Lightweight Dynamic Linear Components for Symmetric Cryptography

S. M. Dehnavi, M. R. Mirzaee Shamsabad

1 Kharazmi University, Iran,dehnavism@ipm.ir
2 Shahid Beheshti University, Iran,m_mirzaee@sbu.ac.ir

Abstract. In this paper, using the concept of equivalence of mappings we characterize all of the one-XOR matrices which are used in hardware applications and propose a family of lightweight linear mappings for software-oriented applications in symmetric cryptography. Then, we investigate interleaved linear mappings and based upon this study, we present generalized dynamic primitive LFSRs along with dynamic linear components for construction of diffusion layers.

From the mathematical viewpoint, this paper presents involutive sparse binary matrices as well as sparse binary matrices with sparse inverses. Another interesting result of our investigation is that, by our characterization of one-XOR matrices, the search space for finding a k such that $x^n + x^k + 1$ is a primitive trinomial could be reduced.

Keywords: One-XOR matrix, Linear Dynamic Component, Hardware implementation, Software implementation, Generalized LFSR, Diffusion layer, Primitive trinomial

1 Introduction

Linear mappings have many applications in symmetric cryptography. For example, LFSRs are linear mappings which are used extensively in stream ciphers to provide a sequence with a desirably long period and good statistical properties [6, 18]. As another example, the diffusion layers of many symmetric ciphers such as block ciphers, stream ciphers, hash functions and authenticated encryption schemes use linear mappings of desired branch numbers [2, 7, 9, 10]. These linear diffusion layers usually apply some component linear mappings: the lighter are these component mappings, the lighter would be the diffusion layer.

The component linear mappings of lightweight symmetric ciphers should be implemented in the target platforms (hardware and/or software) with a low implementation cost [17, 14, 9, 10]. Some papers study the concept of optimizing the implementation of MDS matrices from various aspects [1, 12, 11, 13]. In [1] the authors investigate lightweight multiplication in $\mathbb{F}_{2^n}$. They study the mappings $x \to \alpha x$ in the field $\mathbb{F}_{2^n}$ and present such elements with the lightest implementation in hardware: one-XOR or two-XOR component matrices. In [12], the study of one-XOR and two-XOR matrices for the use in symmetric cryptography is continued and a conjecture from [1] is proved. The paper [11] continues these examinations and proves another conjecture from [1]. In this paper, we investigate this topic from another viewpoint and somehow more generally: our results are independent of the field $\mathbb{F}_{2^n}$, $n > 1$. Based on the concept of equivalence of matrices, we characterize all the one-XOR matrices for hardware applications.

Then, after investigating a family of software-oriented lightweight linear mappings for the use in symmetric cryptography, we examine interleaved linear mappings and based on this concept, we propose lightweight and/or dynamic linear mappings for the use in software implementations. Most notably, based upon a previous representation of the ring of binary matrices [16], we present a variety of linear components with provable properties for construction of software-oriented diffusion layers.

As for another application, we present generalized dynamic primitive LFSRs along with dynamic component mappings for hardware and/or software applications. The dynamic components could be used in the design of lightweight diffusion layers such as MDS diffusion layers. These kind of component mappings could make symmetric ciphers more resistant against cryptanalysis [15, 4].

As a mathematical result, the current paper presents sparse involutive matrices as well as sparse matrices wirth a sparse inverse. Another interesting result of this paper is that, by our characterization of one-XOR matrices, the search space for finding a k such that the trinomial $x^n + x^k + 1$ is primitive, could be reduced.

2 Preliminary Notations and Definitions

In this paper, we use the usual notation $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. The inverse of a permutation P is denoted by P^{-1}. The r-times composition of the function P with itself is denoted by P^r. We denote by $\mathcal{M}_n(\mathbb{F}_2)$ the set (ring) of all $n \times n$ bibary matrices.

The operation of XOR is denoted by $+$ and the AND operation as well as the composition of permutations are denoted by juxtaposition of symbols. The finite field with 2 elements is denoted by $\mathbb{F}_2$ and the n-dimensional linear space over $\mathbb{F}_2$ by $\mathbb{F}_2^n$. The right cyclic shift or rotation $x \ggg i$ is denoted by x^i. We denote the zero vector by $\mathbf{0}$, the all-one vector by $\mathbf{1}$ and every identity matrix by I.

Let $X \in \mathbb{F}_2^{mk}$ be a vector over $\mathbb{F}_2^m$; i.e. $X = (X_{k-1}, \cdots, X_0)$, where $X_i \in \mathbb{F}_2^m$, $0 \le i < k$. The weight of X with respect to m-bit words is denoted by $\mathbf{w}_m(X)$ and is defined as

$$\mathbf{w}_m(X) = |\{i : 0 \le i < k, X_i \neq \mathbf{0}\}|.$$

The matrix $A \in \mathcal{M}_n(\mathbb{F}_2)$, $n = mk$, could also be represented as follows

$$A = [A_{i,j}]_{k \times k}, \quad A_{i,j} \in \mathcal{M}_m(\mathbb{F}_2), \quad 1 \le i, j \le k. \tag{1}$$

The (differential) branch number of A with respect to m-bit words is defined as

$$\mathcal{B}_d^m(A) = \min_{X \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} \{\mathbf{w}_m(X) + \mathbf{w}_m(AX^T)\},$$

where X^T is the transpose of X and the linear branch number of A with respect to m-bit words as

$$\mathcal{B}_l^m(A) = \min_{X \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} \{\mathbf{w}_m(X) + \mathbf{w}_m(A^T X^T)\}.$$

For a linear mapping $A \in \mathcal{M}_n(\mathbb{F}_2)$, we denote the order of A i.e. the least integer m such that $A^m = I$, by $\mathcal{O}(A)$ and the number of fixed points of A, i.e. the number of $X \in \mathbb{F}_2^n$ such that $AX = X$, by $\mathcal{F}(A)$.

Let n be a natural number and $\mathfrak{p}$ be a permutation of $\mathbb{Z}_n$. The permutation $\mathfrak{p}$ induces a permutation P on $\mathbb{F}_2^n$ with

$$P(x_{n-1}, \ldots, x_0) = (x_{\mathfrak{p}(n-1)}, \ldots, x_{\mathfrak{p}(0)}).$$

Hereafter, we call such a mapping P a *coordinate permuting permutation* on $\mathbb{F}_2^n$ and denote the set of all such permutations by $\mathcal{P}(\mathbb{F}_2^n)$. Further, we call $\mathfrak{p}$ the *base permutation* of P.

