Direct Constructions of (Involutory) MDS Matrices from Block Vandermonde and Cauchy-like Matrices

Qiuping Li[1], Baofeng Wu[2], and Zhuojun Liu[3]

[1] University of Chinese Academy of Sciences
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, wubaofeng@iie.ac.cn
[3] Key Laboratory of Mathematics Mechanization Academy of Mathematics and Systems Science, Chinese Academy of Sciences

Abstract. MDS matrices are important components in the design of linear diffusion layers of many block ciphers and hash functions. Recently, there have been a lot of work on searching and construction of lightweight MDS matrices, most of which are based on matrices of special types over finite fields. Among all those work, Cauchy matrices and Vandermonde matrices play an important role since they can provide direct constructions of MDS matrices. In this paper, we consider constructing MDS matrices based on block Vandermonde matrices. We find that previous constructions based on Vandermonde matrices over finite fields can be directly generalized if the building blocks are pairwise commutative. Different from previous proof method, the MDS property of a matrix constructed by two block Vandermonde matrices is confirmed adopting a Lagrange interpolation technique, which also sheds light on a relationship between it and an MDS block Cauchy matrix. Those constructions generalize previous ones over finite fields as well, but our proofs are much simpler. Furthermore, we present a new type of block matrices called block Cauchy-like matrices, from which MDS matrices can also be constructed. More interestingly, those matrices turn out to have relations with MDS matrices constructed from block Vandermonde matrices and the so-called reversed block Vandermonde matrices. For all these constructions, we can also obtain involutory MDS matrices under certain conditions. Computational experiments show that lightweight involutory MDS matrices can be obtained from our constructions.

Keywords: MDS matrix · involutory matrix · block Vandermonde matrix · block Cauchy-like matrix

1 Introduction

In the design of modern cryptographic primitives, confusion and diffusion are two basic requirements and they are defined by Claude Shannon [27]. Confusion means that every character of the ciphertext should depend on several parts of the plaintext and the key, obscuring the connections between them; diffusion means that changing a single character of the input will influence many characters of the output. In general, the confusion layers of a cipher are non-linear substitutions, while the diffusion layers are linear permutations. Focusing on the diffusion layer, the branch number of it can be used to estimate the number of actives S-boxes in differential and linear analysis of, for example, a two-round SPN cipher, thus reflecting the ability of a cipher to resist these two main cryptanalysis methods and to some extent, the diffusion power. Therefore, a security design target of a diffusion layer is to make its branch number as large as possible, and this is usually known as the "wide trail" design strategy [8]. Linear diffusion layers achieving maximal branch numbers are called MDS (maximal distance separable), and the matrices representing them are called MDS matrices. Such matrices are used in the design of many block ciphers and Hash functions such as AES [25], SHARK [26], Anubis [24], Twofish [31], Maelstrom [12] and Grϕstl [14]. In addition, they also have deep relationships with MDS codes in coding theory.

In recent years, there has been a lot of work on finding MDS matrices. Some designers directly search them from special matrices such as circulant matrices [21, 22], Hadamard matrices [28], Toeplitz matrices [30], etc. We call this a *structured searching* approach. An obvious advantage of these types of matrices is that all of their rows are similar, thus can reduce the search space. However, it is difficult to check the MDS properties of them in the searching process. Therefore, instead of structured searching, some other designers devote to directly constructing MDS matrices. With this approach, Cauchy matrices [7, 11, 34], Vandermonde matrices [20, 29], rotational-XOR matrices [15] and some matrices obtained from certain famous MDS codes such as BCH codes [2, 13], Gabidulin codes [4], etc., play an improtant role. An advantage of this way is that they can obtain MDS matrices of arbitrary dimension.

With the rapid development of lightweight cryptography, good hardware efficiency has become an important design goal. In order to save implementation costs, the MDS matrices used in the design of a cipher should also be as light as possible. A commonly and most frequently used metric to evaluate the weight of a matrix is its XOR count [19], which roughly speaking is the number of XOR operations needed to perform multiplication of the matrix with any vector (this is called the d-XOR count in [17]). After this, [5] proposed the idea of reusing intermediate results to decrease the XOR count, resulting in a new metric called s-XOR count [17]. Very recently, Kranz et al. [18] presented a new technique to further optimize the implementation costs based on shorter linear straight-line programs for MDS matrices. In this paper, we focus on theoretical constructions, so we only compute the s-XOR count to assure the validity of our theoretical results. In addition to these quantitative metrics, some other strategies are also adopted to save implementation costs, and this is often achieved by imposing new structures on the MDS matrices. For example, in the design of the PHOTON family of Hash function [9] and the LED block cipher [10], Guo et al. proposed to use recursive MDS matrices, which can be implemented by linear feedback shift registers (LFSRs). Another important idea is to use involutory MDS matrices. A matrix is called involutory if its inverse is itself. Obviously, this property saves hardware gates in implementation because the same structure can be used in both encryption and decryption. There were some work on constructing or searching of involutory MDS matrices. For example, as early as in 1997, Youssef et al. [34] provided a method to construct involutory MDS matrices with Cauchy matrices. After that, some other special matrices including Vandermonde matrices [29], (generalized) circulant matrices [21, 22] and Hadamard matrices [22, 28] were adopted to find involutory MDS matrices. Notably, [29] and [11] presented novel ideas on constructing MDS involutions based on Vandermonde matrices and Cauchy matrices over finite fields, respectively, and their constructions contain involutory MDS Hadamard matrices. As a matter of fact, in the sense of deriving involutory MDS Hadamard matrices, the work of [11] can be seen as special cases of that of [29]. However, the approach to prove the main results in [11] is much simpler than the one used in [29].

