A Family of Nonlinear MDS Diffusion Layers over $\mathbb{F}_{2^{4n}}$

M. R. Mirzaee Shamsabad[1] and S. M. Dehnavi[2]

[1] Department of Mathematical Sciences, Shahid Beheshti University, Tehran, Iran
m_mirzaee@sbu.ac.ir
[2] Department of Mathematical and Computer Sciences, University of Kharazmi
Tehran, Iran
dehnavism@ipm.ir

Abstract. Nonlinear diffusion layers are less studied in cryptographic literature, up to now. In 2018, Liu, Rijmen and Leander studied nonlinear non-MDS diffusion layers and mentioned some advantages of them. As they stated, nonlinear diffusion layers could make symmetric ciphers more resistant against statistical and algebraic cryptanalysis. In this paper, with the aid of some special maps over the finite field $\mathbb{F}_{2^n}$, we examine nonlinear MDS mappings and present a family of 4×4 nonlinear MDS diffusion layers. Next, we determine the Walsh and differential spectrum as well as the algebraic degree of the proposed diffusion layers.

Keywords: Nonlinear MDS diffusion layer. Linear structure. Algebraic degree. Walsh spectrum. Differential spectrum.

1 Introduction and Main Results

Diffusion layers are critical components of symmetric ciphers. MDS diffusion layers have applications in the design of block ciphers, stream ciphers and hash functions. For instance, the Advanced Encryption Standard (AES) [4] uses an MDS matrix as the main part of its diffusion layer (Mix-Column), the stream cipher ZUC [7] which is used in 4G mobile systems, applies an MDS matrix in its design, and moreover, the SHA-3 finalist hash function Grostl [8] has an MDS matrix in its diffusion layer.

MDS diffusion layers have been studied from various aspects. Numerous papers [9, 14, 15, 18, 19] study them in order to minimize their implementation cost in software and/or hardware applications. Also, these components have been studied from a variety of mathematical viewpoints. For example, Dong et. al. [6] characterize MDS mappings resulted from the action of a module over a ring. Augot et. al. [1] study MDS matrices on rings and [11, 17] give some nonlinear MDS diffusion layers over $\mathbb{Z}_{2^n}$.

For the first time in the cryptographic literature, Voudenay et. al. [21] introduced the general form of MDS maps (multi-permutations) and [20] used nonlinear 2×2 MDS maps in the design of CS-Cipher. Klimov and Shamir presented some kinds of nonlinear MDS maps in [11]. Recently, Liu et. al. [13] investigate nonlinear diffusion layers and show that they could be more resistant against various kinds

of cryptanalysis. Their proposed nonlinear diffusion layers are non-MDS. They discuss the advantages of them over the classic linear ones, but do not present the linear branch number of their proposed diffusion layers. On the other hand, they do not study the implementation cost of them. In [17] some kinds of randomized and/or nonlinear MDS diffusion layers over $\mathbb{F}_2$ are presented. Our proposed nonlinear diffusion layers are MDS over 4 inputs and their linear and differential branch numbers are 5. They are defined on $\mathbb{F}_{2^n}$, $n > 8$. Also, as we show in Algorithm 1 and Algorithm 2, our proposed diffusion layers as well as their inverses have a suitable implementation cost over a variety of modern processors.
In this paper, we examine nonlinear 4×4 MDS diffusion layers over $\mathbb{F}_{2^n}$. We present a family of these diffusion layers based on some theoretical investigations. More precisely, we study the parametric square sub-functions of the proposed maps and based upon Theorem 1 in [12], we give the sufficient conditions for invertibility of some maps of the form $x + \gamma f(x)$ with $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ and $\gamma \in \mathbb{F}_{2^n}$. We use the criteria given in [2, 12] to find functions that make $x + \gamma f(x)$ invertible. Then, we compute the Walsh and differential spectrum of the proposed maps, along with their algebraic degree.
In Section 2, we give the preliminary notations and definitions. Section 3 provides theoretical tools for construction of nonlinear 4×4 MDS diffusion layers. In Section 4, we present some concrete examples of nonlinear 4×4 MDS diffusion layers and Section 5 is devoted to the conclusion.

2 Notations and Definitions

The finite field with 2^n elements is denoted by $\mathbb{F}_{2^n}$ and the n-dimensional linear space over $\mathbb{F}_2$ by $\mathbb{F}_2^n$. We denote the addition in the field $\mathbb{F}_{2^n}$ as well as the ring $\mathbb{Z}$ by $+$.

Definition 1. [2] *Let $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ and $c \in \mathbb{F}_2$. An element $a \in \mathbb{F}_{2^n} \setminus \{0\}$ is called a c-linear structure of f if for all $x \in \mathbb{F}_{2^n}$, $f(x) + f(x + a) = c$.*

Every map $\phi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ has a unique algebraic representation called its Algebraic Normal Form (ANF) [3]:

$$\phi(x) = \bigoplus_{u \in \mathbb{F}_2^n} h_u x^u, \quad h_u \in \mathbb{F}_2.$$

The algebraic degree of ϕ is denoted by $deg(\phi)$ and is defined as

$$deg(\phi) = \max_{h_u \neq 0} wt(u).$$

Here, $wt(u)$ is the Hamming weight of u. Also, each map f on $\mathbb{F}_2^n$ can be viewed as $(f_{n-1}, \cdots, f_0)$. Similarly, f could be represented as

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} h_u x^u, \quad h_u \in \mathbb{F}_2^n.$$

The algebraic degree of f is defined as

$$deg(f) = \max_{0 \le i < n} deg(f_i). \tag{1}$$

For a map f on $\mathbb{F}_{2^n}$, it can be shown that f has a representation (unique up to the choice of the representing irreducible polynomial)

