On Constructions of MDS Matrices From Circulant-Like Matrices For Lightweight Cryptography

Technical Report No. ASU/2014/1
Dated : 14th February, 2014

Kishan Chand Gupta
Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road, Kolkata 700108, INDIA.
kishan@isical.ac.in

Indranil Ghosh Ray
Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road, Kolkata 700108, INDIA.
indranil_r@isical.ac.in

On Constructions of MDS Matrices From Circulant-Like Matrices For Lightweight Cryptography

Kishan Chand Gupta and Indranil Ghosh Ray

Applied Statistics Unit, Indian Statistical Institute.
203, B. T. Road, Kolkata 700108, INDIA.
kishan@isical.ac.in, indranil_r@isical.ac.in

Abstract. Maximum distance separable (MDS) matrices have applications not only in coding theory but are also of great importance in the design of block ciphers and hash functions. It is highly nontrivial to find MDS matrices which could be used in lightweight cryptography. In a SAC 2004 paper, Junod et. al. constructed a new class of efficient MDS matrices whose submatrices were circulant matrices and they coined the term circulating-like matrices for these new class of matrices which we rename as circulant-like matrices. In this paper we study this construction and propose efficient 4×4 and 8×8 circulant-like MDS matrices. We prove that such $d \times d$ circulant-like MDS matrices can not be involutory or orthogonal which are good for designing SPN networks. Although these matrices are efficient, but the inverse of such matrices are not guaranteed to be efficient. Towards this we design a new type of circulant-like MDS matrices which are by construction involutory. Our construction is based on the scheme which was initially proposed in SAC 1997 by Youssef et. al. where they considered the construction of $2d \times 2d$ involutory MDS matrices starting from some $d \times d$ submatrix which is an MDS matrix. In our construction we take the $d \times d$ submatrix as circulant MDS matrices. We prove the nonexistence of such $2d \times 2d$ involutory MDS matrices whenever d is even. Using this construction and taking $d = 3$, we construct 6×6 involutory MDS matrices which are suitable for SPN networks.

Key words: Diffusion, InvMixColumn operation, Involutory matrix, MDS matrix, MixColumn operation, Orthogonal matrix.

1 Introduction

Claude Shannon, in his paper "Communication Theory of Secrecy Systems" [29], defined *confusion* and *diffusion* as two properties, required in the design of block ciphers. One possibility of formalizing the notion of perfect diffusion is the concept of *multipermutation*, which was introduced in [28, 32]. Another way to define it is using MDS matrices. *Maximum Distance Separable (MDS) matrices* offer diffusion properties and is one of the vital constituents of modern age ciphers like Advanced Encryption Standard (AES) [9], Twofish [26, 27], SHARK [23], Square [8], Khazad [2], Clefia [31] and MDS-AES [15]. The stream cipher MUGI [33] uses MDS matrix in its linear transformations. MDS matrices are also used in the design of hash functions. Hash functions like Maelstrom [10], Grϕstl [11] and PHOTON family of light weight hash functions [12] use MDS matrices as main part of their diffusion layers.

There are two very popular approaches for the design of large MDS matrices. One involves *Cauchy matrices* [36] and the other uses *Vandermonde matrices* [13, 19, 24]. In some recent works [1, 5, 12, 14, 25, 34], MDS matrices have been constructed recursively from some suitable *companion matrices* for lightweight applications. But the constructed matrices are not circulant in general.

In [35], authors proposed a special class of *substitution permutation networks (SPNs)* that uses same network for both the encryption and decryption operations. The idea was to use *involutory* MDS matrix for incorporating diffusion. It may be noted that for ciphers like FOX [17] and WIDEA-n [18] that follow the Lai-Massey scheme, there is no need of involutory matrices. In SPN networks, two different modules are used for encryption and decryption. In SAC 2004 [16] paper, authors constructed efficient MDS matrices for encryption but the inverse of such matrices were not guaranteed to be efficient, which they left for the future work.