Let A be a finite set and P be a permutation of A. It is well-known that P could be decomposed into disjoint cycles D_i, $1 \leq i \leq z$, for some z. In this case, we write

$$P = D_1 D_2 \dots D_z,$$

where $D_i = (d_{i,1}, \dots, d_{i,t_i})$, $1 \leq i \leq z$, such that $P(d_{i,r}) = d_{i,r+1}$, for $1 \leq r < t_i$ and $P(d_{i,t_i}) = d_{i,1}$. In the case that $z = 1$ we call P a single cycle or say that P is a single-cycle permutation.
Let P and Q be permutations on A and

$$P = D_1 D_2 \dots D_z,$$

$$Q = D'_1 D'_2 \dots D'_{z'},$$

with $|D_i| = t_i$, $1 \leq i \leq z$, and $|D'_j| = t'_j$, $1 \leq j \leq z'$. Now, suppose that we have $z = z'$ and (possibly permuting D_i's) we have $t_i = t'_i$, $1 \leq i \leq z$. In this case, P and Q have the same cyclic structure: we write $P \equiv Q$.
Let P and H be permutations of a finite set A. We denote the permutation HPH^{-1} by P_H. It is well-known that $P \equiv P_H$. This notation shall be used extensively in the sequel.
Let j be a non-negative integer. We define $e_j = (x_{n-1}, \dots, x_j, \dots, x_0)$ with

$$x_i = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

We also define $I^{j,k}$ on $\mathbb{F}_2^n$ as follows

$$I^{j,k}(x_{n-1}, \dots, x_0) = (x_{r_{n-1}}, \dots, x_{r_0}),$$

where

$$r_t = \begin{cases} t & t \neq j, k, \\ k & t = j, \\ j & t = k. \end{cases}$$

In [16], an equivalent representation for the set of all $n \times n$ binary matrices $\mathcal{M}_n(\mathbb{F}_2)$ is given. We denote by $\mathfrak{R}_n$ the ring presented in [16] which is isomorphic to the ring of all $n \times n$ binary matrices. Suppose that $\mathfrak{p}$ is a single-cycle permutation on $\mathbb{Z}_n$. In the same manner as done in [16], we see that another ring isomorphic to the ring of all $n \times n$ binary matrices could be defined with the aid of $\mathfrak{p}$ which we denote by $\mathfrak{R}_n^{\mathfrak{p}}$. The addition and multiplication in $\mathfrak{R}_n^{\mathfrak{p}}$ shall be demonstrated through the following example. Note that we show the effect of $\mathfrak{p}$ on x by $x^{\mathfrak{p}}$, and we have $x^{\mathfrak{p}^i} x^{\mathfrak{p}^j} = x^{\mathfrak{p}^t}$, $t = i + j \ mod \ n$.

Example 1. Suppose that

$$r_1 = ax^{\mathfrak{p}^2} + bx^{\mathfrak{p}} + c,$$

$$r_2 = dx^{\mathfrak{p}} + e.$$

Then, in $\mathfrak{R}_n^{\mathfrak{p}}$, we have

$$r_1 + r_2 = ax^{\mathfrak{p}^2} + (b + d)x^{\mathfrak{p}} + (c + e),$$

and

$$r_1 r_2 = ad^{\mathfrak{p}^2} x^{\mathfrak{p}^3} + (ae^{\mathfrak{p}^2} + bd^{\mathfrak{p}})x^{\mathfrak{p}^2} + (be^{\mathfrak{p}} + cd)x^{\mathfrak{p}} + ce.$$

This means that if we define $f_1(x) = aP^2(x) + bP(x) + cx$ and $f_2(x) = dP(x) + ex$, such that $\mathfrak{p}$ is the base permutation of P, then we have

$$f_1(f_2(x)) = ad^{\mathfrak{p}^2} P^3(x) + (ae^{\mathfrak{p}^2} + bd^{\mathfrak{p}})P^2(x) + (be^{\mathfrak{p}} + cd)P(x) + (ce)x.$$

Here, for example we have $a^{\mathfrak{p}^2} := P^2(a)$.

In the case of hardware applications, the lightest linear matrices are obviously one-XOR matrices; i.e. matrices that could be implemented by only one XOR in hardware. One can check that all the one-XOR $n \times n$ binary matrices could be represented as follows

$$f(x) = P(x) + e_j I^{j,k}(x).$$

We use this representation extensively in the sequel.
In the case of software-oriented applications, the lightest ones or one category of the lightest ones (which satisfy good cryptographic propeties) are of the form

$$f(x) = (x \ggg i) \oplus (c \wedge x),$$

which is equivalent to the element $x^i + c$ in the ring $\mathfrak{R}_n$. We also use this representation, hereafter.
Let L be a linear mapping defined on $\mathbb{F}_2^n$. We call L a primitive mapping, if the consecutive outputs of L (refrain from $\mathbf{0}$) construct a single cycle of length $2^n - 1$. The companion matrices of primitive LFSR's are well-known examples of primitive linear mappings.

3 Lightweight and/or dynamic linear components

In this section, based on the idea of equivalence of mappings we investigate hardware-oriented as well as software-oriented lightweight linear mappings. These lightweight mappings could be used as components in (lightweight) symmetric ciphers. Also, after examining interleaved linear mappings, dynamic components for the use in symmetric ciphers are presented.

3.1 Algebra of lightweight mappings

In this subsection, we lay a mathematical foundation for the next two subsections. Firstly, we give a lemma concerning the invertibility of linear mappings.

Lemma 1. *Let $P \in \mathcal{P}(\mathbb{F}_2^n)$ with the base permutation $\mathfrak{p} \in \mathbb{Z}_n$ and let $c \in \mathbb{F}_2^n$. Consider the function $f(x) = P(x) + cx$ on $\mathbb{F}_2^n$. Let $\mathfrak{p} = D_1 D_2 \ldots D_z$, with*

$$D_i = (D_{i,1}, \ldots, D_{i,t_i}), \quad 1 \leq i \leq z,$$

and

$$\mathbf{c}_i = (c_{D_{i,1}}, \ldots, c_{D_{i,t_i}}), \quad 1 \leq i \leq z.$$

In fact, $\mathbf{c}_i$'s are bitwise nonregular segments of c, corresponding to cyclic decomposition of $\mathfrak{p}$. In this case, f is invertible iff for each $1 \leq i \leq z$, we have $\mathbf{c}_i \neq \mathbf{1}$.