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_i \in \mathbb{F}_{2^n}$, $0 \le i < 2^n$. The algebraic degree of f is defined as

$$deg(f) = \max_{0 \le i < 2^n, a_i \ne 0} wt(i). \tag{2}$$

It is well-known that the two notions (1) and (2) for the algebraic degree of f coincide. The algebraic degree of a map is one of the measures of resistance against algebraic attacks.
Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For any $a \ne 0, b \in \mathbb{F}_{2^n}$, set

$$D_f(a, b) = \{x \in \mathbb{F}_{2^n} : f(x) + f(x + a) = b\}.$$

The multi-set

$$\varDelta_f = \{|D_f(a, b)| : a \ne 0, b \in \mathbb{F}_{2^n}\},$$

is called the differential spectrum of the function f. Also, for any $a, b \ne 0 \in \mathbb{F}_{2^n}$, define

$$L_f(a, b) = \{x \in \mathbb{F}_{2^n} : a \cdot x = b \cdot f(x)\}.$$

Here, $\cdot$ stands for the standard dot product in $\mathbb{F}_2^n$. The multi-set

$$\varLambda_f = \{2|L_f(a, b)| - 2^n : a, b \ne 0 \in \mathbb{F}_{2^n}\},$$

is called the Walsh spectrum of the function f.
For any $X = (x_1, \ldots, x_m) \in \mathbb{F}_{2^n}^m$, denote the weight of X over $\mathbb{F}_{2^n}$ by $wt_n(X)$ or simply $wt(X)$, which is defined as follows

$$wt(X) = |\{i : 1 \le i \le m,\ x_i \ne 0\}|.$$

Let F be a map on $\mathbb{F}_{2^n}^m$. The branch number of F over $\mathbb{F}_{2^n}$ is defined as

$$Br_n(F) = \min_{X,Y \in \mathbb{F}_{2^n}^m,\, X \ne Y} \{wt(X + Y) + wt(F(X) + F(Y))\},$$

which we simply denote by $Br(F)$.

Definition 2. *The map F on $\mathbb{F}_{2^n}^m$ is called MDS (over $\mathbb{F}_{2^n}$) if $Br(F) = m + 1$.*

One can check that a corresponding $(2n, 2^{nm}, m+1)$-code over $\mathbb{F}_{2^n}$ could be constructed by F in Definition 2, which is MDS [16].
A form of the following discussions are given in [5, 11]. Suppose that F is a map on $\mathbb{F}_{2^n}^4$ with

$$F(x,y,z,t) = (f_1(x,y,z,t), f_2(x,y,z,t), f_3(x,y,z,t), f_4(x,y,z,t)),$$

where $f_i : \mathbb{F}_{2^n}^4 \to \mathbb{F}_{2^n}$, $1 \leq i \leq 4$. Fix $1 \leq i \leq 4$. For any three arguments of F, without loss of generality, say x, y and z, we define the 1×1 family of sub-functions

$$F^i_{x,y,z} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$

$$F^i_{x,y,z}(t) = f_i(x,y,z,t),$$

and say that $F^i_{x,y,z}$ is parametric in 3 variables. Note that there are 16 families of 1×1 sub-functions and there are 2^{3n} functions in each family.
Now, fix $1 \leq i < j \leq 4$. For any two arguments of F, without loss of generality, say x and y, we define the 2×2 family of sub-functions

$$F^{i,j}_{x,y} : \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}^2,$$

$$F^{i,j}_{x,y}(z,t) = (f_i(x,y,z,t), f_j(x,y,z,t)),$$

and say that $F^{i,j}_{x,y}$ is parametric in 2 variables. Note that there are 36 families of 2×2 sub-functions and there are 2^{2n} functions in each family.
Finally, fix $1 \leq i < j < k \leq 4$. For any argument of F, without loss of generality, say x, we define the 3×3 family of sub-functions

$$F^{i,j,k}_{x} : \mathbb{F}_{2^n}^3 \to \mathbb{F}_{2^n}^3,$$

$$F^{i,j,k}_{x}(y,z,t) = (f_i(x,y,z,t), f_j(x,y,z,t), f_k(x,y,z,t)),$$

and say that $F^{i,j,k}_{x}$ is parametric in 1 variable. Note that there are 16 families of 3×3 sub-functions and there are 2^n functions in each family.

Definition 3. *Let F be a map on $\mathbb{F}_{2^n}^4$. We say that an $i \times i$, $1 \leq i \leq 3$, family of sub-functions of F is parametric invertible if all the $2^{(4-i)n}$ many functions (corresponding to $2^{(4-i)n}$ admissible parameters) are invertible.*

We illustrate the above definitions via the following example.

Example 1. Consider the map F on $\mathbb{F}_{2^n}^4$ with

$$F(x,y,z,t) = (f_1(x,y,z,t), f_2(x,y,z,t), f_3(x,y,z,t), f_4(x,y,z,t)),$$

where,

$$f_1(x,y,z,t) = x + y,$$

$$f_2(x,y,z,t) = y,$$

$$f_3(x,y,z,t) = xyzt,$$

$$f_4(x,y,z,t) = x + z.$$

Since $F^1_{y,z,t}(x) = x + y$ and y, z, t are parameters, so, for any $y = a$, $z = b$ and $t = c$ with $a, b, c \in \mathbb{F}_{2^n}$, the function $F^1_{a,b,c}(x) = x + a$ is invertible. Therefore, $F^1_{a,b,c}$ is a 1×1 parametric invertible sub-function. On the other hand, $F^3_{x,y,z}$ is not parametric invertible, because $F^3_{0,0,0}(t) = 0$. For another example, the 2×2 family of sub-functions $F^{1,2}_{z,t}(x,y) = (x+y, y)$ is parametric invertible; but the 2×2 family of sub-functions $F^{2,3}_{x,y}(z,t) = (y, xyzt)$ is not parametric invertible, because $F^{2,3}_{0,0}(z,t) = (0,0)$.

3 Theoretical Aspects

In this section, first we prove a theorem to characterize the MDS property of mappings on $\mathbb{F}^4_{2^n}$. Next, we present the Walsh and differential spectra of the proposed maps, as well as their algebraic degree. Then, we investigate the statistical and algebraic properties of the proposed diffusion layers and show that why they are more resistant against cryptanalysis, compared with the classic ones.
The following lemmas are used in the proof of Theorem 2.

