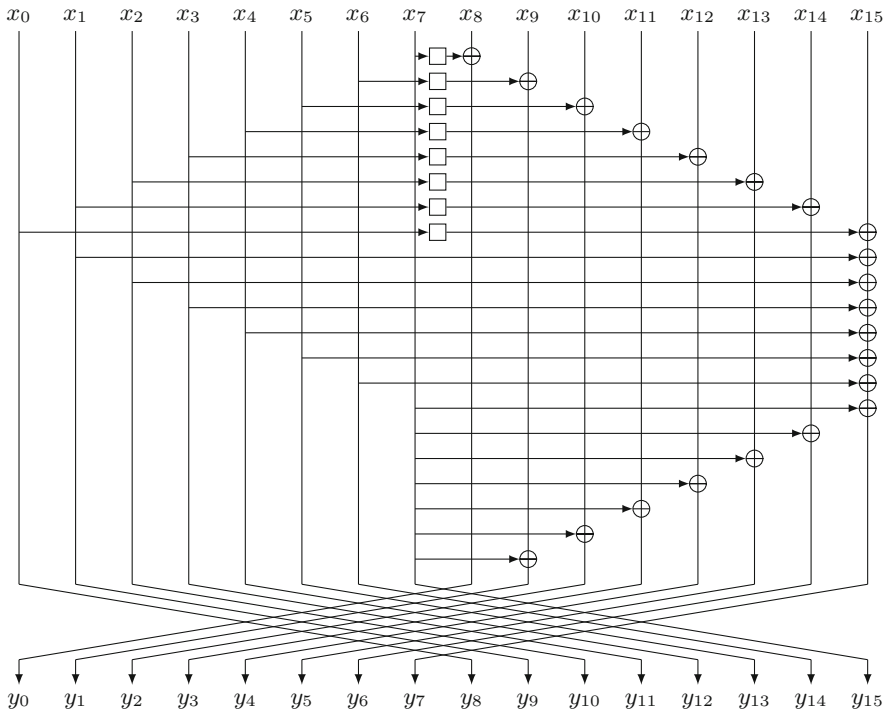


Fig. 5. EGFN with $k = 16$ blocks and $s = 8$ round-functions that reaches full diffusion in $d = 4$ rounds.

that $\mathcal{A}^2$ has no zero coefficient. Then $\mathcal{M}^2 = \begin{pmatrix} \mathcal{A}^2+\mathcal{I} & \mathcal{A} \\ \mathcal{A} & \mathcal{I} \end{pmatrix}$. If $k = 2$ then $\mathcal{M}^2$ has no zero coefficient, hence $d^+ = 2$. But if $k > 2$, it still has. Computing $\mathcal{M}^3 = \begin{pmatrix} \mathcal{A}^3+2\mathcal{A} & \mathcal{A}^2+\mathcal{I} \\ \mathcal{A}^2+\mathcal{I} & \mathcal{A} \end{pmatrix}$ shows it still has zero coefficients, as $\mathcal{A}$ does. Compute then $\mathcal{M}^4 = \begin{pmatrix} \mathcal{A}^4+3\mathcal{A}^2+\mathcal{I} & \mathcal{A}^3+2\mathcal{A} \\ \mathcal{A}^3+2\mathcal{A} & \mathcal{A}^2+\mathcal{I} \end{pmatrix}$. Thus $\mathcal{M}^4$ has no zero coefficient, hence if $k \geq 4$, $d^+ = 4$. To conclude, just note that $\mathcal{M}^{-1} = \begin{pmatrix} 0 & \mathcal{I} \\ \mathcal{I} & -\mathcal{A} \end{pmatrix}$, which implies $d^- = d^+ = d$. □

Thanks to Theorem 7, we then have a family of EGFNs with $s = \frac{k}{2}$ round-functions and a diffusion delay of $d = 4$, thus with total cost $c = 2k$. In comparison, [30] gives a family of Type-2 GFNs that diffuse in $d = 2\log_2 k$ rounds. Their total cost is then $c = k\log_2 k$. For $k > 4$, we achieve full diffusion at a cheaper cost than they do.

3 Security Analysis of Our Proposed Feistel Scheme

As done in [30], we analyze the proposed scheme with essentially $k = 8$ and $k = 16$ as parameters regarding first the pseudorandomness of the scheme and second its resistance to classical attacks.