Proof. Without loss of generality, we prove the theorem for a permutation D with the single-cycle base permutation $\mathfrak{d}$, $|\mathfrak{d}| = t$. Since f is linear, we must prove that if $D(x)+cx = \mathbf{0}$, then $x = \mathbf{0}$. We have

$$\begin{cases} x_{(0)} + c_0 x_0 = 0, \\ x_{\mathfrak{d}(1)} + c_1 x_1 = 0, \\ \vdots \\ x_{\mathfrak{d}(t-1)} + c_{t-1} x_{t-1} = 0. \end{cases} \tag{2}$$

At first, suppose that $c = \mathbf{1}$. In this case $x = \mathbf{1}$ is a non-zero solution of the system of Equation 2, or equivalently, $x = \mathbf{1}$ is a solution of $f(x) = \mathbf{0}$. This means that f is not invertible. Conversely, suppose that at least one coordinate in c, say c_r, $1 \leq r \leq t$, is zero: $c_r = 0$. So, we have $x_{\mathfrak{d}(r)} = 0$. It follows that $x_{\mathfrak{d}^{(2)}(r)} = 0$, $x_{\mathfrak{d}^{(3)}(r)} = 0$, and so on. Since $\mathfrak{d}$ is a single cycle, we deduce that $x = \mathbf{0}$. □

Let P and Q be permutations on $\mathbb{F}_2^n$. It is obvious that $f(x) = P(x) + cQ(x)$ on $\mathbb{F}_2^n$ is invertible iff the function $g(x) = f(Q^{-1}(x))$ is invertible. So, we have the next corollary.

Corollary 1. *Suppose that $P, Q \in \mathcal{P}(\mathbb{F}_2^n)$ with corresponding base permutations $\mathfrak{p}, \mathfrak{q} \in \mathbb{Z}_n$ and let $c \in \mathbb{F}_2^n$. Consider the function $f(x) = P(x) + cQ(x)$ on $\mathbb{F}_2^n$. Let*

$$\mathfrak{p}\mathfrak{q}^{-1} = D_1 D_2 \dots D_z,$$

where D_i's, $1 \leq i \leq z$, are disjoint cycles in cyclic decopmposition of $\mathfrak{p}\mathfrak{q}^{-1}$. Let

$$D_i = (D_{i,1}, \dots, D_{i,t_i}), \quad 1 \leq i \leq z,$$

and

$$\mathbf{c}_i = (c_{D_{i,1}}, \dots, c_{D_{i,t_i}}), \quad 1 \leq i \leq z.$$

Then, f is invertible iff for each $1 \leq i \leq z$, we have $\mathbf{c}_i \neq \mathbf{1}$.

In the following lemma, we give a sufficient condition for invertibility of a special kind of lightweight mappings which have a lightweight inverse. We also give the direct form of their inverses.

Lemma 2. *Suppose that $P, Q \in \mathcal{P}(\mathbb{F}_2^n)$ with base permutations $\mathfrak{p}, \mathfrak{q}$ and let $c \in \mathbb{F}_2^n$. Consider the function $f(x) = P(x) + cQ(x)$ on $\mathbb{F}_2^n$. Suppose that $R = QP^{-1}$ with base permutation $\mathfrak{r}$. If $cc^{\mathfrak{r}} = \mathbf{0}$, then f is invertible and its inverse is*

$$f^{-1}(x) = P^{-1}(x) + c^{\mathfrak{p}^{-1}} P^{-1}QP^{-1}(x).$$

Note that, as stated in Section 2, $c^{\mathfrak{r}}$ stands for $R(c)$.

Proof. Simply, we see that

$$\begin{aligned} f(f^{-1}(x)) &= P(P^{-1}(x) + c^{\mathfrak{p}^{-1}} P^{-1}QP^{-1}(x)) \\ &\quad + cQ(P^{-1}(x) + c^{\mathfrak{p}^{-1}} P^{-1}QP^{-1}(x)) \\ &= x + cR(x) + cR(x) + cc^{\mathfrak{r}} R^2(x) \\ &= x + cc^{\mathfrak{r}} R^2(x) = x, \end{aligned}$$

because $cc^{\mathfrak{r}} = \mathbf{0}$. □

Remark 1. In Lemma 2, put $P = I$. Then, we have a sparse involutive linear mapping $f(x) = x + cQ(x)$, provided that $cc^{\mathfrak{q}} = \mathbf{0}$. It is not hard to see that the number of ones in the binary matrix representing f is less than $2n$ and each matrix in this family of matrices could be implemented with at most $n - 1$ XORs.

Remark 2. We know that the inverse of a sparse matrix is not sparse in general. An interesting result of Lemma 2 is providing a large family of invertible sparse matrices with sparse inverses. It is straightforward to see that the number of ones in the the binary matrix representing f as well as its inverse is less than $2n$ and they could be implemented with at most $n - 1$ XORs.

The proof of next theorem is not hard.

Theorem 1. *Fix $P, Q \in \mathcal{P}(\mathbb{F}_2^n)$ with corresponding base permutations $\mathfrak{p}$ and $\mathfrak{q}$ and let $c \in \mathbb{F}_2^n$. Consider the function $f(x) = P(x) + cQ(x)$ on $\mathbb{F}_2^n$. Let $\mathfrak{p}\mathfrak{q}^{-1} = D_1 D_2 \dots D_z$, with*

$$D_i = (D_{i,1}, \dots, D_{i,t_i}), \quad 1 \leq i \leq z.$$

Then, there are exactly

$$\prod_{i=1}^{z} (2^{t_i} - 1)$$

many $c \in \mathbb{F}_2^n$ such that f is invertible.

Based upon the previous lemma, we have the following corollary.

Corollary 2. *Consider the function $f(x) = x^i + cx$ on $\mathbb{F}_2^n$, where $x^i = x \ggg i$, as stated in the notations. Then, f is invertible if $cc^i = \mathbf{0}$. In this case we have*

$$f^{-1}(x) = x^{-i} + c^{-i}x^{-2i}.$$

Note that the indices are computed modulo n, in the previous corollary. Also, in the next corollary, $j - i$ and $2j - 2i$ are computed modulo n.

Corollary 3. *Consider the function $f(x) = x^i + cx^j$ on $\mathbb{F}_2^t$. Then f is invertible if $cc^{j-i} = \mathbf{0}$. In this case, we have*

$$f^{-1}(x) = x^{j-i} + c^{j-i}x^{2j-2i}.$$

Similar to the method provided in [3], the next theorem could be proved.