It should be pointed out that the MDS property is actually defined for block matrices (see Definition 2 in Section 2) over the binary field $\mathbb{F}_2$, but most work on constructing or searching of (involutory) MDS matrices is based on matrices over a finite extension of $\mathbb{F}_2$ (see e.g., [7, 11, 13, 21, 28–30]). As we all know, every element of a finite field $\mathbb{F}_{2^m}$ has a matrix representation over $\mathbb{F}_2$ of size $m \times m$, so those MDS matrices over $\mathbb{F}_{2^m}$ actually correspond to MDS block matrices over $\mathbb{F}_2$ with block size $m \times m$. However, we also know that not every matrix over $\mathbb{F}_2$ can represent an element of $\mathbb{F}_{2^m}$ (this depends on whether its minimal polynomial is irreducible or not), so it seems that we will lose some MDS matrices (and maybe some with good implementation features) when searching or constructing MDS matrices only considering matrices over $\mathbb{F}_{2^m}$. In fact, focusing on block matrices, some designers can find MDS matrices with good properties [1, 22, 35] that may not be obtained from matrices over finite fields. However, there are few papers on this topic and little previous work on direct constructions of MDS block matrices.

Our contribution. In this paper, we devote to constructing MDS matrices and involutory MDS matrices from block matrices of special types. To simplify the analysis and make use of the special structures of the matrices considered, we only focus on those block matrices whose building blocks are pairwise commutative. The contributions include the following:

– We define block Vandermonde matrices and prove that for two such matrices V_1 and V_2, $V_1V_2^{-1}$ turns out to be MDS or involutory MDS under certain conditions, which generalizes the results of [20, 29]. However, for the involutory construction the proof technique used in [20, 29] dost not work any more. We proceed our proof based on Lagrange interpolation, and this technique can shed light on the deeper structure of matrices of the form $V_1V_2^{-1}$. More precisely, we find that $V_1V_2^{-1} = D_1CD_2$, where C is a block Cauchy matrix and $D_1,\ D_2$ are two block diagonal matrices. As a result, it can be seen in a more simple and clear way that under certain conditions involutory MDS matrices of the form $V_1V_2^{-1}$ coincide with those constructed from block Cauchy matrices;

– We present a new type of block matrices called block Cauchy-like matrices, from which MDS matrices can also be constructed. Most interestingly, those matrices turn out to have relations with MDS matrices constructed as $V_1V_2^{-1}$ where V_1 and V_2 are a block Vandermonde matrix and a reversed block Vandermonde matrix, respectively. By a reversed block Vandermonde matrix, we mean a matrix modified from a block Vandermonde matrix by reversing the order of its block columns. By modifying the matrix $V_1V_2^{-1}$, involutory MDS matrices can be obtained as well;

– For all our constructions of involutory MDS matrices, by choosing the blocks to be polynomials of a given matrix, we can obtain pairwise commutative blocks, and computational experiments show that lightweight involutory MDS matrices exist. More precisely, we can find 4×4 block matrices with block size 8×8 that have XOR count 160 from the construction based on two block Vandermonde matrices, and have XOR count 151 from the construction based on a block Vandermonde matrix and a reversed block Vandermonde matrix.

The rest of the paper is organized as follows. In Section 2, we give some basic definitions and properties related to MDS matrices and their XOR counts. After that we briefly introduce some properties of Cauchy matrices and Vandermonde matrices over an arbitrary field. In Section 3, we construct MDS matrices and involutory MDS matrices with block Vandermonde matrices and block Cauchy-like matrices. Concluding remarks are given in Section 4.

2 Preliminaries

In this section, we first give some notations that will be used throughout the paper. Secondly, we give the definition of MDS matrices and some properties of them. We also recall the definition of XOR count of a matrix. At last, we simply state some properties of Cauchy matrices and Vandermonde matrices.

In this paper, the matrices considered are all square matrices and a block matrix means that the entries of the matrix are also matrices of a smaller dimension. The matrices $A_i \in \mathcal{M}_m(\mathbb{F}_2)(0 \le i \le n-1)$ are pairwise commutative that imply $A_iA_j = A_jA_i$ for all $0 \le i,\ j \le n-1$.

2.1 Notations

2.2 MDS matrices and their properties

Given a vector $v = (v_0, v_1, \cdots, v_{n-1})^T \in (\mathbb{F}_2^m)^n$, where each component $v_i^T \in \mathbb{F}_2^m$ $(0 \le i \le n-1)$ is also a vector, its bundle weight $wt_b(v)$ is defined as the number of non-zero components. The branch number of an $n \times n$ diffusion matrix M is defined as follows.

Definition 1 (See [23]). *Let M be an $n \times n$ matrix over $\mathcal{M}_m(\mathbb{F}_2)$ (i.e., M is an $mn \times mn$ block matrix with block size $m \times m$). The differential branch number of M is defined as*

$$B_d(M) = \min_{v \neq 0} \{wt_b(v) + wt_b(Mv)\},$$

m:	dimension of the blocks of a block matrix
n:	dimension of the square matrix considered
$M_{i,j}$ or $M[i,j]$:	(i,j)-entry of an $n \times n$ matrix M, where $0 \leq i,\ j \leq n-1$
$(M_{i,j})$ or $(M[i,j])$:	$n \times n$ matrix whose (i,j)-entry is $M_{i,j}$
$\det(M)$:	determinant of a matrix M
$\mathbb{F}_2$:	the binary finite field
$\mathbb{F}_{2^m}$:	the finite field with 2^m elements
$\mathcal{M}_m(\mathbb{F}_2)$:	matrix ring formed by all $m \times m$ matrices over $\mathbb{F}_2$
$\frac{A}{B}$:	matrix multiplication AB^{-1}, where B is invertible

and the linear branch number of M is defined as

$$B_\ell\left(M\right) = \underset{v \neq 0}{min}\left\{wt_b(v) + wt_b(M^T v)\right\}.$$

For an $n \times n$ matrix M' over $\mathbb{F}_{2^m}$, the definition of its branch number is similar to Definition 1. It just needs to replace bundle weight by Hamming weight over finite fields. It can be easily seen that an upper bound of B_d and B_ℓ of any matrix is $n+1$. Thus we have:

Definition 2. *An $n \times n$ matrix M over $\mathcal{M}_m(\mathbb{F}_2)$ is called an MDS matrix if $B_d(M) = B_\ell(M) = n+1$.*

From the definition, we can see an MDS matrix has the maximal branch number, so the diffusion layer designed from it is also called an optimal diffusion layer. The following theorem is an important way to characterize MDS matrices from a pure linear algebra point of view.