Lemma 1. *Define g on $\mathbb{F}_{2^n}$ with $g(x) = Mf(x) + x$, where f is a map on $\mathbb{F}_{2^n}$ and M is an invertible linear map on $\mathbb{F}_{2^n}$. If g is invertible, then the map $h(x) = Mf(x+\alpha) + x + \beta$ on $\mathbb{F}_{2^n}$ is invertible for each $\alpha, \beta \in \mathbb{F}_{2^n}$. Moreover, its inverse is*

$$h^{-1}(x) = g^{-1}(x + \alpha + \beta) + \alpha.$$

Note that, for simplicity, we have denoted $M(f(x))$ by $Mf(x)$.

Proof. It suffices to check that $h^{-1}(h(x)) = x$. We have

$$\begin{aligned} h^{-1}(h(x)) &= g^{-1}(Mf(x+\alpha) + x + \beta + \alpha + \beta) + \alpha \\ &= g^{-1}(g(x+\alpha)) + \alpha = x. \qquad \square \end{aligned}$$

Lemma 2. *Let f be an arbitrary map on $\mathbb{F}_{2^n}$ and $\rho(x) = f(M(x)) + x$ be an invertible map on $\mathbb{F}_{2^n}$, where M is an invertible linear map on $\mathbb{F}_{2^n}$. Then, the map $\phi(x) = f(M(x) + \alpha) + x + \beta$ on $\mathbb{F}_{2^n}$ is invertible for each $\alpha, \beta \in \mathbb{F}_{2^n}$ and its inverse is*

$$\phi^{-1}(x) = \rho^{-1}(x + M^{-1}(\alpha) + \beta) + M^{-1}(\alpha).$$

Proof. We have

$$\begin{aligned} \phi^{-1}(\phi(x)) &= \rho^{-1}(f(M(x)+\alpha) + x + \beta + M^{-1}(\alpha) + \beta) + M^{-1}(\alpha) \\ &= \rho^{-1}(\rho(x + M^{-1}(\alpha))) + M^{-1}(\alpha) = x. \qquad \square \end{aligned}$$

Lemma 3. *Let $f = (g_1, g_2, g_3, g_4)$ be an invertible map on $(\mathbb{F}_{2^n})^4$, where g_i, $1 \le i \le 4$, are from $(\mathbb{F}_{2^n})^4$ to $\mathbb{F}_{2^n}$. Moreover, let $f^{-1} = (h_1, h_2, h_3, h_4)$ be such that $h_i : (\mathbb{F}_{2^n})^4 \to \mathbb{F}_{2^n}$, $1 \le i \le 4$, are parametric invertible in 1 variable. Then, g_i, $1 \le i \le 4$, are parametric invertible in 3 variables.*

Proof. Without loss of generality, suppose that g_1 is not parametric invertible in the first 3 variables. So,

$$g_1(a, b, c, t_1) = g_1(a, b, c, t_2) = x,$$

for some $a, b, c, t_1, t_2, x \in \mathbb{F}_{2^n}$, such that $t_1 \neq t_2$. Put $A = (a, b, c, t_1)$ and $B = (a, b, c, t_2)$. Then

$$f(A) = (x, g_2(A), g_3(A), g_4(A)), \qquad f(B) = (x, g_2(B), g_3(B), g_4(B)),$$

and

$$A = f^{-1}f(A) = (h_1(f(A)), h_2(f(A)), h_3(f(A)), h_4(f(A))),$$
$$B = f^{-1}f(B) = (h_1(f(B)), h_2(f(B)), h_3(f(B)), h_4(f(B))).$$

So,

$$h_1(f(A)) = h_1(f(B)) = a,$$
$$h_2(f(A)) = h_2(f(B)) = b,$$
$$h_3(f(A)) = h_3(f(B)) = c.$$

Now, from

$$h_1(x, g_2(A), g_3(A), g_4(A)) = h_1(x, g_2(B), g_3(B), g_4(B)) = a,$$

and parametric invertibility of h_1 in the first variable, we get $g_2(A) = g_2(B)$, $g_3(A) = g_3(B)$ and $g_4(A) = g_4(B)$. This means that $f(A) = f(B)$, which contradicts with invertibility of f. □

Theorem 1. *The map F on $\mathbb{F}_{2^n}^4$ with $F = (f_1, f_2, f_3, f_4)$ is MDS with $Br(F) = 5$ if F is invertible and all $i \times i$, $1 \leq i \leq 3$, families of sub-functions of F are parametric invertible.*

Proof. Suppose that F is not MDS and $Br(F) \leq 4$. Then, there exist $X, Y \in \mathbb{F}_{2^n}^4$, $X \neq Y$, such that

$$wt(X + Y) + wt(F(X) + F(Y)) \leq 4.$$

Suppose that $wt(X + Y) = s$. We distinguish 4 cases:
Case 1) $s = 4$: in this case, $wt(F(X) + F(Y)) = 0$, which means that F is not invertible.
Case 2) $s = 3$: without loss of generality, suppose that X and Y are distinct at their first 3 positions. By $wt(F(X) + F(Y)) \leq 1$, we deduce that $F(X)$ and $F(Y)$ are equal in at least 3 positions, say f_1, f_2 and f_3. This means that $F_t^{1,2,3}$ is not parametric invertible.
Case 3) $s = 2$: similar to Case 2, $F_{z,t}^{1,2}$ is not parametric invertible.
Case 4) $s = 1$: similar to Case 2, $F_{y,z,t}^{1}$ is not parametric invertible. □

Remark 1. It is worth noting that nonlinear MDS maps, i. e. such maps f on $\mathbb{F}_{2^n}$, for some natural n, with $deg(f) > 1$, are less studied up to now in the cryptographic literature. So, even the existence of them is an open problem. The interesting point here is that, it is straightforward to see that, any permutation f on $\mathbb{F}_{2^n}$ with $deg(f) > 1$ is a 1×1 nonlinear MDS map [4,16]. Also, consider the map ϕ on $\mathbb{F}_{2^n}^2$ with $\phi(x, y) = (x+y, x+f(y))$, where f is a map on $\mathbb{F}_{2^n}$. One can check that ϕ is a 2×2 nonlinear MDS map if f is an orthomorphism [10] on $\mathbb{F}_{2^n}$ with $deg(f) > 1$. In [11], nonlinear 4×4 MDS diffusion layers are presented based on the theory of T-functions. These maps are not defined on finite field $\mathbb{F}_{2^n}$ with $n > 1$. In [17], nonlinear and/or randomized 4×4 MDS diffusion layers are presented based on the theory of bi-partite rings and bi-epimorphisms. These maps are not defined on finite field $\mathbb{F}_{2^n}$ with $n > 1$.Our proposed diffusion layers are nonlinear over $\mathbb{F}_{2^n}$, $n > 1$.