Theorem 2. *Fix $1 \leq i, j < 2^t$ such that $i - j$ is odd. Then, the function $f(x) = x^i + cx^j$ on $\mathbb{F}_2^t$ with $c \in \mathbb{F}_2^t$ is invertible for exactly $F_{2^t+1} + F_{2^t-1}$ number of c's. Here, F_i denotes the i-th Fibonacci number: $F_1 = F_2 = 1$ and*

$$F_i = F_{i-1} + F_{i+1}, \quad i > 2.$$

Now, we show the applicability of the concept of equivalence, for construction of mappings useful in symmetric cryptography.

Theorem 3. *Let $L, M \in \mathcal{M}_n(\mathbb{F}_2)$. Note that we identfy these matrices with their corresponding linear mappings on $\mathbb{F}_2^n$. Let $L \equiv M$ and suppose that $L^r + I$ is invertible for some r. Then, $M^r + I$ is also invertible.*

Proof. Suppose that $M^r + I$ is not invertible. So we have $M^r(x) + x = 0$ for some nonzero $x \in \mathbb{F}_2^n$. It follows that $M^r(x) = x$, which means that x is on a cycle of length t such that t is a divisor of r. Since $L \equiv M$, so L has also a cycle of length t. Suppose that $y \neq \mathbf{0}$ is on this cycle. It follows that $L^t(y) = y$, or $L^r(y) = y$. We deduce that $L^r(y) + y = 0$ for a nonzero y. Therefore, $L^r + I$ is not invertible, which is a contradiction. □

Corollary 4. *Let L and M be two linear mappings on $\mathbb{F}_2^n$ with $L \equiv M$. Suppose that for any r_i, $1 \leq i \leq n$, the linear mapping $L^{r_i} + I$ is invertible. In this case, for every r_i, $1 \leq i \leq n$, the linear mapping $M^{r_i} + I$ would also be invertible.*

Remark 3. In Table 1 of [14], some mappings presented with the property that $L^{2^i} + I$ are invertible for $0 \leq i < 14$. Now, suppose that L is a fixed matrix of this table. Then, any matrix $M \equiv L$ also satisfies the presented property, i.e. $M^{2^i} + I$ is invertible. Now, we can see that, based on the concepts presented up to now, there are a lot of lightweight matrices which are equivalent to L. This provides more flexibility and a vast variety of matrices for the designers of (lightweight) symmetric ciphers

The proof of next corollary is straightforward.

Corollary 5. *Let L and M be two linear mappings on $\mathbb{F}_2^n$ with $L \equiv M$. Suppose that L is primitive. Then, M is also primitive.*

Remark 4. Similar to the case of the Remark 3, Corollary 5 presents a variety of primitive linear mappings through the concept of equivalence.

The following lemma illustrates the crucial application of the concept of equivalence in symmetric cryptography.

Lemma 3. *Consider the function $f(x) = P(x) + cQ(x)$ with $P, Q \in \mathcal{P}(\mathbb{F}_2^n)$ and $c \in \mathbb{F}_2^n$. Let $H \in \mathcal{P}(\mathbb{F}_2^n)$ with base permutation $\mathfrak{h}$. Then we have*

$$f_H(x) = P_H(x) + c^{\mathfrak{h}} Q_H(x).$$

Proof. Since P, Q and H are linear, we have

$$f_H(x) = HfH^{-1}(x) = H(PH^{-1}(x) + cQH^{-1}(x))$$

$$= HPH^{-1}(x) + H(c)HQH^{-1}(x) = P_H + c^{\mathfrak{h}} Q_H(x).$$

□

Lemma 3 shows that for a given mapping of the presented form, there are many equivalent linear mappings with the same cyclic structure. The important point in the previous lemma is the fact that $\mathbf{w}(c) = \mathbf{w}(H(c))$, which means that f and f_H have the same implementation cost in hardware applications.

Corollary 6. *Let $f(x) = x^i + cx^j$ and $g(x) = x^i + c^r x^j$ be defined on $\mathbb{F}_2^n$. Here, $1 \leq r < n$, is arbitrary. Then, f and g are equivalent.*

In almost all applications in symmetric cryptography, the component linear mappings are such that they must not have any fixed points. The next theorem gives a useful criterion for the lightweight linear mappings without any fixed points.

Theorem 4. *Let $P \in \mathcal{P}(\mathbb{F}_2^n)$ with the base permutation $\mathfrak{p}$. Define $f(x) = P(x) + e_j I^{j,k}(x)$ with $j \neq \mathfrak{p}(k)$. The function $g(x) = f(x) + x$ is invertible, iff $\mathfrak{p}$ is a single-cycle.*

Proof. Firstly we prove that, if $\mathfrak{p}$ is not a single cycle, then g is not invertible. Since g is linear, it suffices to prove that $g(x) = 0$ has a non-zero solution, which is equivalent to the fact that f has a non-zero fixed-point. Suppose that

$$D_i = (d_{i,1}, \ldots, d_{i,j_i}), \ \ 1 \leq i \leq z,$$

with $z \geq 1$, are the cycles of $\mathfrak{p}$. Let $k \in D_r$ and $h \in D_s$, $1 \leq r, s \leq z$. If $r = s$, then $x = (x_{n-1}, \ldots, x_0)$ with

$$x_i = \begin{cases} 1 & i \in D_r = D_s, \\ 0 & i \notin D_r = D_s, \end{cases}$$

is a non-zero solution for $g(x) = 0$.
Now suppose that $r \neq s$. The vector $x = (x_{n-1}, \ldots, x_0)$ with

$$x_i = \begin{cases} 1 & i \in D_r, \\ 0 & i \in D_s, \end{cases}$$

is a non-zero solution for $g(x) = 0$.
Conversely, suppose that $\mathfrak{p}$ is a single cycle. Since g is linear, it suffices to prove that $g(x) = 0$ has no non-zero solution. Consider $g(x) = 0$. We have

$$\begin{cases} x_{\mathfrak{p}(i)} + x_i = 0 & i \neq j, \\ x_{\mathfrak{p}(j)} + x_j + x_k = 0 & i = j. \end{cases}$$

Since $\mathfrak{p}$ is single-cycle, from the above equations we get $x_0 = x_1 = \cdots = x_{n-1}$ and since we have $x_{\mathfrak{p}(j)} + x_j + x_k = 0$, they can not be all one. □

3.2 Hardware Applications

In this subsection we investigate one-XOR matrices. In the next lemma, we give the inverse of one-XOR mappings, in general. The interesting point is that, these inverses are also one-XOR mappings.