Theorem 1 (See [6]). *An $n \times n$ matrix M over $\mathcal{M}_m(\mathbb{F}_2)$ is MDS if and only if all square block sub-matrices of M are non-singular.*

We can immediately have the following lemma from Theorem 1.

Lemma 1. *Let $M = (M_{i,j})$ be an $n \times n$ MDS matrix over $\mathcal{M}_m(\mathbb{F}_2)$, and $D = diag(D_0, D_1, \ldots, D_{n-1})$ be a block diagonal matrix over $\mathcal{M}_m(\mathbb{F}_2)$. If $\det(D) \neq 0$, then $D \cdot M$ and $M \cdot D$ are MDS matrices.*

Proof. Since $\det(D) \neq 0$, we have $\det(D_i) \neq 0,\ 0 \leq i \leq n-1$. Since D is a block diagonal matrix and M is an MDS matrix, for any $k \times k (1 \leq k \leq n)$ sub-matrix of $D \cdot M$, we have

$$\begin{aligned} &\det\begin{pmatrix} D_{i_0}M_{i_0,j_0} & \cdots & D_{i_0}M_{i_0,j_{k-1}} \\ D_{i_1}M_{i_1,j_0} & \cdots & D_{i_1}M_{i_1,j_{k-1}} \\ \vdots & & \vdots \\ D_{i_{k-1}}M_{i_{k-1},j_0} & \cdots & D_{i_{k-1}}M_{i_{k-1},j_{k-1}} \end{pmatrix} \\ &= \det(D_{i_0})\det(D_{i_1})\cdots\det(D_{i_{k-1}})\det(M_{k\times k}) \neq 0, \end{aligned}$$

where $M_{k\times k}$ is a $k \times k$ sub-matrix of M. This shows any $k \times k$ sub-matrix of $D \cdot M$ is non-singular, thus $D \cdot M$ is an MDS matrix by Theorem 1. Similarly, we also have $M \cdot D$ is an MDS matrix.

Theorem 1 provides a general way to check whether a matrix is MDS or not, but it may not be so efficient. Especially for a block matrix over $\mathcal{M}_m(\mathbb{F}_2)$, a $k \times k$ sub-matrix is actually a $km \times km$ matrix over $\mathbb{F}_2$, and we should compute determinant of this matrix. However, when the blocks of a matrix are pairwise commutative, we can compute the determinants of sub-matrices in a simpler manner thanks to the following theorem.

Lemma 2 (See [32]). *Let $\mathbb{F}$ be a field and $A = (a_{i,j})$ be an $n \times n$ matrix, where $a_{i,j} \in \mathcal{M}_m(\mathbb{F})$ are pairwise commutative, $0 \le i, j \le n-1$. Then*

$$\det(A) = \det\left(\sum_{j_0 \cdots j_{n-1}} (-1)^{\tau(j_0 \cdots j_{n-1})} a_{0,j_0} \cdots a_{n-1,j_{n-1}}\right),$$

where $\tau(j_0 \cdots j_{n-1})$ denotes the number of inverse-ordered pairs in the permutation $(j_0 \cdots j_{n-1})$ (an inverse-ordered pair is a pair whose number on the left side is larger than its number on the right side).

Lemma 2 says that, if the entries of a block matrix over $\mathcal{M}_m(\mathbb{F})$ are pairwise commutative, or equivalently, the matrix is defined over a commutative sub-ring of the matrix ring $\mathcal{M}_m(\mathbb{F})$, we can compute its determinant by computing the determinant of it as a matrix over this sub-ring firstly to obtain a matrix in $\mathcal{M}_m(\mathbb{F})$, and then computing determinant of this resulting matrix. This lemma will help us a lot in our constructions of MDS matrices based on block Vandermonde and Cauchy-like matrices.

2.3 XOR counts of matrices over $\mathbb{F}_2$

In 2014, the authors of [19] proposed using XOR count to estimate the implementation cost of cryptographic primitives. The XOR count of a matrix over $\mathbb{F}_2$ is the number of XOR operations of the matrix-vector multiplication, which is called d-XOR count. Afterwards, [5] proposed the idea of reusing intermediate results to decrease the XOR count, resulting a new metric called s-XOR count. In this paper, we use the metric s-XOR count to calculate the implementation cost of a matrix.

Definition 3. *[5] An invertible matrix A has an s-XOR count of t over $\mathbb{F}_2$, denoted by $XOR(A) = t$, if t is the minimal number such that A can be written as*

$$A = P \prod_{k=1}^{t} (I + E_{i_k,j_k})$$

with $i_k \neq j_k$ for all k, where E_{i_k,j_k} is the matrix with a unique non-zero element 1 at the $(i_k, j_k$-th entry, $k \in \{1, \cdots, t\}$.

As an example, consider

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} b_2 \oplus b_1 \\ b_1 \\ b_3 \oplus b_2 \oplus b_1 \end{pmatrix}.$$

We can reuse the intermediate result $b_2 \oplus b_1$, so we get its s-XOR count is 2. For the block matrices we consider the form

$$A = \begin{pmatrix} A_{0,0} & A_{0,1} & \cdots & A_{0,n-1} \\ A_{1,0} & A_{1,1} & \cdots & A_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ A_{n-1,0} & A_{n-1,1} & \cdots & A_{n-1,n-1} \end{pmatrix}$$

where $A_{i,j} \in \mathcal{M}_m(\mathbb{F}_2)$, $0 \le i, j \le n-1$, it can be easily derived that its s-XOR count is

$$XOR(A) = \sum_{i,j=0}^{n-1} XOR(A_{i,j}) + n \times (n-1) \times m. \tag{1}$$

2.4 Cauchy matrix and Vandermonde matrix

Cauchy matrix and Vandermonde matrix are two important kinds of special matrices in linear algebra. They both have the feature that their determinants can be represented into nice formulas. If the elements appearing in the formulas are pairwise distinct, then the determinants of them are non-zero. For simplification, we only consider Cauchy and Vandermonde matrices over finite fields here.

