*Journal of Computer Science and Cybernetics, V.32, N.1 (2016), 1–17*
DOI: 10.15625/1813-9663/32/1/7732

# DIRECT EXPONENT AND SCALAR MULTIPLICATION TRANSFORMATIONS OF MDS MATRICES: SOME GOOD CRYPTOGRAPHIC RESULTS FOR DYNAMIC DIFFUSION LAYERS OF BLOCK CIPHERS

LUONG TRAN THI[1], CUONG NGUYEN NGOC[2]

[1,2]*Academy of Cryptographic Technique of Viet Nam Government Information Security Commission;*
*Email:* [1]*luongtranhong@gmail.com;* [2]*nguyenngoccuong189@gmail.com*

**Abstract.** MDS (Maximum Distance Separable) matrices have an important role in the design of block ciphers and hash functions. The methods for transforming an MDS matrix into other ones have been proposed by many authors in the literature. In this paper, some new results from direct exponent and scalar multiplication transformations are given including the preservation of good cryptographic properties (the coefficient of fixed points and involutory property) of MDS matrices and other important cryptographic properties obtained from studying equivalence relations based on these transformations. An estimation of the number of $m \times m$ MDS matrices over $GF(p^r)$ is also presented. In addition, these results are shown to be an important theoretical basis for building efficient dynamic diffusion layer algorithms for block ciphers.

**Keywords.** MDS matrix, direct exponent transformation, scalar multiplication transformation, dynamic algorithm...

## 1. INTRODUCTION

The viability of using MDS matrices in block ciphers was first introduced by Serge Vaudenay in FSE'95 [1] as a linear case of multipermutations. Multipermutations characterize the notion of perfect diffusion [2] which requires that the change of any $t$out of $m$ input bits must affect at least $m - t + 1$ output bits.

The branch number is one of the important criteria for diffusion layer design in SPN structure [3, 4]. It has an important role for resistance against strong attacks (such as linear and differential attacks) on block ciphers. It is always to be expected to have the maximum branch number for block cipher designers. As MDS matrices give maximum branch numbers for the linear transformations corresponding with them, they have been used for diffusion in many block ciphers such as: AES [5,6], SHARK [7], Square, Twofish [8], Anubis, Khazad, Manta, Hierocrypt and Camellia. They are also used in stream ciphers like MUGI and cryptographic hash functions like WHIRLPOOL.

"Dynamic" block ciphers (block ciphers which are made dynamic in one of their components) have been under study in order to further enhance the security of the block ciphers, for example [9–11]. In [9,10] the authors constructed a key-dependent diffusion layer by creating MDS matrices depending on a secret key for each round. In [11], the authors constructed a dynamic block cipher in both substitution and permutation layers by building a bank of S-boxes and MDS matrices depending on a secret key.

Accordingly, some MDS matrix transformations have been studied to generate dynamic MDS matrices from an existing one such as: scalar multiplication [12], permutations of rows and columns [13, 14], direct exponent [12]. The direct exponent and scalar multiplication transformations were first introduced by Ghulam Murtaza and Nassar Ikram in [12]. However, no studies have ever shown the conservation of good cryptographic properties of MDS matrices under these transformations. Moreover, no studies have also indicated how effective to apply these transformations to build dynamic diffusion layer algorithms for block ciphers. In this paper, some new results from direct exponent and scalar multiplication transformations are presented including the preservation of good cryptographic properties of MDS matrices such as the preservation of the coefficient of fixed points and involutory property. Moreover, the properties of equivalence relations based on these transformations are also given. In addition, these results are shown to be an important theoretical basis for building efficient dynamic diffusion layer algorithms for block ciphers.

The paper is organized as follows. Section 2 presents some related works. In Section 3, some new results about the direct exponent and scalar multiplication transformations are given. In Section 4, some examples are given. Section 5 provides important applications of these results for building efficient dynamic diffusion layer algorithms for block ciphers. And conclusion of the paper is in Section 6.

## 2. PRELIMINARY AND RELATED WORKS

### 2.1. MDS matrices

MDS matrices provide perfect diffusion so they are useful for block ciphers and hash functions. The idea comes from coding theory, in particular from maximum distance separable code (MDS). In this context, two important theorems from coding theory are stated.

**Theorem 1.** [15] *If $C$ is a $[n, k, d]$ code then $n - k \geq d - 1$..*

Codes with $n - k = d - 1$(or $d = n - k + 1$), are called maximum distance separable code, or MDS code for short.

**Theorem 2.** [15] *A $[n, k, d]$ code $C$ with generator matrix $G = [I|A]$ where $A$ is a $k \times (n - k)$ matrix, is MDS if and only if every square submatrix (formed from any $i$ rows and any $i$ columns, for any $i = 1, 2, \ldots, \min\{k, n - k\}$) of $A$ is nonsingular.*

The following fact is another way to characterize an MDS matrix.

### 2.2. Fixed points in Linear transformations [16]

Consider a linear transformation $L : F_{2^r}^m \to F_{2^r}^m$. Define $A = [a_{i,j}]_{m \times m}$ as a nonsingular matrix with elements in the field $F_{2^r}$ that represents the linear transformation $L$. The transformation $L$ maps an element $X = [X_0, X_1, \ldots, X_{m-1}]^T \in F_{2^r}^m$ to an element $Y = [Y_0, Y_1, \ldots, Y_{m-1}]^T \in F_{2^r}^m$ by $Y = AX$ as follows:

$$\begin{bmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{m-1} \end{bmatrix} = \begin{bmatrix} a_{0,0}a_{0,1} & \cdots & a_{0,m-1} \\ a_{1,0}a_{1,1} & \cdots & a_{1,m-1} \\ \vdots & \vdots & \vdots \\ a_{m-1,0}a_{m-1,1} & \cdots & a_{m-1,m-1} \end{bmatrix} = \begin{bmatrix} X_0 \\ X_1 \\ \vdots \\ X_{m-1} \end{bmatrix} \tag{1}$$

Let $I$ denote the $m \times m$ identity matrix. The set of all fixed points for the linear transformation $L$ can be obtained by solving the following equation:

$$[A - I]\, X = 0, \tag{2}$$

where 0 is the all-zero vector of length $m$. The number of fixed points for this transformation is given by:

$$F_A = 2^{r(m-rank[A-I])}. \tag{3}$$

This is the number of input blocks that are unchanged by the linear transformation $L$, so the output blocks are equal to the corresponding input blocks.

