*Journal of Computer Science and Cybernetics, V.31, N.4 (2015), 291–303*
DOI: 10.15625/1813-9663/31/4/7059

# THE PRESERVATION OF GOOD CRYPTOGRAPHIC PROPERTIES OF MDS MATRIX UNDER DIRECT EXPONENT TRANSFORMATION

TRAN THI LUONG[1], NGUYEN NGOC CUONG[2], LUONG THE DUNG[1,*]

[1] *Academy of Cryptography Techniques, Hanoi, Vietnam;*
*ttluong@bcy.gov.vn; *ltdung@bcy.gov.vn*
[2] *Vietnam Government Information Security Commission, Hanoi, Vietnam;*
*nguyenngoccuong189@gmail.com*

**Abstract.** Maximum Distance Separable (MDS) code has been studied for a long time in the coding theory and has been applied widely in cryptography. The methods for transforming an MDS into other ones have been proposed by many authors in the literature. These methods are called MDS matrix transformations in order to generate different MDS matrices (dynamic MDS matrices) from an existing one. In this paper, some new results on the preservation of many good cryptographic properties of MDS matrices under direct exponent transformation are presented. These good cryptographic properties include *MDS, involutory*, *symmetric, recursive* (*exponent of a companion matrix*), *the number of* $1's$ *and distinct elements in a matrix, circulant and circulant-like.* In addition, these results are 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.
**Keywords.** MDS matrix, dynamic MDS matrix, direct exponent matrix, cryptographic properties.

## 1. INTRODUCTION

Claude Shannon, in his paper of "Communication Theory of Secrecy Systems" [1] defined *confusion* and *diffusion* as two mandatory properties, required for the design of block ciphers. Confusion is to make the relationship of statistical independence between ciphertext string and plaintext string more complicated while diffusion is associated with dependency of output bits on input bits.

As we know, MDS matrices were first introduced by Serge Vaudenay in FSE'95 [2] as a linear case of multipermutations. Multipermutations or MDS matrices characterize the notion of perfect diffusion [3], which requires that the change of some $t$ out of $m$ input bits must affect at least $m - t + 1$ output bits. The branch number of diffusion layer in Substitution-Permutation Network (SPN) structure has been regarded as an important criterion for diffusion layer design. For block ciphers, the resistance against strong attacks (such as linear and differential attacks) depends on the branch number of diffusion layers of the ciphers. The greater the branch number is the higher security of block cipher will be. As an MDS matrix corresponds to a permutation with maximum branch number, it provides the best level of diffusion. Therefore, MDS matrices have been used for diffusion in many block ciphers such as: AES [4,5], SHARK [6], Square, Twofish [7], Anubis, Khazad, Manta, Hierocrypt and Camellia. These are also used in stream ciphers like MUGI and cryptographic hash functions like WHIRLPOOL.

Thank to the usefulness of MDS matrices, besides building MDS matrices from MDS codes (e.g. Reed-Solomon codes), there are lots of methods for constructing them such as: Cauchy matrices [8], Hadamard matrices [9], Vandermonde matrices [10], Companion matrices [11], recursive MDS matrices and so on.

However, the construction of the MDS diffusion layers (the diffusion layer represented by MDS matrices [12,13]) with low-cost implementation is a major challenge for the designers. There are three main research directions on MDS matrices to obtain low-cost implementation, namely: the construction of MDS matrices having a large number of $1s$ and a small number of different constants [14,15], the construction of involutory MDS matrices [9,10,16–18], the construction of recursive MDS matrices [11–13,19,20]. In addition, some circulant and circulant-like MDS matrices were proposed [14,15]. The MDS matrices satisfying simultaneously all afore mentioned properties are desirable for block cipher designers and have good cryptographic properties. However, they are very challenging to construct. To further enhance the security of the block ciphers, dynamic block ciphers (block ciphers which are made dynamically in one of their components) have been under study, for example [21–23]. In [21,22], the authors constructed a key-dependent diffusion layer by creating MDS matrices depending on a secret key for each round. In [23], 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: direct exponent, scalar multiplication [24], and permutations of rows and columns [15,22]. However, no studies have ever shown the conservation of good cryptographic attributes of an MDS matrix as mentioned above under these transformations. The concept of direct exponent of an MDS matrix was first presented by Ghulam Murtaza and Nassar Ikram [24]. In this paper, some novel results on the direct exponent transformation are presented including: direct $p$ exponent of an MDS matrix over $GF(p^r)$ which is an MDS matrix; the cycle of the direct $p$ exponent transformation; the conservation of many good cryptographic properties of MDS matrices under direct exponent transformation such as: *MDS, involutory*, *symmetric, recursive* (*exponent of a companion matrix*), *the number of* $1s$ *and distinct elements in a matrix, circulant and circulant-like*. In addition, these results are shown to have important applications in constructing dynamic diffusion layers for block cipher systems.