Definition 4. *Given $x_0, x_1, \ldots, x_{n-1} \in \mathbb{F}_{2^m}$ and $y_0, y_1, \ldots, y_{n-1} \in \mathbb{F}_{2^m}$, such that $x_i + y_j \neq 0$ for all $0 \le i, j \le n-1$, the matrix $C = (c_{i,j}) = \left(\frac{1}{x_i + y_j}\right)$ is called a Cauchy matrix.*

It is well known that the determinant of C is

$$\det(C) = \frac{\prod_{0 \le i < j \le n-1} (x_i + x_j)(y_i + y_j)}{\prod_{0 \le i,j \le n-1} (x_i + y_j)}.$$

So if x_i's and y_j's are pairwise distinct for all $0 \le i, j \le n-1$, then $\det(C) \neq 0$, i.e. C is non-singular.

It is easy to see that any square sub-matrix of a Cauchy matrix is still a Cauchy matrix, so we have the following proposition.

Proposition 1 (See [11]). *For pairwise distinct $x_i, y_j \in \mathbb{F}_{2^m}$ $(0 \le i, j \le n-1)$, the Cauchy matrix $C = (\frac{1}{x_i + y_j})$ is an MDS matrix.*

Definition 5 (See [29]). *The matrix*

$$V = van(x_0, x_1, \cdots, x_{n-1}) = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{pmatrix}$$

is called a Vandermonde matrix, where $x_i \in \mathbb{F}_{2^m} (0 \le i \le n-1)$.

It is well known the determinant of V is $\det(V)=\prod_{0\leq i<j\leq n-1}(x_i+x_j)$, namely, we have $\det(V)\neq 0$ if and only if all of $x_i(0\leq i\leq n-1)$ are distinct.

Proposition 2 (See [20]). *Let $V_1=van(x_0,x_1,\cdots,x_{n-1})$ and $V_2=van(y_0,y_1,\cdots,y_{n-1})$ be two $n\times n$ invertible Vandermonde matrices over $\mathbb{F}_{2^m}$ satisfying $x_i\neq y_j, 0\leq i,j\leq n-1$. Then $V_1V_2^{-1}$ is an MDS matrix.*

Proposition 3 (See [29]). *Notations and assumptions are the same with those in Proposition 2 and further assume that $x_i=y_i+r$ for some $r\in\mathbb{F}_{2^m}^*$. Then $V_1V_2^{-1}$ is an involutory MDS matrix.*

3 MDS matrices and involutory MDS matrices constructed from block matrices

In this section, we construct MDS matrices and involutory MDS matrices from block Vandermonde matrices and block Cauchy-like matrices.

3.1 (Involutory) MDS matrices from Block Vandermonde matrices

Before we construct MDS matrices, we first introduce some properties of block Cauchy matrix.

Definition 6. *Let $A_0,A_1,\ldots,A_{n-1}$ and $B_0,B_1,\ldots,B_{n-1}$ be $m\times m$ matrices over $\mathbb{F}_2$ satisfying that A_i+B_j is non-singular for any $0\leq i,j\leq n-1$. Then the matrix $C=(\frac{I}{A_i+B_j})$ is called a block Cauchy matrix over $\mathcal{M}_m(\mathbb{F}_2)$.*

Under certain conditions, applying Lemma 2, the determinant of a block Cauchy matrix computed is similar to Cauchy matrix over finite field. We can easily have the determinant of a block Cauchy matrix as follows.

Proposition 4. *Let $A_0,A_1,\ldots,A_{n-1},B_0,B_1,\ldots,B_{n-1}$ be $m\times m$ matrices over $\mathbb{F}_2$ which are pairwise commutative, satisfying that A_i+B_j is non-singular for any $0\leq i,j\leq n-1$. Then the determinant of the block Cauchy matrix $C=(\frac{I}{A_i+B_j})$ is*

$$\det(C)=\frac{\prod_{0\leq i<j\leq n-1}\det(A_i+A_j)\det(B_i+B_j)}{\prod_{0\leq i,j\leq n-1}\det(A_i+B_j)}.$$

.

By Proposition 4 and Theorem 1, we can give a construction of MDS matrices with block Cauchy matrices as follows.

Theorem 2. *Assume $\{A_0,\ldots,A_{n-1},B_0,\ldots,B_{n-1}\}$ is a set of $m\times m$ matrices over $\mathbb{F}_2$ which are pairwise commutative, and the sum of any two elements of it is non-singular. Then the block Cauchy matrix $C=(\frac{I}{A_i+B_j})$ is an MDS matrix.*

Proof. From the definition of a block Cauchy matrix, it is obvious any square sub-matrix of it is still a block Cauchy matrix. It is clear from Proposition 4 that all sub-matrices of C are non-singular under the conditions of this theorem.

In [29], the authors construct MDS matrices with Vandermonde matrices over finite fields. In the following we consider the construction of MDS matrices with block Vandermonde matrices.

Definition 7. *The matrix*

$$V = Van(A_0, A_1, \cdots, A_{n-1}) = \begin{pmatrix} I & A_0 & A_0^2 & \cdots & A_0^{n-1} \\ I & A_1 & A_1^2 & \cdots & A_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ I & A_{n-1} & A_{n-1}^2 & \cdots & A_{n-1}^{n-1} \end{pmatrix}$$

is called a block Vandermonde matrix, where $A_i \in \mathcal{M}_m(\mathbb{F}_2)(0 \le i \le n-1)$.

Now we give the construction of an MDS matrix with two block Vandermonde matrices.