Lemma 4. *The function $f(x) = P(x) + e_j I^{j,k}(x)$ on $\mathbb{F}_2^n$ is invertible iff $k \neq P(j)$ and its inverse is as follows*

$$f^{-1}(x) = P^{-1}(x) + e_{P(j)} I^{P(j),P^{-1}(k)}.$$

Proof. Let

$$f(x_{n-1}, \dots, x_0) = (y_{n-1}, \dots, y_0),$$

and

$$f^{-1}(y_{n-1}, \dots, y_0) = (z_{n-1}, \dots, z_0).$$

We have

$$y_t = \begin{cases} x_{P(t)} & t \neq j, \\ x_{P(j)} + x_k & t = j, \end{cases}$$

and

$$z_i = \begin{cases} y_{P^{-1}(t)} & i \neq P(j), \\ y_j + y_{P^{-1}(k)} & i = P(j). \end{cases}$$

Now if $i \neq P(j)$, then

$$z_i = y_{P^{-1}(j)} = x_{P(P^{-1}(i))} = x_i,$$

and if $i = P(j)$, then

$$z_i = y_i + y_{P^{-1}(k)} = x_{P(j)} + x_k + x_{P(P^{-1}(k))} = x_i.$$

□

Now, we characterize all the equivalent one-XOR matrices.

Lemma 5. *Define $f(x) = P(x) + e_j I^{i,j}(x)$ on $\mathbb{F}_2^n$ and let $H \in \mathcal{P}(\mathbb{F}_2^n)$. Then*

$$f_H(x) = P_H(x) + e_{H(j)} I^{H(j),H(k)}(x).$$

Proof. The mapping $e_j P(x)$ is zero at all coordinates but the j-th, which is $x_{P^{-1}(j)}$. So, to find $e_{H(j)} H I^{i,j} H^{-1}(x)$ with $x = H(j)$, we have

$$\begin{aligned}(HI^{j,k}H^{-1})^{-1}(H(j)) &= HI^{j,k}H^{-1}(H(j)) \\ &= HI^{j,k}(j) = H(k).\end{aligned}$$

□

Remark 5. Let $P \in \mathcal{P}(\mathbb{F}_2^n)$ with the base permutation $\mathfrak{p}$. We define $L_{\mathfrak{p}}(0) = 0$ and for $r > 0$, $s := L_{\mathfrak{p}}(r)$ iff $r = \mathfrak{p}^s(0)$. We know that P is equivalent to $f(x) = x^1$; i.e. there is an H such that $HPH^{-1} = x^1$. Here, we present the base permutation $\mathfrak{h}$ for such an H:

$$\mathfrak{h} : \mathbb{Z}_n \to \mathbb{Z}_n,$$

$$\mathfrak{h}(r) = L_{\mathfrak{p}}(r).$$

Now, let $P \in \mathcal{P}(\mathbb{F}_2^n)$ with the single-cycle base permutation $\mathfrak{p}$. Consider

$$f(x) = P(x) + e_j I^{j,k}(x)$$

with $j \neq \mathfrak{p}(k)$. We have $f_H(x) = P_H(x) + e_{_{H(j)}} I^{H(j),H(k)}(x)$, or with the presented notations,

$$f_H(x) = x^1 + e_{_{L_\mathfrak{p}(j)}} I^{L_\mathfrak{p}(j),L_\mathfrak{p}(k)}(x).$$

Now consider $H'(x) = x^{L_{P(j)}+1}$ and $K = HH'$. Then

$$f_K(x) = x^1 + e_{n-1} I^{n-1,L_\mathfrak{p}(k)+L_\mathfrak{p}(j)}.$$

In the next example, we illustrate the presented concept.

Example 2. Let

$$f : \mathbb{F}_2^8 \to \mathbb{F}_2^8,$$

$$f(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) = (x_3, x_1, x_4, x_2, x_6 + x_6, x_7, x_0, x_5).$$

By our notations, we have $f(x) = P(x) + e_3 I^{3,6}$, where

$$P(x_7, x_6, x_5, x_4, x_3, x_2, x_1) = (x_3, x_1, x_4, x_2, x_6, x_7, x_0, x_5),$$

with the single-cycle base permutation

$$\mathfrak{p} : \mathbb{Z}_8 \to \mathbb{Z}_8,$$

$$\mathfrak{p}(0) = 5,\ \mathfrak{p}(1) = 0,\ \mathfrak{p}(2) = 7,\ \mathfrak{p}(3) = 6,\ \mathfrak{p}(4) = 2,\ \mathfrak{p}(5) = 4,\ \mathfrak{p}(6) = 1,\ \mathfrak{p}(7) = 3.$$

Now, we have

$$L_\mathfrak{p}(0) = 0,\ L_\mathfrak{p}(1) = 7,\ L_\mathfrak{p}(2) = 3,\ L_\mathfrak{p}(3) = 5,\ L_\mathfrak{p}(4) = 2,\ L_\mathfrak{p}(5) = 1,\ L_\mathfrak{p}(6) = 6,\ L_\mathfrak{p}(7) = 4.$$

Notations as above, f is equivalent to

$$g(x) = x^1 + e_7 I^{7,3},$$

because $L_\mathfrak{p}(3) + L_\mathfrak{p}(6) = 3 \mod 8$.

It is worth noting that, using the previous study and the criteria given in [16] for non-primitivity of trinomials, the search space for checking the primitivity (imprimitivity) of trinomials, could be reduced.

Before we end this section, we give some interesting algebraic facts.

Remark 6. Note that, with notations presented in Section 2,
a) In the ring $\mathfrak{R}_n^\mathfrak{p}$ we have

$$(x^\mathfrak{p} + c)^{-1} = x^{\mathfrak{p}^{n-1}} + c^{\mathfrak{p}^{n-1}} x^{\mathfrak{p}^{n-2}},$$

provided that $cc^\mathfrak{p} = 0$.
b) In the ring $\mathfrak{R}_n$ we have

$$(x + c)^{-1} = x^{n-1} + c^{n-1} x^{n-2},$$

provided that $cc^1 = 0$.
c) In the ring $\mathfrak{R}_n^\mathfrak{p}$ we have

$$(x^\mathfrak{p} + e_j x^{\mathfrak{p}^k})^{-1} = x^{\mathfrak{p}^{n-1}} + e_{_{P^{-1}(j)}} x^{\mathfrak{p}^{k-2}}.$$

Here, $k - 2$ is computed modulo n.
d) In the ring $\mathfrak{R}_n$ we have

$$(x + e_j x^k)^{-1} = x^{n-1} + e_{_{j-1}} x^{k-2}.$$

Here, $k - 2$ and $j - 1$ are computed modulo n.

