Efficient Recursive Diffusion Layers for Block Ciphers, and Hash Functions [⋆]

Mahdi Sajadieh[1], Mohammad Dakhilalian[2], Hamid Mala[3], and Pouyan Sepehrdad[4]

[1] Department of Electrical Engineering , Islamic Azad University, Khorasgan Branch, Isfahan, Iran
[2] Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
[3] Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran
[4] EPFL, Lausanne, Switzerland
m.sajadieh@khuisf.ac.ir,
mdalian@cc.iut.ac.ir,
h.mala@eng.ui.ac.ir,
pouyan.sepehrdad@epfl.ch

Abstract. Many modern block ciphers use maximum distance separable (MDS) matrices as the main part of their diffusion layers. In this paper, we propose a very efficient new class of diffusion layers constructed from several rounds of Feistel-like structures whose round functions are linear. We investigate the requirements of the underlying linear functions to achieve the maximal branch number for the proposed 4×4 words diffusion layer, which is an indication of highest level of security with respect to linear and differential attacks. We try to extend our results for up to 8×8 words diffusion layers. The proposed diffusion layers only require simple operations such as word-level XORs, rotations, and they have simple inverses. They can replace the diffusion layer of several block ciphers and hash functions in the literature to increase their security, and performance. Furthermore, it can be deployed in the design of new efficient lightweight block ciphers and hash functions in future.

Keywords: Block ciphers, Diffusion layer, Branch number, MDS matrix

1 Introduction

Block ciphers are one of the most important building blocks in many security protocols. Modern block ciphers are cascades of several rounds where every round consists of confusion and diffusion layers. In many block ciphers, while the confusion layer is often realized as a parallel application of non-linear substitution boxes (S-boxes), the diffusion layer is built from a linear transformation. The diffusion layer plays an efficacious role in providing resistance against the most well-known attacks on block ciphers, such as differential cryptanalysis (DC) [2], and linear cryptanalysis (LC) [8].

When considering a word-based linear transformation, where the word size is equal to the input/output size of the S-box, the branch number provides a lower bound on the number of active S-boxes throughout the diffusion layer for differential and linear attacks. The goal for a designer is to maximize this number, in order to diffuse the non-linear properties of the S-Boxes faster to the subsequent rounds of the cipher. The faster this non-linearity spreads, the less number of rounds the cipher requires to become secure against linear and differential attacks. It has been shown that the maximal branch number for a linear transformation of s words is $s+1$ and diffusion layers with maximal branch number can be achieved by using MDS matrices [4].

An MDS matrix (Maximum Distance Separable) is a matrix representing a function with certain diffusion properties that have useful applications in cryptography. Technically, an $m \times n$ matrix A over a finite field K is an MDS matrix if it is the transformation matrix of a linear transformation $f(x) = Ax$ from K^n to K^m such that no two different $(m+n)$-tuples of the form $(x, f(x))$ coincide in n or more components. Equivalently, the set of all $(m+n)$-tuples $(x, f(x))$ is an MDS code, i.e. a linear code that reaches the Singleton bound.

[⋆] This paper was solicited by the Editors-in-Chief as one of the best papers from FSE 2012, based on the recommendation of the program committee.

In 1994, Vaudenay [11, 12] suggested using MDS matrices in cryptographic primitives to produce what he called multipermutations, not-necessarily linear functions with the same property. These functions have what he called perfect diffusion: changing t of the inputs change at least $m-t+1$ of the outputs. He showed how to exploit imperfect diffusion to cryptanalyze functions that are not multipermutations. MDS matrices were later used in many block ciphers such as Square, SHARK, AES, Twofish, Hierocrypt, and Camelia and in the stream cipher MUGI and the cryptographic hash function Whirlpool.

The common approach to construct MDS matrices is to extract them from MDS codes such as Reed-Solomon codes [7]. However, constructing MDS diffusion layers with low-cost implementations is a challenge for designers. Another problem arises when MDS diffusion layers are exploited in substitution-permutation networks (SPN), where the MDS matrix is used in the encryption and its inverse is used in the decryption process. Thus, constructing MDS matrices with low-cost inverse is of great importance.

In this paper, we propose a new method to construct low-cost diffusion layers with an extra property that their inverse can also be implemented efficiently. We call the proposed layer a recursive diffusion layer. It is constructed from several rounds of Feistel-like structures whose round functions are linear. It consists of simple linear operations such as shift, rotation and XOR with very similar inversion operations. We are going to elaborate on the conditions for the underlying linear function to be an MDS matrix using one or multiple such linear functions by proposing a systematic method to find them. We believe that our proposed solution would be a rather simple recipe for designing a diffusion layer with maximal branch number and will be useful for future designs of cryptographic algorithms.

1.1 Notations

Let $\mathbf{x}$ be an array of s n-bit elements $\mathbf{x} = [x_{0(n)}, x_{1(n)}, \cdots, x_{s-1(n)}]$. The number of non-zero elements in $\mathbf{x}$ is denoted by $w(\mathbf{x})$, also known as the Hamming weight of $\mathbf{x}$. The following notations are used throughout this paper:

$\oplus$	: The bit-wise XOR operation
&	: The bit-wise AND operation
L_i	: Any linear function
$\mathcal{L}_i$	: The linear operator corresponding to the linear function L_i
$(L_1 \oplus L_2)(x)$	: $L_1(x) \oplus L_2(x)$
$L_1L_2(x)$	: $L_1(L_2(x))$
$L_1^2(x)$	: $L_1(L_1(x))$
$I(\cdot)$ function	: Identity function, $I(x) = x$
$x \gg m$ $(x \ll m)$	: Shift of a bit string x by m bits to the right (left)
$x \ggg m$ $(x \lll m)$	: Circular shift of a bit string x by m bits to the right (left)
$\lvert \cdot \rvert$	: Determinant of a matrix in $\mathsf{GF}(2)$
$a \vert\vert b$	: Concatenation of two bit strings a and b
$x_{(n)}$	: An n-bit value x

For a diffusion layer D applicable on $\mathbf{x}$, we have the following definitions:

Definition 1 **([4]).** *The differential branch number of a linear diffusion layer D is defined as:*

$$\beta_d(D) = \min_{\mathbf{x} \neq 0} \{w(\mathbf{x}) + w(D(\mathbf{x}))\}$$

We know that the linear function D can be shown as a binary matrix $\mathbf{B}$, and D^t is a linear function obtained from $\mathbf{B}^t$, where $\mathbf{B}^t$ is the transposition of $\mathbf{B}$.