Theorem 3. *Let $V_1 = Van(A_0, A_1, \cdots, A_{n-1})$ and $V_2 = Van(B_0, B_1, \cdots, B_{n-1})$ be two block Vandermonde matrices, where $A_i, B_j \in \mathcal{M}_m(\mathbb{F}_2), 0 \le i, j \le n-1$, are commutative and the sum of any two of them is non-singular. Then $V = V_1 V_2^{-1}$ is an MDS matrix.*

Proof. Assume the inverse of V_2 is $V_2^{-1} = (S_{i,j})$, where $S_{i,j} \in \mathcal{M}_m(\mathbb{F}_2), 0 \le i, j \le n-1$. Then we have

$$V_2 V_2^{-1}[i,j] = \sum_{k=0}^{n-1} S_{k,j} B_i^k = \begin{cases} 0 & i \neq j \\ I & i = j. \end{cases}$$

Let $p_j(X) = \sum_{k=0}^{n-1} S_{k,j} X^k$ be a matrix polynomial. Then we can see that $p_j(X)$ is actually the Lagrange interpolation polynomial, that is,

$$p_j(X) = \sum_{k=0}^{n-1} S_{k,j} X^k = \prod_{\substack{k=0 \\ k \neq j}}^{n-1} \frac{X + B_k}{B_j + B_k}. \tag{2}$$

Therefore, we have

$$V_1 V_2^{-1}[i,j] = \sum_{k=0}^{n-1} S_{k,j} A_i^k = p_j(A_i) = \prod_{\substack{k=0 \\ k \neq j}}^{n-1} \frac{A_i + B_k}{B_j + B_k}. \tag{3}$$

Let $C = ((A_i+B_j)^{-1})$, which is a block Cauchy matrix. Let $D_1 = diag(\prod_{k=0}^{n-1}(A_0+B_k), \prod_{k=0}^{n-1}(A_1+B_k), \cdots, \prod_{k=0}^{n-1}(A_{n-1}+B_k))$ and $D_2 = diag(\prod_{k=1}^{n-1}(B_0+B_k)^{-1}, \prod_{\substack{k=0 \\ k \neq 1}}^{n-1}(B_1+$

$B_k)^{-1}, \cdots, \prod_{k=0}^{n-2}(B_{n-1}+B_k)^{-1})$ be two block diagonal matrices. Then we have

$$D_1CD_2[i,j] = \prod_{k=0}^{n-1}(A_i+B_k)(A_i+B_j)^{-1}\prod_{\substack{k=0\\k\neq j}}^{n-1}(B_j+B_k)^{-1} = \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{A_i+B_k}{B_j+B_k} = V_1V_2^{-1}[i,j]$$

Since $A_i+B_j, A_i+A_k, B_i+B_k, 0 \leq i,j,k \leq n-1$ and $i \neq k$, are non-singular, we know the block Cauchy matrix C is MDS, and $\det(D_1) \neq 0$ and $\det(D_2) \neq 0$. From Lemma 1, we know $V = V_1V_2^{-1} = D_1CD_2$ is an MDS matrix.

Theorem 3 is a direct generalization of the result over finite fields given in [29]. However, our proof technique is quite different from the one used in [29]. In fact, the MDS property is confirmed by computing the branch number in [29]. The main argument is based on the basic fact that the polynomial $p(x) = \sum_{i=0}^{n-1} p_ix^i$ has at most $n-1$ different roots in any finite field, where $p_i \in \mathbb{F}_{2^m}$. However, following this approach to prove our result of Theorem 3, we will meet some difficulties since it seems we do not have such argument that the polynomial $P(X) = \sum_{i=0}^{n-1} P_iX^i$ has at most $n-1$ roots, which are $m \times m$ matrices over $\mathbb{F}_2$, where $P_i \in \mathbb{F}_2^m$. Therefore, we provide a new method to prove Theorem 3. The advantage of this approach is that it can reflect the deeper structure of the matrix $V_1V_2^{-1}$ for two block Vandermonde matrices V_1, V_2.

Based on Theorem 3, we can easily obtain the following theorem.

Theorem 4. *The matrix V of Theorem 3 is an involutory MDS matrix if $B_i = A_i + R$, where $R \in \mathcal{M}_m(\mathbb{F}_2)$ and $R \neq A_i, i = 0, 1, \ldots, n-1$.*

Proof. From (3) and $B_i = A_i + R$, we know

$$V_1V_2^{-1}[i,j] = \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{A_i+B_k}{B_j+B_k} = \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{A_i+R+A_k}{A_j+R+A_k+R} = \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{B_i+A_k}{A_j+A_k}.$$

Similarly we have

$$V_2V_1^{-1}[i,j] = \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{B_i+A_k}{A_j+A_k},$$

which is equal to $V_1V_2^{-1}[i,j]$. So the matrix $V = V_1V_2^{-1}$ is an involutory MDS matrix.

We need to notice that the elements used to form the block Vandermonde matrices in the above constructions should be pairwise commutative and the sum of any two of them should be non-singular. It seems difficult to find such kind of elements in the matrix ring. However, we can give a simple way to deal with this problem by considering matrix polynomials. More precisely, we replace $A_i, B_j, R, 0 \leq i,j \leq n-1$ with $f_i(B), g_j(B), r(B), 0 \leq i,j \leq n-1$, where $B \in \mathcal{M}_m(\mathbb{F}_2)$ and $f_i(x), g_j(x), r(x) \in \mathbb{F}_2[x]$. Now naturally they are pairwise commutative. In order to ensure that $f_i(B)+f_k(B), g_i(B)+g_k(B), f_i(B)+g_j(B), 0 \leq i,j,k \leq n-1$ and $i \neq k$, are non-singular, we need the following proposition [35].

Proposition 5 (See [35]). *Let $\mathbb{F}$ be a field, $B \in \mathcal{M}_m(\mathbb{F}), m_B(x)$ be the minimal polynomial of B , and $g(x) \in \mathbb{F}[x]$. Then $\det(g(B)) \neq 0$ if and only if $GCD(g(x), m_B(x)) = 1$, where $GCD(g(x), m_B(x))$ denotes the greatest common divisor of $g(x)$ and $m_B(x)$.*

According to Proposition 5, we construct the desired $A_i, B_j, R, 0 \leq i, j \leq n-1$ of Theorem 4 by replacing them with $f_i(B), g_j(B), r(B)$, $0 \leq i, j \leq n-1$, where $B \in \mathcal{M}_m(\mathbb{F}_2)$ and $f_i(x), g_j(x), r(x) \in \mathbb{F}_2[x]$. As an example, we give a 4×4 involutory block MDS matrix over $\mathcal{M}_8(\mathbb{F}_2)$ as follows.