Our Contribution: By efficient MDS matrix we mean an MDS matrix with maximum number of 1's and minimum number of distinct elements with low hamming weights. In linear algebra, *circulant matrix* is a special kind of matrix where each row vector is rotated one element to the right relative to the preceding row vector. In the AES MixColumn operation, the MDS matrix is a *circulant matrix* having elements of low hamming weights, but the number of 1's in this matrix is eight. In a SAC 2004 paper, Junod et. al. showed that maximum number of 1's in 4×4 MDS matrix was nine and towards this they constructed a new class of efficient MDS matrices whose submatrices were circulant matrices. They coined the term *circulating-like matrices* for these new class of matrices which we rename as circulant-like matrices. In this paper we study this construction and propose efficient 4×4 and 8×8 such type of *circulant-like MDS matrices.* We prove that such *circulant-like MDS matrices* can not be involutory or orthogonal which are ideally good for designing SPN networks. Although these matrices are efficient, but the inverse of such matrices were not guaranteed to be efficient. Towards this we design a new type of *circulant-like MDS matrices* which are by construction involutory. The basic idea was initially proposed in SAC 1997 by Youssef et. al. where they considered the construction of $2d \times 2d$ involutory MDS matrices M starting from a basic building block A, which was any random $d \times d$ MDS matrix. But no such MDS matrix M was reported for $d = 4$. In our construction we take A as circulant matrices which makes M a new type of *circulant-like* matrix. We prove that M is not MDS whenever d is even. Using this construction and taking A as 3×3 circulant MDS matrices, we construct 6×6 involutory MDS matrices which are suitable for SPN networks.

Previous Work: Nearly all the ciphers use predefined MDS matrices for incorporating the diffusion property. In some ciphers however the possibility of random selection of MDS matrices with some constraints is provided [36]. In this context we would like to mention that in papers [5,12–14,16,19,24,36], different constructions of MDS matrices are provided. In [5], author constructed MDS matrices by applying the theory of Gabidulin codes. In [12], authors constructed lightweight MDS matrices from companion matrices by exhaustive search. In [13], new involutory MDS matrices were constructed using properties of Cauchy matrices over additive subgroup of $\mathbb{F}_{2^n}$ and its equivalence with Vandermonde matrices based construction under some constraints were proved. In [14], authors provably constructed new MDS matrices from companion matrices over $\mathbb{F}_{2^n}$. Efficient 4×4 and 8×8 MDS matrices to be used in block ciphers were constructed in [16]. *Involutory* MDS matrices using Vandermonde matrices were constructed in [19,24]. New involutory MDS matrices using properties of Cauchy matrices were constructed in [36].

The organization of the paper is as follows: In Section 2 we provide definitions and preliminaries. In Section 3, we study some interesting and relevant properties of *circulant-like matrices* of two different forms that are useful to construct efficient MDS matrices. In Section 4 and its subsections, we propose new and efficient $d \times d$ *circulant-like matrices* for $d = 4, 6$ and 8.

2 Definition and Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements and $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. Elements of $\mathbb{F}_{2^n}$ can be represented as polynomials of degree less than n over $\mathbb{F}_2$. For example, let $\beta \in \mathbb{F}_{2^n}$, then β can be represented as $\sum_{i=0}^{n-1} b_i\alpha^i$, where $b_i \in \mathbb{F}_2$ and α is the root of generating polynomial of $\mathbb{F}_{2^n}$. Another compact representation uses hexadecimal digits. Here the hexadecimal digits are used to express the coefficients of corresponding polynomial representation. For example $\alpha^7+\alpha^4+\alpha^2+1 = 1.\alpha^7+0.\alpha^6+0.\alpha^5+1.\alpha^4+0.\alpha^3+1.\alpha^2+0.\alpha+1 = (10010101)_2 = 95_x \in \mathbb{F}_{2^8}$.

The Hamming weight of an integer i is the number of non zero coefficients in the binary representation of i and is denoted by $\mathrm{H}(i)$. For example $\mathrm{H}(5) = 2$, $\mathrm{H}(8) = 1$.

Definition 1. *Let $\mathbb{F}$ be a finite field and p and q be two integers. Let $x \to M \times x$ be a mapping from $\mathbb{F}^p$ to $\mathbb{F}^q$ defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs $(x, M \times x)$ is an MDS code, i.e. a linear code of dimension p, length $p + q$ and minimal distance $q + 1$.*

An MDS matrix provides diffusion properties that have useful applications in cryptography. The idea comes from coding theory, in particular from maximum distance separable code (MDS). In this context we state two important theorems from coding theory.

Theorem 1. *[21, page 33] If C is an $[n, k, d]$ code, then $n - k \geq d - 1$.*

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

Theorem 2. *[21, page 321] An $[n, k, d]$ 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.

Fact: 1 *A square matrix A is an MDS matrix if and only if every square submatrices of A are nonsingular.*

It is to be noted that MDS property remains invariant under elementary row (or column) operations, namely permutations of rows (or column), multiplying a row (or column) of a matrix by a scalar except zero. Also MDS property is invarient under transpose operation. So we have the following fact.