3.1 Pseudorandomness

As we have defined a new block cipher structure, it is legitimate to introduce the pseudo-random-permutation advantage (prp-advantage) and the strong-pseudo-random-permutation advantage (sprp-advantage) of an adversary as done in several works such as [10,16,21]. For this purpose, we introduce the two advantage notations as:

$$\mathrm{Adv}_{\mathsf{C}}^{\mathsf{prp}}(q) =_{\mathrm{def}} \max_{\mathsf{A}:q\text{-}\mathsf{CPA}} \left|\Pr[\mathsf{A}^{\mathsf{C}} = 1] - \Pr[\mathsf{A}^{\mathsf{P}_n} = 1]\right| \tag{1}$$

$$\mathrm{Adv}_{\mathsf{C}}^{\mathsf{sprp}}(q) =_{\mathrm{def}} \max_{\mathsf{A}:q\text{-}\mathsf{CCA}} \left|\Pr[\mathsf{A}^{\mathsf{C},\mathsf{C}^{-1}} = 1] - \Pr[\mathsf{A}^{\mathsf{P}_n,\mathsf{P}_n^{-1}} = 1]\right| \tag{2}$$

where C is the encryption function of an n-bit block cipher composed of uniform random functions (URFs) as internal modules [16] whereas C^{-1} is its inverse; P_n is an n-bit uniform random permutation (URP) uniformly distributed among all the n-bit permutations; P_n^{-1} is its inverse. The adversary, A, tries to distinguish C from P_n using q queries in a CPA (Chosen Plaintext Attack) attack and tries to distinguish, always using q queries, $(\mathsf{C}, \mathsf{C}^{-1})$ from $(\mathsf{P}_n, \mathsf{P}_n^{-1})$ in a CCA (Chosen Ciphertext Attack) attack. The notation means that the final guess of the adversary A is either 0 if A thinks that the computations are done using P_n, or 1 if A thinks that the computations are done using C. The maximums of Eqs. (1,2) are taken over all possible adversaries A with q queries and an unbounded computational power. Many results [10,16,21] have appear evaluating the security of Feistel variants in this model. For example, Luby and Rackoff in their seminal work [16] proved the security of a $2n$-bit classical Feistel cipher with 3 rounds in the prp model and with 4 rounds in the sprp model considering that the classical Feistel cipher is composed of n-bit-to-n-bit URFs (the bounds they found are in $\mathcal{O}(q^2/2^n)$ for both cases). Those initial results have been generalized in many ways [19,33].

To prove the bounds of our scheme in those models, we follow the methodology of [30] based on the results of [20]. To do so, we introduce the following notations: Let $\Phi_{kn,r}$ denote our k-block scheme acting on n-bit blocks, using r rounds and with diffusion delay d. We first introduce the following definition that will be useful for the next lemma:

Definition 5. *Let H be a keyed permutation over $(\{0,1\}^n)^k$ and let $\boldsymbol{x} = (x_0, \cdots, x_{k-1}) \in (\{0,1\}^n)^k$ with $\boldsymbol{x}_{[i]} = x_i$. H is said to be an ϵ-AU (ϵ Almost Universal) function if:*

$$\max_{\boldsymbol{x} \neq \boldsymbol{x'}} \Pr[H(\boldsymbol{x})_{[i]} = H(\boldsymbol{x'})_{[i]}, \text{for } i \in \{0, \cdots, k-1\}] \leq \epsilon$$

Lemma 1. *Let H and H' be two keyed permutations over $(\{0,1\}^n)^k$ that are respectively ϵ-AU and ϵ'-AU; Let denote by $\Phi_{kn,r}$ our r-round EGFN with k branches acting on n-bit blocks with a diffusion delay d where all n-bit round-functions are independent URFs. Then we have:*

$$\mathrm{Adv}^{\mathsf{prp}}_{\Phi_{kn,2}\circ H}(q) \leq \left(\epsilon + \frac{k}{2^n}\right) \cdot \binom{q}{2} \tag{3}$$

$$\mathrm{Adv}^{\mathsf{sprp}}_{H'^{-1}\circ\Phi_{kn,2}\circ H}(q) \leq \left(\epsilon + \epsilon' + \frac{k}{2^{n-1}}\right) \cdot \binom{q}{2} \tag{4}$$