Remark 2. The formal matrices (5) and (6) in Theorem 2, use the following notations:
a) We have $M(x)$ for a linear invertible map on $\mathbb{F}_{2^n}$, which we represent by M. For example $L^3 + L^2 + I$ in (6) means that the linear map $M(x) = L^3(x) + L^2(x) + x$ should be invertible.
b) We have $f(M(x)) + x$ which we denote by $f(M) + I$. This means that the map $\rho(x) = f(M(x) + \alpha) + x + \beta$ is invertible, for any parameters $\alpha, \beta \in \mathbb{F}_{2^n}$: obviously, we have used Lemma 2 to justify this representation.
c) We have $M(f(x)) + x$ which we represent by $Mf + I$. Similar to the case **b**, we use Lemma 1, here.

Theorem 2 is the main theorem of the current paper. In Section 4, we provide some concrete applications, based upon Theorem 2.

Theorem 2. *Let L and f be a linear and an arbitrary invertible map on $\mathbb{F}_{2^n}$, respectively. Define the map $F : \mathbb{F}_{2^n}^4 \to \mathbb{F}_{2^n}^4$ as*

$$F(x, y, z, t) = (X, Y, Z, T),$$

with

$$\begin{gathered} X = x + y + t + L(x + z) + f(y) + L(f(y)), \\ Y = x + z + t + L(x + t) + f(y) + L(f(y)), \\ Z = y + z + t + L(x + z + t) + L(f(y)), \\ T = x + y + z + L(z + t) + f(y). \end{gathered} \tag{3}$$

Then, F is an MDS map with branch number 5 on $\mathbb{F}_{2^n}$, if the following maps on $\mathbb{F}_{2^n}$ are invertible:

$$\begin{gathered}
L^3+I=(L+I)(L^2+L+I),\\
L^7+I=(L+I)(L^3+L+I)(L^3+L^2+I),\\
(L+I)f+I,\\
Lf+I,\\
f+I,\\
(L^2+L+I)f+I,\\
f(L^3+L^2+I)+I,\\
f(L^3+L^2+L)+I,\\
f(L^2+L+I)+I,\\
f(L^3+L+I)+I,\\
(L^{-1}+L+I)f+I,\\
(L^2+L+I)(L+I)^{-1}f+I,\\
L^2f+I.
\end{gathered}$$

Proof. By Theorem 1, we should verify the invertibility of F and parametric invertibility of all $i\times i$ sub-functions of F, $1\leq i\leq 3$. One can check that F is invertible and

$$F^{-1}(X,Y,Z,T)=(x,y,z,t),$$

with

$$\begin{gathered}
x=f(L^3(X+Y+T)+L^2(X+Y+Z)+L(Y+Z+T)+X+Z+T)+X+Y+T,\\
y=L^3(X+Y+T)+L^2(X+Y+Z)+L(Y+Z+T)+X+Z+T,\\
z=L^2(X+Y+T)+L(X+Y+Z)+Y+Z+T,\\
t=L(X+Y+T)+X+Y+Z.
\end{gathered}\tag{4}$$

To verify the parametric invertibility of 1×1 sub-functions of F, it suffices to consider the equations (3). For instance

$$F^1_{y,z,t}(x)=x+L(x)+\alpha,$$

is invertible if the map $x\to x+L(x)$ is invertible. Here

$$\alpha=y+t+L(z)+f(y)+L(f(y)),$$

is independent of x. Note that, this corresponds to the entry in the first row and the first column of the formal matrix (5), considering Remark 2.

$$\begin{pmatrix}
L+I & (L+I)f+I & L & I\\
L+I & (L+I)f & I & L+I\\
L & Lf+I & L+I & L+I\\
I & f+I & L+I & L
\end{pmatrix}.\tag{5}$$

The proof of invertibility for the remaining 1×1 sub-functions of F is done in a similar manner. A schematic representation of this 1×1 sub-functions is given

in the formal matrix (5).
To verify the parametric invertibility of 2×2 sub-functions of F, we consider the equations presented in the Appendix. For example, consider

$$F^{2,4}_{z,t}(x,y) = (x + L(x) + f(y) + Lf(y) + \alpha, x + y + f(y) + \beta),$$

where, $\alpha = z + t + L(t)$ and $\beta = z + L(z + t)$ are independent of x and y, respectively.Therefore, by (3), we should prove that the system of equations

$$\begin{gathered} x + L(x) + f(y) + L(f(y)) + \alpha = Y, \\ x + y + f(y) + \beta = T, \end{gathered}$$

has a unique solution (in variables x and y). Put $w = x+f(y)$. Then, $w+L(w) = \alpha + Y$ or $w = (L + I)^{-1}(\alpha + y)$. So

$$\begin{gathered} x + f(y) = (L + I)^{-1}(\alpha + y), \\ x + y + f(y) = \beta + T. \end{gathered}$$

Thus

$$\begin{gathered} y = \beta + T + (L + I)^{-1}(\alpha + y), \\ x = f(\beta + T + (L + I)^{-1}(\alpha + y)) + (L + I)^{-1}(\alpha + y). \end{gathered}$$

We have verified all the other 35 cases. The formula for these parametric invertible maps are given in the Appendix and the conditions for parametric invertibility of them is given in Table 1.
To check the invertibility of 3×3 sub-functions of F, we refer the reader to Lemma 3 and (4). All the 1×1 sub-functions of F^{-1} are given in the formal matrix (6), considering Remark 2.

$$\begin{pmatrix} f(L^3 + L^2 + I) + I & f(L^3 + L^2 + L) + I & f(L^2 + L + I) & f(L^3 + L + I) + I \\ L^3 + L^2 + I & L^3 + L^2 + L & L^2 + L + I & L^3 + L + I \\ L^2 + L & L^2 + L + I & L + I & L^2 + I \\ L + I & L + I & I & L \end{pmatrix} \tag{6}$$

□

Although our primary concern in the current paper is not investigating the efficiency of the proposed diffusion layers, but for completeness, we examine the implementation of F and F^{-1} in Algorithm 1 and Algorithm 2, respectively. Note that, the implementation costs of F and F^{-1} are nearly the same.
We present the $C++$ pseudo-code for implementation of (3) in Algorithm 1.