Definition 2 **([4]).** *The linear branch number of a linear diffusion layer D is defined as:*

$$\beta_l(D) = \min_{\mathbf{x} \neq 0} \{w(\mathbf{x}) + w(D^t(\mathbf{x}))\}$$

It is well known that for a diffusion layer acting on s-word inputs, the maximal β_d and β_l are $s+1$ [4]. A diffusion layer D taking its maximal β_d and β_l is called a perfect or MDS diffusion layer. Furthermore, a diffusion layer with $\beta_d = \beta_l = s$ is called an almost perfect diffusion layer [4].

1.2 Our contribution

In this paper, we define the notion of a *recursive diffusion layer*, and propose a method to construct such perfect diffusion layers.

Definition 3. *A diffusion layer D with s words x_i as the input and s words y_i as the output is called a recursive diffusion layer if it can be represented in the following form:*

$$D : \begin{cases} y_0 = x_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \\ y_1 = x_1 \oplus F_1(x_2, x_3, \dots, x_{s-1}, y_0) \\ \vdots \\ y_{s-1} = x_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \end{cases} \tag{1}$$

where F_0, F_1,..., F_{s-1} are arbitrary linear functions.

An advantage of this structure is that the inverse of D is very similar to D, and does not require the inverse of F_i functions. The inverse can be computed as:

$$D^{-1} : \begin{cases} x_{s-1} = y_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \\ x_{s-2} = y_{s-2} \oplus F_{s-2}(x_{s-1}, y_0, \dots, y_{s-3}) \\ \vdots \\ x_0 = y_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \end{cases} \tag{2}$$

As an example, consider a 2-round Feistel structure with a linear round function L as a recursive diffusion layer with $s = 2$. The input-output relation for this diffusion layer is:

$$D : \begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$$

The quarter-round function of the stream cipher Salsa20 is an example of a non-linear recursive diffusion layer [1].

$$D : \begin{cases} y_1 = x_1 \oplus ((x_0 + x_3) \lll 7) \\ y_2 = x_2 \oplus ((x_0 + y_1) \lll 9) \\ y_3 = x_3 \oplus ((y_1 + y_2) \lll 13) \\ y_0 = x_0 \oplus ((y_2 + y_3) \lll 18) \end{cases}$$

Also, the lightweight hash function PHOTON [5] and the block cipher LED [6] use MDS matrices based on Eq. (1). In these ciphers, an $m \times m$ MDS matrix $\mathbf{B}^m$ was designed based on the following matrix $\mathbf{B}$ for the performance purposes:

$$\mathbf{B} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & Z_1 & Z_2 & \cdots & Z_{m-1} \end{pmatrix}$$

By matrix $\mathbf{B}$, one element of m inputs is updated and other elements are shifted. If we use $\mathbf{B}^m$, all inputs are updated, but we must check if this matrix is MDS. One example for $m = 4$ is the PHOTON matrix working over $\mathsf{GF}(2^8)$:

$$\mathbf{B} = \begin{pmatrix} 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 1\,2\,1\,4 \end{pmatrix} \Rightarrow \mathbf{B}^4 = \begin{pmatrix} 1 & 2 & 1 & 4 \\ 4 & 9 & 6 & 17 \\ 17 & 38 & 24 & 66 \\ 66 & 149 & 100 & 11 \end{pmatrix}$$

In this paper, we propose a new approach to design linear recursive diffusion layers with the maximal branch number in which F_i's are composed of one or two linear functions and a number of XOR operations. The design of the proposed diffusion layer is based on the invertibility of some simple linear functions in $\mathsf{GF}(2)$. Linear functions in this diffusion layer can be designed to be low-cost for different sizes of the input words, thus the proposed diffusion layer might be appropriate for resource-constrained devices, such as RFID tags. Although these recursive diffusion layers are not involutory, they have similar inverses with the same computational complexity.

This paper proceeds as follows: In Section 2, we introduce the general structure of our proposed recursive diffusion layer. Then, for one of its instances, we systematically investigate the required conditions for the underlying linear function to achieve the maximal branch number. In Section 3, we propose some other recursive diffusion layers with less than 8 input words and only one linear function. We use two linear functions to have a perfect recursive diffusion layer for $s > 4$ in Section 4. Finally, we conclude the paper in Section 5.

2 The Proposed Diffusion Layer

In this section, we introduce a new perfect linear diffusion layer with a recursive structure. The diffusion layer D takes s words x_i for $i = \{0, 1, \ldots, s-1\}$ as input, and returns s words y_i for $i = \{0, 1, \ldots, s-1\}$ as output. So, we can represent this diffusion layer as:

$$y_0||y_1||\cdots||y_{s-1} = D(x_0||x_1||\cdots||x_{s-1})$$

The first class of the proposed diffusion layer D is represented in Fig. 1, where L is a linear function, $\alpha_k, \beta_k \in \{0, 1\}$, $\alpha_0 = 1$ and $\beta_0 = 0$. This diffusion layer can be represented in the form of Eq. (1) in which the F_i functions are all the same and can be represented as

$$F_i(x_1, x_2, \ldots, x_{s-1}) = \bigoplus_{j=1}^{s-1} \alpha_j x_j \oplus L\left(\bigoplus_{j=1}^{s-1} \beta_j x_j\right)$$

```
Input : $s$ $n$-bit words $x_0, \ldots, x_{s-1}$
Output : $s$ $n$-bit words $y_0, \ldots, y_{s-1}$
for $i = 0$ to $s-1$ do
    $y_i = x_i$
end for
for $i = 0$ to $s-1$ do
    $y_i = y_i \oplus \left(\bigoplus_{j=0, j\neq i}^{s-1} \alpha_{[(j-i) \mod s]} y_j\right) \oplus L\left(\bigoplus_{j=0, j\neq i}^{s-1} \beta_{[(j-i) \mod s]} y_j\right)$
end for
```

Fig. 1. The first class of the recursive diffusion layers

To guarantee the maximal branch number for D, the linear function L and the coefficients α_j and β_j must satisfy some necessary conditions. Conditions on L are expressed in this section and those of α_j's and

β_j's are expressed in Section 3. The diffusion layer described by Eq. (3) is an instance that satisfies the necessary conditions on α_j, and β_j with $s = 4$. In the rest of this section, we concentrate on the diffusion layers of this form and show that we can find invertible linear functions L such that D becomes a perfect diffusion layer.

$$D : \begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases} \tag{3}$$

As shown in Fig. 2, This diffusion layer has a Feistel-like (GFN) structure, i.e.,

$$F_0(x_1, x_2, x_3) = x_2 \oplus x_3 \oplus L(x_1 \oplus x_3)$$

The inverse transformation, D^{-1}, has a very simple structure and does not require the inversion of the linear function L. The inverse of D is:

$$D^{-1} : \begin{cases} x_3 = y_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \\ x_2 = y_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ x_1 = y_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ x_0 = y_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \end{cases}$$

D and D^{-1} are different, but they have the same structure and properties. To show that D has the maximal branch number, first we introduce some lemmas and theorems.