Fact: 2 *If A is an MDS matrix over $\mathbb{F}_{2^n}$, then A', obtained by multiplying a row (or column) of A by any $c \in \mathbb{F}_{2^n}^*$ or by permutations of rows (or columns) is MDS. Also if A is MDS, so is A^T.*

Fact: 3 *If A is an MDS matrix over $\mathbb{F}_{2^n}$, then $c.A$ is MDS for any $c \in \mathbb{F}_{2^n}^*$.*

The inverse of an MDS matrix is MDS. This can be checked easily as the code defined by the matrix $[I|A]$ is the same as the code defined by $[A^{-1}|I]$. So the code defined by $[I|A^{-1}]$ has the same minimal distance and is also MDS. We record this in the following fact.

Fact: 4 *The inverse of an MDS matrix is MDS.*

For efficient implementation of perfect diffusion layer, it is desirable to have maximum number of 1's and minimum number of different entries in the MDS matrix. In [16], authors studied these two properties and proposed some bounds. Here we restate their definitions and few results, which we will use in our constructions.

Definition 2. *[16] Let $M = ((m_{i,j}))$ be a $q \times p$ MDS matrix over $\mathbb{F}_{2^n}$.*

- *Let $v_1(M)$ denotes the number of (i, j) pairs such that $m_{i,j}$ is equal to one. We call it the number of occurrences of one. Also let $v_1^{p,q}$ be the maximal value of $v_1(M)$.*
- *Let $c(M)$ be the cardinality of $\{m_{i,j} | i = 1, \ldots, q; j = 1, \ldots, p\}$. This is called the number of entries. Also let $c^{p,q}$ be the minimal value of $c(M)$.*
- *If $v_1(M) > 0$, then $c_1(M) = c(M) - 1$. Otherwise $c_1(M) = c(M)$. This is called the number of nontrivial entries.*

Fact: 5 *[16] $v_1^{4,4} = 9$, $v_1^{6,6} = 16$, $v_1^{8,8} = 24$.*

Remark 1. High value of v_1 and low value of c and c_1 with low hamming weight elements are desirable for constructing efficient MDS matrices.

In the AES MixColumn operation [9], the MDS matrix is a circulant matrix having elements of low hamming weights.

Definition 3. *[22, page 290] The $d \times d$ matrix of the form*

$$\begin{pmatrix} a_0 & a_1 \ldots a_{d-1} \\ a_{d-1} & a_0 \ldots a_{d-2} \\ \vdots & \vdots \; \vdots \; \vdots \\ a_1 & a_2 \ldots a_0 \end{pmatrix}$$

is called a circulant matrix and will be denoted by $Circ(a_0, \ldots, a_{d-1})$.

The number of 1's in the circulant matrix used in AES [9] diffusion layer is eight. In [16], authors proved that number of 1's can be increased to nine and proposed the construction of *circulant-like* MDS matrices. We restate differently and equivalently their proposed structure of circulant-like matrices.

Definition 4 (Type-I circulant-like matrix). *[16] The $d \times d$ matrix*

$$\begin{pmatrix} a & \mathbf{1} \\ \mathbf{1}^T & A \end{pmatrix}$$

is called Type-I circulant-like matrix, where $A = Circ(1, a_1, \ldots, a_{d-2})$, $\mathbf{1} = \underbrace{(1, \ldots, 1)}_{d\text{-}1 \text{ times}}$, 1 is the unit element and a_i's and a are any nonzero elements of the underlying field other than 1. This matrix is denoted as $TypeI(a, Circ(1, a_1, \ldots, a_{d-2}))$.

Remark 2. For 4×4 *Type-I circulant-like matrix* M, $v_1(M) = 9 = v_1^{4,4}$, but for 8×8 *Type-I circulant-like matrix* M, $v_1(M) = 21 < 24 = v_1^{8,8}$.

We observe that the inverses of *Type-I circulant-like matrices* are almost of same form. So we have the following definition.

Definition 5 (AlmostType-I circulant-like matrix). *The $d \times d$ matrix*

$$\begin{pmatrix} a & \boldsymbol{b} \\ \boldsymbol{b}^T & A \end{pmatrix}$$

is called AlmostType-I circulant-like matrix, where $A = Circ(a_0, a_1, \ldots, a_{d-2})$, $\boldsymbol{b} = \underbrace{(b, \ldots, b)}_{\text{d-1 times}}$, and a, b and a_i's are any elements of the underlying field. This matrix is denoted as $AlmostTypeI(a, b, Circ(a_0, \ldots, a_{d-2}))$.