To extend the definition of fixed points, Muhammad Reza Z'aba [16] considered simple linear relationships between the input and output blocks. Let $I_{(l)} = \left[\alpha_{i,j}^{(l)}\right]$ denote the $m \times m$ matrix based on the identity matrix $I = [\alpha_{i,j}]$ where $I_{(0)} = I$. The elements of matrix $I_{(l)}$ are determined by the rotation parameter $l \in \{0, 1, \ldots, m-1\}$ where $\alpha_{i,j}^{(l)} = \alpha_{i,(j-l)modm}$. The following are examples of the matrices $I_{(1)}$ and $I_{(2)}$ for $m = 4$.

$$I_{(1)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \qquad I_{(2)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Consider input blocks that have the following simple relationship by $L$ which is an extension of (2):

$$\left[A - I_{(l)}\right] X = 0. \tag{4}$$

For $l = 0$, the above equation is the same as (2).

For $l > 0$, the solution to the above linear relationship gives the set of all input blocks that are only rotated $lr$ bits to the left by the linear transformation $L$ to produce output blocks. This relationship is given as follows where $\hat{X}$ represents particular input blocks to $L$:

$$L\left(\hat{X}\right) = \hat{X} <<< lr. \tag{5}$$

The number of input blocks satisfying the relationship in (4) is calculated as:

$$F_{A_{(l)}} = 2^{r\left(m-rank\left[A-I_{(l)}\right]\right)} \tag{6}$$

where $l \in \{0, 1, \ldots, m-1\}$.

Then, the diffusion based on the fixed points and the simple linear relationships is denoted by the number $D(A)$ defined as follows:

$$D(A) = \frac{1}{m2^{mr}} \sum_{l=0}^{m-1} F_{A_{(l)}} = \frac{1}{m2^{mr}} \sum_{l=0}^{m-1} 2^{r\left(m-rank\left[A-I_{(l)}\right]\right)}. \tag{7}$$

The number $D(A)$ is called the coefficient of fixed points of $L$ and denote the average fraction of input blocks to $L$ that have the linear relationship in (4).

*For more generally*, we consider a linear transformation $L : F_{p^r}^m \to F_{p^r}^m$ which is represented by a matrix $A = [a_{i,j}]_{m\times m}$ as a nonsingular matrix with elements in the field $F_{p^r}$. Then it is based on the theory of linear algebra, it is to have:

The number of fixed points satisfying (2) for this transformation is given by:

$$F_A = p^{r(m-rank[A-I])}. \tag{8}$$

Similarly, the number of input blocks satisfying the relationship in (4) for this transformation is calculated as:

$$F_{A_{(l)}} = p^{r\left(m-rank\left[A-I_{(l)}\right]\right)}. \tag{9}$$

where $l \in \{0, 1, \ldots, m-1\}$.

And the coefficient of fixed points $D(A)$ of $L$ is:

$$D(A) = \frac{1}{mp^{mr}} \sum_{l=0}^{m-1} F_{A_{(l)}} = \frac{1}{mp^{mr}} \sum_{l=0}^{m-1} p^{r\left(m-rank\left[A-I_{(l)}\right]\right)}. \tag{10}$$

### 2.3. The results of previous works

The direct exponent and scalar multiplication transformations were introduced by Ghulam Murtaza and Nassar Ikram in [12]. In this section, results in [12] are summarized.

The definition of direct exponent of an MDS matrix was defined as follow:

**Definition 1.** [12] Let $F$ be a Galois field. Let matrix $A = [a_{i,j}]_{m\times m}, a_{i,j} \in F$, then $A_{d^e} = \left[a_{i,j}^e\right]_{m\times m}$, $(e = 1, 2, 3\ldots)$ is called direct $e$ exponent matrix of $A$. And $A_{d^2}$ is called direct square matrix of $A$.

The following theorem about direct square of an MDS matrix was stated:

**Theorem 3.** [12] *If $A = [a_{i,j}]_{m\times m}, a_{i,j} \in F$ is an MDS matrix, then direct square matrix $A_{d^2}$ of $A$ is an MDS matrix.*

However this theorem was shown to be incorrect in both it's statement and proof by the authors in [17].

The class of MDS matrices was also defined in [12] as follow:

**Definition 2.** [12] Define direct exponent class of MDS matrix $A$ as

$$Cl_{d^e}(A) = \left\{ \overset{\text{`}}{A} : \overset{\text{`}}{A} = A_{d^i}, i = 2, 3, 4, \ldots, Ord(F) \right\}.$$

The number of MDS matrices in a class was shown in the following theorem.

**Theorem 4.** [12] *If an element $a'$ of MDS matrix $A$ such that $|a'| = \max|a_{i,j}|$, then* $\frac{log|a'|}{\log 2} - 1 \leq \#\{$ *MDS matrices in* $Cl_{d^e}(A)\} \leq Ord(F) - 1$.

It can be seen that the number of MDS matrices in a class was only shown as an inequality.

Next, the theorem about scalar multiplication was stated.

**Theorem 5.** [12] *Let* $A = \begin{bmatrix} A_1 \\ \vdots \\ A_m \end{bmatrix}$, $A_i = [a_{i,1} \cdots a_{i,n}]$, $a_{i,j} \in F_q$ *be an MDS matrix, and* $E = [e_i]$, *i = 1, 2, . . . , m, then scalar multiplication* $EA = \begin{bmatrix} e_1 A_1 \\ \vdots \\ e_m A_m \end{bmatrix}$, $e_i A_i = [e_i a_{i,1} \cdots e_i a_{i,n}]$ *is an MDS matrix.*

An equivalence class based on this scalar multiplication was defined and the number of MDS matrices in a class was also given as follows.

**Definition 3.** [12] Define scalar multiplication class of an MDS matrix $\underset{m\times n}{\overset{\text{‘}}{A}}$ by a scalar value $E = \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}$ *as* $Cl_{sm}\left(A_{m\times n}\right) = \left\{ \underset{m\times n}{\overset{\text{‘}}{A}} : \underset{m\times n}{\overset{\text{‘}}{A}} = EA_{m\times n}, \forall e_i \neq 0 \in F, \forall i \right\}$.

**Theorem 6.** [12] *Number of elements in class* $Cl_{sm}\left(\underset{m\times n}{\overset{\text{‘}}{A}}\right)$ *is* $\left(Ord\left(F\right) - -1\right)^m$.

## 3. SOME NEW RESULTS

In this Section, some new results from the direct exponent and scalar multiplication transformations are presented.

### 3.1. $\mathcal{R}_p$ equivalence relation and the preservation of coefficient of fixed points of MDS matrices

It was showed that direct $p$ exponent of an MDS matrix over $GF\left(p^r\right)$ also results in an MDS matrix as stated and proven in Theorem 1 [18]. The cycle of the direct $p$ exponent transformation was also given in Theorem 2 [18]. It was showed that the direct exponent transformation is capable of preserving many good cryptographic properties of MDS matrices such as MDS, involutory, symmetric, the number of 1's and distinct elements in matrix, circulant and circulant-like in [19].

