Recursive Diffusion Layers for Block Ciphers and Hash Functions

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

[1] Cryptography & System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
[2] Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran
[3] EPFL, Lausanne, Switzerland
{sadjadieh@ec, 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 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. The proposed diffusion layers only require word-level XORs, rotations, and they have simple inverses. They can be replaced in the diffusion layer of the block ciphers MMB and Hierocrypt to increase their security and performance, respectively. Finally, we try to extend our results for up to 8×8 words diffusion layers.

Keywords: Block ciphers, Diffusion layer, Branch number, Provable security

1 Introduction

Block ciphers are one of the most important building blocks in many security protocols. Modern block ciphers are cascades of several rounds and each round consists of confusion and diffusion layers. In many block ciphers, non-linear substitution boxes (S-boxes) form the confusion layer, and a linear transformation provides the required diffusion. 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) [10].

In 1994, Vaudenay [15, 16] suggested using MDS matrices in cryptographic primitives to produce what he called multipermutations, not-necessarily linear functions with this same property. These functions have what he called perfect

⋆ This work has been supported in part by the European Commission through the ICT program under contract ICT-2007-216646 ECRYPT II.

diffusion. He showed how to exploit imperfect diffusion to cryptanalyze functions that are not multipermutations. This notion was later used by Daemen named as the branch number. Block ciphers exploiting diffusion layers with small branch number may suffer from critical weaknesses against DC and LC, even though their substitution layers consist of S-boxes with strong non-linear properties.

Two main strategies for designing block ciphers are Feistel-like and substitution permutation network (SPN) structures. In the last 2 decades, from these two families several structures have been proposed with provable security against DC and LC. Three rounds of Feistel structure [11, 12], five rounds of RC6-like structure [9] and SDS (substitution-diffusion-substitution) structure with a perfect or almost perfect diffusion layer are examples of such structures [8].

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 $w(\mathbf{x})$ and is 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
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 $\mathsf{GF}(2)$
$a \lvert b$	: 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 [8].

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:*

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

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

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 Salsa20 is also 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:

$$\mathbf{B} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & & \\ 0 & 0 & 0 & \cdots & 1 \\ Z_0 & Z_1 & Z_2 & \cdots & Z_{m-1} \end{pmatrix}$$

By matrix $\mathbf{B}$, one elements 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. Another approach which is not recursive was picked by Junod and Vaudenay in [7] to design efficient MDS matrices.

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

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

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

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s - 1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s - 1$ **do**
7: $\quad y_i = y_i \oplus \left(\bigoplus_{j=0, j\neq i}^{s-1} \alpha_{[(j-i) \mod s]} y_j \right) \oplus L\left(\bigoplus_{j=0, j\neq i}^{s-1} \beta_{[(j-i) \mod s]} y_j \right)$
8: **end for**

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

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. (2) 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.

$$D : \begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases} \tag{2}$$

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

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

and for each $i > 0$, y_i is obtained by $(x_i, x_{i+1}, \ldots, x_{s-1})$ and $(y_0, y_1, \ldots, y_{i-1})$.

The inverse transformation, D^{-1}, has a very simple structure and does not require the inversion of the linear function L. Based on the recursive nature of D, if we start from the last equation of Eq. (2), x_3 is immediately obtained from y_i's. Then knowing x_3 and y_i's, we immediately obtain x_2 from the third line of Eq. (2). x_1 and x_0 can be obtained in the same way. Thus, 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.

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

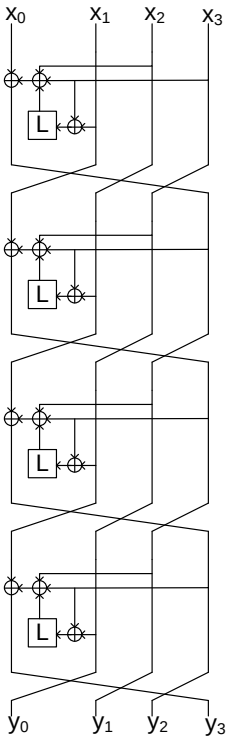

Fig. 2. The proposed recursive diffusion layer of Eq. (2)

As a result of Theorem 4, if we prove that the diffusion layer D represented in Eq. (2) 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. *For m linear functions L_1, L_2, ..., L_m, the proposition*

$$a \neq 0 \Rightarrow L_1(a) \oplus L_2(a) \oplus ... \oplus L_m(a) \neq 0$$

implies that the linear function $L_1 \oplus L_2 \oplus ... \oplus L_m$ is invertible.