Example 1. Let $f_0(x) = 1, f_1(x) = x^7 + x^3 + x^2 + 1, f_2(x) = x^7 + x^2, f_3(x) = x^3, r(x) = 1$ and $m_B(x) = x^8+x^7+x^5+x^4+x^3+x+1 = (x^4+x+1)(x^4+x^3+1)$. Then we obtain an involutory block MDS matrix V by Theorem 4 for

$$B = \begin{pmatrix} 0&1&0&0&0&1&1&0 \\ 1&1&0&0&1&1&0&1 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&1 \\ 1&1&0&1&0&1&1&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \end{pmatrix}. \tag{4}$$

The XOR count of V is 160.

It is worth noting that the minimal polynomial $m_B(x)$ in Example 1 is a reducible polynomial. If the minimal polynomial $m_B(x)$ is an irreducible polynomial, then the matrix B will be similar to a matrix representation of an element of the finite field $\mathbb{F}_{2^8}$.

3.2 (Involutory) MDS matrices from Block Cauchy-like matrix

In this section, we will give a new structure to construct MDS matrices and involutory MDS matrices.

Definition 8. *Let $A_0, A_1, \ldots, A_{n-1}$ and $B_0, B_1, \ldots, B_{n-1}$ be $m \times m$ matrices over $\mathbb{F}_2$ satisfying that $I + A_iB_j$ is non-singular for any $0 \leq i, j \leq n-1$. Then the matrix $T = (\frac{I}{I+A_iB_j})$ is called a block Cauchy-like matrix over $\mathcal{M}_m(\mathbb{F}_2)$.*

We find that block Cauchy-like matrices share some beautiful features with block Cauchy matrices. For example, any square sub-matrix of a block Cauchy-like matrix is still a block Cauchy-like matrix; the determinant of a block Cauchy-like matrix computed is similar to block Cauchy matrix, so we have the following proposition.

Proposition 6. *Let $A_0, A_1, \ldots, A_{n-1}, B_0, B_1, \ldots, B_{n-1}$ be $m \times m$ matrices over $\mathbb{F}_2$ which are pairwise commutative, satisfying that $I + A_iB_j$ is non-singular for any $0 \leq i, j \leq n-1$. Then the determinant of the block Cauchy-like matrix $T = (\frac{I}{I+A_iB_j})$ is*

$$\det(T) = \frac{\prod_{0 \leq i < j \leq n-1} \det(A_i + A_j) \det(B_i + B_j)}{\prod_{0 \leq i,j \leq n-1} \det(I + A_iB_j)}.$$

Theorem 5. *Assume $\{A_0, \ldots, A_{n-1}, B_0, \ldots, B_{n-1}\}$ is a set of $m \times m$ matrices over $\mathbb{F}_2$ which are pairwise commutative, and $I + A_iB_j, (0 \leq i, j \leq n-1)$ and $A_i + A_k, B_i + B_k, (0 \leq i < k \leq n-1)$ are non-singular. Then the block Cauchy-like matrix $T = (\frac{I}{I+A_iB_j})$ is an MDS matrix.*

The proof is very simple based on previous arguments, so we omit it here.

In Theorem 4, we use two block Vandermonde matrices to construct involutory MDS matrices. In the following we introduce another novel approach based on two block Vandermonde matrices.

Theorem 6. *Let $V_1 = Van(A_0, A_1, \cdots, A_{n-1})$ and $V_2 = Van(B_0, B_1, \cdots, B_{n-1})$ be two block Vandermonde matrices, where $A_i, B_j \in \mathcal{M}_m(\mathbb{F}_2), 0 \leq i, j \leq n-1$, are pairwise commutative and $I + A_iB_j, 0 \leq i, j \leq n-1$, and $A_i + A_k, B_i + B_k, 0 \leq i < k \leq n-1$,are non-singular. Then $V^* = V_1(V_2P)^{-1}$ is an MDS matrix, where $P = \begin{pmatrix} & & I \\ & \iddots & \\ I & & \end{pmatrix}$ and I is an $m \times m$ identity matrix.*

Proof. Assume the inverse of V_2 is $V_2^{-1} = (S_{i,j})$, where $S_{i,j} \in \mathcal{M}_m(\mathbb{F}_2), 0 \leq i, j \leq n-1$. It is easy to see the inverse of P is also P. Then we have

$$(V_1(V_2P)^{-1})[i,j] = ((V_1P)V_2^{-1})[i,j] = \sum_{k=0}^{n-1} S_{k,j}A_i^{n-1-k}.$$

Let $p_j^*(X) = \sum_{k=0}^{n-1} S_{k,j}X^{n-1-k}$ be a matrix polynomial. We can see that it can be viewed as the reciprocal polynomial of the polynomial

$$p_j(X) = \sum_{k=0}^{n-1} S_{k,j}X^k = \prod_{\substack{k=0 \\ k \neq j}}^{n-1} \frac{X + B_k}{B_j + B_k}.$$

Thus we have

$$p_j^*(X) = \prod_{\substack{k=0 \\ k \neq j}}^{n-1} \frac{I + B_kX}{B_j + B_k}.$$

This leads to

$$(V_1(V_2P)^{-1})[i,j] = \sum_{k=0}^{n-1} S_{k,j}A_i^{n-1-k} = p_j^*(A_i) = \prod_{\substack{k=0 \\ k \neq j}}^{n-1} \frac{I + B_kA_i}{B_j + B_k}. \tag{5}$$

Let $D_3 = diag(\prod_{k=0}^{n-1}(I + A_0B_k), \prod_{k=0}^{n-1}(I + A_1B_k), \cdots, \prod_{k=0}^{n-1}(I + A_{n-1}B_k))$ and $D_4 = diag(\prod_{k=1}^{n-1}(B_0 + B_k)^{-1}, \prod_{\substack{k=0 \\ k \neq 1}}^{n-1}(B_1 + B_k)^{-1}, \cdots, \prod_{k=0}^{n-2}(B_{n-1} + B_k)^{-1})$ be two block diagonal matrices. We have

$$\begin{aligned} D_3TD_4[i,j] &= \prod_{k=0}^{n-1}(I+A_iB_k)(I+A_iB_j)^{-1}\prod_{\substack{k=0\\k\neq j}}^{n-1}(B_j+B_k)^{-1} \\ &= \prod_{\substack{k=0\\k\neq j}}^{n-1}\frac{I+A_iB_k}{B_j+B_k} = (V_1(V_2P)^{-1})[i,j] \end{aligned}$$

Since $I+A_iB_j, 0\leq i,j\leq n-1$, and $A_i+A_k, B_i+B_k, 0\leq i<k\leq n-1$, are nonsingular, we know the block Cauchy-like matrix T is MDS by Theorem 5, and $\det(D_3)\neq 0$, $\det(D_4)\neq 0$. From Lemma 1, we know $V^*=V_1(V_2P)^{-1}=D_3TD_4$ is an MDS matrix.