In this section, the equivalence relation based on the direct exponent transformation will be defined and a necessary condition for two matrices in order to belong to the same equivalence class on this relation will be shown. Then the conservation of coefficient of fixed points of MDS matrices under the direct exponent transformation will be stated and proven.

#### 3.1.1. $\mathcal{R}_p$ equivalence relation based on the direct exponent transformation

Here, a relation based on the direct exponent transformation is defined.

**Definition 4.** Let $\mathcal{D}$ be a set of $m \times m$ MDS matrices over $GF\left(p^r\right)$. Then it is said that matrix $B \in \mathcal{D}$ has a direct p exponent relation with $A \in \mathcal{D}$, denoted by $A\mathcal{R}_p B$, if there exists a non-negative integer $k$ such that $B = A_{d^{p^k}}$, or $A\mathcal{R}_p B \leftrightarrow B = A_{d^{p^k}}$.

Denote $\tau_A$ is the cycle of the direct $p$ exponent transformation of matrix $A$ (in [18], $\tau_A$ was given exactly, but in Definition 2 [12], $\#Cl_{d^e}\left(A\right)$ was only estimated). Then $\tau_A \leq r$ (by the Theorem 2 [12]). On the other hand, if $k = r$ or $k = 0$ then $A_{d^{p^k}} = A$, so it can be limited $0 \leq k \leq r - 1$.

It is to prove easily the following result:

**Proposition 1**. *$\mathcal{R}_p$ relation on $\mathcal{D}$ is an equivalence relation.*

Denote the *equivalence Class* that contains matrix $A \in \mathcal{D}$ on the $\mathcal{R}_p$ relation is. (It is clear that $Cl_{d^e}(A)$ in [12] is an *equivalence Class* containing $A\,[A]_p$). Next, a necessary condition for two matrices to be equivalent on the $\mathcal{R}_p$ relation is given in Theorem 7.

**Theorem 7.** *If two any MDS matrices belong to the same equivalence class on the $\mathcal{R}_p$ relation over $\mathcal{D}$ then:*

1. *They have the same cycle of the direct p exponent transformation.*
2. *The positions containing element 1 of the two matrices coincide each other.*
3. *Two any corresponding elements of the two matrices must have the same orders.*

***Proof***.

Suppose $A, B \in D$ are two MDS matrices of the same equivalence class on the $\mathcal{R}_p$ relation.

*Item* 1.

Then $\exists k \in N, 0 \le k \le \tau_A - 1: \quad B = A_{d^{p^k}}$. Implementing direct $p$ exponent for this equation for $\tau_A$ times will obtain:

$$B_{d^{p^{\tau_A}}} = A_{d^{p^{\tau_A+k}}} \leftrightarrow B_{d^{p^{\tau_A}}} = A_{d^{p^k}} \text{ or } B_{d^{p^{\tau_A}}} = B.$$

Thus, $\tau_B | \tau_A$. Because of the symmetry of $\mathcal{R}_{\surd}$, it also has $\tau_A | \tau_B$. Thus, it follows that $\tau_A = \tau_B$, or MDS matrices in the same equivalence class have the same cycle.

Denote their cycle is $\tau$.

*Item* 2.

To prove that the positions containing element 1 of the two matrices coincide each other, it is first proved that, $a_i^{p^k} \ne 1$ is always true for $0 \le k \le \tau - 1$ and for $a_i$ other than 1 of $A$ (obviously $a_i \ne 0$ because $A$ is an MDS matrix).

Indeed, consider the case when $r = 1$. For any element other than 0 and 1, $a \in GF(p)$, if $a^p = 1$ there must be $p | (p-1)$. This is ridiculous.

Suppose $r > 1$. For any element other than 0 and 1, $a \in GF(p^r)$, if $a^p = 1$ it is to infer that $p | (p^r - 1)$. Then there exists a positive integer $d$ such that: $p^r - 1 = dp$ (for $p^r - 1 > d \ge 1$). This equation is equivalent to:

$$p^r - dp = 1 \leftrightarrow p\left(p^{r-1} - d\right) = 1.$$

Obviously, the left side of the obtained equation is an integer divisible by $p$, but its right side is not divisible by $p$. This leads to contradiction.

Consequently, for any element other than 0 and 1, $a \in GF(p^r), (r \ge 1)$, it is always true that $a_i^{p^k} \ne 1$. This entails $a^{p^k} \ne 1$, $(0 \le k \le \tau - 1)$.

Therefore, for $\forall a_i \in A : a_i \ne 1$, it is always to have $a_i^{p^k} \ne 1 \quad (0 \le k \le \tau - 1)$. Because of the symmetry of $\mathcal{R}_p$, this is also true for any element other than 1 of matrix $B$.

In addition, element 1 is unchanged when performing direct $p^k\,(0 \le k \le \tau - 1)$ exponent of an MDS matrix. Because of the symmetry of $\mathcal{R}_p$, the positions of $B$ containing element 1 must also coincide with the positions of $A$ containing element 1. Item 2 is proven.

*Item* 3.

Assuming that $a \in A$ and $b \in B$ are two any corresponding elements (i.e both of them are in row $i$ and column $j$) of the two matrices; suppose $x$ is the order of $a$ and $y$ is the order of $b$. It will be to prove that $x = y$.

Indeed, by assumption, it is to have:

$$B = A_{d^{p^k}} (0 \leq k \leq \tau - 1) \text{ or } b = a^{p^k}. \tag{11}$$

Since $y$ is the order of $b$ then:

$$b^y = 1. \tag{12}$$

Replace (11) into (12), it becomes: $a^{yp^k} = 1$. As $x$ is the order of $a$, it follows that $x | yp^k$. So,

$$\exists u_1 \in N^+ : yp^k = u_1 x. \tag{13}$$

On the other hand, because the elements of $A, B$ are in $GF(p^r)$, so: $x | (p^r - 1)$. Therefore,

$$\exists v_1 \in N^+ : p^r - 1 = v_1 x. \tag{14}$$

Multiply both sides of (11) by $v_1$, and multiply both sides of (12) by $u_1$, it is to have:

$$v_1 y p^k = u_1 (p^r - 1) \leftrightarrow p^k \left( u_1 p^{r-k} - v_1 y \right) = u_1. \tag{15}$$

The left side of (13) is divisible by $p^k$, so its right side must be also divisible by $p^k$. As a result,

$$\exists d_1 \in N^+ : u_1 = d_1 p^k. \tag{16}$$

Replace (14) into (11), it becomes: $y = d_1 x$, $(d_1 \in N^+)$. For this reason, $y \geq x$.