Proof. We know that $(L_1 \oplus L_2 \oplus ... \oplus L_m)(x)$ is a linear function and it can be represented as a binary matrix $\mathbf{M}$. So, $\mathbf{M}$ is invertible if and only if $|\mathbf{M}| \neq 0$. □

Lemma 6. *Assume the linear operator ℓ_i corresponds to the linear function $L_i(x)$. If the linear operator ℓ_3 can be represented as the multiplication of two operators ℓ_1 and 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.*

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 $L_3(x) = L^3(x) \oplus x$ ($\ell_3 = \ell^3 \oplus I$) as $L_3(x) = L_1(L_2(x))$, where $L_1(x) = L(x) \oplus x$ ($\ell_1 = \ell \oplus I$) and $L_2(x) = L^2(x) \oplus L(x) \oplus x$ ($\ell_2 = \ell^2 \oplus \ell \oplus I$). 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. (2), 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:

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

Now, we show that if the number of active (non-zero) words in the input is m, where $m = 1, 2, 3, 4$, then the number of non-zero words in the output is greater than or equal to $5 - m$. The diffusion layer represented in Eq. (2) 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. (3) 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^2 yields the invertibility of L. Considering Lemma 6, if the other three subcases 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. (3) is simplified to:

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

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. (4), 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, for $\triangle y_2$ and $\triangle y_3$ to be non-zero, considering Lemma 5, we conclude that the functions $x \oplus L(x)$ and $L^2(x)$ must be 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. (4), 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 the Eq. (3) for $\triangle x_3 = 0$ as follows:

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

When $\triangle y_0 = \triangle y_1 = 0$, from the first 2 lines of Eq. (5), $\triangle x_0$ 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 $x \oplus L(x)$ and $x \oplus L(x) \oplus L^2(x)$ 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 $\mathsf{GF}(2)$. By using 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 $\mathsf{GF}(2)$. We introduce some lightweight linear functions with n-bit inputs/outputs in Table 1 that satisfy the above conditions. Note that there exist many linear functions which satisfy the conditions of Theorem 7.

Unlike the shift and XOR operations, rotation cannot be implemented as a single instruction on many processors. So, to have more efficient diffusion layers, we introduce new L functions for 32-bit and 64-bit inputs in Table 2 that only use shift and XOR operations.

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 $L(x) = (x \lll 24) \oplus (x \;\&\; \mathsf{0xFF})$
64	$L(x) = (x \oplus x \ll 63) \lll 1$ or $L(x) = (x \lll 8) \oplus (x \;\&\; \mathsf{0xFFFF})$

Table 2. Some examples for the linear function L satisfying Theorem 7 without a circular shift

n	Sample linear functions L
32	$L(x) = (x \ll 3) \oplus (x \gg 1)$
64	$L(x) = (x \ll 15) \oplus (x \gg 1)$

We can use this diffusion layer with $L(x) = (x \ll 3) \oplus (x \gg 1)$ instead of the diffusion layers used in the block ciphers MMB [3] or Hierocrypt [13]. In MMB, the diffusion layer is a 4×4 binary matrix with branch number 4. If we use the proposed diffusion layer in this cipher, it becomes stronger against LC and DC attacks. This change also prevents the attacks presented on this block cipher in [17]. By computer simulations, we observed that this modification reduces the performance of MMB by about 10%. Also, if we use our proposed diffusion layer with the same $L(x)$, instead of the binary matrix of the block cipher Hierocrypt (called $\mathrm{MDS_H}$ [13]), we can achieve a 2 times faster implementation with the same level of security.

Moreover, in the nested SPN structure of Hierocrypt, we replaced the MDS matrix of AES in $\mathsf{GF}(2^{32})$ (because inputs of $\mathrm{MDS_H}$ are 4 32-bit words) with irreducible polynomial $x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$ [14] instead of the binary matrix $\mathrm{MDS_H}$. We observed that the replacement of our proposed diffusion layer instead of $\mathrm{MDS_H}$ yields 5% better performance than the replacement of the AES matrix in $\mathsf{GF}(2^{32})$.

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 $x \in \mathsf{GF}(2^4)$, PHOTON MDS matrix is obtained [5]. If we change $\mathbf{B}$ to Eq. (2) and define $L(x) = 2x$, we have:

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

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. (2). 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 the 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

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

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 [14].

Lemma 8. *Assume the diffusion layer has m inputs/outputs bits and 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 $\boldsymbol{ML}_D$ is non-singular.*

If we construct the $\mathbf{ML}_D$ of Eq. (2), we have:

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

If we calculate 69 sub-matrix determinant of $\mathbf{ML}_D$, we find the result 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 (α_i, β_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 3. We observed that for $s = 5, 6, 7$ the diffusion layer introduced in Fig. 1 cannot be perfect.

Table 3. 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 $x \oplus L^{15}(x)$

Note that some linear functions in Table 1 and Table 2 such as $L(x) = (x \ll 15) \oplus (x \gg 1)$ cannot be used in the diffusion layers for which $x \oplus L^{15}(x)$ must be invertible.