Algorithm 1 *Input:* (x, y, z, t),
Output: $(X, Y, Z, T) = F(x, y, z, t)$.

```
$x+ = f(y)$,
$y+ = L(z)$,
$z+ = L(t)$,
$t+=L(x)$,
$X=x+y+t$,
$Y=x+z+t$,
$Z=y+z+t$,
$T=x+y+z$.
```

The $C++$ pseudo-code for implementation of (4) is presented in Algorithm 2.

Algorithm 2 *Input:* (X,Y,Z,T),
Output: $(x,y,z,t)=F^{-1}(X,Y,Z,T)$.

```
$x=X+Y+T$,
$y=X+Z+T$,
$z=Y+Z+T$,
$t=X+Y+Z$,
$t+=L(x)$,
$z+=L(t)$,
$y+=L(z)$,
$x+=f(y)$.
```

As we stated, Theorem 2 lays a theoretical foundation for construction of applicable nonlinear 4 × 4 MDS diffusion layers. Nonlinear diffusion layers could make symmetric ciphers more resistant against statistical and algebraic attacks. Proposition 1 gives the algebraic degree of the proposed diffusion layer (also, see Remark 4). Here, we study linear and differential properties of the proposed diffusion layers. Regarding the definitions and notations of Section 2, one could verify the correctness of the following lemmas. We shall use them in the next section.

Lemma 4. *Let f be an arbitrary map on $\mathbb{F}_{2^n}$ and F be defined as in* Theorem 2. *For any $\alpha,\beta,\gamma,\delta,\alpha',\beta',\gamma',\delta'\in\mathbb{F}_{2^n}$ such that $(\alpha',\beta',\gamma',\delta')\neq(0,0,0,0)$, we have:*

$$L_F((\alpha,\beta,\gamma,\delta),(\alpha',\beta',\gamma',\delta'))=A\cup B,$$

where,

$$A=\{(x,y,z,t)\in\mathbb{F}_{2^n}^4:\psi_1\cdot x+\psi_3\cdot z+\psi_4\cdot t=0\ \&\ y\in L_f(\psi_2,\psi)\},$$

$$B=\{(x,y,z,t)\in\mathbb{F}_{2^n}^4:\psi_1\cdot x+\psi_3\cdot z+\psi_4\cdot t=1\ \&\ y\in L_f^C(\psi_2,\psi)\}.$$

and

$$\begin{gathered}\psi_1=\alpha+\alpha'+\beta'+\delta'+\alpha'^TL+\beta'^TL+\gamma'^TL,\\ \psi_2=\beta+\alpha'+\gamma'+\delta',\\ \psi_3=\gamma+\beta'+\gamma'+\delta'+\alpha'^TL+\gamma'^TL+\delta'^TL,\\ \psi_4=\delta+\alpha'+\beta'+\gamma'+\beta'^TL+\gamma'^TL+\delta'^TL,\\ \psi=\alpha'+\beta'+\delta'+\alpha'^TL+\beta'^TL+\gamma'^TL.\end{gathered}$$

Here, $L_f^C(\psi_2,\psi)$ is the complement of $L_f(\psi_2,\psi)$ and the superscript T stands for the transpose of a matrix.

Lemma 5. *Let f be an arbitrary map on $\mathbb{F}_{2^n}$ and F be defined as in* Theorem 2. *For any $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta' \in \mathbb{F}_{2^n}$ such that $(\alpha, \beta, \gamma, \delta) \neq (0, 0, 0, 0)$, we have:*

$$D_F((\alpha, \beta, \gamma, \delta), (\alpha', \beta', \gamma', \delta')) = D_f(\beta, \psi_1) \times D_f(\beta, \psi_2) \times D_f(\beta, \psi_3) \times D_f(\beta, \psi_4),$$

where, × is the Cartesian product and

$$\begin{aligned}\psi_1 &= (L+I)^{-1}(\alpha' + \alpha + \beta + \delta + L(\alpha + \gamma)),\\ \psi_2 &= (L+I)^{-1}(\beta' + \alpha + \gamma + \delta + L(\alpha + \delta)),\\ \psi_3 &= L^{-1}(\gamma' + \beta + \gamma + \delta + L(\alpha + \gamma + \delta)),\\ \psi_4 &= \delta' + \alpha + \beta + \gamma + L(\gamma + \delta).\end{aligned}$$

Remark 3. Suppose that M is an MDS matrix over $\mathbb{F}_{2^n}^4$, which induces a map $M : \mathbb{F}_{2^n}^4 \to \mathbb{F}_{2^n}^4$ with $M(X) = MX$. For every

$$A = (\alpha, \beta, \gamma, \delta),\ B = (\alpha', \beta', \gamma', \delta') \in \mathbb{F}_{2^n}^4,$$

such that $A \neq (0, 0, 0, 0)$, we have

$$Pr(M(X) + M(X + A) = B) = \begin{cases} 1 & B = MA \\ 0 & O.W. \end{cases}. \tag{7}$$

The main difference between an MDS matrix and a nonlinear MDS mapping like the one in Theorem 2, is that the differential probability (7) would take values other than 0 and 1, in the nonlinear case. This could impose more complexity in the cryptanalysis of symmetric ciphers. A concrete example shall be given in Section 4.

Remark 4. Note that the algebraic degree of the MDS mapping F defined in Theorem 2 is equal to $deg(f)$.

4 Concrete Examples of Nonlinear 4 × 4 MDS Diffusion Layers

In this section, we present some nonlinear 4×4 MDS diffusion layers, based upon the theoretical examinations of Section 3. The next theorem is proved in [2, 12].