Because of the symmetry of the $\mathcal{R}_p$ relation, we also have $x \geq y$. Consequently, $x = y$. ■

### 3.1.2. The preservation of coefficient of fixed points of MDS matrices under the direct exponent transformation

Now, the direct $p$ exponent transformation is proven to be able to preserve the $D(A)$ coefficient.

**Theorem 8.** *Let $A = [a_{i,j}]_{m \times m}, a_{i,j} \in GF(p^r)$ be an MDS matrix where $p$ is a prime number. Let $\tau$ is the cycle of the direct p exponent transformation of matrix $A$. Then direct $p^k (1 \leq k \leq \tau)$ exponent of matrix $A$ preserves the coefficient of fixed points of $A$.*

***Proof.***

Consider the direct $p$ exponent of $A$ is: $B = A_{d^p}$.

According to the proof of the Theorem 1 [18], it was showed that the determinant of any submatrix of size $k$ $(1 \leq k \leq m)$ of $B$ is $p$ exponent of the the determinant of the corresponding submatrix of size $k$ of $A$. (17)

Now suppose that $L$ is the linear transformation represented by matrix $A$. Then the number of input blocks satisfying (4) of $L$ is given by (9), i.e: $F_{A_{(l)}} = p^{r\left(m - rank[A - I_{(l)}]\right)}$, for $l \in \{0, 1, \ldots, m-1\}$. And the coefficient of fixed points of $L$ is given by (10), denoted by $D(A)$.

Suppose $L^{'}$ is the linear transformation represented by matrix $B$. Then the number of input blocks satisfying (4) of $L^{'}$ is given by (9), i.e: $F_{B_{(l)}} = p^{r\left(m-rank\left[B-I_{(l)}\right]\right)}$, for $l \in \{0, 1, \ldots, m-1\}$. And the coefficient of fixed points of $L^{'}$ is given by (10), denoted by $D(B)$.

It will be to prove that $F_{A_{(l)}} = F_{B_{(l)}}$, for $l \in \{0, 1, \ldots, m-1\}$, i.e. $D(A) = D(B)$.

Indeed, consider the matrix $\left[B - I_{(l)}\right] = \left[A_{d^p} - I_{(l)}\right] = \left[\left(a_{i,j}^p - \alpha_{i,j}^{(l)}\right)\right]$, for $l \in \{0, 1, \ldots, m-1\}$. Any element of $I_{(l)} = \left[\alpha_{i,j}^{(l)})\right]$ can only be 0 or 1. So it is to have:

$$\left[B - I_{(l)}\right] = \left[\left(a_{i,j}^p - \alpha_{i,j}^{(l)}\right)\right] = \left[\left(a_{i,j} - \alpha_{i,j}^{(l)}\right)^p\right]. \tag{18}$$

According to (17), the determinant of any submatrix of $\left[B - I_{(l)}\right]$ is equal to $p$ exponent of the determinant of the corresponding submatrix of $\left[A - I_{(l)}\right]$, i.e.:

$$rank\left[A - I_{(l)}\right] = rank\left[B - I_{(l)}\right] = d.$$

From the formulae of $F_{A_{(l)}}$, $F_{B_{(l)}}$, it follows that $F_{A_{(l)}} = F_{B_{(l)}}$, for $l \in \{0, 1, \ldots, m-1\}$, i.e. $D(A) = D(B)$. ∎

### 3.2. $\mathcal{R}_M$ equivalence relation and the preservation of involutory property of MDS matrices

In this section, the definition of scalar multiplication transformation is given. As a consequence, many corresponding results are also presented. A definition of an equivalence relation based on this transformation is provided; a necessary condition for two MDS matrices to be equivalent on the relation is stated; the cycle of that transformation and the number of different elements in an equivalence class are specified. As a consequence, the possible number of $m \times m$ MDS matrices over $GF(p^r)$ is also given. Then, the preservation of the involutory property of MDS matrices under the transformation will be stated and proven.

#### 3.2.1. $\mathcal{R}_M$ equivalence relation based on the scalar multiplication transformation

Consider $A \in \mathcal{D}$. It is known that $A$ is an MDS matrix if and only if all of its square submatrices are nonsingular. Applying this, it is easy to see that if multiplying all elements of a row of $A$ with an element $e0 \in GF(p^r)$ then the result matrix is also an MDS matrix.

Extend this result, multiplying all elements of row $i$ of $A$ with an element $e_i 0 \in GF(p^r)$, (for $i = 1, \ldots, m$) will also result in an MDS matrix. The same is true when multiplying all elements of column $j$ of $A$ with an element $f_j \neq 0 \in GF(p^r)$, (for $j = 1, \ldots, m$).

Denote $E = [e_1, e_2, \ldots, e_m]$, $F = [f_1, f_2, \ldots, f_m]$, (for $e_i, f_i \neq 0 \in GF(p^r)$) are vectors over $GF(p^r)$. From now on, the elements $e_i, f_j$, $(i, j = 1, \ldots, m)$ of vectors $E$ and $F$ are always assumed to be other than 0. Multiply row $i$ of $A$ by $e_i$, multiply column $j$ of $A$ by $f_j$, (for $i, j = 1, \ldots, m$). Then the result matrix is denoted by $(E, F)(A)$.

Denote the "inverse" vector of $E$ is $E^{-1} = \left[e_1^{-1}, e_2^{-1}, \ldots, e_m^{-1}\right]$. Obviously, the elements $e_i^{-1} \neq 0 \in GF(p^r)$, because $e_i \neq 0 \in GF(p^r)$), (for $i = 1, \ldots, m$).

Multiplying of the two vectors $E$ and $F$ is denoted by: $E.F = [e_1 f_1, e_2 f_2, \ldots, e_m f_m]$. Note that, products $e_i f_i \neq 0 \in GF(p^r)$.

First, a relation based on the scalar multiplication transformation is defined as follows:

**Definition 5.** It is said that matrix $B \in \mathcal{D}$ has an $M$ relation with matrix $A \in \mathcal{D}$, denoted by $A\mathcal{R}_M B$, if there exists two vectors $E, F$ over $GF(p^r)$ such that $B = (E,F)(A)$.

It is possible to prove the following result:

**Proposition 2.** *$\mathcal{R}_M$ relation over $\mathcal{D}$ is an equivalence relation.*

Now, let $E = [e_1, e_2, \ldots, e_m]$ and $F = [f_1, f_2, \ldots, f_m]$ are two fixed vectors over $GF(p^r)$. Perform consecutive the following procedure: $A_1 = (E,F)(A), A_2 = (E,F)(A_1) = (E,F)(E,F)(A) = (E,F)^2(A), \ldots, A_n = (E,F)^n(A)$, and so on. It is to have the following result:

**Theorem 9.** *The sequence of matrices $A_1, A_2, \ldots$ has a finite cycle $t$.*

***Proof.***

Note that for every positive integer $n$, the element in the row $i$ and column $j$ of matrix $A_n$ is $(e_i f_j)^n . a_{i,j}$.