If $L(x)$ can be written as $a \cdot x$ in a finite field, then Eq. (3) can be expressed as a matrix representation as below:

$$\mathbf{B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & a & 1 & a+1 \end{pmatrix} \Rightarrow \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \mathbf{B}^4 \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{4}$$

We can construct MDS matrix similar to PHOTON matrix by the proposed diffusion layer. In Eq. (1), if $F_i(x_1, x_2, x_3) = F_0(x_1, x_2, x_3) = L(x_1) \oplus x_2 \oplus L^2(x_3)$, where $L(x) = 2x$ and $x \in \mathsf{GF}(2^8)$, PHOTON MDS matrix is obtained [5]. If we change $\mathbf{B}$ to Eq. (3), and define $L(x) = 2x$, we have:

$$\mathbf{B} = \begin{pmatrix} 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 1\,2\,1\,3 \end{pmatrix} \Rightarrow \mathbf{B}^4 = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 7 & 1 & 4 \\ 4 & 11 & 3 & 13 \\ 13 & 30 & 6 & 20 \end{pmatrix}$$

Theorem 4 ([4]). *A Boolean function F has maximal differential branch number if, and only if it has maximal linear branch number.*

As a result of Theorem 4, if we prove that the diffusion layer D represented in Eq. (3) has the maximal differential branch number, its linear branch number will be maximal too. Thus, in the following, we focus on the differential branch number.

Lemma 5. *A linear functions $L(x)$is invertible if, and only if for any non-zero value a, $L(a) \neq 0$.*

Proof. For any linear function $L(x)$, we have $L(0) = 0$. If there exists $a \neq 0$ such that $L(a) = 0$, then $L(x)$ is not invertible. On the other hand, suppose $a = 0$ is the unique zero of $L(x)$, and $L(x)$ is not invertible. So, there exist two values b and c ($b \neq c$) such that $L(b) = L(c)$. Since $L(x)$ is a linear function, we have $L(b \oplus c) = L(b) \oplus L(c) = 0$, while $b \oplus c \neq 0$. This contradicts the assumption that $a = 0$ is the unique zero of $L(x)$. □

Lemma 6. *Assume the linear operator $\mathcal{L}_i$ corresponds to the linear function $L_i(x)$. If the linear operator $\mathcal{L}_3$ can be represented as the multiplication of two operators $\mathcal{L}_1$ and $\mathcal{L}_2$, then the corresponding linear function $L_3(x) = L_2(L_1(x))$ is invertible if, and only if the linear functions $L_1(x)$ and $L_2(x)$ are invertible.*

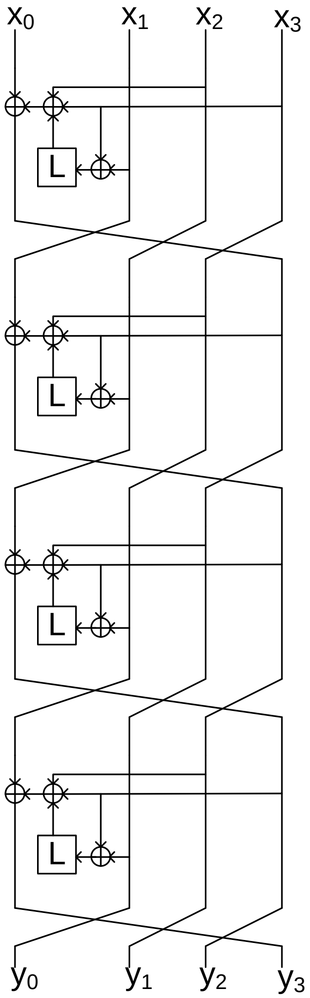

Fig. 2. The proposed recursive diffusion layer of Eq. (3)

Proof. If $L_1(x)$ and $L_2(x)$ are invertible, clearly $L_3(x)$ is invertible too. On the other hand, if $L_3(x)$ is invertible then $L_1(x)$ must be invertible, otherwise, there are distinct x_1, and x_2 such that $L_1(x_1) = L_1(x_2)$. Thus, $L_3(x_1) = L_2(L_1(x_1)) = L_2(L_1(x_2)) = L_3(x_2)$ which contradicts the invertibility of $L_3(x)$. The invertibility of $L_2(x)$ is proved in the same way.

□

Example 1: We can rewrite the linear function $L_3(x) = L^3(x) \oplus x$ ($\mathcal{L}_3 = \mathcal{L}^3 \oplus I$) as $L_3(x) = L_2(L_1(x))$, where $L_1(x) = L(x) \oplus x$ ($\mathcal{L}_1 = \mathcal{L} \oplus I$) and $L_2(x) = L^2(x) \oplus L(x) \oplus x$ ($\mathcal{L}_2 = \mathcal{L}^2 \oplus \mathcal{L} \oplus I$). Thus, the invertibility of $L_3(x)$ is equivalent to the invertibility of the two linear functions $L_1(x)$ and $L_2(x)$.

Theorem 7. *For the diffusion layer represented in Eq. (3), if the four linear functions $L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$ are invertible, then this diffusion layer is perfect.*

Proof. We show that the differential branch number of this diffusion layer is 5. First, the 4 words of the output are directly represented as functions of the 4 words of the input:

$$D : \begin{cases} y_0 = x_0 \oplus L(x_1) \oplus x_2 \oplus x_3 \oplus L(x_3) \\ y_1 = x_0 \oplus L(x_0) \oplus x_1 \oplus L(x_1) \oplus L^2(x_1) \oplus x_2 \oplus L^2(x_3) \\ y_2 = L^2(x_0) \oplus x_1 \oplus L(x_1) \oplus L^3(x_1) \oplus x_2 \oplus L(x_2) \oplus x_3 \oplus L^2(x_3) \oplus L^3(x_3) \\ y_3 = x_0 \oplus L^2(x_0) \oplus L^3(x_0) \oplus L(x_1) \oplus L^2(x_1) \oplus L^3(x_1) \oplus L^4(x_1) \\ \qquad \oplus L(x_2) \oplus L^2(x_2) \oplus L^2(x_3) \oplus L^4(x_3) \end{cases} \qquad (5)$$

In the proof, we look at all different cases for the Hamming weight of the input. In other words, we show that if the Hamming weight of the input is $m = 1, 2, 3, 4$, then the Hamming weight of the output is greater than or equal to $5 - m$. Each case will pose different conditions on L which in the end can be summarized to the condition given in the theorem. The diffusion layer represented in Eq. (3) is invertible. Consider $m = 4$, then all of the 4 words in the input are active, and we are sure at least one of the output words is active too. Thus, the theorem is correct for $m = 4$. The remainder of the proof is performed for the 3 cases of $w(\Delta(\mathbf{x})) = m$, for $m = 1, 2, 3$ separately. In each of these cases, some conditions are forced on the linear function L.