The paper is organized as follows. Section 2 presents some preliminaries and related works including the theorem in [24] about direct square of an MDS matrix and the opposite opinion of the authors in [25] about this theorem. In Section 3, some new theorems on the preservation of good cryptographic properties of MDS matrices are established. Section 4 provides important applications of the new results achieved in this paper in block ciphers. And conclusion of the paper is in Section 5.

## 2. PRELIMINARY AND RELATED WORKS

### 2.1. MDS matrices

Since MDS matrices provide perfect diffusion, they are extremely 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** ( [26, page 33]). *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** ( [26, page 321]). *A $[n, k, d]$ code $C$ with generator matrix $G = [I \vee A]$ 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.

**Fact:** *A square matrix $A$ is an MDS matrix if and only if every square submatrices of $A$ are nonsingular.*

### 2.2. Direct exponent of an MDS matrix

The definition of direct exponent of an MDS matrix was introduced by Ghulam Murtaza and Nassar Ikram in [22]. The authors gave the direct exponent definition, as follows:

**Definition 1** ( [24]). *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 result of [24] is as follows:

**Theorem 3** ( [24]). *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.*

In [25], the authors proved that the above theorem was not correct. In the next section, this issue will be further developed.

## 3. THE PRESERVATION OF GOOD CRYPTOGRAPHIC PROPERTIES OF MDS MATRICES THROUGH THE DIRECT EXPONENT TRANSFORMATION

In this Section, the statement and proof of the Theorem 3 [22] above is adjusted. In addition, the theorem on the preservation of good cryptographic properties of MDS matrices under the direct exponent transformation is stated and proven.

Consider the following theorem:

**Theorem 4.** *Let $A = [a_{i,j}]_{m\times m}$, $a_{i,j} \in GF(p^r)$ be an MDS matrix, for some prime number $p$, then direct $p$ exponent matrix $A_{d^p} = \left[a_{i,j}^p\right]_{m\times m}$ of $A$ is an MDS matrix.*

*Proof.* According to the supposition, matrix

$A = [a_{i,j}]_{m\times m}$, $a_{i,j} \in GF(p^r)$ is MDS, thus all the submatrices of $A$ are nonsingular.

We know that, if $a_i, (i = 1, 2, \ldots n) \in GF(p^r)$ then:

$$(a_1 + a_2 + \cdots + a_n)^p = (a_1^p + a_2^p + \ldots + a_n^p) \tag{1}$$

Consider matrix $A_{d^p} = \left[a_{i,j}^p\right]_{m\times m}$ over $GF(p^r)$. As $A$ is an MDS matrix, so $a_{i,j} \neq 0$, result in $a_{i,j}^p \neq 0$. Therefore, all submatrices of size 1 of $A_{d^p}$ are nonsingular.

Next, it is to prove that all $2 \times 2$ submatrices of $A_{d^p}$ are nonsingular. Indeed, consider an arbitrary $2 \times 2$ submatrix of $A_{d^p}$, such as the following matrix:

$$MP_2 = \begin{bmatrix} a^p b^p \\ c^p d^p \end{bmatrix}$$

then apply (1), the determinant of this matrix is:

$$a^p d^p - b^p c^p = (ad - bc)^p$$

Let $U_2 = (ad - bc)$, then $U_2$ is exact determinant of corresponding $2 \times 2$ submatrix of $A$ as the following:

$$\begin{bmatrix} ab \\ cd \end{bmatrix}$$

Since $A$ is an MDS matrix, so $U_2 \neq 0$. As a result, the determinant of matrix $MP_2$ is $U_2^p \neq 0$. Thus matrix $MP_2$ is nonsingular. Consequently, all $2 \times 2$ submatrices of $A_{d^p}$ are nonsingular.

Suppose inductively that all submatrices of size $(k-1)$ of $A_{d^p}$ have determinants equal to $p$ exponent of determinants of corresponding submatrices of size $(k-1)$ of $A$, and we will prove that this is true for $k\,(k \leq m)$.

Consider an arbitrary $k \times k$ submatrix of $A_{d^p}$, such as:

$$MP_k = \begin{bmatrix} b_{0,0}^p b_{0,1}^p ... b_{0,k-1}^p \\ b_{1,0}^p b_{1,1}^p ... b_{1,k-1}^p \\ \vdots \ddots \\ b_{k-1,0}^p b_{k-1,1}^p ... b_{k-1,k-1}^p \end{bmatrix}$$