Consider the positive integer: $d = lcm(ord(e_i f_j), i, j = 1, 2, \ldots, m)$. Then $(e_i f_j)^d = 1$, for $i, j = 1, 2, \ldots, m$. As a result: $A_d = (E,F)^d(A) = A$.

Now, suppose $\exists d_1 \in N^+ : A_{d_1} = (E,F)^{d_1}(A) = A$. It is to infer $(e_i f_j)^{d_1} = 1, \quad i, j = 1, 2, \ldots, m$ and therefore $ord(e_i f_j) | d_1, i, j = 1, 2, \ldots, m$. It yields $d | d_1$ or $d$ is the smallest positive integer satisfying the condition: $(E,F)^d(A) = A$.

Consequently, the sequence of $A_1, A_2, \ldots$ has a finite cycle $t = d$. ■

Note that the cycle $t$ reaches the maximum value if there exists an element $e_i f_j$ is an element with order $p^r - 1$ (or a primitive element) in $GF(p^r)$, and then $d = p^r - 1$.

The following theorem shows the number of different elements in an equivalence class on the $\mathcal{R}_M$relation.

**Theorem 10.** *Let $A \in \mathcal{D}$. Then the equivalence class $[A]_M$ has exactly $P^{2m-1}$ different elements, where $P = p^r - 1$.*

***Proof.***

Consider $A \in \mathcal{D}$. Multiply $A$ by all of possible vectors $E, F$ over $GF(p^r)$, it is to obtain an equivalence class of $A$ on the $\mathcal{R}_M$ relation, denoted by $[A]_M$. As a result, the class $[A]_M$ includes $(p^r - 1)^{2m} = P^{2m}$ elements generated by this way, where $P = p^r - 1$.

Now, suppose $(E,F)(A) = (E',F')(A)$. It yields $e_i f_j = e_i' f_j'$ or $\dfrac{e_i}{e_i'} = \dfrac{f_j'}{f_j}$ for $i, j = 1, \ldots, m$.

It follows that $\dfrac{e_i}{e_i'} = \dfrac{f_j'}{f_j} = c$, for $c$ is a constant other than 0 in $GF(p^r)$, or $e_i' = c^{-1} e_i$ and $f_j' = c f_j$ for $i, j = 1, \ldots, m$. Therefore, for each pair of $(E,F)$ it will have $P = p^r - 1$ pairs of $(E',F')$ satisfying $(E,F)(A) = (E',F')(A)$ corresponding to $P$ values of above $c$. This yields that each equivalence class containing $A$ will have $P^{2m}/P = P^{2m-1}$ different elements (not depending on $A$).

■

The $\mathcal{R}_M$ relation will split the set $\mathcal{D}$ into separate classes, each class has $P^{2m-1}$ different elements. So it is to have the following corollary.

**Corollary 1.** *If there exists $m \times m$ MDS matrices over $GF(p^r)$ then the number of such MDS matrices is a multiple of $P^{2m-1}$, where $P = p^r - 1$.*

For example, for $m = 1$, there are actually $P$ MDS matrices of size $m = 1$. On the other hand, $P^{2m-1} = P^{2.1-1} = P$.

Next, a necessary condition for two MDS matrices to belong to the same equivalence class on the $\mathcal{R}_M$ relation is showed in the Theorem 11.

**Theorem 11.** *If* $A = [a_{i,j}]_{m\times m}, B = [b_{i,j}]_{m\times m} \in \mathcal{D}$ *satisfy* $A\mathcal{R}_M B$ *for* $B = (E,F)(A)$ *then any corresponding elements of* $A$ *and* $B$ *in rows* $i, h(1 \le i < h \le m)$, *and columns* $j, k(1 \le j < k \le m)$ *satisfy the following relation:*

$$(b_{h,k}b_{i,j})(b_{h,j}b_{i,k})^{-1} = (a_{h,k}a_{i,j})(a_{h,j}a_{i,k})^{-1}.$$

***Proof.***

According to the assumption, $B = (E,F)(A)$, i.e $B = [b_{i,j}]_{m\times m} = B = [e_i f_j a_{i,j}]_{m\times m}$.

Consider two elements in row $i$ and columns $j, k$ of $B$ as follows:

$$\begin{cases} b_{i,j} = e_i f_j a_{i,j} \\ b_{i,k} = e_i f_k a_{i,k} \end{cases} \leftrightarrow \begin{cases} e_i = f_j^{-1} a_{i,j}^{-1} b_{i,j} \\ b_{i,k} = f_j^{-1} f_k a_{i,j}^{-1} b_{i,j} a_{i,k}. \end{cases} \tag{19}$$

It is the same for two elements in row $h$ and columns $j, k$ of $B$:

$$\begin{cases} b_{h,j} = e_h f_j a_{h,j} \\ b_{h,k} = e_h f_k a_{h,k} \end{cases} \leftrightarrow \begin{cases} e_h = f_j^{-1} a_{h,j}^{-1} b_{h,j} \\ b_{h,k} = f_j^{-1} f_k a_{h,j}^{-1} b_{h,j} a_{h,k} \end{cases} \tag{20}$$

for $1 \le i < h \le m$ and $1 \le j < k \le m$.

By (19), it yields $f_j^{-1} f_k = b_{i,k} a_{i,j} b_{i,j}^{-1} a_{i,k}^{-1}$ and replaces this into (20), so:

$$b_{h,k} = b_{i,k} a_{i,j} b_{i,j}^{-1} a_{i,k}^{-1} b_{h,j} a_{h,k} \rightarrow (b_{h,k}b_{i,j})(b_{h,j}b_{i,k})^{-1} = (a_{h,k}a_{i,j})(a_{h,j}a_{i,k})^{-1}.$$

The corollary is proven. ■

### 3.2.2. The preservation of involutory property of MDS matrices under the scalar multiplication transformation

In this section, a sufficient condition for the scalar multiplication transformation to be able to preserve of involutory property of MDS matrices is stated and proven. As a consequence, the number of different involutory MDS matrices can be obtained from an original involutory matrix through the scalar multiplication transformation is well defined.