Case 1: $w(\triangle\mathbf{x}) = 1$

To study this case, first the subcase

$$(\triangle x_0 \neq 0, \triangle x_1 = \triangle x_2 = \triangle x_3 = 0 \ \text{ or } \ \triangle\mathbf{x} = \triangle x_0||0||0||0)$$

is analyzed. For this subcase, Eq. (5) is simplified to:

$$D : \begin{cases} \triangle y_0 = \triangle x_0 \\ \triangle y_1 = (I \oplus L)(\triangle x_0) \\ \triangle y_2 = L^2(\triangle x_0) \\ \triangle y_3 = (I \oplus L^2 \oplus L^3)(\triangle x_0) \end{cases}$$

If D is a perfect diffusion layer, then $\triangle y_0$, $\triangle y_1$, $\triangle y_2$ and $\triangle y_3$ must be non-zero. Clearly, $\triangle y_0$ is non-zero and based on Lemma 5, the conditions for $\triangle y_1$, $\triangle y_2$ and $\triangle y_3$ to be non-zero are that the linear functions $I \oplus L$, L^2 and $I \oplus L^2 \oplus L^3$ must be invertible. Note that based on Lemma 6, the invertibility of L yields the invertibility of L^2. Considering Lemma 6, if the other three sub-cases are studied, it is induced that the linear functions $x \oplus L(x) \oplus L^2(x)$ and $x \oplus L(x) \oplus L^3(x)$ must also be invertible.

Case 2: $w(\triangle\mathbf{x}) = 2$

In this case, there exist exactly two active words in the input difference, and we obtain some conditions on the linear function L to guarantee the branch number 5 for D. In the following, we only analyze the subcase

$$(\triangle x_0, \triangle x_1 \neq 0 \ \text{ and } \ \triangle x_2 = \triangle x_3 = 0 \ \text{ or } \ \triangle\mathbf{x} = \triangle x_0||\triangle x_1||0||0)$$

With this assumption, Eq. (5) is simplified to:

$$D: \begin{cases} \triangle y_0 = \triangle x_0 \oplus L(\triangle x_1) \\ \triangle y_1 = (I \oplus L)(\triangle x_0) \oplus (I \oplus L \oplus L^2)(\triangle x_1) \\ \triangle y_2 = L^2(\triangle x_0) \oplus (I \oplus L \oplus L^3)(\triangle x_1) \\ \triangle y_3 = (I \oplus L^2 \oplus L^3)(\triangle x_0) \oplus (L \oplus L^2 \oplus L^3 \oplus L^4)(\triangle x_1) \end{cases} \tag{6}$$

To show that $w(\triangle \mathbf{y})$ is greater than or equal to 3, we must find some conditions on L such that if one of the $\triangle y_i$'s is zero, then the other three $\triangle y_j$'s cannot be zero. Let $\triangle y_0 = 0$, then:

$$\triangle x_0 \oplus L(\triangle x_1) = 0 \Rightarrow \triangle x_0 = L(\triangle x_1)$$

If $\triangle x_0$ is replaced in the last three equations of Eq. (6), we obtain $\triangle y_1$, $\triangle y_2$ and $\triangle y_3$ as follows:

$$\begin{cases} \triangle y_1 = \triangle x_1 \\ \triangle y_2 = \triangle x_1 \oplus L(\triangle x_1) \\ \triangle y_3 = L^2(\triangle x_1) \end{cases}$$

Obviously, $\triangle y_1$ is not zero. Furthermore, considering Lemma 5, for $\triangle y_2$ to be non-zero, we conclude that the function $x \oplus L(x)$ must be invertible. For $\triangle y_1 \Rightarrow \triangle y_3$, $L^2(x)$ is invertible. This condition was already obtained in the Case 1. We continue this procedure for $\triangle y_1 = 0$.

$$\begin{aligned} &\triangle y_1 = \triangle x_0 \oplus L(\triangle x_0) \oplus x_1 \oplus L(\triangle x_1) \oplus L^2(\triangle x_1) = 0 \Rightarrow \\ &\triangle x_0 \oplus L(\triangle x_0) = x_1 \oplus L(\triangle x_1) \oplus L^2(\triangle x_1) \end{aligned}$$

From the previous subcase, we know that if $\triangle y_0 = 0$, then $\triangle y_1 \neq 0$. Thus, we conclude that $\triangle y_0$ and $\triangle y_1$ cannot be simultaneously zero. Therefore, by contraposition, we obtain that if $\triangle y_1 = 0$, then $\triangle y_0 \neq 0$. So, we only check $\triangle y_2$ and $\triangle y_3$. From the third equation in Eq. (6), we have:

$$\begin{aligned} (I \oplus L)(\triangle y_2) &= L^2(\triangle x_1) \oplus L^3(\triangle x_1) \oplus L^4(\triangle x_1) \oplus \triangle x_1 \\ &\quad \oplus L^2(\triangle x_1) \oplus L^3(\triangle x_1) \oplus L^4(\triangle x_1) \\ &= \triangle x_1 \end{aligned}$$

$x \oplus L(x)$ is invertible, thus we conclude that with the two active words $\triangle x_0$ and $\triangle x_1$ in the input, $\triangle y_1$ and $\triangle y_2$ cannot be zero simultaneously. With the same procedure, we can prove that $\triangle y_1$, and $\triangle y_3$ cannot be zero simultaneously.

Here we only gave the proof for the case ($\triangle x_0, \triangle x_1 \neq 0$, $\triangle x_2 = \triangle x_3 = 0$). We performed the proof procedure for the other cases, and no new condition was added to the previous set of conditions in Case 1.