Apply (1) then the determinant of $MP_k$ is calculated as follows (developing follow the first row of $MP_k$):

$$b_{0,0}^p \begin{vmatrix} b_{1,1}^p b_{1,2}^p \ldots b_{1,k-1}^p \\ \vdots \ddots \\ b_{k-1,1}^p b_{k-1,2}^p \ldots b_{k-1,k-1}^p \end{vmatrix} - b_{0,1}^p \begin{vmatrix} b_{1,0}^p b_{1,2}^p \ldots b_{1,k-1}^p \\ \vdots \ddots \\ b_{k-1,1}^p b_{k-1,2}^p \ldots b_{k-1,k-1}^p \end{vmatrix} + \ldots + (-1)^{k-1} b_{0,k-1}^p \begin{vmatrix} b_{1,0}^p b_{1,1}^p \ldots b_{1,k-2}^p \\ \vdots \ddots \\ b_{k-1,0}^p b_{k-1,1}^p \ldots b_{k-1,k-2}^p \end{vmatrix}$$

$$b_{0,0}^p U_{k-1,1}^p - b_{0,1}^p U_{k-1,2}^p + \ldots + (-1)^{k-1} b_{0,k-1}^p U_{k-1,k}^p$$

$$\left[ b_{0,0} U_{k-1,1} - b_{0,1} U_{k-1,2} + \ldots + (-1)^{k-1} b_{0,k-1} U_{k-1,k} \right]^p$$

where $U_{k-1,1}, U_{k-1,2}, \ldots, U_{k-1,k}$ are in turn determinants of $k$ submatrices of size $(k1)$ of $A$ corresponding with $k$ submatrices of size $(k1)$ of $MP_k$ in the above formula.

Let $U_k = b_{0,0} U_{k-1,1} - b_{0,1} U_{k-1,2} + \ldots + (-1)^{k-1} b_{0,k-1} U_{k-1,k}$

It is clear that $U_k$ is exact determinant of the corresponding $k \times k$ submatrix of $A$ as follow (corresponds with matrix $MP_k$):

$$\begin{bmatrix} b_{0,0} b_{0,1} ... b_{0,k-1} \\ b_{1,0} b_{1,1} ... b_{1,k-1} \\ \vdots \ddots \\ b_{k-1,0} b_{k-1,1} ... b_{k-1,k-1} \end{bmatrix}$$

Since matrix $A$ is MDS, so $U_k \neq 0$, as a result $U_k^p \neq 0$. Therefore, the determinant of matrix $MP_k$ is $U_k^p \neq 0$. Thus matrix $MP_k$ is nonsingular. Consequently, all submatrices of size $k$ of $A_{d^p}$ are nonsingular.

With above inductive proof, it concludes that $A_{d^p}$ is an MDS matrix. □

**Comment 1.**
1. After the Theorem 4 it can be seen that for a given $m \times m$ MDS matrix, it is possible to generate other ones of the same size by doing the direct $p$ exponent transformations. Moreover, all the square submatrices of an MDS matrix are MDS, so one can also generate many different MDS matrices of smaller size from an original MDS matrix by this method.
2. For $GF(p^r)$, direct $e$ exponent of matrix $A$ is $A_{d^e}$ may not be an MDS matrix if $e \neq p$. The authors in [23] provided an example of a $3 \times 3$ matrix over $GF(7), (p = 7, r = 1)$]:

$$A = \begin{bmatrix} 625 \\ 433 \\ 551 \end{bmatrix}$$

$A$ is an MDS matrix. But the direct square matrix $A_{d^2}$ $(e = 2)$ of $A$ is not MDS:

$$A_{d^2} = \begin{bmatrix} 6^2 2^2 5^2 \\ 4^2 3^2 3^2 \\ 5^2 5^2 1^2 \end{bmatrix} (mod 7) = \begin{bmatrix} 144 \\ 222 \\ 441 \end{bmatrix}$$

Because the submatrix $\begin{bmatrix} 44 \\ 22 \end{bmatrix}$ of $A_{d^2}$ is singular.

Consider direct $p$ exponent matrix of $A$, $A_{d^p} = A_{d^7}$:

$$A_{d^7} = \begin{bmatrix} 6^7 2^7 5^7 \\ 4^7 3^7 3^7 \\ 5^7 5^7 1^7 \end{bmatrix} (mod 7) = \begin{bmatrix} 625 \\ 433 \\ 551 \end{bmatrix}$$

In this case, matrix $A_{d^7}$ is the original matrix $A$, thus it is obvious that $A_{d^7}$ is an MDS matrix.

**Corollary 1.** *Let $A = [a_{i,j}]_{m \times m}$, $a_{i,j} \in GF(p^r)$ be an MDS matrix, for a prime number $p$, then $A_{d^{p^k}} = \left[a_{i,j}^{p^k}\right]_{m \times m}, (k = 1, 2, \ldots)$ of $A$ is an MDS matrix.*

Next, it is to show the $\tau$ number (cycle) that when doing direct $p$ exponent of an MDS matrix for $\tau$ times will result in the original MDS matrix.

Consider matrix $A = [a_{i,j}]_{m \times m}$, $a_{i,j} \in GF(p^r)$, with $p$ is a prime number.

Suppose that there are $c$ distinct elements in matrix $A$, denoted by $a_1, a_2, \ldots, a_c$. They are all other than 1 and orders of them over $GF(p^r)$ are in turn $n_1, n_2, \ldots, n_c$. Denote $+?N^{\square}$ is the set of positive integers and $lcm(n_1, n_2, \ldots, n_c)$ is the least common multiple of $n_1, n_2, \ldots, n_c$.