**Theorem 12.** *Let* $E = [e_1, e_2, \ldots, e_m]$, $F = [f_1, f_2, \ldots, f_m]$, (*where* $e_i, f_i \ne 0 \in GF(p^r)$). *Let* $A, B \in \mathcal{D}, A\mathcal{R}_M B$ *where* $B = (E,F)(A)$ *and* $A$ *is involutory. If* $e_i f_i = a \in GF(p^r)$ *and* $a^2 = 1$, *for* $i = 1, \ldots, m$ *then* $B$ *is also involutory.*

***Proof.***

As $A$ is an involutory matrix so: $A = A^{-1}$ or $A^2 = I$. Then,

$$\sum_{j=1}^{m} a_{i,j}a_{j,i} = 1, \text{ for } i = 1, 2, \ldots, m, \tag{21}$$

$$\sum_{t=1}^{m} a_{i,t}a_{t,j} = 0 \text{ for } i, j = 1, 2, \ldots, m \text{ and } i \ne j. \tag{22}$$

According to the assumption, $B = (E,F)(A)$, so it is to have: $B = [b_{i,j}]_{m\times m} = [e_i f_j a_{i,j}]_{m\times m}$.

The elements of the main diagonal of $B^2$ have the below form:

$$b_{i,i} = \sum_{j=1}^{m} e_i e_j f_i f_j a_{i,j} a_{j,i}, \text{ for} i = 1, 2, \ldots, m$$

or

$$b_{i,i} = e_i f_i \left( \sum_{j=1}^{m} e_j f_j a_{i,j} a_{j,i} \right), \text{ for } i = 1, 2, \ldots, m. \tag{23}$$

If $e_i f_i = a \in GF(p^r)$ and $a^2 = 1$ for $i = 1, \ldots, m$,then from (21) and (23), it is to infer:

$$b_{i,i} = a^2 = 1, \text{ for } i = 1, \ldots, m. \tag{24}$$

The elements outside the main diagonal of $B^2$ have the below form:

$$b_{i,j} = \sum_{t=1}^{m} e_i e_t f_t f_j a_{i,t} a_{t,j}, \text{ for } i, j = 1, 2, \ldots, m, \text{ and } i \neq j.$$

or

$$b_{i,j} = e_i f_j \left( \sum_{t=1}^{m} e_t f_t a_{i,t} a_{t,j} \right), \text{ for } i, j = 1, 2, \ldots, m, \text{ and } i \neq j. \tag{25}$$

If $e_i f_i = a \in GF(p^r)$, for $i = 1, \ldots, m$, then from (22) and (25), it follows that:

$$b_{i,j} = e_i f_j a \left( \sum_{t=1}^{m} a_{i,t} a_{t,j} \right) = 0, \text{ for } i, j = 1, 2, \ldots, m, \text{ and } i \neq j. \tag{26}$$

From (24) and (26), it is to infer: $B^2 = I$ or $B = B^{-1}$. Thus, matrix $B$ is involutory. ■

**Notice.**

Suppose the equation $a^2 = 1$ has $k$ solutions. Then there are two circumstances occur:

If $p = 2$ then $k = 1$ and $a = 1$ (i.e the above equation has only one solution $a = 1$).

If $p$ is an odd prime number then $k = 2$ (i.e the above equation has two different solutions in $GF(p^r)$).

For example, let $p = 3$ and the field $GF\left(3^2\right)$ has the primitive polynomial $x^2 + 2x + 2$. Then, there exists two elements of order 2 as 1 and 2. Let $p = 5$ and the field $GF\left(5^2\right)$ has the primitive polynomial $x^2 + 2x + 3$. Then, there exists two elements of order 2 as 1 and 4.

Next, the Corollary 2 indicates the number of possible involutory MDS matrices generated from an original MDS matrix through the scalar multiplication transformation.

**Corollary 2.** *Let $A \in \mathcal{D}$ be involutory. Then it is possible to generate $kP^{m-1}(k = 1$ or $k = 2)$ involutory MDS matrices from matrix $A$ through the scalar multiplication transformation, where $P = p^r - 1$.*

***Proof.***

By the condition of the Theorem 10, it has $P^m$ ways to choose randomly the vector $E$ over $GF(p^r) \setminus \{0\}$, then the vector $F$ will be calculated according to $E$ by the condition $e_i f_i = a$, in detail: $f_i = a e_i^{-1}$. In addition, because it has $k$ $(k = 1$ *or* $k = 2)$ different values of $a$ in $GF(p^r)$

satisfying $a^2 = 1$, so it is to have $kP^m$ different pairs of $(E, F)$ satisfying the condition of the Theorem 12, and it can be obtained $kP^m$ involutory matrices. The question is how many different involutory matrices generated in this way?

Let $A \in \mathcal{D}$ and $(E, F)$ satisfy the condition of the Theorem 12. Suppose $(E', F')$ satisfies $(E, F)(A) = (E', F')(A)$, i.e $e'_i f'_j = e_i f_j;\ i, j = 1, 2, \ldots, m$. Similar arguments are as in the proof of the Theorem 10, there exists $c$ being an other than 0 element in $GF(p^r)$ such that $e'_i = c^{-1} e_i$ and $f'_j = c f_j$ for all $i, j = 1, 2, \ldots, m$. Then, it is to have $f'_i = c f_i = c a e_i^{-1} = c a c^{-1} e_i'^{-1} = a e_i'^{-1}$ i.e $(E', F')$ also generated by the above way and not depending on $c$.

Thus, there are $P = p^r - 1$ pairs of $(E', F')$ corresponding to $P$ values of $c$, satisfying the condition of the Theorem 12 and multiplying $A$ by them results in the same matrix as multiplying $A$ by $(E, F)$.

Consequently, there are $kP^m/P = kP^{m-1}$ different involutory MDS matrices in total generated by the condition of the Theorem 12.

In case of $p = 2$, it is to have $k = 1$, and that number is $P^{m-1} = (p^r - 1)^{(m-1)}$.

If $p$ is an odd prime number then $k = 2$, and that number is $2P^{m-1} = 2(p^r - 1)^{(m-1)}$. ■

For example, for $m = 1$ and $p$ is an odd prime number, there are only two involutory MDS matrices are $[a_1]$ and $[a_2]$, for $a_1$ and $a_2$ are the solutions in $GF(p^r)$ of the equation $x^2 = 1$. When multiplying any row of an involutory matrix by $e0$ and multiplying its any column by $f = ae^{-1}$ will result in following matrices: $\left[eae^{-1}a_i\right] = [aa_i]$, $i = 1, 2$. It means that the two result matrices are obtained. On the other hand, it is to have the following equation: $2P^{m-1} = 2P^0 = 2$..

### 3.3. The relationship between $\mathcal{R}_M$ and $\mathcal{R}_p$

The relationship between $\mathcal{R}_M$ and $\mathcal{R}_p$ is presented by the Theorem 13.