In SPN networks two different modules are needed for encryption and decryption operations. In [13,35], authors proposed a special class of SPNs that uses same network for both the encryption and decryption operation. The idea was to use involutory MDS matrices for incorporating diffusion. Also orthogonal matrices are of similar interest as encryption and decryption can be implemented with almost same circuitry with same computational cost.

Definition 6. *A square matrix A is called involutory matrix if it satisfies the condition $A^2 = I$, i.e. $A = A^{-1}$.*

Definition 7. *A square matrix A is called orthogonal matrix if $AA^T = I$.*

In this paper, we prove that *Type-I circulant-like MDS matrices* of even dimension can not be involutory or orthogonal. We also propose new type of *circulant-like matrices* (Type-II), which are involutory, are suitable for SPN networks.

Definition 8 (Type-II circulant-like matrix). *The $2d \times 2d$ matrix*

$$\begin{pmatrix} A & A^{-1} \\ A^3 + A & A \end{pmatrix}$$

is called Type-II circulant-like matrix, where $A = Circ(a_0, \ldots, a_{d-1})$. This matrix is denoted as $TypeII(Circ(a_0, \ldots, a_{d-1}))$.

3 Some Useful Results On Circulant-Like Matrices of Type-I and Type-II

In this section we study some important properties of *circulant-like matrices.* Recall that to design diffusion layers for lightweight applications, efficient *involutory MDS matrices* are desirable as the same circuitry can be used for both encryption and decryption. Efficient *orthogonal MDS matrices* are also of similar interest as almost same circuitry can be used for both encryption and decryption. But we will see in this section that $d \times d$ *Type-I circulant-like MDS matrices* (see Definition 4) can not be involutory or orthogonal for even values of d. Also the inverses of efficient *Type-I circulant-like MDS matrices* may not be efficient. Towards this we study and propose a new kind of construction of $2d \times 2d$ *Type-II circulant-like MDS matrices* (see Definition 8), which are involutory. In [36], authors searched for $2d \times 2d$ MDS matrix $M = \begin{pmatrix} A & A^{-1} \\ A^3 + A & A \end{pmatrix}$ by random search on the submatrix A of dimension $d \times d$ for d up to 4, but no such MDS matrix was found for $d = 4$. In Lemma 3, we prove that whenever d is even and A is $d \times d$ circulant matrix (i.e M is *Type-II circulant-like matrix*), M is not MDS. In Subsection 4.2, we construct efficient 6×6 *Type-II involutory circulant MDS matrices* M by taking A as 3×3 efficient circulant MDS matrices.

Lemma 1. *Any $2d \times 2d$ Type-I circulant-like matrix over $\mathbb{F}_{2^n}$ can not be involutory.*

Proof. Let $M = \begin{pmatrix} a & \mathbf{1} \\ \mathbf{1}^T & A \end{pmatrix}$, where $A = Circ(1, a_1, \dots, a_{2d-2})$. Now, $M^2 = \begin{pmatrix} a^2+1 & \mathbf{c} \\ \mathbf{c}^T & B \end{pmatrix}$, where $\mathbf{c} = \underbrace{(c, \dots, c)}_{\text{2d-1 times}}$, $c = a + 1 + \sum_{i=1}^{2d-2} a_i$, $B = U + A^2$ and $U = Circ(1, \dots, 1)$ is $(2d-1) \times (2d-1)$ matrix. It is easy to check that $A^2[0][0] = 1$. Thus $M^2[1][1] = B[0][0] = 1 + 1 = 0$ and so $M^2 \neq I$. Hence M is not involutory. □

Remark 3. In Lemma 1, if $d = 4$ and $A = Circ(1, b, a)$, $M^2 =$
$\begin{pmatrix} a^2+1 & (b+1) & (b+1) & (b+1) \\ (b+1) & 0 & (1+a^2) & (1+b^2) \\ (b+1) & (1+b^2) & 0 & (1+a^2) \\ (b+1) & (1+a^2) & (1+b^2) & 0 \end{pmatrix} \neq I$. So M is not involutory. When $a = \alpha$ and $b = 1 + \alpha^{-1}$ where α is the root of the generating polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$ of $\mathbb{F}_{2^8}$, we get the matrix M which is used in block cipher FOX64 [17] (up to the permutation).