Proof. Intuitively, for Eq. (3), this lemma uses the fact that after the application of H the inputs of function $\Phi_{kn,2}$ are sufficiently distinct and are random strings. We then have rare collisions at the outputs of $\Phi_{kn,2}$. For Eq. (4), same arguments hold in both directions. The proof of this lemma is omitted as it is similar to those of Theorem 3.1 and Theorem 3.2 of [22] or is a direct extension of Lemma 9 and Theorem 7 of [19]. □

Theorem 8. *Given the r-round EGFN $\Phi_{kn,r}$ with k branches acting on n-bit blocks with a diffusion delay d where all n-bit round functions are independent URFs. Then we have:*

$$\mathrm{Adv}^{\mathsf{prp}}_{\Phi_{kn,d+2}}(q) \leq \frac{kd}{2^n}q^2 \tag{5}$$

$$\mathrm{Adv}^{\mathsf{sprp}}_{\Phi_{kn,2d+2}}(q) \leq \frac{kd}{2^{n-1}}q^2 \tag{6}$$

Proof. To demonstrate Theorem 8, we have first to show that $\Phi_{kn,d}$ is an ϵ-AU function and second that $\overline{\Phi_{kn,d}}$ which is $\Phi^{-1}_{kn,d}$ without the final shuffle is also an ϵ-AU function.

Let us first demonstrate (as done in [30]) that

$$\Pr[\Phi_{kn,d}(\mathbf{x})_{[i]} = \Phi_{kn,d}(\mathbf{x'})_{[i]}] \leq \frac{d}{2^n}, \text{ for all } i \in \{0, \cdots, k-1\}] \tag{7}$$

We assume that $(x_{k/2-1}, x_{k/2-2}, x_{k/2+1}) \neq (x'_{k/2-1}, x'_{k/2-2}, x'_{k/2+1})$, without loss of generality. We then estimate the probability that $\Phi_{kn,d}(\mathbf{x})_{[0]} = \Phi_{kn,d}(\mathbf{x'})_{[0]}$. By definition of d, there is an appropriate path of length d on the graph of $\Phi_{kn,d}$ starting and finishing at vertex 0. For $h = 1, \cdots, d$, we can define a sequence of internal inputs $Y_h = \Phi_{kn,h}(\mathbf{x})_{[s(h)]}$ following the appropriate path. It is straightforward to see that $\Pr[Y_1 = Y'_1] = \Pr[F(x_{k/2-2}) \oplus x_{k/2-1} \oplus x_{k/2+1} = F(x'_{k/2-2}) \oplus x'_{k/2-1} \oplus x_{k/2+1}] \leq 1/2^n$ because the round function F is a URF (using the same reasoning, this result also holds for probabilities of the other branches, even the branch x_{k-1} due to the presence of an F function). Then, $\Pr[Y_d = Y'_d]$ is over bounded by $\sum_{j=2}^{d} \Pr[Y_j = Y'_j | Y_{j-1} \neq Y'_{j-1}] + \Pr[Y_1 = Y'_1] \leq d/2^n$ because all round functions are independent, i.e. $\Pr[Y_j = Y'_j | Y_{j-1} \neq Y'_{j-1}] \leq 1/2^n$. This proves Eq. (7). Thus, $\Phi_{kn,h}$ is a $\frac{kd}{2^n}$-AU function. Equation (5) of Theorem 8 is straightforwardly proved using Eq. (3) of Lemma 1.

To prove the second equation of Theorem 8, we use exactly the same reasoning on $\overline{\Phi_{kn,d}}$ to show that $\Pr[Y_d = Y'_d] \leq d/2^n$ with $Y_h = \overline{\Phi_{kn,h}}(\mathbf{x})_{[s(h)]}$ for $h = 1, \cdots, d$. We then deduce that $\overline{\Phi_{kn,d}}$ is a $\frac{kd}{2^n}$-AU function. Combining the fact that $\Phi_{kn,d}$ is a $\frac{kd}{2^n}$-AU function and that $\overline{\Phi_{kn,d}}$ is a $\frac{kd}{2^n}$-AU function through Eq. (4) of Lemma 1, we obtain Eq. (6). □

3.2 Evaluation of Security Against Classical Attacks

Differential/Linear Cryptanalysis. Differential and linear cryptanalysis are the most famous attacks on block ciphers. They have been introduced respectively in [5] and in [18]. Since their discovery, many works have been done to first show the links between both forms of cryptanalysis [8] and to find better ways to prevent those attacks from happening for a given cipher [9]. The usual consensus about this last point is to count the minimal number of active S-boxes crossed all along the cipher by differential and linear characteristics and thus to estimate the induced maximal differential/linear probability, under the independence assumption.