Case 3: $w(\triangle \mathbf{x}) = 3$

In this case, assuming three active words in the input, we show that the output has at least 2 non-zero words. Here, only the case

$$(\triangle x_0, \triangle x_1, \triangle x_2 \neq 0 \text{ and } \triangle x_3 = 0 \text{ or } \triangle \mathbf{x} = \triangle x_0 || \triangle x_1 || \triangle x_2 || 0)$$

is analyzed. The result holds for the other three cases with $w(\triangle \mathbf{x}) = 3$. Let rewrite Eq. (5) for $\triangle x_3 = 0$ as follows:

$$D: \begin{cases} \triangle y_0 = \triangle x_0 \oplus L(\triangle x_1) \oplus \triangle x_2 \\ \triangle y_1 = (I \oplus L)(\triangle x_0) \oplus (I \oplus L \oplus L^2)(\triangle x_1) \oplus \triangle x_2 \\ \triangle y_2 = L^2(\triangle x_0) \oplus (I \oplus L \oplus L^3)(\triangle x_1) \oplus (I \oplus L)(\triangle x_2) \\ \triangle y_3 = (I \oplus L^2 \oplus L^3)(\triangle x_0) \oplus (L \oplus L^2 \oplus L^3 \oplus L^4)(\triangle x_1) \oplus (L \oplus L^2)(\triangle x_2) \end{cases} \tag{7}$$

When $\triangle y_0 = \triangle y_1 = 0$, from the first 2 lines of Eq. (7), $\triangle x_0$ and $\triangle x_1$ are obtained as the function of $\triangle x_2$.

$$\begin{cases} \triangle y_0 = \triangle x_0 \oplus L(\triangle x_1) \oplus \triangle x_2 = 0 \\ \triangle y_1 = \triangle x_0 \oplus L(\triangle x_0) \oplus \triangle x_1 \oplus L(\triangle x_1) \\ \qquad \oplus L^2(\triangle x_1) \oplus \triangle x_2 = 0 \end{cases} \Rightarrow \begin{cases} \triangle x_1 = L(\triangle x_2) \\ \triangle x_0 = \triangle x_2 \oplus L^2(\triangle x_2) \end{cases}$$

Now, replacing $\triangle x_0 = \triangle x_2 \oplus L^2(\triangle x_2)$ and $\triangle x_1 = L(\triangle x_2)$ into $\triangle y_2$ and $\triangle y_3$ yields:

$$\begin{cases} \triangle y_2 = L^2(\triangle x_0) \oplus (I \oplus L \oplus L^3)(\triangle x_1) \oplus (I \oplus L)(\triangle x_2) = \triangle x_2 \\ \triangle y_3 = (I \oplus L^2 \oplus L^3)(\triangle x_0) \oplus (L \oplus L^2 \oplus L^3 \oplus L^4)(\triangle x_1) \oplus (L \oplus L^2)(\triangle x_2) \\ \qquad = (I \oplus L)(\triangle x_2) \end{cases}$$

From Case 1, we know that the functions $x \oplus L(x)$ are invertible. Therefore, $\triangle y_2$, and $\triangle y_3$ are non-zero. If the other sub-cases with three active words in the input are investigated, it is easy to see that no new condition is added to the present conditions on L. Finally, we conclude that the diffusion layer D presented in Fig. 1 is perfect if the linear functions

$$\begin{cases} L_1(x) = L(x) \\ L_2(x) = x \oplus L(x) \\ L_3(x) = x \oplus L(x) \oplus L^2(x) \\ L_4(x) = x \oplus L(x) \oplus L^3(x) \\ L_5(x) = x \oplus L^2(x) \oplus L^3(x) \end{cases}$$

are invertible. We know that $L_3(L_2(x)) = x \oplus L^3(x)$ and $L_5(L_4(L_2(x))) = x \oplus L^7(x)$. Thus, by Lemma 6, we can summarize the necessary conditions on the linear function L as the invertibility of $L(x)$, $(I \oplus L)(x)$, $(I \oplus L^3)(x)$ and $(I \oplus L^7)(x)$.

□

Next, we need a simple method to check whether a linear function L satisfies the conditions of Theorem 7 or not. For this purpose, we use the binary matrix representation of L. Assume that x_i is an n-bit word. Hence, we can represent a linear function L with an $n \times n$ matrix $\mathbf{A}$ with elements in $\mathsf{GF}(2)$. As a result of Lemma 5, if L is invertible, $\mathbf{A}$ is not singular over $\mathsf{GF}(2)$ ($|\mathbf{A}| \neq 0$). To investigate whether a linear function L satisfies the conditions of Theorem 7, we construct the corresponding matrix $\mathbf{A}_{n\times n}$ from L, and check the non-singularity of the matrices $\mathbf{A}$, $\mathbf{I} \oplus \mathbf{A}$, $\mathbf{I} \oplus \mathbf{A}^3$, and $\mathbf{I} \oplus \mathbf{A}^7$ in $\mathsf{GF}(2)$.

In the following, we construct concrete functions L which are lightweight and satisfy the conditions mentioned in Theorem 7. For example, the functions $L(x) = x$, $L(x) = x \gg a$ and $L(x) = x \ggg a$ are the examples of the most lightweight linear functions. However, they do not satisfy Theorem 7 conditions, because at least one of the two functions $L(x)$ and $x \oplus L(x)$ are not invertible. A set of candidates for lightweight linear functions can be expressed as:

$$L(x_{(n)}) = (x_{(n)} \ll a) \oplus (x_{(n)} \gg b)\,. \tag{8}$$

If $(a + b)|n$, then $L(x)$ is invertible [15]. The remaining conditions $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$ have to be checked. Although the linear function in Eq. (8) has a complicated inverse, it does not require circular shift which is considered as an advantage for this function. Note that circular shift is not supported by some compilers. Another proposal for $L(x)$ is:

$$L(x_{(n)}) = (x_{(n)} \oplus (x_{(n)} \gg a)) \lll b \tag{9}$$

The linear function in Eq. (9), for $a > n/2$, has a lightweight inverse $L(x_{(n)}) = (x_{(n)} \ggg b) \oplus (x_{(n)} \ggg b) \gg a$ which will be used in diffusion layer proposed in Section 4.

We introduce some lightweight linear functions with n-bit inputs/outputs in Table 1 which satisfy the conditions of Theorem 7. Note that for $n = 8$, there does not exist any linear function of the form Eq. (8) or Eq. (9) satisfying conditions of Theorem 7.