We have the following theorem:

**Theorem 5.** *Let $A = [a_{i,j}]_{m \times m}$ , $a_{i,j} \in GF(p^r)$ be an MDS matrix, for some prime number $p$,then we have $A_{d^{p^\tau}} = A$ for $\tau = min\{B\}$ and:*

$$+ : lcm(n_1, \ldots, n_c) \vee \left(p^k - 1\right)$$
$$k \in N^{\square}$$
$$B = ?$$

*Moreover, $\tau$ is the smallest value such that $A_{d^{p^\tau}} = A$.*

*Proof.* As $A$ is an MDS matrix then all of elements of $A$ are nonzero and have finite orders. So $lcm\,(n_1,\ldots,n_c)$ exists and it is a positive integer.

Obviously $r{\in}B$, because $p^r-1$ is divisible by the orders of any elements other than 0, $a{\in}GF\,(p^r)$. Therefore, $p^r-1$ is divisible by $lcm\,(n_1,\ldots,n_c)$. As the result, there exists the number $\tau = min\,\{B\}\leq r$.

From the definition of $\tau$, there exists the positive integer $d$ such that $p^\tau{-}1 = d.lcm\,(n_1,\ldots,n_c)$ and then for all $a{\in}A$, so $a^{p^\tau-1} = a^{d.lcm(n_1,\ldots,n_c)} = 1$, or $a^{p^\tau} = a$. Consequently, $A_{d^{p^\tau}} = A$.

Suppose that there exists a positive integer $t$ satisfying $A_{d^{p^t}} = A$. Then for an element $a{\in}A$, it yields $a^{p^t} = a$. It follows that $ord\,(a) \vee \left(p^t-1\right)$, so it is induced that $lcm\,(n_1,\ldots,n_c) \vee \left(p^t-1\right)$. Therefore $t{\in}B$, then $\tau{\leq}t$. □

The number $\tau$ is called *cycle* of the direct $p$ exponent transformation of matrix $A$.

**Comment 2.** *With cycle $\tau$, perform direct p exponent of the MDS matrix for $\tau$ times then the resulting matrix is equal to the original MDS matrix. By this method, it can obtain $\tau$-1 different MDS matrices from an existing MDS matrix if $\tau > 1$.*

**Example 1.** *Let $A = [a_{i,j}]_{m\times m}$ be an MDS matrix over $GF\,(p^r)$ where $p = 3$, $r = 8$. Note that the number $3^8 - 1 = 6560$ is divisible by the orders of elements in $GF\left(3^8\right)$. Suppose that matrix A includes four distinct elements (other than 0 and 1), they are: $a_1$, $a_2$, $a_3$, $a_4$. Let the orders of these elements over $GF\left(3^8\right)$ be in turn: $n_1 = 2, n_2 = 5, n_3 = 8, n_4 = 10$. (Obviously, the number 6560 is divisible by these orders).*

$$\rightarrow lcm\,(n_1,n_2,n_3,n_4) = 40$$

We try in turn numbers $k = 1, 2, .., 7$ until the first one is found satisfying the condition:

$$p^k - 1 = d.lcm\,(n_1,n_2,n_3,n_4)$$

In this case, it is found that the first number satisfying this condition is $k = 4$, i.e. $3^4 1 = 80 = 2.40$.

Then, the cycle is $\tau = 4$.

Therefore, doing direct $p$ exponent matrix $A$ for four times yields the original matrix $A$.

**Theorem 6.** *Let $A = [a_{i,j}]_{m\times m}$ , $a_{i,j}{\in}GF\,(p^r)$ be an MDS matrix, for some prime number p. 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 following properties:*

1. *MDS*
2. *Involutory (i.e. if $\left(A = A^{-1}\right)$ then $A_{d^{p^k}} = \left(A_{d^{p^k}}\right)^{-1}$)*
3. *Symmetric (i.e. if $\left(A = A^T\right)$ then $A_{d^{p^k}} = \left(A_{d^{p^k}}\right)^T$)*
4. *Recursive (exponent of a companion matrix)*
5. *The number of 1s and distinct elements in matrix A.*
6. *Circulant and circulant-like.*

-Item 1: comes directly from the Theorem 1 and Corollary 1.