Theorem 3. *Let $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and $\gamma \in \mathbb{F}_{2^n} \setminus \{0\}$. The map $g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $g(x) = x + \gamma\phi(x)$ is invertible if and only if γ is a 0-linear structure of ϕ.*

Based on Theorem 3, we prove the following theorem, which is used in construction of concrete examples of nonlinear 4 × 4 MDS diffusion layers for the use in symmetric cryptography.

Theorem 4. *Let V be the subspace generated by $S = \{\gamma_1, \ldots, \gamma_m\} \subseteq \mathbb{F}_{2^n}$ and $V_0, \ldots, V_{t-1}$ be the cosets of V, where $V_0 = V$ and $t = \frac{2^n}{|V|}$. Define $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $\phi|_{V_0} = 0$ and for $0 < i < t$, $\phi|_{V_i}$ is constant. Then, γ_i, $1 \leq i \leq m$, are 0-linear structures of ϕ.*

Proof. We must show that for any $x \in \mathbb{F}_{2^n}$ and $1 \leq i \leq m$, $\phi(x) = \phi(x+\gamma_i)$. Fix $1 \leq i \leq m$. If $x \in V_0 = V$, then $x, x+\gamma_i \in V$ and $\phi(x) = \phi(x+\gamma_i) = 0$. Now, suppose that $x \in V_j$, $0 < j < t$; then $x = \alpha + V$ for some $\alpha \in \mathbb{F}_{2^n}$ and $v \in V$. Since $x + \gamma_i = \alpha + (v + \gamma_i) = \alpha + v'$ for some $v' \in V$, so $\phi(x) = \phi(x+\gamma_i)$, due to the fact that ϕ is constant on V_j. □

The next example presents a family of maps $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ which makes the proposed diffusion layers in Theorem 2, MDS. The next proposition characterizes an algebraic degree for the maps used in Example 2.

Proposition 1. *Let g be a map on $\mathbb{F}_{2^n}$ with $deg(g) = d > 1$. Define $f(x) = x + \gamma g(x)$ on $\mathbb{F}_{2^n}$, where $\gamma \in \mathbb{F}_2 \setminus \{0\}$. Then, $deg(f) = d$.*

Proof. Let the polynomial representation of g be

$$g(x) = \sum_{i=0}^{2^n-1} a_i x^i.$$

We have $f(x) = x + \sum_{i=0}^{2^n-1} \gamma a_i x^i$. Suppose that $wt(j) = d$. Since $\gamma \neq 0$ and $d > 1$, the coefficient a_j dose not vanish and we have $deg(d) = d$. □

Example 2. Let $n \geq 8$ be a multiple of 4 and consider the map $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ with

$$\phi(x) = \begin{cases} 0 & x \in \mathbb{F}_{2^4}, \\ 1 & x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^4}. \end{cases}$$

Put $s = \frac{2^n-1}{15}$. One can check that

$$\phi(x) = \sum_{i=1}^{s-1} x^{15i}.$$

Let $\alpha \in \mathbb{F}_{2^4}$. Define $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as

$$f(x) = \alpha x + \phi(x) = \alpha x + \sum_{i=1}^{s-1} x^{15i}.$$

Suppose that $\beta \in \mathbb{F}_{2^4} \setminus \{\alpha^{-1}\}$. Consider the function g on $\mathbb{F}_{2^n}$ with

$$g(x) = \beta f(x) + x = (\alpha\beta + 1)x + \beta\phi(x).$$

The function g is invertible if and only if $(\alpha\beta+1)^{-1}g$ is invertible. We have

$$(\alpha\beta + 1)^{-1} g(x) = x + (\alpha\beta + 1)^{-1}\beta\phi(x).$$

Now, since $\alpha, \beta \in \mathbb{F}_2^4$, so $(\alpha\beta+1)^{-1}$ is a 0-linear structure of ϕ, by definition of ϕ and using the Theorem 4: note that, here, we have used the fact that $\beta \neq \alpha^{-1}$. Now, consider Theorem 2 and Example 2. Suppose that the linear map L in Theorem 2 is defined as $L(x) = \theta x$, where $\theta \in \mathbb{F}_2^4$, $\theta \neq 0$, $\theta^3 \neq 1$ and $\theta^7 \neq 1$.

One can check that, all of the required conditions of Theorem 2 are satisfied. For example, L^7+I should be invertible, which is equivalent to the fact that $\theta^7 \neq 1$. For another example, $Lf+I$ must be invertible, which is equivalent to invertibility of $x \to (\alpha\theta+1)x+\theta\phi(x)$, which in turn is equivalent to invertibility of the map $\theta(\alpha\theta+1)^{-1}x+\phi(x)$. Now, since $\alpha, \theta \in \mathbb{F}_2^4$, so, $\theta(\alpha\theta+1)^{-1} \in \mathbb{F}_2^4$ and by Theorem 4, $\theta(\alpha\theta+1)^{-1}$ is a 0-linear structure of ϕ.
Fix a $\rho \in \mathbb{F}_2^n$ and put $\alpha=\beta=\gamma=\delta=\rho \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^4}$ and $\alpha'=1$, $\beta'=1$, $\gamma'=\theta(\theta+1)^{-1}(\rho+1)+(\theta+1)\rho$ and $\delta'=(\theta+1)^{-1}(\rho+1)+\rho$. According to Lemma 5, we have

$$\psi_1=\psi_2=\psi_3=\psi_4=(\theta+1)^{-1}(\rho+1),$$

and

$$D_F((\rho,\rho,\rho,\rho),(\alpha',\beta',\gamma',\delta')=D_f(\rho,(\theta+1)^{-1}(\rho+1))^4.$$

Now, we have

$$D_f(\rho,(\theta+1)^{-1}(\rho+1))=A\cup B\cup C,$$

where,

$$A=\begin{cases}\mathbb{F}_{2^4} & \alpha\rho+1=(\theta+1)^{-1}(\rho+1),\\ \phi & O.W.\end{cases}$$

$$B=\begin{cases}\{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^4} : x+\rho\in\mathbb{F}_{2^4}\} & \alpha\rho+1=(\theta+1)^{-1}(\rho+1),\\ \phi & O.W.\end{cases}$$

$$C=\begin{cases}\{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^4} : x+\rho\notin\mathbb{F}_{2^4}\} & \alpha\rho=(\theta+1)^{-1}(\rho+1),\\ \phi & O.W.\end{cases}$$