If the maximal differential/linear probability of an S-box is denoted by DP/LP and if the minimal number of active S-boxes is N, then the best differential/linear attack against the cipher has a complexity of about $1/(DP^N)$ (resp. $1/(LP^N)$) operations. Thus, a cipher is supposed to be secure against differential/linear cryptanalysis as soon as $1/(DP^N)$ (resp. $1/(LP^N)$) is greater than the entire codebook, equal here to 2^{kn}.

In Table 3, we evaluate the minimal number of active S-boxes up to 20 rounds for our scheme and compare it the results of [30] for their optimal construction. We obtain a greater number of active S-boxes in our case.

Table 3. Number of active S-boxes for every round compared with results of [30].

	Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$k = 8$	[30]	0	1	2	3	4	6	8	10	12	12	14	16	16	18	20	20	22	24	24	26
$k = 8$	Ours	0	1	2	6	9	9	12	14	15	19	19	22	24	25	29	29	32	34	35	39
$k = 16$	[30]	0	1	2	3	4	6	8	11	14	19	21	24	25	27	30	31	33	36	37	39
$k = 16$	Ours	0	1	2	10	17	17	18	26	33	33	34	42	49	49	50	58	65	65	66	74

Finally, if we want to estimate the number of rounds that could be attacked using differential/linear cryptanalysis, we could estimate DP and LP for classical n-bit S-box construction, i.e. we write F the internal n-bit function as $F(x) = S(K \oplus x)$ where K is a subkey different at each round. We have the following bounds on DP and LP for such an F function: if we assume n is even, then DP and LP are over bounded by 2^{-n+2}; if n is odd then DP and LP are over bounded by 2^{-n+1}. For example, if we assume that F works on 8-bit words with $k = 8$, our scheme ciphers 64-bit plaintexts. We have $DP = LP = 2^{-6}$ and the maximal number of active S-boxes that could be crossed is equal to 10 to have $2^{64} > 1/(DP^N) = 2^{6 \cdot 10}$. From Table 3, we could deduce that, under those hypotheses, our scheme is resistant to differential/linear cryptanalysis as soon as 7 rounds have been performed. In the same way, with $k = 16$ and $n = 4$, $DP = LP = 2^{-2}$, the maximal number of S-boxes that could be crossed is equal to 31 and at least 9 rounds of our 16 branches scheme must at least be performed.

The total number of rounds to perform for preventing differential/linear attacks is smaller than the one required for the schemes proposed in [30] because the number of S-boxes crossed at each round is more important.

Integral Attack. In [15] L. Knudsen and D. Wagner analyze integral cryptanalysis as a dual to differential attacks particularly applicable to block ciphers with bijective components. A first-order integral cryptanalysis considers a particular collection of m words in the plaintexts and ciphertexts that differ on a particular component. The aim of this attack is thus to predict the values in the sums (i.e. the integral) of the chosen words after a certain number of rounds of encryption. The same authors also generalize this approach to higher-order integrals: the original set to consider becomes a set of ml vectors which differ in l components and where the sum of this set is predictable after a certain number of rounds. The sum of this set is called an lth-order integral. In [27], the authors improve the already known results in the case of Feistel structure noticing that computations of the XOR sum of the partial decryptions can be divided into two independent parts through a meet-in-the-middle approach. We define the following properties for a set of 2^n n-bit words:

- 'C' (for Constant) in the ith entry, means that the values of all the ith words in the collection of texts are equal.
- 'A' (for All) means that all words in the collection of texts are different.
- '?' means that the sum of words can not be predicted.
- 'B' (for Balanced) means that the sum of all words taken on a particular word is equal to 0.