-Item 2: Follow the assumption $A = A^{-1}$, so $A^2 = I$, then all of elements on the main diagonal of $A$ are 1 and other elements are zero. Therefore, it results in:

$$\begin{cases} \sum\limits_{j=1}^{m} a_{i,j}a_{j,i} = 1 & \text{for } i = 1, 2, \ldots, m. \\ \sum\limits_{j=1}^{m} a_{i,j}a_{j,t} = 0 & \text{for } i, t = 1, 2, \ldots, m \wedge i \neq t \end{cases} \tag{2}$$

Suppose that $B = A_{d^{p^k}} = \left[a_{i,j}^{p^k}\right]_{m\times m}$ is direct $p^k\,(1\leq k\leq \tau)$ exponent of matrix $A$. Then elements on the main diagonal of $B^2$ are: $\sum\limits_{j=1}^{m} a_{i,j}^{p^k}a_{j,i}^{p^k} for i = 1, 2, \ldots, m$. Apply (1), it yields:

$$\sum_{j=1}^{m} a_{i,j}^{p^k}a_{j,i}^{p^k} = \sum_{j=1}^{m} (a_{i,j}a_{j,i})^{p^k} = \left(\sum_{j=1}^{m} a_{i,j}a_{j,i}\right)^{p^k}, (i = 1, 2, \ldots, m).$$

From (2) it is to infer: $\sum\limits_{j=1}^{m} a_{i,j}^{p^k}a_{j,i}^{p^k} = 1, for i = 1, 2, \ldots, m.$

Similarly, the elements that do not belong to the main diagonal of $B^2$ are: $\sum\limits_{j=1}^{m} a_{i,j}^{p^k}a_{j,t}^{p^k} for i, t = 1, 2, \ldots, m \wedge i \neq t.$

Apply (1), it results in:

$$\sum_{j=1}^{m} a_{i,j}^{p^k}a_{j,t}^{p^k} = \sum_{j=1}^{m} (a_{i,j}a_{j,t})^{p^k} = \left(\sum_{j=1}^{m} a_{ij}a_{jt}\right)^{p^k}, (i, t = 1, 2, \ldots, m; i \neq t)$$

From (2) it is to infer: $\sum\limits_{j=1}^{m} a_{i,j}^{p^k}a_{j,t}^{p^k} = 0 for i, t = 1, 2, \ldots, m \wedge i \neq t.$

Therefore, obviously $B^2 = I$ or $B = B^{-1}$.

-Item 3: Follow the assumption $A = A^T$, so $a_{i,j} = a_{j,i} for i = 1, 2, \ldots, m-1; j = i+1, \ldots, m$. Suppose $B = A_{d^{p^k}} = [b_{ij}]_{m\times m} = \left[a_{i,j}^{p^k}\right]_{m\times m}$ is direct $p^k\,(1\leq k\leq \tau)$ exponent of matrix $A$. Since $a_{i,j} = a_{j,i} \rightarrow a_{i,j}^{p^k} = a_{j,i}^{p^k}$ then for matrix $B$ it yields: $b_{i,j} = b_{j,i} for i = 1, 2, \ldots, m-1; j = i+1, \ldots, m$. Hence, $B = B^T$.

Item 4: Follow the assumption $A$ is a recursive matrix that is exponent of a companion matrix. Suppose $S$ is this companion matrix, i.e. $A = S^m$, where $S$ has following form:

$$S = \begin{bmatrix} 010\cdots0 \\ 001\cdots0 \\ \vdots\vdots\cdots\vdots \\ 000\cdots1 \\ s_1s_2s_3\cdots s_m \end{bmatrix}$$

and elements $s_i\,(1\leq i\leq m) \in GF\,(p^r)$.

As $A = S^m$ then every element of $A$ is a function of variables $s_i\,(1{\leq}i{\leq}m)$. Hence, an arbitrary element of row $i$ and column $j$ of matrix $A$ has following form:

$$\begin{aligned} a_{i,j} =& f_{i,j}\,(s_1, s_2, \ldots, s_m) \\ =& b_0 + \sum_{1\leq u\leq m} b_u s_u + \sum_{1\leq u<v\leq m} b_{u,v} s_u s_v + \ldots + b_{1,2,\ldots,m} s_1 s_2 \ldots s_m \end{aligned} \tag{3}$$

where $b_u\,(1{\leq}u{\leq}m)\,; b_{u,v}\,(1{\leq}u<v{\leq}m)\,; \ldots; b_{1,2,\ldots,m}$ are coefficients of function $f_{ij}$ corresponding to $a_{i,j}$. For example, when $u$ is fixed, $b_u$ is number of elements $s_u$ in the presentation of $a_{i,j}$. Because $GF\,(p^r)$ has characteristic $p$ then the coefficients are computed as modulo $p$. Therefore, the coefficients $b_u\,(1{\leq}u{\leq}m)\,; b_{u,v}\,(1{\leq}u<v{\leq}m)\,; \ldots; b_{1,2,\ldots,m}$ are all in $GF\,(p)$.