For a block Vandermonde matrix V, we call the matrix VP a reversed block Vandermonde matrix.

Based on the matrix V^* in Theorem 6, we can also give a construction of involutory MDS matrices.

Theorem 7. *Notations and assumptions are the same with those in Theorem 6. Then* $\widetilde{V}=(R^{\frac{n-1}{2}}V^*[i,j])$ *is an involutory MDS matrix if* $B_i=A_iR$, *where* $R\in\mathcal{M}_m(\mathbb{F}_2)$, $R\neq 0$ *and it is the square of a matrix when* n *is even.*

Proof. From the definition of $\widetilde{V}$, we have

$$\widetilde{V}=(R^{\frac{n-1}{2}}V^*[i,j])=diag(R^{\frac{n-1}{2}},R^{\frac{n-1}{2}},\cdots,R^{\frac{n-1}{2}})V^*.$$

From Lemma 1, we know $\widetilde{V}$ is an MDS matrix.

From (5) and $B_i=A_iR$, we have

$$\widetilde{V}[i,j]=R^{\frac{n-1}{2}}\prod\nolimits_{\substack{k=0\\k\neq j}}^{n-1}\tfrac{I+A_iB_k}{B_j+B_k}=R^{\frac{n-1}{2}}\prod\nolimits_{\substack{k=0\\k\neq j}}^{n-1}\tfrac{I+RA_iA_k}{R(A_j+A_k)}=R^{-\frac{n-1}{2}}\prod\nolimits_{\substack{k=0\\k\neq j}}^{n-1}\tfrac{I+B_iA_k}{A_j+A_k}.$$

Similarly we can derive

$$\widetilde{V}^{-1}[i,j]=R^{-\frac{n-1}{2}}(V^*)^{-1}[i,j]=R^{-\frac{n-1}{2}}V_2(V_1P)^{-1}[i,j]=R^{\frac{n-1}{2}}\prod\nolimits_{\substack{k=0\\k\neq j}}^{n-1}\tfrac{I+B_iA_k}{A_j+A_k}=\widetilde{V}[i,j].$$

So the matrix $\widetilde{V}$ is an involutory MDS matrix.

Similar to the approach used in the previous subsections, we can also obtain lightweight involutory MDS matrices based on Theorem 7 using matrix polynomials. We give an example in the following.

Example 2. Let $f_0(x)=0, f_1(x)=x^3+x, f_2(x)=x, f_3(x)=x^7+x^5$, $r(x)=1$ and $m_B(x)=x^8+x^2+1=(x^4+x+1)^2$. Then we have an involutory MDS matrix $\widetilde{V}$ by Theorem 7 with

$$B = \begin{pmatrix} 0\,1\,0\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,0\,0\,1 \\ 1\,0\,1\,0\,1\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1\,0 \\ 0\,0\,0\,1\,0\,1\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \end{pmatrix}. \tag{6}$$

The XOR counts of $\widetilde{V}$ is 151.

In the following we will give some comparisons of our construction with previous constructions in Table 1.

Table 1. Comparison of 4 × 4 involutory MDS matrices

Elements	Reference	Matrix type	XOR count
$\mathcal{M}_8(\mathbb{F}_2)$	Theorem 4	Block Vandermonde	$64 + 4 \times 3 \times 8 = 160$
$\mathcal{M}_8(\mathbb{F}_2)$	Theorem 7	Permutation of block Vandermonde	$38 + 4 \times 3 \times 8 = 151$
$\mathbb{F}_{2^8}$	[28]	Hadamard	$40 + 4 \times 3 \times 8 = 152$
$\mathbb{F}_{2^8}$	[3]	Hadamard	$80 + 4 \times 3 \times 8 = 176$

Here, we only compare with the lightest results over finite field because we are generalized some constructions of finite field. Note that the 4 × 4 involutory reversed block Vandermonde MDS matrices over $\mathcal{M}_8(\mathbb{F}_2)$ are lighter than previous constructions over finite field. While it is possible to search for more lightweight involutory reversed Vandermonde MDS matrices over sub-field or non-commutative ring, it requires very different search strategy and it is beyond the scope of our work.

4 Conclusion

In this paper, we construct MDS matrices and involutory MDS matrices directly using block Vandermonde matrices and block Cauchy-like matrices. Some of our results are direct generalizations of previous ones obtained over finite fields, but we give a deeper understandings and simpler proofs. A novel structure named block Cauchy-like matrix which was not considered before in the constructions of MDS matrices is also presented. It is interesting that they also have relationships with block Vandermonde matrices. With the approaches introduced in this paper, we can also obtain some new lightweight involutory MDS matrices.