**Theorem 13.** *Let the set $\mathcal{D}$ for $m \geq 2$ and $A \in \mathcal{D}$. Assuming that matrix $B \in \mathcal{D}$ satisfies simultaneously $A\mathcal{R}_M B$ and $A\mathcal{R}_p B$. Then there exists $l \in \{0, 1, \ldots, r-1\}$ such that:*

$$\left(\frac{ad}{bc}\right)^{p^l - 1} = 1,$$

*for $\begin{bmatrix} ab \\ cd \end{bmatrix}$ is any submatrix of size 2 of matrix $A$.*

***Proof.***

Suppose that there exists a matrix $B \in \mathcal{D}$ satisfying simultaneously $A\mathcal{R}_M B$ and $A\mathcal{R}_p B$.

By the Theorem 11, the elements $a, b, c, d$ in $A$ satisfy the following relation:

$$\left(\bar{a}\bar{d}\right)(\bar{b}\bar{c})^{-1} = (ad)(bc)^{-1} \tag{27}$$

for $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ are elements in $B$ corresponding to the elements $a, b, c, d$.

According to the assumption, $A\mathcal{R}_p B$ , so $\exists\, l$, $(0 \leq l \leq r-1)$ such that $B = A_{d^{p^l}}$.

As a result, it is to have: $\bar{a} = a^{p^l}, \bar{b} = b^{p^l}$. Replacing these values into (16) obtains:

$$\left(a^{p^l} d^{p^l}\right)\left(b^{p^l} c^{p^l}\right)^{-1} = (ad)(bc)^{-1}$$

or

$$(ad)^{p^l} (bc)^{-p^l} = (ad) (bc)^{-1},$$

or

$$\left(\frac{ad}{bc}\right)^{p^l} = \frac{ad}{bc}$$

From this equation, the theorem is proven. ■

## 4. EXAMPLES

In this Section, two following examples are given to demonstrate some results. Let $A$ and $B$ are MDS matrices over $GF\left(2^8\right)$ with the irreducible polynomial $0x169$ $(x^8 + x^6 + x^5 + x^3 + 1)$ and they are recursive matrices.

First, matrix $A$ has the following hexa form:

$$A = \begin{bmatrix} 29 & 46 & 5A & 85 \\ 2F & D2 & 3D & A5 \\ CB & 87 & A1 & ED \\ 8B & 87 & E6 & CA \end{bmatrix}$$

According to our calculation, matrix $A$ has the branch number equal to 5, number of fixed points equal to $2^0$ and coefficient of fixed points equal to $2.93874e\text{-}039(2^{-127.9999})$. Moreover, matrix $A$ is a recursive matrix:

$$A = S^4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 29 & 46 & 5A & 85 \end{bmatrix}^4$$

The cycle of direct 2 exponent transformation of matrix $A$ is 8.

Consider matrix $A' = A_{d^{2^4}}$. It is to have:

$$A' = \begin{bmatrix} 3D & 53 & 48 & FB \\ 5D & B8 & 29 & C8 \\ A7 & F8 & CD & 92 \\ F2 & FB & 9F & A6 \end{bmatrix}$$

Matrix $A'$ is calculated and as a result it has the same branch number, number of fixed ints and coefficient of fixed points as the matrix $A$. Again this shows that the direct exponent transformation can preserve the branch number, number of fixed points and coefficient of fixed points of the matrix $A$.

In addition, matrix $A'$ is also a recursive matrix:

$$B = \begin{bmatrix} 14 & E6 & A2 & F6 \\ 86 & 20 & 9E & 73 \\ E3 & DA & A8 & 84 \\ 71 & 6D & 88 & 95 \end{bmatrix}.$$

Next, matrix $B$ has the following hexa form:

$$B' = \begin{bmatrix} 14 & E6 & A2 & 4F \\ 86 & 20 & 9E & D6 \\ E3 & DA & A8 & 46 \\ 4F & 07 & 8B & 6A \end{bmatrix}.$$

According to the calculation, matrix $B$ has the branch number equal to 5, number of fixed points equal to $2^0$ and coefficient of fixed points equal to 2.93874e-039($2^{-127.9999}$). Matrix $B'$ is generated from $B$ by multiplying row 4 in $B$by $0 \times 06$ and multiplying column 4 in $B$ by $0 \times 05$. It is to have:

The cycle of this scalar multiplication transformation is 15. The branch number of $B'$ is 5. Fortunately, matrix $B'$ has the the same number of fixed points and coefficient of fixed points as matrix $B$ in this case. Matrix $B'$ may not be a recursive matrix.

It is known that the number of fixed points of the MDS matrix in AES is $2^{16}$ (it is big a bit). Therefore, it is possible to replace that matrix by $A'$ or $B'$ to reduce the number of fixed points. This will limit some attacks based on fixed points on block ciphers. In addition, as $A'$ is a recursive matrix it is efficient for hardware implementation.

However, the two above examples are only to demonstrate some our results. In order to use these matrices for practical applications it is to have to consider many other points.

## 5. APPLICATIONS OF THE NEW RESULTS ABOUT THE MDS MATRIX TRANSFORMATIONS ON BLOCK CIPHERS

It can be seen that MDS matrices have been studied because of their preeminent properties. Dynamic MDS matrices have been also under study in order to improve the security of block ciphers.

The results of Theorem 1, Theorem 2 in [18] show that it can be obtained many different MDS matrices from an existing MDS matrix by the direct exponent transformation.

When generating dynamic MDS matrices for block ciphers, it is very important to verify whether the result matrix still owns good cryptographic properties or not? The results of Theorem 6 in [19] show that the direct exponent transformation indeed preserves good cryptographic properties including MDS, involutory, symmetric, recursive (exponent of a serial matrix), the number of 1's and distinct elements in a matrix, circulant and circulant-like. Therefore, from an MDS matrix with good cryptographic properties, many different MDS matrices with the good cryptographic properties can be created. Those suggest us an efficient method for constructing a dynamic diffusion layer for block ciphers based on the direct exponent transformation.

In this paper, by the Theorem 8, it can be seen that the direct exponent transformation can also preserve the coefficient of fixed points of MDS matrices. This also suggests us a good way for constructing a dynamic diffusion layer for block ciphers by using the the direct exponent transformation for an input MDS matrix having a small coefficient of fixed points. Then, the different MDS matrices with the same small coefficient of fixed points as the input MDS matrix can be generated. These matrices can be used for the diffusion layer in different rounds of block ciphers because they are very useful for limiting some attacks based on fixed points on block ciphers.

Indeed, the direct exponent transformation is very useful for constructing a dynamic diffusion layer. Firstly, the storage space can be saved because it may be only an original MDS matrix need to be stored, then for each round the direct exponent transformation can be used to generate a corresponding MDS matrix from the original MDS matrix. Secondly, we just only perform exponent

of each element of the original matrix to create a new matrix, so it is simple. Third, from an original MDS matrix with good cryptographic properties one can create MDS matrices having similar properties to use for the encryption rounds.