Now, suppose that $\theta((\theta+1)\alpha+1)^{-1}\notin\mathbb{F}_{2^4}$ and $\alpha\rho+1=(\theta+1)^{-1}(\rho+1)$. So, we have

$$|D_f(\rho,(\theta+1)^{-1}(\rho+1))|=|A|+|B|=2^5.$$

Therefore,

$$Pr(F(x,y,z,t)+F(x+\rho,y+\rho,z+\rho,t+\rho)=(\theta+1)^{-1}(\rho+1))=\frac{(2^5)^4}{2^{4n}}=2^{20-4n}.$$

This shows that, in any differential cryptanalysis using the corresponding differences on a symmetric cipher which applies the proposed diffusion layer in its design, a factor of 2^{20} would be multiplied by the complexity of the attack. Note that, as stated in Remark 1, this is impossible in the case that we have an MDS matrix (which is linear). A similar discussion could be done for linear cryptanalysis. On the other hand, by Remark 2 and proposition 1, the algebraic degree of F in Theorem 2 is equal to 4, for the mapping f in Example 2. Compare this degree with the algebraic degree 1 for any MDS matrix. This shows that a nonlinear MDS mapping could be more resistant against algebraic cryptanalysis, in comparison to the classic (linear) MDS matrices.

5 Conclusion

In this paper, we study nonlinear diffusion layers. We present a family of 4 × 4 nonlinear MDS diffusion layers, based upon a mathematical investigation on some special maps over $\mathbb{F}_{2^n}$. Then, we compute the differential and Walsh spectrum along with the algebraic degree of the proposed mappings.
As Liu, Rijmen and Leander stated in 2018, by use of the presented nonlinear diffusion layers in the design of modern symmetric ciphers, they could be more resistant against various kinds of cryptanalysis. Applying these components in the design of block ciphers, stream ciphers, hash functions and authenticated encryption schemes could be a good line of research in the continuation of the studies of this paper.

References

1. D. Augot and M. Finiasz. *Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions.* ISIT, 1551-1555, 2013.
2. P. Charpin and G. M. M. Kyureghyan. *When does $G(x)+\gamma Tr(H(x))$ permute $\mathbb{F}_{p^n}$?* Finite Fields and Their Applications, 15, 5, 615–632, 2009.
3. Y. Crama and P. L. Hammer. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* Cambridge University Press, 2010.
4. J. Daemen and V. Rijmen. *The Design of Rijndael: AES.* The Advanced Encryption Standard. Information Security and Cryptography. Springer, 2002.
5. S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad. *Characterization of MDS mappings.* IACR Cryptology ePrint Archive, Report 2015/002, 2015.
6. X. D. Dong, C. B. Son and E. Gunawan. *Matrix characterization of MDS linear codes over modules.* Linear Algebra and its Applications, 277(1-3), 1998.
7. ETSI/SAGE Specification. *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3. Document 2: ZUC Specification.* Version: 1.6. June 28, 2011.
8. P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlffer and S. S. Thomsen. *Grostl - a SHA-3 candidate.* Symmetric Cryptography 2009.
9. Z. Guo, R. Liu, W. Wu and D. Lin. *Direct construction of lightweight rotational-xor MDS diffusion layers.* IACR Cryptology ePrint Archive, Report 2016/1036, 2016.
10. H. Han, X. Xu and S. Zhu. *The Properties of Orthomorphisms on the Galois Field.* Maxwell Scientific Organization, 2013.
11. A. Klimov. *Applications of T-functions in Cryptography.* Thesis for the degree of Ph.D., Weizmann Institute of Science, 2005.
12. G. M. M. Kyureghyan. *Constructing permutations of finite fields via linear translators.* J. Comb. Theory, Ser. A, 118, 1052–1061, 2011.
13. Y. Liu, V. Rijmen and G. Leander. *Nonlinear diffusion layers.* Designs, Codes and Cryptography, 20, Jan, 2018.
14. M. Liu and S. M. Sim. *Lightweight MDS generalized circulant matrices.* In Fast Software Encryption 23rd International Conference. FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers, pages 101-120, 2016.
15. Y. Li and M. Wang. *On the Construction of Lightweight Circulant Involutory MDS Matrices.* Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers.

16. S. Ling and Ch. Xing. *Coding Theory: A First Course.* Cambridge University Press, 2004.
17. M. R. Mirzaee Shamsabad and S. M. Dehnavi *Randomized Nonlinear Software-oriented MDS Diffusion Layers.* Groups Complexity Cryptology 11(2): 123-131 (2019)
18. M. Sajadieh, M. Dakhilalian, H. Mala and P. Sepehrdad. *Efficient recursive diffusion layers for block ciphers and hash functions.* J. Cryptology, 28(2):240-256, 2015.
19. S. Sarkar and H. Syed. *Lightweight Diffusion Layer: Importance of Toeplitz Matrices.* IACR Trans. Symmetric Cryptol., 2016, 1, 95–113, 2016.
20. J. Stern and S. Vaudenay. *CS-Cipher.* Fast Software Encryption, 5th International Workshop, FSE '98, 1998.
21. S. Vaudenay. *On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER0.* In B. Preenel, editor, Fast Software Encryption. Proceedings, LNCS 1008, (1995), 286-297.