Table 1. Some instances of the linear function L satisfying Theorem 7

n	Some linear functions L
4	$L(x) = (x \oplus x \ll 3) \lll 1$
8	$L(x) = (x \oplus (x \,\&\, \mathsf{0x2}) \ll 1) \lll 1$
16	$L(x) = (x \oplus x \ll 15) \lll 1$
32	$L(x) = (x \oplus x \ll 31) \lll 15$ or $L(x) = (x \lll 24) \oplus (x \,\&\, \mathsf{0xFF})$ or $L(x) = (x \ll 3) \oplus (x \gg 1)$
64	$L(x) = (x \oplus x \ll 63) \lll 1$ or $L(x) = (x \lll 8) \oplus (x \,\&\, \mathsf{0xFFFF})$ or $L(x) = (x \ll 15) \oplus (x \gg 1)$

2.1 Application of the Proposed Diffusion Layer in Current Block Ciphers

Together with designing new lightweight block ciphers, the proposed diffusion layer can also be applied to diffuse the non-linearity of big-size S-boxes. One of these block ciphers is MMB [3] that uses 32-bit S-boxes. Each round of MMB is composed of four transformations:

- σ: bit-wise XOR of the intermediate value and the round key.
- γ: modular multiplication of each 32-bit word of the intermediate value with a fixed 32-bit constant G_i modulo $2^{32} - 1$.
- η: an operation on two of the four input words.
- θ: the only diffusion operation in MMB which is an involutory binary matrix as below:

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

We can use the proposed diffusion layer with $L(x_{(32)}) = (x_{(32)} \ll 3) \oplus (x_{(32)} \gg 1)$ instead of the diffusion layer used in the block cipher MMB. If we use the proposed diffusion layer in this cipher, it becomes stronger against differential and linear attacks, because branch number of the binary matrix of MMB is 4 while branch number of the proposed diffusion layer is 5. This change also prevents the attacks presented against this block cipher in [13]. By computer simulations in C using a PC with CPU: 2.93 Ghz and RAM: 2GB, we observed that this modification reduces the performance of MMB by making it 30% slower in the software implementations. This was achieved by comparing the running time of the protocol for 1 million encryptions.

Another block cipher where we can replace the diffusion layer by the proposed one is Hierocrypt [9]. Hierocrypt does not explicitly use big size S-boxes, but it constructs 32 bit S-boxes by using nested SPN structure together with four 8-bit S-boxes and the MDS_L matrix. For diffusion within those 32-bit S-boxes, a 16×16 binary matrix called MDS_H is used, which is MDS for four 32-bit inputs. If we use our proposed diffusion layer with the same $L(x)$, instead of the MDS_H [9], we can achieve a 2 times faster implementation with the same level of security.

AES Mix-column layer has a simple implementation. As another comparison, we decided to replace the MDS_H matrix in Hierocrypt with the MDS matrix of AES. But, since MDS code of AES is over $\mathsf{GF}(2^8)$ and the inputs of MDS_H are four 32-bit words, we modified the corresponding irreducible polynomial in AES and replaced it with $x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$ [10] to work over $\mathsf{GF}(2^{32})$, which would still remain MDS. We call this new construction, sch_1. As another construction, we replaced the MDS_H in Hierocrypt with the MDS code we proposed above in our solution and we called it sch_2. We observed that sch_2 still brings on 5% better performance compared to sch_1.

3 Other Desirable Structures for the Proposed Diffusion Layer

In Section 2, the general form of the proposed diffusion layer was introduced in Fig. 1. Then, by assuming a special case of α_i's and β_i's, an instance of this diffusion layer was given in Eq. (3). In this section, we obtain all sets of α_i's and β_i's such that the diffusion layer of Fig. 1 becomes perfect. We know some properties of α_i's and β_i's; for instance if all the words of the output are directly represented as a function of input words, a function of each x_i $(0 \leq i \leq s-1)$ must appear in each equation. Another necessary condition is obtained for two active words of the input. Assume there exist only two indices i, j such that $x_i, x_j \neq 0$. If we write each two output words y_p, y_q in a direct form as a function of x_i and x_j, we obtain:

$$\begin{cases} y_p = L_{p_i}(x_i) \oplus L_{p_j}(x_j) \\ y_q = L_{q_i}(x_i) \oplus L_{q_j}(x_j) \end{cases}$$

If

$$\frac{\mathcal{L}_{p_i}}{\mathcal{L}_{q_i}} = \frac{\mathcal{L}_{p_j}}{\mathcal{L}_{q_j}} \qquad \text{or} \qquad \begin{vmatrix} \mathcal{L}_{p_i} & \mathcal{L}_{p_j} \\ \mathcal{L}_{q_i} & \mathcal{L}_{q_j} \end{vmatrix} = 0$$

then, $y_p = 0$ is equivalent to $y_q = 0$. Thus, the minimum number of active words in the input and output is less than or equal to s and the branch number will not reach the maximal value $s+1$. This procedure must be repeated for 3, and more active words in the input. As an extension, we can use Lemma 3 of [10].

Lemma 8. *[10] Assume the diffusion layer has m inputs/outputs bits, and $\mathcal{L}$ is the linear operator of $L(x)$, and I is the linear operator of $I(x)$. Moreover, $\boldsymbol{ML}_D$ is an $m \times m$ matrix representation of the operator of the diffusion layer. If D is perfect, then all the sub-matrices of $\boldsymbol{ML}_D$ are non-singular.*

If we construct the $\mathbf{ML}_D$ of Eq. (3), we have:

$$\mathbf{ML}_D = \begin{pmatrix} I & \mathcal{L} & I & I \oplus \mathcal{L} \\ I \oplus \mathcal{L} & I \oplus \mathcal{L} \oplus \mathcal{L}^2 & I & \mathcal{L}^2 \\ \mathcal{L}^2 & I \oplus \mathcal{L} \oplus \mathcal{L}^3 & I \oplus \mathcal{L} & I \oplus \mathcal{L}^2 \oplus \mathcal{L}^3 \\ I \oplus \mathcal{L}^2 \oplus \mathcal{L}^3 & \mathcal{L} \oplus \mathcal{L}^2 \oplus \mathcal{L}^3 \oplus \mathcal{L}^4 & \mathcal{L} \oplus \mathcal{L}^2 & \mathcal{L}^2 \oplus \mathcal{L}^4 \end{pmatrix}$$

when calculating 69 sub-matrix determinants of $\mathbf{ML}_D$, we observe that these submatrices are non-singular only if L fulfills the condition of Theorem 7. However, by following this procedure, it is complicated to obtain all sets of α_i's and β_i's analytically. So, by systematizing the method based on Lemma 8, we performed a computer simulation to obtain all sets of α_i's, and β_i's in the diffusion layer in Fig. 1 that yield a perfect diffusion. We searched for all α_i's and β_i's that make the diffusion layer of Fig. 1 a perfect diffusion layer. This procedure was repeated for $s = 2, 3, \ldots, 8$. We found one set of $(\alpha_i,\ \beta_i)$ for $s = 2$, four sets for $s = 3$, and four sets for $s = 4$. The obtained diffusion layers along with the conditions on the underlying linear function L are reported in Table 2. We observed that for $s = 5, 6, 7, 8$ the diffusion layer introduced in Fig. 1 cannot be perfect.