3.3 Software Applications

In this subsection, firstly we investigate a family of software-orientd lightweight linear mappings. Then, we study interleaved linear mappings and their cryptographic applications.

3.3.1 A Family of Lightweight Mappings

In the case of software-oriented lightweight linear mappings, we present a very useful theorem concerning the lightest linear ones.

Theorem 5. *Consider the mapping $f(x) = x^1 + cx$ on $\mathbb{F}_2^n$. Let c be such that for some i, we have $c_{i-1} + c_i = 0$, where $c = (c_{n-1}, \dots, c_0)$. Suppose that $\mathfrak{c}$ is such that*

$$\mathfrak{c}_j = \begin{cases} c_j & j \neq i, i-1, \\ \overline{c_j} & j = i-1, i. \end{cases}$$

Put $g(x) = x^1 + \mathfrak{c}x$. Then, we have $f \equiv g$.

Proof. Put $u(x) = x + e_i I^{i,i-1}(x)$ and $R(x) = u(f(u(x)))$. We show that $g = R$. Now, since u is an involution we have also $g(x) = u(f(u^{-1}(x)))$, which means that $f \equiv g$. To show that $R(x) = u(f(u(x)))$, firstly define $Z(x) = f(u(x))$ and suppose that z_j is the j-th output bit of $Z(x)$. We have

$$z_j = \begin{cases} c_j x_j + x_{j+1} & j \neq i, i-1, \\ x_{i-2} + c_{i-1}x_{i-1} + c_{i-1}x_i & j = i-1, \\ x_{i-1} + \overline{c_i}x_i & j = i. \end{cases}$$

Now, put $T(x) = u(f(x))$ and suppose that t_j is the j-th output bit of $T(x)$. Then,

$$t_j = \begin{cases} c_j x_j + x_{j+1} & j \neq i, i-1, \\ x_{i-2} + \overline{c_{i-1}}x_{i-1} + c_{i-1}x_i & j = i-1, \\ x_{i-1} + c_i x_i & j = i. \end{cases}$$

According to the formula for the j-th output bits of Z and T and supposing that r_j is the j-th output bit of R, we have

$$r_j = \begin{cases} c_j x_j + x_{j+1} & j \neq i, i-1, \\ x_{i-2} + \overline{c_{i-1}}x_{i-1} + \overline{(c_{i-1} + c_i)}x_i & j = i-1, \\ x_{i-1} + \overline{c_i}x_i & j = i. \end{cases}$$

So, if $c_{i-1} = 0$ and $c_i = 1$, we have

$$r_j = \begin{cases} c_j x_j + x_{j+1} & j \neq i, i-1, \\ x_{i-2} + x_{i-1} & j = i-1, \\ x_{i-1} & j = i, \end{cases}$$

and if $c_{i-1} = 1$ and $c_i = 0$, we have

$$r_j = \begin{cases} c_j x_j + x_{j+1} & j \neq i, i-1, \\ x_{i-2} & j = i-1, \\ x_{i-1} + x_i & j = i, \end{cases}$$

which shows that $R = g$. This ends the proof. □

Suppose that $u, v \in \mathbb{F}_2^n$, $u \neq \mathbf{1}$, $v \neq \mathbf{1}$ and $\mathbf{w}(u) = \mathbf{w}(v)$. It is not hard to see that u can be transformed into v by interchanging the adjacent zeros and ones. Now, using Theorem 5 we have the next corollary.

Corollary 7. *Let $c, \mathfrak{c} \in \mathbb{F}_2^n$ with $\mathbf{w}(c) = \mathbf{w}(\mathfrak{c})$. Define $f(x) = x^1 + cx$ and $g(x) = x^1 + \mathfrak{c}x$. Then, we have $f \equiv g$.*

The next two examples show a useful application of Theorem 5 and Corollary 7.

Example 3. Suppose that $f(x) = x^1 + cx$ satisfies the conditions of invertibility of $g_i(x) = f^{r_i}(x) + x$, $1 \leq i \leq t$, for some t. Now, using Corollary 7 and Corollary 4, we could design a dynamic (randomized) component with a suitable software implementation. Let m be arbitrary. Then, the linear mapping $h_m(x) = x^1 + c^m(x)$ is equivalent to f. So, for each m, $1 \leq m < n$, the mapping h_m also satisfies the conditions of invertibility of $h_m^{r_i} + x$.

Example 4. Suppose that $f(x) = x^1 + cx$ is a primitive linear mapping. Again, using Corollary 7 and Corollary 4, we could design a dynamic (generalized) LFSR with a suitable software implementation. Let m be arbitrary. Then, the linear mapping $h_m(x) = x^1 + c^m(x)$ is equivalent to f. So, for each m, $1 \leq m < n$, the mapping h_m is also a primitive linear mapping.

3.3.2 Interleaved Mappings

In this subsection, we present a strong tool for construction of parallel (bitsliced) implemention of linear mappings for symmetric cryptography. We use the notations presented in [16] extensively, in the sequel.

Definition 1. Let $L_k = \sum_{i=0}^{n-1} a_i^k x^i$, $1 \leq k \leq m$, be m linear mappings on $\mathbb{F}_2^n$ with $a_i^k = (a_{i,n-1}^k, \dots, a_{i,0}^k)$. Then we define $\Lambda_{k=1}^m L_k$ over $\mathbb{F}_2^{mn}$ as $\sum_{t=0}^{mn-1} \alpha_t x^t$ with

$$\alpha_t = \begin{cases} (a_{r,n-1}^m, \dots, a_{r,0}^m, \dots, a_{r,n-1}^1, \dots, a_{r,0}^1) & t = rm, \\ \mathbf{0} & ow. \end{cases}$$

Example 5. Suppose that $A, B \in \mathfrak{R}_3$ with

$$A = (a_2^2, a_1^2, a_0^2)x^2 + (a_2^1, a_1^1, a_0^1)x^1 + (a_2^0, a_1^0, a_0^0),$$

$$B = (b_2^2, b_1^2, b_0^2)x^2 + (b_2^1, b_1^1, b_0^1)x^1 + (b_2^0, b_1^0, b_0^0).$$

Then, $A \Lambda B \in \mathfrak{R}_6$ is equal to

$$(a_2^2, b_2^2, a_2^1, b_2^1, a_2^0, b_2^0)x^4 + (a_1^2, b_1^2, a_1^1, b_1^1, a_1^0, b_1^0)x^2 + (a_0^2, b_0^2, a_0^1, b_0^1, a_0^0, b_0^0).$$

Remark 7. As the previous example illustrates, one can check that, the action of $\Lambda_{k=1}^m L_k$ on $\mathbb{F}_2^{mn}$ is the parallel action of the mappings L_i, $1 \leq i \leq m$, regularly interleaved (or bit-sliced) together. More precisely, the output bits in the coordinates $(i-1)n + j$, $1 \leq i \leq m$, are the output bits corresponding to the action of the linear mapping L_i on the corresponding coordinates of the input. Note that, we could equivalently suppose that L acts on $(x_1, \dots, x_s)$, through independent action of L_i on x_i, $1 \leq i \leq m$. We use this notation in the proof of the following theorem.