Lemma 2. *Any $2d \times 2d$ Type-I circulant-like MDS matrix over $\mathbb{F}_{2^n}$ is not orthogonal.*

Proof. Let $M = \begin{pmatrix} a & \mathbf{1} \\ \mathbf{1}^T & A \end{pmatrix}$, where $A = Circ(1, a_1, \dots, a_{2d-2})$. Now $M \times M^T = \begin{pmatrix} a^2+1 & \mathbf{c} \\ \mathbf{c}^T & B \end{pmatrix}$, where $\mathbf{c} = \underbrace{(c, \dots, c)}_{\text{2d-1 times}}$, $c = a + 1 + \sum_{i=1}^{2d-2} a_i$, $B = U + A \times A^T$ and $U = Circ(1, \dots, 1)$ is $(2d-1) \times (2d-1)$ matrix. For M to be orthogonal, $M \times M^T = I$, which gives $a^2 + 1 = 1$. So $a = 0$, thus M is not MDS, a contradiction. Hence the proof. □

We next examine the possibility of constructing involutory MDS matrices from *Type-II circulant-like matrices*. Towards this we show in Lemma 3 that such $2m \times 2m$ *Type-II circulant-like matrices* are non MDS whenever m is even.

Lemma 3. *Any $2m \times 2m$ Type-II circulant-like matrix over $\mathbb{F}_{2^n}$ is non MDS for even values of m.*

Proof. Let $m = 2d$ and $A = Circ(a_0, a_1, \dots, a_{2d-1})$. It is easy to check that $A^2 = Circ(a_0^2 + a_d^2, 0, a_1^2 + a_{d+1}^2, 0, \dots, a_{d-1}^2 + a_{2d-1}^2, 0)$. Let $b_i = a_i^2 + a_{d+i}^2$ for $i = 0, \dots, d-1$, so $A^2 = Circ(b_0, 0, b_1, 0, \dots, b_{d-1}, 0)$. Now $A^3 = A \times A^2 = Circ(a_0, a_1, \dots, a_{2d-1}) \times Circ(b_0, 0, b_1, 0, \dots, b_{d-1}, 0) = Circ(e_0, e_1, \dots, e_{2d-1})$, where $e_{2k} = \sum_{i=0}^{d-1} a_{2i} b_{d-i+k}$ and $e_{2k+1} = \sum_{i=0}^{d-1} a_{2i+1} b_{d-i+k}$ for $k = \{0, 1, \dots, (d-1)\}$, where suffixes of a_i's are computed modulo $2d$ and the suffixes of b_j's are computed modulo d.

Let $C_0, \dots, C_{2d-1}$ are the column vectors of A, where $C_0 = (a_0, a_{2d-1}, a_{2d-2}, \dots, a_1)^T$ and C_i is obtained from C_{i-1} by one shift vertically downward. Now,

$$\begin{pmatrix} e_0 \\ e_{2d-1} \\ e_{2d-2} \\ \vdots \\ e_2 \\ e_1 \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{d-1} a_{2i}b_{d-i} \\ \sum_{i=0}^{d-1} a_{2i+1}b_{d-i+d-1} \\ \sum_{i=0}^{d-1} a_{2i}b_{d-i+d-1} \\ \vdots \\ \sum_{i=0}^{d-1} a_{2i}b_{d-i+1} \\ \sum_{i=0}^{d-1} a_{2i+1}b_{d-i} \end{pmatrix} = \begin{pmatrix} a_0b_0 + a_2b_{d-1} + a_4b_{d-2} + \ldots + a_{2d-2}b_1 \\ a_1b_{d-1} + a_3b_{d-2} + a_5b_{d-3} + \ldots + a_{2d-1}b_0 \\ a_0b_{d-1} + a_2b_{d-2} + a_4b_{d-3} + \ldots + a_{2d-2}b_0 \\ \vdots \\ a_0b_1 + a_2b_0 + a_4b_{d-1} + \ldots + a_{2d-2}b_2 \\ a_1b_0 + a_3b_{d-1} + a_5b_{d-2} + \ldots + a_{2d-1}b_1 \end{pmatrix} =$$

$$\begin{pmatrix} a_0b_0 + a_2b_{d-1} + a_4b_{d-2} + \ldots + a_{2d-2}b_1 \\ a_{2d-1}b_0 + a_1b_{d-1} + a_3b_{d-2} + \ldots + a_{2d-3}b_1 \\ a_{2d-2}b_0 + a_0b_{d-1} + a_2b_{d-2} + \ldots + a_{2d-4}b_1 \\ \vdots \\ a_2b_0 + a_4b_{d-1} + a_6b_{d-2} + \ldots + a_0b_1 \\ a_1b_0 + a_3b_{d-1} + a_5b_{d-2} + \ldots + a_{2d-1}b_1 \end{pmatrix} = b_0C_0 + b_{d-1}C_2 + b_{d-2}C_4 + \ldots + b_1C_{2d-2}.$$

It is to be noted that the first column of A^3 can be written as the linear combination of C_0, C_2, C_4, $\ldots$, C_{2d-2}. So the first column of $(A^3 + A)$ is $(b_0 + 1)C_0 + b_{d-1}C_2 + b_{d-2}C_4 + \ldots + b_1C_{2d-2}$.