Note that some linear functions in Table 1 such as $L(x_{(64)}) = (x_{(64)} \lll 15) \oplus (x_{(64)} \gg 1)$ are not suitable for diffusion layers, since $x_{(64)} \oplus L^{15}(x_{(64)})$ must be invertible.

As we can see in Fig. 1, and its instances presented in Table 2, there exists some kind of regularity in the equations defining y_i's, in the sense that the form of y_{i+1} is determined by the form of y_i, and vice versa (F_i's are all the same in Eq. (1)). However, we can present some non-regular recursive diffusion layers with a more general form (F_i's are different) as in Fig. 3, where $A_{i,j}, B_{i,j} \in \{0, 1\}$.

If $A_{i,j} = \alpha_{(j-i) \bmod s}$, and $B_{i,j} = \beta_{(j-i) \bmod s}$, then Fig. 3 is equivalent to Fig. 1. The main property of this new structure is that it still has one linear function L, and a simple structure for the inverse. For example, if $s = 4$, then, the diffusion layer D is:

$$\begin{cases} y_0 = x_0 \oplus A_{0,1} \cdot x_1 \oplus A_{0,2} \cdot x_2 \oplus A_{0,3} \cdot x_3 \oplus L(B_{0,1} \cdot x_1 \oplus B_{0,2} \cdot x_2 \oplus B_{0,3} \cdot x_3) \\ y_1 = x_1 \oplus A_{1,0} \cdot y_0 \oplus A_{1,2} \cdot x_2 \oplus A_{1,3} \cdot x_3 \oplus L(B_{1,0} \cdot y_0 \oplus B_{1,2} \cdot x_2 \oplus B_{1,3} \cdot x_3) \\ y_2 = x_2 \oplus A_{2,0} \cdot y_0 \oplus A_{2,1} \cdot y_1 \oplus A_{2,3} \cdot x_3 \oplus L(B_{2,0} \cdot y_0 \oplus B_{2,1} \cdot y_1 \oplus B_{2,3} \cdot x_3) \\ y_3 = x_3 \oplus A_{3,0} \cdot y_0 \oplus A_{3,1} \cdot y_1 \oplus A_{3,2} \cdot y_2 \oplus L(B_{3,0} \cdot y_0 \oplus B_{3,1} \cdot y_1 \oplus B_{3,2} \cdot y_2) \end{cases}$$

Table 2. Perfect regular recursive diffusion layers for $s < 8$ with only one linear function L

s	Diffusion Layer D	Function that must be invertible
2	$\begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$	$L(x)$ and $x \oplus L(x)$
3	$\begin{cases} y_0 = x_0 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$ and $x \oplus L^3(x)$
3	$\begin{cases} y_0 = x_0 \oplus x_1 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus x_2 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
3	$\begin{cases} y_0 = x_0 \oplus x_2 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_1 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
3	$\begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus x_2 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$ and $x \oplus L^3(x)$
4	$\begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
4	$\begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus x_3 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_1 \oplus L(y_0 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
4	$\begin{cases} y_0 = x_0 \oplus x_2 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$, $x \oplus L^7(x)$ and $x \oplus L^{15}(x)$
4	$\begin{cases} y_0 = x_0 \oplus x_1 \oplus x_3 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus y_0 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus \oplus y_1 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_2 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$, $x \oplus L^7(x)$ and $x \oplus L^{15}(x)$

```
Input : $s$ $n$-bit words $x_0, \ldots, x_{s-1}$
Output : $s$ $n$-bit words $y_0, \ldots, y_{s-1}$
for $i = 0$ to $s - 1$ do
    $y_i = x_i$
end for
for $i = 0$ to $s - 1$ do
    $y_i = y_i \oplus \left( \bigoplus_{j=0, j \neq i}^{s-1} A_{i,j} y_j \right) \oplus L \left( \bigoplus_{j=0, j \neq i}^{s-1} B_{i,j} y_j \right)$
end for
```

Fig. 3. Non-regular recursive diffusion layers

We searched the entire space for $s = 3$ and $s = 4$ (the order of search is $2^{2s(s-1)}$). For $s = 3$, we found 196 structures with branch number 4, and for $s = 4$, 1634 structures with branch number 5. The conditions on linear functions that caused maximal branch number, are different for each structure. Among the 196 structures for $s = 3$, the structure with the minimum number of operations (only 7 XORs, and one L evaluation) is the following:

$$D : \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \\ y_1 = x_1 \oplus x_2 \oplus L(y_0 \oplus x_2) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \end{cases}$$

where $L(x)$ and $x \oplus L(x)$ must be invertible.

This relation is useful to enlarge the first linear function of the hash function JH for 3 inputs [14]. For $s = 4$, we did not find any D with the number of L evaluations less than four. However, the one with the minimum number of XORs is given as below:

$$D : \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0) \end{cases}$$

Searching the whole space for $s = 5, 6, ...$ is too time consuming (note that for $s = 5$, the order of search has complexity 2^{40}), and we could not search all the space for $s \geq 5$.

4 Increasing the Number of Linear Functions

In Section 3, we observed that for $s > 4$ we cannot design a regular recursive diffusion layer in the form of Fig. 1 with only one linear function L. In this section, we increase the number of linear functions to overcome the regular structure of the diffusion layer of Eq. (3). A new structure is represented in Fig. 4, where $\alpha_k, \beta_k, \gamma_k \in \{0, 1\}$, $k \in \{0, 1, ..., s-1\}$, $\alpha_0 = 1, \beta_0 = 0$ and $\gamma_0 = 0$.

```
Input : $s$ $n$-bit words $x_0, \ldots, x_{s-1}$
Output : $s$ $n$-bit words $y_0, \ldots, y_{s-1}$
for $i = 0$ to $s-1$ do
    $y_i = x_i$
end for
for $i = 0$ to $s-1$ do
    $y_i = \left(\bigoplus_{j=0}^{s-1} \alpha_{[(j-i) \mod s]} y_j\right) \oplus L_1 \left(\bigoplus_{j=0}^{s-1} \beta_{[(j-i) \mod s]} y_j\right) \oplus L_2 \left(\bigoplus_{j=0}^{s-1} \gamma_{[(j-i) \mod s]} y_j\right)$
end for
```

Fig. 4. Regular recursive diffusion layers with two linear functions L

If L_1 and L_2 are two distinct linear functions, Fig. 4 is too complicated to easily obtain conditions on L_1 and L_2 that make it a perfect diffusion layer (the order of search for s input/output is $2^{3(s-1)}$). To obtain simplified conditions for a maximal branch number, let L_1 and L_2 have a simple relation like $L_2(x) = L_1^2(x)$ or $L_2(x) = L_1^{-1}(x)$. For the linear functions in Eq. (8), $L^2(x)$ is more complex in comparison to $L(x)$. However, there exist some linear functions in the form of Eq. (9) such that $L^{-1}(x)$ is simpler than $L^2(x)$. As an example, for $L(x_{(32)}) = (x_{(32)} \oplus x_{(32)} \gg 31) \lll 1$, we have $L^{-1}(x_{(32)}) = ((x_{(32)} \ggg 1) \oplus (x_{(32)} \ggg 1) \gg 31)$, but $L^2(x_{(32)}) = (x_{(32)} \oplus (x_{(32)} \gg 31) \lll 1) \oplus ((x_{(32)} \lll 1) \gg 31) \lll 1$.