References

1. Augot, D., Finiasz, M.: Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions. In: Proceedings of 2013

IEEE International Symposium on Information Theory (ISIT), pp. 1551–C1555. IEEE (2013)

2. Augot, D., Finiasz, M.: Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes. In: Cid, C., Rechberger, C.(eds.) Fast Software Encryption 2014. LNCS, vol. 8540, pp. 3–17. Springer, Heidelberg (2015)
3. Barreto, P.S., Rijmen, V.: The Khazad Legacy-Level Block Cipher. Submission to the NESSIE Project
4. Berger, T.P.: Constructions of Recursive MDS Diffusion Layers from Gabidulin Codes. In: Paul, G., Vaudenay, S.(eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 274–285. Springer, Heidelberg (2013)
5. Beierle, C., Kranz, T., Leander, G.: Lightweight Multiplication in GF(2 n) with Applications to MDS Matrices. In Robshaw, M., Katz, J., eds.: CRYPTO 2016. LNCS, vol. 9814, pp. 625–653, Springer, Heidelberg (2016)
6. Blaum, M., Roth, R. M.: On Lowest Density MDS Codes. IEEE Transactions on Information Theory 45(1), 46–59 (1999)
7. Cui, T., Jin, C., Kong, Z.: On Compact Cauchy Matrices for Substitution Permutation Networks. IEEE Transactions on Computers 64(7), 1998–2102 (2015)
8. Daemen, J., Rijmen, V.: The Wide Trail Design Strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
9. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011)
10. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
11. Gupta, K. C., Ray, I. G.: On Constructions of Involutory MDS Matrices. In: Youssef A., Nitaj A., Hassanien A.E. (eds) Progress in Cryptology AFRICACRYPT 2013. LNCS, vol. 7918, pp. 43–60. Springer, Berlin, Heidelberg (2013)
12. Gazzoni Filho, D., Barreto, P., Rijmen, V.: The Maelstrom-0 Hash Function. In Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security (2006)
13. Gupta, K. C., Pandey, S. K., Venkateswarlu, A.: On the Direct Construction of Recursive MDS Matrices. Designs, Codes and Cryptography 82(1-2), 77–94 (2017)
14. Gauravaram, P., Knudsen, L. R., Matusiewicz, K., Mendel, F., Rechberger, C., Schlaffer, M., Thomsen, S.: Grϕstl a SHA-3 Candidate. In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum fu̎r Informatik (2009)
15. Guo, Z., Liu, R., Gao, S., Wu, W., Lin, D.: Direct Construction of Optimal Rotational-XOR Diffusion Primitives. IACR Transactions on Symmetric Cryptology 2017(4), 169-187(2017)
16. Gohberg, I., Olshevsky, V.: Complexity of Multiplication with Vectors for Structured Matrices. Linear Algebra and Its Applications 192, 163–192 (1994)
17. Jean, J., Peyrin, T. and Sim, S.M., Tourteaux, J.: Optimizing Implementations of Lightweight Building Blocks. IACR Transactions on Symmetric Cryptology, 2017(4), 130–168(2017). https://doi.org/10.13154/tosc.v2017.i4.130–168
18. Kranz, T., Leander, G., Stoffelen, K., Wiemer, F.: Shorter Linear Straight-Line Programs for MDS Matrices Yet another XOR Count Paper. IACR Transactions on Symmetric Cryptology, 2017(4), 188-211(2017). https://doi.org/10.13154/tosc.v2017.i4.188–211

19. Khoo, K., Peyrin, T, Poschmann, A., Yap, H.: FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In: Batina L., Robshaw M. (eds) Cryptographic Hardware and Embedded Systems 2014. LNCS, vol. 8731, pp. 433–450. Springer, Heidelberg (2014)
20. Lacan, J., Fimes, J.: Systematic MDS Erasure Codes Based on Vandermonde Matrices. IEEE Communications Letters 8(9), 570–572 (2004)
21. Liu, M., Sim, S. M.: Lightweight MDS Generalized Circulant Matrices. In: Peyrin T. (eds) Fast Software Encryption 2016. LNCS, vol. 9783, pp. 101–119. Springer, Heidelberg (2016)
22. Li, Y. Wang, M.: On the Construction of Lightweight Circulant Involutory MDS Matrices. In: Peyrin T. (eds) Fast Software Encryption 2016. LNCS, vol. 9783, pp. 121–139. Springer, Heidelberg (2016)
23. Li, C., Wang, Q.: Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices. IACR Transactions on Symmetric Cryptology 2017(1), 129–155 (2017)
24. Rijmen, V., Barreto, P.: The Anubis Block Cipher. The NESSIE (2000).
25. Rijmen, V., Daemen, J.: The Design of Rijndael: AES. The Advanced Encryption Standard. Springer, Berlin (2002)
26. Rijmen, V., Daemen, J., Preneel,B., *et al*: The Cipher SHARK. In: Gollmann D. (eds) Fast Software Encryption 1996. LNCS, vol. 1039, pp. 99–111. Springer, Heidelberg (1996)
27. Shannon, C. E.: Communication Theory of Secrecy Systems. Bell System Technical Journal 28(4), 656–715 (1949)
28. Sim, S. M., Khoo, K., Oggier, F. E., Peyrin, T.: Lightweight MDS Involution Matrices. In: Leander G. (eds) Fast Software Encryption 2015. LNCS, vol. 9054, pp. 471–493. Springer, Heidelberg (2015)
29. Sajadieh, M., Dakhilalian, M., Mala, H., Omoomi, B.: On Construction of Involutory MDS Matrices from Vandermond Matrices in GF (2^q). Des. Codes Cryptogr. 2012(64), 287–308 (2012)
30. Sarkar, S., Syed, H.: Lightweight diffusion layer: Importance of Toeplitz Matrices. IACR Transactions on Symmetric Cryptology, 2016(1), 95–113 (2016)
31. Schneier, B., Kelsey, J., Whiting, D., *et al*: Twofish: A 128-bit Block Cipher. NIST AES Proposal 15, 23 (1998)
32. Silvester, J. R. (2000). Determinants of Block Matrices. The Mathematical Gazette 84(501), 460–467 (2000)
33. Xiao, L., Heys, H. M.: Hardware Design and Analysis of Block Cipher Components. In: Lee P.J., Lim C.H. (eds) Information Security and Cryptology 2002. LNCS, vol. 2587, pp. 164–181. Springer, Heidelberg (2002)
34. Youssef, A. M., Mister, S., Tavares, S. E.: On the Design of Linear Transformations for Substitute Permutation Encryption Networks. In Workshop on Selected Areas of Cryptography 1996, 40–48 (1997)
35. Zhao, R., Zhang, R., Li, Y., Wu, B.: On Constructions of a Sort of MDS Block Diffusion Matrices for Block Ciphers and Hash Functions. Science China Information Sciences 2016(59), 99–101 (2016)