Suppose $B = A_{d^{p^k}} = [b_{ij}]_{m\times m} = \left[a_{i,j}^{p^k}\right]_{m\times m}$ is direct $p^k\,(1{\leq}k{\leq}\tau)$ exponent of matrix $A$. Then an arbitrary element $b_{i,j}$ of $B$ has following form:

$$b_{i,j} = a_{i,j}^{p^k} = \left( b_u s_u + \sum_{1\leq u<v\leq m} b_{u,v} s_u s_v + \ldots + b_{1,2,\ldots,m} s_1 s_2 \ldots s_m \right)^{p^k}$$

Apply (1), it yields:

$$b_{i,j} = b_0^{p^k} + \sum_{1\leq u\leq m} = b_u^{p^k} s_u^{p^k} + \sum_{1\leq u<v\leq m} b_{u,v}^{p^k} s_u^{p^k} s_v^{p^k} + \ldots + b_{1,2,\ldots,m}^{p^k} s_1^{p^k} s_2^{p^k} \ldots s_m^{p^k} \tag{4}$$

Now the argument is similar to the coefficients: $b_u\,(1{\leq}u{\leq}m)\,; b_{u,v}\,(1{\leq}u<v{\leq}m)\,; \ldots; b_{1,2,\ldots,m}$, so the coefficients in the presentation of $b_{i,j}$ are also in $GF\,(p)$. Base on the Fermats little theorem, it yields:

$$b_u^p = b_u mod p\,(1{\leq}u{\leq}m)\,,$$

or

$$b_u^p = b_u mod p = b_u, \quad (1{\leq}u{\leq}m)\,.$$

Hence,

$$b_u^{p^k} = b_u, (1{\leq}u{\leq}m)$$

Similarly, there also have: $b_{u,v}^{p^k} = b_{u,v} mod p = b_{u,v}; \ldots; b_{1,2,\ldots,m}^{p^k} = b_{1,2,\ldots,m} mod p = b_{1,2,\ldots,m}$.

Putting these results in (4) results in:

$$\begin{aligned} b_u s_u^{p^k} + \sum_{1\leq u<v\leq m} b_{u,v} s_u^{p^k} s_v^{p^k} + \ldots + b_{1,2,\ldots,m} s_1^{p^k} s_2^{p^k} \ldots s_m^{p^k} \quad (5) \\ b_{i,j} = b_0 + \sum_{1\leq u\leq m} \square \end{aligned} \tag{5}$$

Consider direct $p^k\,(1{\leq}k{\leq}\tau)$ exponent of matrix $S$:

$$\acute{S} = \begin{bmatrix} 010\cdots0 \\ 001\cdots0 \\ \vdots\vdots\ddots\ddots\vdots \\ 000\cdots1 \\ s_1^{p^k}\ s_2^{p^k}\ s_3^{p^k} \cdots s_m^{p^k} \end{bmatrix}$$

Then, it is similar to $S^m$ ($s_i^{p^k}$ instead of $s_i$), an element of row $i$ and column $j$ of $\acute{S}^m$ has form:

$$\begin{aligned} \acute{a}_{i,j} =& f_{i,j}\left(s_1^{p^k}, s_2^{p^k}, \ldots, s_2^{p^k}\right) \\ =& b_u s_u^{p^k} + \sum_{1\le u<v\le m} b_{u,v} s_u^{p^k} s_v^{p^k} + \ldots + b_{1,2,\ldots,m} s_1^{p^k} s_2^{p^k} \ldots s_m^{p^k} \quad (6) \\ & b_0 + \sum_{1\le u\le m} \square \end{aligned} \tag{6}$$

where, $f_{ij}$ and its coefficients are exact the elements in (3).

Compare (5) and (6), one can obtain:

$$b_{i,j} = \acute{a}_{i,j}\,(0\le i,j\le m-1).$$

It means that $B = \acute{S}^m$.

Consequently, if $A = S^m$, $B = A_{d^{p^k}}$ and $\acute{S} = S_{d^{p^k}}$ then $B = \acute{S}^m$.

Item 5: Suppose that matrix $A$ has $c$ distinct elements which are all other than 1 and denoted by $a_1, a_2, \ldots, a_c$. Obviously, these elements are nonzero because $A$ is an MDS matrix. When one performing the direct $p^k\,(1\le k\le\tau)$ exponent transfromation of an MDS matrix how is many times longer then element 1 unchanged.

On the other hand, we prove that the direct $p^k\,(1\le k\le\tau)$ exponent of matrix $A$ , $A_{d^{p^k}} = \left[a_{i,j}^{p^k}\right]_{m\times m}$ always has $a_i^{p^k}\ne 1, (1\le i\le c)$.

Indeed, consider the case when $r = 1$. Let $a\in GF\,(p)$ be an arbitrary element other than 0 and 1. If $a^p = 1$ then $p\vee(p-1)$. This is ridiculous.

Consider the case when $r > 1$. Let $a\in GF\,(p^r)$ be an element other than 0 and 1. If $a^p = 1$ then it yields $p\vee(p^r-1)$. So there exists a positive integer $d$ satisfying: $p^r - 1 = dp$ for $p^r - 1 > d\ge 1$. This equation is equivalent to:

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

Clearly, the left side of the above equation is obtained as an integer divisible by $p$ but the right side is not divisible by $p$. It leads to contradictions.