As we can see in Fig. 1 and its instances presented in Table 3, 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 the following more general form (F_i's are different):

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s - 1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s - 1$ **do**
7: $\quad y_i = y_i \oplus \left(\bigoplus_{j=0, j\neq i}^{s-1} A_{i,j} y_j \right) \oplus L \left(\bigoplus_{j=0, j\neq i}^{s-1} B_{i,j} y_j \right)$
8: **end for**

Fig. 3. Non-regular recursive diffusion layers

where $A_{i,j}, B_{i,j} \in \{0, 1\}$. If $A_{i,j} = \alpha_{(j-i) \mod s}$ and $B_{i,j} = \beta_{(j-i) \mod s}$, 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:

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

We searched the whole space for $s = 3$ and $s = 4$ (the order of search spaces are 2^{12} and 2^{24} respectively). For $s = 3$, we found 196 structures with branch number 4 and for $s = 4$, 1634 structures with branch number 5. The linear functions that must be invertible for each case are different. 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 new hash function JH for 3 inputs [18]. 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. (2). 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 $\gamma_0 = 0$.

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s - 1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s - 1$ **do**
7: $\quad y_i = \bigoplus_{j=0}^{s-1} \alpha_{[(j-i) \mod s]} y_j \oplus L_1 \left(\bigoplus_{j=0}^{s-1} \beta_{[(j-i) \mod s]} y_j \right) \oplus L_2 \left(\bigoplus_{j=0}^{s-1} \gamma_{[(j-i) \mod s]} y_j \right)$
8: **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. 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 Table 2 and Table 3, $L^2(x)$ is more complex in comparison with $L(x)$. However, there exist some linear functions $L(x)$ such that $L^{-1}(x)$ is simpler than $L^2(x)$. As an example, for $L(x_{(n)}) = (x_{(n)} \oplus x_{(n)} \gg b) \lll a$, where $b > \frac{n}{2}$ we have $(x_{(n)} \gg 2b = 0)$:

$$L^{-1}(x_{(n)}) = ((x_{(n)} \ggg a) \oplus (x_{(n)} \ggg a) \gg b)$$

In Table 4, 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 3. 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 4. 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 4 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 family of diffusion layers which are constructed using some rounds of Feistel-like structures whose round functions are linear. These diffusion layers are called recursive diffusion layers. First, for a fixed structure, we determined the required conditions for its underlying linear function to make it a perfect diffusion layer. 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 of Fig. 1. Also, we proposed some other diffusion layers with non-regular forms which can be used for the design of lightweight block ciphers. Finally, diffusion layers with 2 linear functions were proposed. By using two linear functions, we designed perfect recursive diffusion layers for $s = 5, 6, 7, 8$ which cannot be designed based on Fig. 1, i.e., using only one linear function.

The proposed diffusion layers have simple inverses, thus they can be deployed in SPN structures. These proposed diffusion layers can be used to improve the security or performance of some of the current block ciphers and hash functions or in the design of the future block ciphers and hash functions (especially the block ciphers with provable security against DC and LC).

References

1. D.J. Bernstein. The Salsa20 Stream Cipher. Symmetric Key Encryption Workshop (SKEW), 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, and M. Robshaw. The LED Block Cipher. In *CHES'11*, volume 6917, pages 326–341. Springer-Verlag, 2011.
7. P. Junod and S. Vaudenay. Perfect Diffusion Primitives for Block Ciphers. In *SAC'04*, volume 3357, pages 84–99. Springer, 2004.
8. J. Kang, S. Hong, S. Lee, O. Yi, C. Park, and J. Lim. Practical and Provable Security Against Differential and Linear Cryptanalysis for Substitution-Permutation Networks. *ETRI Journal*, 23(4):158–167, 2001.
9. C. Lee, J. Kim, J. Sung, S. Hong, and S. Lee. Provable Security for an RC6-like Structure and a MISTY-FO-like Structure Against Differential Cryptanalysis. In *ICCSA'06*, volume 3982, pages 446–455. Springer-Verlag, 2006.
10. M. Matsui. Linear Cryptanalysis Method for DES Cipher. In *EUROCRYPT'93*, volume 765, pages 386–397. Springer-Verlag, 1993.
11. M. Matsui. New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis. In *FSE'96*, volume 1039, pages 205–218. Springer-Verlag, 1996.
12. K. Nyberg and L. Knudsen. Provable Security Against a Differential Attack. *Journal of Cryptology*, 8(1):27–37, 1995.
13. K. Ohkuma, H. Muratani, F. Sano, and S. Kawamura. The Block Cipher Hierocrypt. In *SAC'01*, volume 2012, pages 72–88. Springer-Verlag, 2001.
14. 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.
15. C. Schnorr and S. Vaudenay. Black Box Cryptoanalysis of Hash Networks Based on Multipermutations. In *EUROCRYPT'94*, volume 950, pages 47–57. Springer, 1994.
16. S. Vaudenay. On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In *FSE'94*, volume 1008, pages 286–297. Springer, 1994.
17. 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.
18. H. Wu. The Hash Function JH. Submission to NIST, 2008.