In Table 3, we introduce some recursive diffusion layers with ($L_1 = L$ and $L_2 = L^{-1}$) or ($L_1 = L$ and $L_2 = L^2$) that have maximal branch numbers. These diffusion layers are obtained similar to that of Table 2.

In this table, for each case, only y_0 is presented. Other y_i's can be easily obtained from Fig. 4, since F_i's are all the same.

Table 3. Some perfect regular diffusion layers for $s = 5, 6, 7, 8$ with two linear functions

s	y_0 in a perfect diffusion Layer
5	$y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_4) \oplus L^2(x_1)$
5	$y_0 = L^{-1}(x_1 \oplus x_2) \oplus x_0 \oplus x_1 \oplus L(x_1 \oplus x_3 \oplus x_4)$
6	$y_0 = x_0 \oplus x_2 \oplus x_4 \oplus x_5 \oplus L(x_3 \oplus x_5) \oplus L^2(x_1 \oplus x_2 \oplus x_3)$
6	$y_0 = L^{-1}(x_1 \oplus x_3) \oplus x_0 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus L(x_1 \oplus x_3 \oplus x_4 \oplus x_5)$
7	$y_0 = x_0 \oplus x_2 \oplus L(x_3 \oplus x_4) \oplus L^2(x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6)$
7	$y_0 = L^{-1}(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6) \oplus x_0 \oplus x_2 \oplus x_3 \oplus x_4 \oplus L(x_1 \oplus x_2 \oplus x_3 \oplus x_5)$
8	$y_0 = x_0 \oplus x_1 \oplus x_3 \oplus x_4 \oplus L(x_2 \oplus x_3 \oplus x_5) \oplus L^2(x_1 \oplus x_5 \oplus x_6 \oplus x_7)$
8	$y_0 = L^{-1}(x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_7) \oplus x_0 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_7 \oplus L(x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7)$

If the 14 linear functions:

$$\begin{array}{lll}
L(x) & I \oplus L(x) & I \oplus L^3(x) \\
I \oplus L^7(x) & I \oplus L^{15}(x) & I \oplus L^{31}(x) \\
I \oplus L^{63}(x) & I \oplus L^{127}(x) & I \oplus L^{255}(x) \\
I \oplus L^{511}(x) & I \oplus L^{1023}(x) & I \oplus L^{2047} \\
I \oplus L^{4095}(x) & I \oplus L^{8191}(x) &
\end{array}$$

are invertible (all irreducible polynomials up to degree 13), then all the diffusion layers introduced in Table 3 are perfect. One example for a 32-bit linear function satisfying these conditions is:

$$L(x_{(32)}) = (x_{(32)} \oplus (x_{(32)} \gg 31)) \lll 29$$

5 Conclusion

In this paper, we proposed a new family of efficient diffusion layers (recursive diffusion layers) which are constructed using several rounds of Feistel-like structures whose round functions are linear. The proposed diffusion layers are very efficient and have simple inverses, thus they can be deployed to improve the security or performance of some of the current block ciphers and hash functions and in the design of the future lightweight block ciphers and hash functions, even providing provable security against differential and linear attacks. For a fixed structure, we determined the required conditions for its underlying linear function to be perfectly secure with respect to linear and differential attacks. Then, for the number of words in input (output) less than 8, we extended our approach, and found all the instances of the perfect recursive diffusion layers with the general form described in Fig. 1. Also, we proposed some other diffusion layers with non-regular forms. Finally, diffusion layers with 2 linear functions were proposed. By using two linear functions, we designed perfect recursive diffusion layers for higher number of words.

References

1. D.J. Bernstein. The Salsa20 Stream Cipher, 2005. http://www.ecrypt.eu.org/stream/salsa20p2.html.
2. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *CRYPTO'90*, volume 537, pages 2–21. Springer-Verlag, 1990.
3. J. Daemen. *Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis.* PhD thesis, Elektrotechniek Katholieke Universiteit Leuven, Belgium, 1995.

4. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.
5. J. Guo, T. Peyrin, and A. Poschmann. The PHOTON Family of Lightweight Hash Functions. In *CRYPTO'11*, volume 6841, pages 222–239. Springer-Verlag, 2011.
6. J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw. The LED Block Cipher. In *CHES'11*, volume 6917, pages 326–341. Springer-Verlag, 2011.
7. S. Lin and D. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice Hall, 2004.
8. M. Matsui. Linear Cryptanalysis Method for DES Cipher. In *EUROCRYPT'93*, volume 765, pages 386–397. Springer-Verlag, 1993.
9. K. Ohkuma, H. Muratani, F. Sano, and S. Kawamura. The Block Cipher Hierocrypt. In *SAC'01*, volume 2012, pages 72–88. Springer-Verlag, 2001.
10. M. Sajadieh, M. Dakhilalian, and H. Mala. Perfect Involutory Diffusion Layers Based on Invertibility of Some Linear Functions. *IET Information Security Journal*, 5(1):228–236, 2011.
11. C. Schnorr and S. Vaudenay. Black Box Cryptoanalysis of Hash Networks Based on Multipermutations. In *EUROCRYPT'94*, volume 950, pages 47–57. Springer, 1994.
12. S. Vaudenay. On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In *FSE'94*, volume 1008, pages 286–297. Springer, 1994.
13. M. Wang, J. Nakahara, and Y. Sun. Cryptanalysis of the Full MMB Block Cipher. In *SAC'09*, volume 5867, pages 231–248. Springer-Verlag, 2009.
14. H. Wu. The Hash Function JH, 2008. http://icsd.i2r.astar.edu.sg/staff/hongjun/jh/jh.pdf.
15. G. Zeng, K. He, and W. Han. A trinomial type of σ-LFSR oriented toward software implementation. In *Science in China Series F-Information Sciences*, volume 50, pages 359–372. Springer-Verlag, 2007.