Integral characteristics are of the form $(\alpha \rightarrow \beta)$ with $\alpha \in \{C, A\}^k$ containing at least one A and $\beta \in \{C, A, ?, B\}^k$ containing at least one A or one C or one B. To find integral characteristics, we apply the method and the properties described in [6]. We first look at characteristics α containing exactly one A subblock, the other ones being C. By definition of d, the state after d rounds does not contain C. If we assume that the state after d rounds contains two As for the most favorable n-bit blocks, say i and j (for example blocks with indices $k/2-1$ and $k-1$), then by adding one more round, the state at the subblock $s = \mathcal{P}(j)$ becomes a $B = (F(A) \oplus A)$ or a $B = (F(A) \oplus A \oplus A)$ subblock for the simplest transformations, the other transformations straightforwardly give same kind of results. After one more round, the state at indice $t = \mathcal{P}(s)$ is of the same form because no F function has been crossed. Adding another round transforms this state into a state of the form $? = F(B) \oplus ?$ or $? = F(B) \oplus B \oplus ?$ or more complicated expressions for y_1. Therefore, an integral characteristic (containing one A and $k-1$ Cs) exists for at most $d+2$ rounds. If we try to extend at the beginning this first order characteristic into an lth-order characteristic, we could add at most d rounds at the beginning due to the definition of d. Thus, the maximum number of rounds that could be reach by an lth order integral characteristic is $d + d + 2 = 2d + 2$. We confirm this bound by experimental analysis being able to find a first order integral characteristic for at most $d+2$ rounds.

Impossible Differential Attack. Impossible differential cryptanalysis [4] is a form of differential cryptanalysis for block ciphers. While ordinary differential cryptanalysis tracks differences that propagate through the cipher with a probability as large as possible, impossible differential cryptanalysis exploits differences with 0 probability in intermediate rounds of the cipher to sieve wrong key candidates.

More formally, impossible differential attacks are represented by a differential transition $\alpha \not\rightarrow \beta$ with $\alpha, \beta \in (\{0,1\}^n)^k$ for a cipher E with k n-bit blocks with $Pr[E(x) + E(x+\alpha) = \beta] = 0$ for any x. Intuitively, if we want to form an impossible differential transition for our EGFN, we need to first form the first part of the impossible differential on r_1 rounds between the input differential $\alpha^0 = (\alpha_0^0, \cdots, \alpha_{k-1}^0)$ and the output differential after r_1 rounds $\alpha^{r_1} = (\alpha_0^{r_1}, \cdots, \alpha_{k-1}^{r_1})$. Then, we form the second part of the impossible differential in the decryption direction on r_2 rounds between $\beta^0 = (\beta_0^0, \cdots, \beta_{k-1}^0)$ and $\beta^{r_2} = (\beta_0^{r_2}, \cdots, \beta_{k-1}^{r_2})$. Then, the impossible differential on $r_1 + r_2$ rounds is $\alpha^0 \not\rightarrow \beta^0$ if the differences α^{r_1} and β^{r_2} are not compatible in the middle of the cipher.

From the $\mathcal{U}$-method of [14] or the UID-method of [17], the differences α^{r_1} and β^{r_2} could be of the types: zero difference (denoted 0), nonzero unfixed difference (denoted δ), non zero fixed difference (denoted γ), exclusive-or of nonzero fixed and nonzero unfixed difference (denoted by $\delta + \gamma$), and unfixed difference (denoted t). As done in [30], we could determine the maximal number of rounds for an impossible differential attack using the $\mathcal{U}$-method described in [14]. This number of rounds mainly depends on d as shown below:

- If α_i^d for i in $\{k/2, \cdots, k-1\}$ has type γ, there exists a data path, P that does not pass through any F (i.e. the equation corresponding to this path does not contain α_i^0 as a part of arguments of F). If α_j^d for j in $\{0, \cdots, k/2-1\}$ has type δ then α_l^{d+1} with $l = \mathcal{P}(i)$ has type $\delta + \gamma$. If β_k^d has type γ, we are able to construct an impossible differential attack on $2d+1$ rounds.
- If all the data paths pass through at least one F function, then both α^d and β^d do not contain differences of type neither γ nor 0. Thus, we could only mount differences on $d-1$ rounds for the direct sens (i.e. α difference) and on d rounds for the decryption sens (i.e. β difference). The maximal number of rounds for this type of impossible differential attack is $2d-1$ rounds.
- By definition of d, there exists α^0 such that α_i^{d-1} has type γ for some i. Similarly, there exists β^0 with β_j^{d-1} has type γ' for some j. If $i = j$ and $\gamma \neq \gamma'$, we can construct an impossible differential attack on $2d-2$ rounds.

Finally, the implementation of the $\mathcal{U}$-method gives us the same results: the maximal number of rounds for our scheme looking at impossible differential attack is equal to $2d-2$, $2d-1$ or $2d+1$.

4 Conclusion

In this article, we have introduced a generic matrix representation that captures most existing Generalized Feistel Networks. We explained diffusion properties

of those schemes through this representation. We then introduce a new kind of schemes called Extended Generalized Feistel Networks that adds a diffusion layer to the classical GFNs. We finally instantiated this class of schemes into two proposals and proved the security of them under classical security and attack models.