The result of the Theorem 12 shows that the scalar multiplication transformation can preserve the involutory property of MDS matrices. Moreover, by the Corollary 2, the number of different involutory MDS matrices generated from an original involutory MDS matrix by the scalar multiplication transformation can be specified. These results also suggest us an interesting method for constructing a dynamic diffusion layer for block ciphers based on that transformation for an input involutory MDS matrix.

By the Proposition 1 and Theorem 7, it can be checked whether two any MDS matrices belong to the same equivalence class on the $\mathcal{R}_p$ relation or not. Then two MDS matrices not belonging to the same equivalence class can be chosen and the number of different MDS matrices obtained by the direct exponent transformation would be a total of matrices from the two equivalence classes. Since if two MDS matrices belonging to the same equivalence class are chosen then the total number of MDS matrices obtained is just equal to the cycle of that equivalence class. More generally, it can be chosen for many different MDS matrices from other equivalence classes on the $\mathcal{R}_p$ relation. Therefore, the total number of MDS matrices obtained by the direct exponent transformation from these equivalence classes will be much larger than the case of the original matrices selected from the same equivalence class.

Same as above, the results of Proposition 2 and Theorem 11 can help us to check whether two any MDS matrices belong to the same equivalence class on the $\mathcal{R}_M$ relation or not.

The Theorem 9 and Theorem 10 enable us to calculate the number of MDS matrices in a cycle of the scalar multiplication transformation and the number of different MDS matrices in an equivalence class on the $\mathcal{R}_M$ relation. Then two MDS matrices not belonging to the same equivalence class can be chosen and the number of different MDS matrices obtained by that transformation would be a total of matrices from the two equivalence classes

By the Theorem 13, it can be checked whether the two given MDS matrices are simultaneously equivalent on $\mathcal{R}_M$ and $\mathcal{R}_p$ relations or not. This makes sense when the dynamic diffusion layer algorithms using both of transformations based on $\mathcal{R}_M$ and $\mathcal{R}_p$. Therefore, the condition of Theorem 13 needs to be checked to indicate the two given MDS matrices are simultaneously equivalent on the $\mathcal{R}_M$ and $\mathcal{R}_p$ relations or not. Meanwhile, the total number of the MDS matrices obtained from these transformations based on $\mathcal{R}_M$ and $\mathcal{R}_p$ in other cases will be larger than in the case of the two original MDS matrices satisfying simultaneously both of the $\mathcal{R}_M$ and $\mathcal{R}_p$ relations.

Interestingly, increasing to the number of dynamic MDS matrices obtained from the original MDS matrices through the direct exponent and scalar multiplication transformations will be significant in the term of increasing to the space of MDS matrices used in dynamic diffusion layer algorithms. Since then, this contributes to enhance the security of these algorithms.

Consequently, the results obtained from the direct exponent and scalar multiplication transformations take an important part in constructing dynamic diffusion layers for block ciphers. As a result, they can serve as an important theoretical basis for creating efficient dynamic algorithms for diffusion layers in block ciphers. These algorithms are not only effective but also contribute to increase the security of the ciphers.

## 6. CONCLUSION

In this paper, some new results from the conservation of many good cryptographic properties of MDS matrices under the direct exponent and scalar multiplication transformations are presented. In addition, other important cryptographic properties obtained from studying the equivalence relations based on these transformations are given. An estimation of the number of $m \times m$ MDS matrices over $GF(p^r)$ is also provided. Finally, these results have been shown to have important applications in constructing dynamic diffusion layers for block ciphers. The strength of the ciphers against developing cryptanalytic techniques can be enhanced by the dynamic MDS diffusion layers.

## REFERENCES

[1] S. Vaudenay, "On the need for multipermutations: Cryptanalysis of md4 and safer," in *International Workshop on Fast Software Encryption*. Springer, 1994, pp. 286–297.

[2] C. P. Schnorr and S. Vaudenay, "Black box cryptanalysis of hash networks based on multipermutations," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1994, pp. 47–57.

[3] D. Kwon, S. H. Sung, J. H. Song, and S. Park, "Design of block ciphers and coding theory," *Trends in Mathematics*, vol. 8, no. 1, pp. 13–20, 2005.

[4] L. Keliher, "Linear cryptanalysis of substitution-permutation networks," Ph.D. dissertation, Queens University, 2003.

[5] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.

[6] F. P. NIST, "197," advanced encryption standard (aes)," november 2001."

[7] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, "The cipher shark," in *International Workshop on Fast Software Encryption*. Springer, 1996, pp. 99–111.

[8] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-bit block cipher," *NIST AES Proposal*, vol. 15, 1998.

[9] G. Murtaza, A. A. Khan, S. W. Alam, and A. Farooqi, "Fortification of aes with dynamic mix-column transformation." *IACR Cryptology ePrint Archive*, vol. 2011, p. 184, 2011.

[10] R. Mohamed, M. Abdulrashid, S. Moesfa, and M. Ramlan, "A method for linear transformation in substitution-permutation network symmetric-key block cipher," May 10 2012, wO Patent App. PCT/MY2011/000,105. [Online]. Available: https://www.google.com/patents/WO2012060685A1?cl=en

[11] F. Ahmed and D. Elkamchouchi, "Strongest aes with s-boxes bank and dynamic key mds matrix (sdk-aes)," *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, p. 530, 2013.

[12] G. Murtaza and N. Ikram, "Direct exponent and scalar multiplication classes of an mds matrix." *IACR Cryptology ePrint Archive*, vol. 2011, p. 151, 2011.

[13] K. C. Gupta and I. G. Ray, "On constructions of mds matrices from companion matrices for lightweight cryptography," in *International Conference on Availability, Reliability, and Security*. Springer, 2013, pp. 29–43.

[14] ——, "On constructions of mds matrices from circulant-like matrices for lightweight cryptography," Technical Report No. ASU/2014/1, Dated: 14th February, Tech. Rep., 2014.

[15] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977.

[16] M. R. Z'aba, "Analysis of linear relationships in block ciphers," 2010.

[17] Y. Jun, Y. Mazhi-xia, and C. Jiang, "On direct exponentiation of maximum distance separable matrices," *Journal of Southwest University for Nationalities. Natural Science Edition*, pp. 1003–2843, 2011.

[18] T. T. Luong, N. N. Cuong, and L. T. Dung, "A new statement about direct exponent of an mds matrix in block ciphers," in *Knowledge and Systems Engineering (KSE), 2015 Seventh International Conference on*. IEEE, 2015, pp. 340–343.

[19] T. T. Luong, N. N. Cuong *et al.*, "The preservation of good cryptographyic properties of mds matrix under direct exponent transformation," *Journal of Computer Science and Cybernetics*, vol. 31, no. 4, p. 291, 2015.

*Received on January 29 - 2016*
*Revised on April 20 - 2016*