Appendix

$$\begin{gathered}
F^{1,2}_{x,y}(z,t) = (t + L(z) + \alpha, z + t + L(t) + \beta) \\
F^{1,2}_{x,z}(y,t) = (y + t + f(y) + Lf(y) + \alpha, t + L(t) + f(y) + Lf(y) + \beta) \\
F^{1,2}_{x,t}(y,z) = (y + L(z) + f(y) + Lf(y) + \alpha, z + f(y) + Lf(y) + \beta) \\
F^{1,2}_{y,z}(x,t) = (x + L(x) + t + \alpha, L(x) + t + L(t) + \beta) \\
F^{1,2}_{y,t}(x,z) = (x + L(x) + L(z) + \alpha, x + L(x) + L(z) + \beta) \\
F^{1,2}_{z,t}(x,y) = (x + L(x) + y + f(y) + Lf(y) + \alpha, x + L(x) + f(y) + Lf(y) + \beta)
\end{gathered}$$

$$\begin{gathered}
F^{1,3}_{x,y}(z,t) = (t + L(z) + \alpha, z + L(z) + t + L(t) + \beta) \\
F^{1,3}_{x,z}(y,t) = (y + t + f(y) + Lf(y) + \alpha, y + t + L(t) + Lf(y) + \beta) \\
F^{1,3}_{x,t}(y,z) = (y + L(z) + f(y) + Lf(y) + \alpha, y + z + L(z) + Lf(y) + \beta) \\
F^{1,3}_{y,z}(x,t) = (x + L(x) + t + \alpha, L(x) + t + L(t) + \beta) \\
F^{1,3}_{y,t}(x,z) = (x + L(x) + L(z) + \alpha, x + L(x) + L(z) + \beta) \\
F^{1,3}_{z,t}(x,y) = (x + L(x) + y + f(y) + Lf(y) + \alpha, L(x) + y + Lf(y) + \beta)
\end{gathered}$$

$$\begin{gathered}
F^{1,4}_{x,y}(z,t) = (L(z) + t + \alpha, z + L(z) + L(t) + \beta) \\
F^{1,4}_{x,z}(y,t) = (y + t + f(y) + Lf(y) + \alpha, y + L(t) + f(y) + \beta) \\
F^{1,4}_{x,t}(y,z) = (y + L(z) + f(y) + Lf(y) + \alpha, y + z + L(z) + f(y) + \beta) \\
F^{1,4}_{y,z}(x,t) = (x + L(x) + t + \alpha, x + L(t) + \beta) \\
F^{1,4}_{y,t}(x,z) = (x + L(x) + L(z) + \alpha, x + z + L(z) + \beta) \\
F^{1,4}_{z,t}(x,y) = (x + L(x) + y + f(y) + Lf(y) + \alpha, x + y + f(y) + \beta)
\end{gathered}$$

$$\begin{gathered}
F^{2,3}_{x,y}(z,t) = (z + t + L(t) + \alpha, z + L(z) + t + L(t) + \beta) \\
F^{2,3}_{x,z}(y,t) = (t + L(t) + f(y) + Lf(y) + \alpha, y + t + L(t) + Lf(y) + \beta) \\
F^{2,3}_{x,t}(y,z) = (z + f(y) + Lf(y) + \alpha, y + z + L(z) + Lf(y) + \beta) \\
F^{2,3}_{y,z}(x,t) = (x + L(x) + t + L(t) + \alpha, L(x) + t + L(t) + \beta) \\
F^{2,3}_{y,t}(x,z) = (x + L(x) + z + \alpha, L(x) + z + L(z) + \beta) \\
F^{2,3}_{z,t}(x,y) = (x + L(x) + f(y) + Lf(y) + \alpha, L(x) + y + Lf(y) + \beta)
\end{gathered}$$

$$\begin{gathered}
F^{2,4}_{x,y}(z,t) = z + t + L(t) + \alpha, z + L(z) + L(t) + \beta) \\
F^{2,4}_{x,z}(y,t) = (t + L(t) + f(y) + Lf(y) + \alpha, y + L(t) + f(y) + \beta) \\
F^{2,4}_{x,t}(y,z) = (z + f(y) + Lf(y) + \alpha, y + z + L(z) + f(y) + \beta) \\
F^{2,4}_{y,z}(x,t) = (x + L(x) + t + L(t) + \alpha, x + L(t) + \beta) \\
F^{2,4}_{y,t}(x,z) = (x + L(x) + z + \alpha, x + z + L(z) + \beta) \\
F^{2,4}_{z,t}(x,y) = (x + L(x) + f(y) + Lf(y) + \alpha, x + y + f(y) + \beta)
\end{gathered}$$

$$\begin{gathered}
F^{3,4}_{x,y}(z,t) = z + L(z) + t + L(t) + \alpha, z + L(z) + L(t) + \beta) \\
F^{3,4}_{x,z}(y,t) = (y + t + L(t) + Lf(y) + \alpha, y + L(t) + f(y) + \beta) \\
F^{3,4}_{x,t}(y,z) = (y + Lf(y) + z + L(z) + \alpha, y + z + L(z) + f(y) + \beta) \\
F^{3,4}_{y,z}(x,t) = (L(x) + t + L(t) + \alpha, x + L(t) + \beta) \\
F^{3,4}_{y,t}(x,z) = (L(x) + z + L(z)\alpha, x + z + L(z) + \beta) \\
F^{3,4}_{z,t}(x,y) = (L(x) + y + Lf(y) + \alpha, x + y + f(y) + \beta)
\end{gathered}$$

Table 1. The conditions for parametric invertibility of all 2×2 sub-functions of F: here, for instance row $(1,2)$ and column (x,y) present such conditions for $F^{1,2}_{x,y}(z,t)$

	(x,y)	(x,z)	(x,t)	(y,z)	(y,t)	(z,t)
$(1,2)$	$L+I$	$L+I$	$L, L+I$	f, L^2+L+I	$L+I, Lf+I$	L^2+L+I
$(1,3)$	L	$-$	L^2+L+I	$f+I, L$	$(L^{-1}+L+I)f+I$	$L+I$
$(1,4)$	L	L^2+L+I	L^2+L+I	$L, (L^2+L+I)f+I$	$(L^2+L+I)(L+I)^{-1}f+I$	L^2+L+I
$(2,3)$	$L+I$	L^2+L+I	$L+I$	$(L^2+L+I)f+I$	$f+I, L+I$	$L, L+I$
$(2,4)$	$L, L+I$	L	$L+I$	L^2f+I	$L+I, (L+I)f+I$	L^2+L+I
$(3,4)$	$L+I$	$L+I$	L^2+L+I	$f, L+I$	$(L^2+L+I)f+I$	$L+I$