Let $M = TypeII(Circ(a_0, \ldots, a_{2d-1}))$ be a $4d \times 4d$ *Type-II circulant-like matrix* whose row vectors are $R_0, R_1, \ldots, R_{4d-1}$ and column vectors are $T_0, T_1, \ldots, T_{4d-1}$. So $(d+1)\times(d+1)$ submatrix of M obtained by the rows R_{2d}, $R_{2d+1}, \ldots, R_{2d+d}$ and the columns T_0, T_{2d}, $T_{2d+2}, \ldots, R_{2d+2d-2}$ is singular. So from Fact 1, M is non MDS. □

Remark 4. In lightweight applications, major constraints are on processors and memory. If constraints on processor is more than that on memory, some preprocessing step may not be affordable. The total number of operations and temporary variables thus may be reduced at the cost of supplementary multiplication tables. We design 4×4 *Type-I circulant-like MDS matrices* M_1 such that $c_1(M_1) = 2$ and 8×8 *Type-I circulant-like MDS matrices* M_2 such that $c_1(M_2) = 6$. So the 4×4 and 8×8 *Type-I circulant-like MDS matrices* may be implemented at the cost of only two or six table lookups respectively. In the design of 6×6 *Type-II circulant-like MDS matrices*, we take these matrices M for which $c_1(M) \leq 8$. For such situations, at the cost of only eight table lookups, the matrices may be implemented. Since these matrices are involutory, inverse operation is achieved with the same implementation.

We have explored certain relevant properties of *Type-I and Type-II circulant-like matrices* that are useful in the study of MDS matrices. In the next section, we will construct efficient 4×4 and 8×8 *Type-I circulant-like MDS matrices* and efficient involutory 6×6 *Type-II circulant-like MDS matrices.*

4 Efficient Circulant-Like MDS Matrices

In this section we construct efficient *Type-I* and *Type-II circulant-like MDS matrices* over finite field. By efficient MDS matrix we mean an MDS matrix with maximum number of 1's and minimum number of distinct elements with low hamming weights (see Remark 1). MDS matrices with elements having low hamming weights are desirable for efficient implementation. In this context it may be noted that multiplication by 1, which is the unit element of $\mathbb{F}_{2^n}$, is trivial. When α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$, the multiplication by α can be implemented by a shift by one bit to the left and a conditional XOR with a constant when a carry bit is set. Similarly multiplication by α^{-1} can be implemented by a shift by one bit to the right and a conditional XOR with a constant when a carry bit is set. It is to be noted that multiplication by α and α^{-1} are of equal cost. Multiplication by $\alpha+1$ is done by a multiplication by α and one XOR operation. Multiplication by α^2 is done by two successive multiplications by α.

4.1 Efficient 4 × 4 and 8 × 8 Type-I Circulant-Like MDS Matrices

In this subsection, we construct efficient $d \times d$ *Type-I circulant-like MDS matrices* $M = TypeI(a, Circ(1, a_1, \ldots, a_{d-2}))$, $a_i \in \mathbb{F}_{2^n}$ for $d = 4$ and 8. Our target is to construct MDS matrices with high v_1 and low c_1 (see Remark 1). For efficient implementation, we aim to restrict a_i's to the form $c_0 + c_1\alpha + c_2\alpha^{-1} + c_3\alpha^2 + c_4\alpha^{-2}$ where $c_i \in \{0, 1\}$.

In Table 1, we provide some efficient 4×4 *Type-I circulant-like MDS matrices* over $\mathbb{F}_{2^8}$ with generating polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$. For more efficient design, we fix $a_2 = a$, so that $c_1(M) = 2$ which is lowest (see Remark 1 and Remark 4).