Hence, for an arbitrary element other than 0 and 1, $a\in GF\,(p^r)\,, (r\ge 1)$, we always have $a^p\ne 1$. This entails $a^{p^k}\ne 1, (1\le k\le\tau)$.

Consequently, for $\forall a_i\in A, (1\le i\le c)$ then $a_i^{p^k}\ne 1,\ (1\le k\le\tau)$.

Thus the direct $p^k\,(1\le k\le\tau)$ exponent transfromation of an MDS matrix preserves the number of $1s$ of the original MDS matrix.

Now it is to prove that for $a_i\ne a_j, (1\le i,j\le c)$ then $a_i^{p^k}\ne a_j^{p^k}$ ( $1\le k\le\tau$).

Indeed, suppose the opposite: $\exists k,(\ 1\le k\le\tau)$: $a_i^{p^k} = a_j^{p^k} \leftrightarrow a_i^{p^k} - a_j^{p^k} = 0$. Apply (1), it is deduced that: $(a_i - a_j)^{p^k} = 0 \leftrightarrow a_i = a_j$. This contradicts with the assumption $a_i\ne a_j$, so $a_i^{p^k}\ne a_j^{p^k}$ , ( $1\le k\le\tau$) for $1\le i,j\le c$.

Thus the direct $p^k\,(1\le k\le\tau)$ exponent transfromation of an MDS matrix also preserves the number of distinct elements of the original MDS matrix.

-Item 6:

+ Suppose $A$ is a circulant matrix, i.e. $A$ has the form:

$$A = \circ(a_0, \ldots, a_{m-1}) = \begin{bmatrix} a_0 & a_1 \ldots a_{m-1} \\ a_{m-1} & a_0 \ldots a_{m-2} \\ \vdots & \vdots \ \vdots \ \vdots \\ a_1 & a_2 \ldots \ a_0 \end{bmatrix}$$

Performing direct $p^k$ $(1 \leq k \leq \tau)$ exponent of matrix $A$, it yields:

$$A_{d^{p^k}} = \begin{bmatrix} a_0^{p^k} & a_1^{p^k} \ldots a_{m-1}^{p^k} \\ a_{m-1}^{p^k} & a_0^{p^k} \cdots a_{m-2}^{p^k} \\ \vdots & \vdots \ \vdots \ \vdots \\ a_1^{p^k} & a_2^{p^k} \cdots \ a_0^{p^k} \end{bmatrix}$$

Obviously the matrix obtained is also a circulant matrix:

$$A_{d^{p^k}} = \circ\left(a_0^{p^k}, \ldots, a_{m-1}^{p^k}\right)$$

+ If $A$ is a Type-I circulant-like matrix ([ [15]]) then $A$ has the following form:

$$A = \begin{bmatrix} a & 1 \\ 1^T & B \end{bmatrix}$$

where $B = \circ(1, a_1, \ldots, a_{m-2})$, $1 = \underbrace{(1, \ldots, 1)}_{m-1 l[1EA7?]n}$, 1 is the unit element and $a_i's$ and $a$ are any nonzero elements of the $GF(p^r)$ other than 1.

When performing direct $p^k$ $(1 \leq k \leq \tau)$ exponent of matrix $A$, one can obtain:

$$A_{d^{p^k}} = \begin{bmatrix} a^{p^k} & 1 \\ 1^T & B^{p^k} \end{bmatrix}$$

Since $B$ is a circulant matrix, according to the above proof it is deduced that $B^{p^k}$ is also a circulant matrix. As element $a$ is other than 0 and 1 in $GF(p^r)$, according to the proof of Item 5 it follows that $a^{p^k}$ is also other than 0 and 1 in $GF(p^r)$. Thus, $A_{d^{p^k}}$ is also a Type-I circulant-like matrix.

**Notice.**

1. The inverse matrix of $A$ has the similar form:

$$A^{-1} = \begin{bmatrix} \acute{a} & \acute{b} \\ \acute{b}^T & \acute{B} \end{bmatrix}$$

   where $\acute{B} = \circ(b_0, b_1, \ldots, b_{m-2})$, $\acute{b} = \underbrace{(b, \ldots, b)}_{m-1 \ times}$ and $\acute{a}, \acute{b}$ and $b_i's$ are any elements of $GF(p^r)$.

2. The inverse matrix of $A_{d^{p^k}}$ also has the same form as matrix $A^{-1}$.

## 4. APPLICATIONS OF THE RESULTS FROM THE DIRECT EXPONENT TRANSFORMATION IN BLOCK CIPHERS

As introduced in the Section 1, MDS matrices have been studied because of their preeminent properties.

There have been several studies on the construction of dynamic diffusion layers for block ciphers recently, for example [21–23]. In [21, 22], the authors constructed a key-dependent diffusion layer by creating MDS matrices depending on a secret key for each round. In [23], 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.