Theorem 6. *Notations as above, let $n = st$. Consider $\Lambda_{k=1}^m L_k$. Then, we have*

a) $\mathcal{B}_l^{tm}(L) = \min_{i=1}^m \mathcal{B}_l^t(L_i)$.

b) $\mathcal{B}_d^{tm}(L) = \min_{i=1}^{m} \mathcal{B}_d^t(L_i)$.

c) $\mathcal{O}(L) = lcm(\mathcal{O}(L_1), \ldots, \mathcal{O}(L_m))$.

d) $\mathcal{F}(L) = \prod_{i=1}^{m} \mathcal{F}(L_i)$.

Proof. **a)** We know that each L_i, $1 \leq i \leq m$, acts on s many t-bit words and $\Lambda_{k=1}^m L_k$ acts on s number of mt-bit words. Now, according to Remark 7, we know that $\Lambda_{k=1}^m L_k$ acts independently on sn number of t-bit words, through L_i's, $1 \leq i \leq m$. We firstly prove that

$$\mathcal{B}_l^{tm}(L) \leq \min_{i=1}^{m} \mathcal{B}_l^t(L_i). \tag{3}$$

Let L_r be such that $b = \mathcal{B}_l^t(L_r) = \min_{i=1}^{m} \mathcal{B}_l^t(L_i)$. Suppose that there are p nonzero input and q nonzero output s-bit words for L_r such that $p + q = b$. Now, consider the input words of L such that the corresponding sub-words of L are the mentioned $p + q$ words and all the other sub-words are zero. In this case, we have p nonzero input and q nonzero output sm-bit words for L, which proves (3).
Conversely, we prove that

$$\mathcal{B}_l^{tm}(L) \geq \min_{i=1}^{m} \mathcal{B}_l^t(L_i). \tag{4}$$

Suppose that $d = \mathcal{B}_l^{tm}(L) < \min_{i=1}^{m} \mathcal{B}_l^t(L_i)$. So, there are p nonzero input and q nonzero output sm-bit words for L with $p + q = d$, which means that there is at least one of the L_i's, say L_z, such that it has p nonzero input and q nonzero output s-bit words. It follows that $\mathcal{B}_l^t(L_z) < \min_{i=1}^{m} \mathcal{B}_l^t(L_i)$. This contradict (4).
b) Similar to the proof of Case **a**.
c) Note that, if f be a permutation such that its cycles in the cyclic decomposition are of distinct lengths h_i, $1 \leq i \leq e$, for some e, then

$$\mathcal{O}(f) = lcm(h_1, \ldots, h_e).$$

Firstly, we prove that $\mathcal{O}(L) \geq lcm(\mathcal{O}(L_1), \ldots, \mathcal{O}(L_m))$. Suppose that an L_i, $1 \leq i \leq m$, has a cycle of length l. According to Remark 7, considering all the inputs of the other L_j's, $h \neq i$, we observe that L has a cycle of length l. It follows that $\mathcal{O}(L) \geq lcm(\mathcal{O}(L_1), \ldots, \mathcal{O}(L_m))$, because, for $1 \leq i \leq m$, we have $\mathcal{O}(L_i) = lcm(l_1, \ldots, l_v)$, where L_i's, $1 \leq i \leq v$, are the distinct cycle lengths of L_i.
Now, we prove that $L^{lcm(\mathcal{O}(L_1),\ldots,\mathcal{O}(L_m))} = I$. For simplicity, we suppose that L acts on x_i's, $1 \leq i \leq m$. Again, by Remark 7 we see that each L_i acts independently on x_i. Now, since for each i, we have $L_i^{\mathcal{O}(L_i)} = I$, we deduce that

$$L^{lcm(\mathcal{O}(L_1),\ldots,\mathcal{O}(L_m))} = I,$$

which ends the proof.
d) Again, we suppose that L acts on x_i's, $1 \leq i \leq m$. By Remark 7 we see that each L_i acts independently on x_i. On one hand, considering a fixed-point of L_i, for some $1 \leq i \leq m$, shows that $\mathcal{F}(L) \geq \prod_{i=1}^{m} \mathcal{F}(L_i)$. On the other hand, if $x = (x_1, \ldots, x_m)$ is a fixed-point of L, then for each i, x_i should be a fixed-point of L_i. So, $\mathcal{F}(L) \leq \prod_{i=1}^{m} \mathcal{F}(L_i)$. This ends the proof. □

Example 6. Let $L = \sum_{i=0}^{n-1} a_i x^i$, be a linear mapping on $\mathbb{F}_2^n$ with $a_i = (a_{i,n-1}, \ldots, a_{i,0})$. Then, we have

$$\Lambda_{k=1}^m L = \sum_{t=0}^{mn-1} \alpha_t x^t,$$

which is defined over over $\mathbb{F}_2^{mn}$ and,

$$\alpha_t = \begin{cases} (a_{r,n-1}, \ldots, a_{r,0}, \ldots, a_{r,n-1}, \ldots, a_{r,0}) & t = rm, \\ \mathbf{0} & ow. \end{cases}$$

Corollary 8. *Notations as above, consider $\Lambda_{k=1}^{m} L$. Then, we have*

a) $\mathcal{B}_l^{km}(\Lambda_{k=1}^{m} L) = \mathcal{B}_l^{n}(L)$.

b) $\mathcal{B}_d^{km}(\Lambda_{k=1}^{m} L) = \mathcal{B}_d^{n}(L)$.

c) $\mathcal{O}(\Lambda_{k=1}^{m} L) = \mathcal{O}(L)$.

d) $\mathcal{F}(\Lambda_{k=1}^{m} L) = (\mathcal{F}(L))^m$.

Similar to the case of equivalent mappings, we have the following facts.