Our further work will be to propose a complete block cipher using small S-boxes for round-functions and based on our EGFNs proposals that have proved security bounds and provide a more efficient diffusion with a reasonable additional cost, and confront our theoretical study to the ruthless world of cryptanalysis and of cryptanalysts.

References

1. Adams, C., Gilchrist, J.: The CAST-256 encryption algorithm. Network Working Group, RFC 2612, June 1999. http://tools.ietf.org/html/rfc2612 (1999)
2. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: *Camellia*: a 128-bit block cipher suitable for multiple platforms - design and analysis. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001)
3. Arnault, F., Berger, T.P., Minier, M., Pousse, B.: Revisiting LFSRs for cryptographic applications. IEEE Trans. Info. Theory **57**(12), 8095–8113 (2011)
4. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
5. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
6. Biryukov, A., Shamir, A.: Structural cryptanalysis of SASAS. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 394–405. Springer, Heidelberg (2001)
7. Burwick, C., Coppersmith, D., D'Avignon, E., Gennaro, R., Halevi, S., Jutla, C., Matyas Jr, S.M., O'Connor, L., Peyravian, M., Stafford, D., Zunic, N.: MARS - a candidate cipher for AES. *NIST AES Proposal* (1999)
8. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
9. FIPS 197. Advanced encryption standard. Federal Information Processing Standards Publication 197, Department of Commerce/N.I.S.T., U.S. (2001)
10. Gilbert, H., Minier, M.: New results on the pseudorandomness of some blockcipher constructions. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 248–266. Springer, Heidelberg (2002)
11. Hirose, S., Kuwakado, H., Yoshida, H.: SHA-3 Proposal: Lesamnta. http://www.hitachi.com/rd/yrl/crypto/lesamnta/index.html (2008)
12. Hoang, V.T., Rogaway, P.: On generalized feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010)
13. Hong, D., Sung, J., Hong, S.H., Lim, J.-I., Lee, S.-J., Koo, B.-S., Lee, C.-H., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J.-S., Chee, S.: HIGHT: a new block cipher suitable for low-resource device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006)

14. Kim, J., Hong, S., Lim, J.: Impossible differential cryptanalysis using matrix method. Discrete Math. **310**(5), 988–1002 (2010)
15. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
16. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988)
17. Luo, Y., Wu, Z., Lai, X., Gong, G.: A unified method for finding impossible differentials of block cipher structures. IACR Cryptology ePrint Archive 2009:627 (2009)
18. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
19. Maurer, U.M.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 110–132. Springer, Heidelberg (2002)
20. Mitsuda, A., Iwata, T.: Tweakable pseudorandom permutation from generalized feistel structure. In: Baek, J., Bao, F., Chen, K., Lai, X. (eds.) ProvSec 2008. LNCS, vol. 5324, pp. 22–37. Springer, Heidelberg (2008)
21. Moriai, S., Vaudenay, S.: On the pseudorandomness of top-level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289–302. Springer, Heidelberg (2000)
22. Naor, M., Reingold, O.: On the construction of pseudorandom permutations: Luby-Rackoff revisited. J. Cryptol. **12**(1), 29–66 (1999)
23. National Bureau of Standards: U.S. Department of Commerce. Data Encryption Standard (1977)
24. Nyberg, K.: Generalized feistel networks. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996)
25. Rivest, R.L.:. A description of the RC2(r) encryption algorithm. Network Working Group, RFC 2268, March 1998. http://tools.ietf.org/html/rfc2268 (1998)
26. Rivest, R.L., Robshaw, M.J.B., Sidney, R., Yin, Y.L.: The RC6 block cipher, august 1998. http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf (1998)
27. Sasaki, Y., Wang, L.: Meet-in-the-middle technique for integral attacks against feistel ciphers. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 234–251. Springer, Heidelberg (2013)
28. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007)
29. SHS. Secure hash standard. In: FIPS PUB 180–4, Federal Information Processing Standards Publication (2012)
30. Suzaki, T., Minematsu, K.: Improving the generalized feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19–39. Springer, Heidelberg (2010)
31. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013)
32. Yanagihara, S., Iwata, T.: Improving the permutation layer of Type 1, Type 3, Source-Heavy, and Target-Heavy generalized feistel structures. IEICE Trans. **96–A**(1), 2–14 (2013)
33. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (1990)