When generating dynamic MDS matrices for block ciphers, it is very important to verify whether the resulting matrix still owns good cryptographic properties for implementation or not? According to Theorem 4, 5, 6 (Section 3), the MDS matrix transformation based on direct $p^k$ $(1 \leq k \leq \tau)$ exponent indeed preserves good cryptographic properties. 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.

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. For example, for a given involutory MDS matrix many different involutory MDS matrices by the direct $p^k$ $(1 \leq k \leq \tau)$ exponent transformation can be obtained. These matrices can be used in dynamic diffusion layers for rounds of a block cipher.

Thus, the direct exponent transformation takes an important part in constructing dynamic diffusion layers for block ciphers. Consequently, it can serve as a 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.

## 5. CONCLUSION

In this paper, some new results on the conservation of many good cryptographic properties of MDS matrices under the direct exponent transformation are presented. In addition, 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] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] S. Vaudenay, "On the need for multipermutations: Cryptanalysis of md4 and safer," in *Fast Software Encryption*. Springer, 1995, pp. 286–297.

[3] C. P. Schnorr and S. Vaudenay, "Black box cryptanalysis of hash networks based on multipermutations," in *Advances in CryptologyEUROCRYPT'94*. Springer, 1995, pp. 47–57.

[4] J. Daemen and V. Rijmen, "Aes proposal: Rijndael (version 2). nist aes website," 1999.

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

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

[7] 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.

[8] J. Nakahara Jr and E. Abrahao, "A new involutory mds matrix for the aes." *IJ Network Security*, vol. 9, no. 2, pp. 109–116, 2009.

[9] R. Elumalai and A. R. Reddy, "Improving diffusion power of aes rijndael with 8x8 mds matrix," *International Journal of Scientific & Engineering Research*, vol. 2, pp. 1–5, 2011.

[10] M. Sajadieh, M. Dakhilalian, H. Mala, and B. Omoomi, "On construction of involutory mds matrices from vandermonde matrices in gf (2 q)," *Designs, Codes and Cryptography*, vol. 64, no. 3, pp. 287–308, 2012.

[11] K. C. Gupta and I. G. Ray, "On constructions of mds matrices from companion matrices for lightweight cryptography," in *Security Engineering and Intelligence Informatics*. Springer, 2013, pp. 29–43.

[12] D. Augot and M. Finiasz, "Exhaustive search for small dimension recursive mds diffusion layers for block ciphers and hash functions," in *2013 IEEE International Symposium on Information Theory Proceedings (ISIT)*. IEEE, 2013, pp. 1551–1555.

[13] S. Wu, M. Wang, and W. Wu, "Recursive diffusion layers for (lightweight) block ciphers and hash functions," in *Selected Areas in Cryptography*. Springer, 2013, pp. 355–371.

[14] P. Junod and S. Vaudenay, "Perfect diffusion primitives for block ciphers building efficient mds matrices, selected areas in cryptography 2004: Waterloo, canada, august 9-10, 2004. revisited papers," *Lecture Notes in Computer Science. Springer-Verlag.*

[15] K. C. Gupta and I. G. Ray, "On constructions of mds matrices from circulant-like matrices for lightweight cryptography," institution, Tech. Rep. ASU/2014/1, 2014.

[16] A. Youssef, S. Mister, and S. Tavares, "On the design of linear transformations for substitution permutation encryption networks," in *Workshop on Selected Areas of Cryptography (SAC96): Workshop Record*, 1997, pp. 40–48.

[17] K. C. Gupta and I. G. Ray, "On constructions of involutory mds matrices," in *Progress in Cryptology–AFRICACRYPT 2013*. Springer, 2013, pp. 43–60.

[18] A. Youssef, S. Tavares, and H. Heys, "A new class of substitution-permutation networks," in *Proceedings of Third Annual Workshop on Selected Areas in Cryptography (SAC96), Queens University, Kingston, Canada*, 1996, pp. 132–147.

[19] J. Guo, T. Peyrin, and A. Poschmann, "The photon family of lightweight hash functions," in *Advances in Cryptology–CRYPTO 2011*. Springer, 2011, pp. 222–239.

[20] M. Sajadieh, M. Dakhilalian, H. Mala, and P. Sepehrdad, "Recursive diffusion layers for block ciphers and hash functions," in *Fast Software Encryption*. Springer, 2012, pp. 385–401.

[21] 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.

[22] W. Mohamed, Ridza and M. Abdulrashid, "A method for linear transformation in substitution-permutation network symmetric-key block cipher," international application published under the patent cooperation treaty, 10 may 2012, pp. 3-14.

[23] 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.

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

[25] J. Yang, Z.-X. Ma, J. Yang, and J. Cheng, "On direct exponentiation of maximum distance separable matrices," *Xinan Minzu Daxue Xuebao(Ziran Kexue Ban)*, vol. 37, no. 3, pp. 452–455, 2011.

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

*Received on October 04 - 2014*
*Revised on August 31 - 2015*