Theorem 7. *Let L_i, $1 \leq i \leq m$, be m linear mappings on $\mathbb{F}_2^n$ such that for each $1 \leq i \leq m$, $L_i^r + I$ is invertible. Put $L = \Lambda_{k=1}^{m} L$. Then, $L^r + i$ is invertible.*

Proof. Suppose that $L^r + I$ is not invertible. So we have $L^r(x) + x = 0$ for some nonzero $x \in \mathbb{F}_2^{mn}$. It follows that $L^r(x) = x$, which means that x is on a cycle of length t such that t is a divisor of r. We deduce that for each $1 \leq i \leq m$, there is an $x_i \in \mathbb{F}_2^n$ such that $L_i^r(x_i) = x_i$. This contradicts the fact that $L_i^r + I$ is invertible. □

Corollary 9. *Let L_i, $1 \leq i \leq m$, be m linear mappings on $\mathbb{F}_2^n$ such that for each $1 \leq i \leq m$, and every j, $1 \leq j \leq s$, the linear mapping $L_i^{r_j} + I$ is invertible. Let $L = \Lambda_{k=1}^{m} L$. Then, for every j, $1 \leq j \leq s$, the linear mapping $L^{r_j} + I$ is invertible.*

Now, we give two examples illustrating the usage of the concept of interleaving.

Example 7. Let $f_i(x) = x^1 + c_i x$, $1 \leq i \leq m$, be defined on $\mathbb{F}_2^n$. Here, $c_i = (c_{i,n-1}, \ldots, c_{i,0})$. Then, $f = \Lambda_{i=1}^{m} f_i$ on $\mathbb{F}_2^{mn}$ is

$$f(x) = x^m + \mathcal{C}x,$$

where

$$\mathcal{C} = (c_{m,n-1}, \ldots, c_{1,n-1}, \ldots, c_{m,0}, \ldots, c_{1,0}).$$

Remark 8. Note that, the above example provides a method for construction of dynamic (randomized) linear components with little extra cost in software implementations: as studied in [16], these dynamic components could make symmetric ciphers more resistant against various kinds of cryptanalysis.

Example 8. Let $f(x) = \sum_{i=1}^{m} x^{i_j}$, $1 \leq i \leq m$. Then,

$$\Lambda_{i=1}^{m} f = \sum_{i=1}^{m} x^{m i_j}.$$

Remark 9. Another proof of Theorem 3.5 in [5] could be given by the concepts studied in this paper.

4 Conclusion

In this paper, we present the concept of equivalence of mappings and based on this stusy, we characterize all of one-XOR matrices which are used in hardware applications. Also, we present a family of lightweight linear mappings for software-oriented applications in symmetric cryptography. Then, we investigate interleaved linear mappings and based upon this concept, we presente generalized dynamic primitive LFSRs along with dynamic linear components for construction of diffusion layers.
As a mathematical result, we presente invoutive sparse binary matrices as well as sparse binary matrices with sparse inverses. Another interesting result of this study is that, with the aid of our characterization of one-XOR matrices, the search space for finding a k such that $x^n + x^k + 1$ is primitive, could be reduced

References

[1] C. Beierle, T. Kranz, and G. Leander. *Lightweight Multiplication in GF(2^n) with Applications to MDS Matrices.* CRYPTO 2016, Part I. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 625653.

[2] J. Daemen and V. Rijmen. *AES proposal: Rijndael. Selected as the advanced encryption standard. http://nist.gov/aes.*

[3] S. M. Dehnavi, M. R. M. Shamsabad, and A. M. Rishakani. *Lightweight Involutive Components for Symmetric Cryptography.* ISCISC 2019: 61-66..

[4] M. R. M. Shamsabad, andS. M. Dehnavi. *Nonlinear* 4×4 *MDS Diffusion Layers.* Journal of Information and Optimization Sciences 43 (4), 663-676, 2022.

[5] S. M. Dehnavi, A. M. Rishakani, and M. R. M. Shamsabad. *On Cryptographic Applications of Matrices Acting on Finite Commutative Groups and Rings.* Cryptol. ePrint Arch. 2014: 91 (2014).

[6] P. Ekdahl, T. Johansson, A. Maximov, and J. Yang. *A new SNOW stream cipher called SNOW-V.* IACR Trans. Symmetric Cryptol. 2019(3): 1-42 (2019).

[7] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker. *The Skein hash function family, version 1.2. September 15, 2009.*

[8] Z. Guo, R. Liu, W. Wu, and D. Lin. *Direct construction of lightweight rotational-xor MDS diffusion layers.* IACR Transactions on Symmetric Cryptology ISSN 2519-173X, Vol. 2017, No. 4, pp. 169187.

[9] J. Guo, T. Peyrin, and A. Poschmann. *The PHOTON family of lightweight hash functions.* In P. Rogaway, editor, Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, volume 6841 of Lecture Notes in Computer Science, pages 222239. Springer, 2011.

[10] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. *The LED Block Cipher.* In: CHES 2011. Ed. by Bart Preneel and Tsuyoshi Takagi. Vol. 6917. LNCS. Springer, Heidelberg, Sept. 2011, pp. 326341.

[11] L. Kolsch. *A XOR-counts and lightweight multiplication with ficed elements in binary finite fields.* IACR Cryptology ePrint 2019:229 (2019).

[12] S. Mesnager, K. H. Kim, D. Jo, J. Choe, M. Han, and D. N. Lee. *A proof of Beierle-Kranz-Leander conjecture related to lightweight multiplication in* $\mathbb{F}_{2^n}$. Des. Codes Cryptogr. 8(1): 51-62 (2020).

[13] M. K. Pehlivanoglu, F. B. Sakalli, S. Akieyelec, and M. T. Sakalli. *On the Construction of New Lightweight Involutory MDS Matrices in Generalized Subfield Form.* IEEE Access 11: 32708-32715 (2023).

[14] 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.

[15] M. R. M. Shamsabad, and S. M. Dehnavi. *Randomized nonlinear software-oriented MDS diffusion layers.* Groups Complex. Cryptol. 11(2): 123-131 (2019).

[16] M. R. M. Shamsabad, and S. M. Dehnavi. *Dynamic MDS diffusion layers with efficient software implementation.* Int. J. Appl. Cryptogr. 4(1): 36-44 (2020).

[17] G. Zeng, W. Han and K. He. *High Efficiency Feedback Shift Rgister: sigma-LFSR.* IACR Cryptology ePrint 20079:114 (2007).

[18] 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.