Table 1. 4×4 *Type-I circulant-like MDS matrices* over $\mathbb{F}_{2^8}$ with generating polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$ where elements of these matrices are polynomials in α and α^{-1} of degree at most 2 and α is the root of the generating polynomial:

Type-I circulant-like MDS Matrix M	**Inverse Matrices** M^{-1}
$TypeI(\alpha, Circ(1, 1+\alpha+\alpha^{-1}+\alpha^{-2}, \alpha))$	$AlmostTypeI(1+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6+\alpha^7, \alpha,$ $Circ(1, \alpha^4+\alpha^6+\alpha^7, 1+\alpha^2+\alpha^4+\alpha^6+\alpha^7))$
$TypeI(1+\alpha, Circ(1, \alpha+\alpha^{-1}, 1+\alpha))$	$AlmostTypeI(1, \alpha,$ $Circ(\alpha^2+\alpha^4+\alpha^6, 1+\alpha+\alpha^3+\alpha^4+\alpha^5, 1+\alpha^4+\alpha^6+\alpha^7))$
$TypeI(\alpha^{-1}, Circ(1, \alpha+\alpha^{-1}, \alpha^{-1}))$	$AlmostTypeI(\alpha+\alpha^2, \alpha$ $Circ(\alpha+\alpha^2+\alpha^3+\alpha^5+\alpha^6, \alpha^2+\alpha^3+\alpha^4+\alpha^5, 1+\alpha+\alpha^4+\alpha^6))$

Remark 5. By Lemma 1 and Lemma 2, the 4×4 matrices of Table 1 and 8×8 matrices of Table 2 are neither involutory nor orthogonal.

Remark 6. The MDS Matrix used in FOX64 is $TypeI(\alpha, Circ(1, 1+\alpha^{-1}, \alpha))$ (up to the permutation), whose inverse is $AlmostTypeI(1+\alpha+\alpha^6+\alpha^7, \alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6, Circ(1+\alpha^5+\alpha^6+\alpha^7, \alpha^4+\alpha^5+\alpha^7, 1+\alpha^2+\alpha^3+\alpha^5+\alpha^7))$. Compared to this matrix, the inverse of the 2nd matrix proposed in Table 1 i.e. $AlmostTypeI(1, \alpha, Circ(\alpha^2+\alpha^4+\alpha^6, 1+\alpha+\alpha^3+\alpha^4+\alpha^5, 1+\alpha^4+\alpha^6+\alpha^7))$ has elements of lower hamming weights. So whenever the inverse operation is needed, this matrix is a better candidate.

In Table 2, we provide some efficient 8×8 *Type-I circulant-like MDS matrices* over $\mathbb{F}_{2^8}$. For more efficient design, we fix $a_6 = a$, so that $c_1(M) = 6$ (see Remark 1 and Remark 4).

Remark 7. Similar to Remark 6, the MDS Matrix used in FOX128 is $TypeI(1+\alpha, Circ(1, 1+\alpha, \alpha^{-1}+\alpha^{-2}, \alpha, \alpha^2, \alpha^{-1}, \alpha^{-2}))$ (up to the permutation), whose inverse is $AlmostTypeI(\alpha+\alpha^3+\alpha^5+\alpha^6+\alpha^7, \alpha+\alpha^2+\alpha^6+\alpha^7, Circ(\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6+\alpha^7, 1+\alpha+\alpha^2+\alpha^4+\alpha^5+\alpha^7, \alpha+\alpha^4+\alpha^6+\alpha^7, \alpha^2+\alpha^3, 1+\alpha^2+\alpha^3+\alpha^5+\alpha^6, 1+\alpha+\alpha^4+\alpha^5+\alpha^6, \alpha+\alpha^3+\alpha^4+\alpha^5))$. Compared to this matrix, the inverse of the 2nd matrix proposed in Table 2 i.e. $AlmostTypeI(1+\alpha+\alpha^6+\alpha^7, \alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6, Circ(\alpha+\alpha^3+\alpha^4, \alpha+\alpha^4+\alpha^5+\alpha^6+\alpha^7, \alpha+\alpha^4+\alpha^5+\alpha^7, \alpha^4+\alpha^5, 1+\alpha^2+\alpha^3, \alpha^4+\alpha^7, \alpha+\alpha^3, 1))$ has elements of lower hamming weights. So whenever the inverse operation is needed, this matrix is a better candidate.

Table 2. 8×8 *Type-I circulant-like MDS matrices* over $\mathbb{F}_{2^8}$ with generating polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$ where elements of these matrices are polynomials in α and α^{-1} of degree at most 2 and α is the root of the generating polynomial:

Type-I circulant-like MDS Matrix M	**Inverse Matrices** M^{-1}
$TypeI(\alpha, Circ(1, 1+\alpha, \alpha+\alpha^2, \alpha^{-1}+\alpha^2, 1+\alpha^{-1}+\alpha^2, \alpha^{-2}, \alpha))$	$AlmostTypeI(\alpha+\alpha^2+\alpha^3+\alpha^7, \alpha^2+\alpha^5+\alpha^6+\alpha^7,$ $Circ(1+\alpha+\alpha^3+\alpha^4+\alpha^5+\alpha^6, 1+\alpha^2+\alpha^4+\alpha^5,$ $1+\alpha^5+\alpha^6, \alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^7, 1+\alpha^2+\alpha^6,$ $1+\alpha+\alpha^3+\alpha^5+\alpha^6+\alpha^7, \alpha+\alpha^2+\alpha^3+\alpha^5))$
$TypeI(\alpha, Circ(1, 1+\alpha^{-1}, \alpha+\alpha^{-1}+\alpha^2, 1+\alpha+\alpha^{-1}+\alpha^2,$ $\alpha^{-1}+\alpha^{-2}, 1+\alpha^{-1}+\alpha^{-2}, \alpha))$	$AlmostTypeI(1+\alpha+\alpha^6+\alpha^7, \alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6,$ $Circ(\alpha+\alpha^3+\alpha^4, \alpha+\alpha^4+\alpha^5+\alpha^6+\alpha^7,$ $\alpha+\alpha^4+\alpha^5+\alpha^7, \alpha^4+\alpha^5,$ $1+\alpha^2+\alpha^3, \alpha^4+\alpha^7, \alpha+\alpha^3, 1))$

4.2 Efficient 6×6 Type-II Circulant-Like MDS Matrices

In Table 3 we present some 6×6 *Type-II circulant-like MDS Matrices* $M = TypeII(Circ(a_0, a_1, a_2))$ over $\mathbb{F}_{2^8}$ with generating polynomial $x^8 + x^4 + x^3 + x^2 + 1$ where a_i's are restricted in $\{01_x, 02_x, \ldots, 07_x\}$ and one of them is taken as 1. Note that these matrices are involutory and $v_1(M) \geq 6$. We get no such M for which $v_1(M) > 6$. Also note that $c_1(M) \leq 8$.

Table 3. 6×6 Type-II circulant-like MDS Matrices over $\mathbb{F}_{2^8}$ with generating polynomial $x^8+x^4+x^3+x+1$:

Type-II circulant-like MDS Matrix M
$TypeII(Circ(02_x, 01_x, 05_x)$
$TypeII(Circ(02_x, 01_x, 06_x)$
$TypeII(Circ(03_x, 01_x, 06_x)$
$TypeII(Circ(04_x, 01_x, 03_x)$
$TypeII(Circ(05_x, 01_x, 06_x)$

5 Conclusion

In [16], authors introduced the idea of *circulant-like* matrices for efficient design of diffusion layer. We redefined this form of matrices as *Type-I circulant-like MDS matrices* and studied the properties and constructions of 4×4 and 8×8 *Type-I circulant-like MDS matrices*. We also introduced a new type of involutory *circulant-like* matrices which we call *Type-II circulant-like MDS matrices* and construct efficient 6×6 involutory MDS matrices which are suitable for SPN networks. We proved that $2d \times 2d$ *Type-I circulant-like matrices* can not be involutory. We also proved that *Type-I circulant-like MDS matrices* can not be orthogonal. In [16], authors mentioned that inverse of such *Type-I circulant-like matrices* were not guaranteed to be efficient which they left for future work. Towards this we revisited the general scheme of [36] to construct involutory matrices. Using circulant matrices in the scheme, we proposed efficient $2d \times 2d$ *Type-II circulant-like MDS matrices* for odd values of d. In [36], authors were unable to obtain any MDS matrix after a random search for $d = 4$. We proved that $2d \times 2d$ *Type-II circulant-like matrices* are non MDS whenever d is even.

References

1. D. Augot, M. Finiasz, *Exhustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions*, Proceedings of the 2013 IEEE International Symposium on Information Theory. IEEE (2013).

2. P. Barreto and V. Rijmen, *The Khazad Legacy-Level Block Cipher*, Submission to the NESSIE Project (2000). Available at http://cryptonessie.org.
3. P. S. Barreto and V. Rijmen, *The Anubis block cipher*, NESSIE Algorithm Submission (2000). Available at http://cryptonessie.org
4. P. S. L. M. Barreto and V. Rijmen, *Whirlpool*, Encyclopedia of Cryptography and Security (2nd Ed.), 2011, pp. 1384–1385.
5. T. P. Berger, *Construction of Recursive MDS Diffusion Layers from Gabidulin Codes*, INDOCRYPT 2013, pp. 274–285, 2013.
6. W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comput, 24(3-4):235-265, 1997, Computational algebra and number theory (London, 1993).
7. J. Choy, H. Yap, K. Khoo, J. Guo, T. Peyrin, A. Poschmann and C.H. Tan, *SPN-Hash: Improving the Provable Resistance against Differential Collision Attacks*, AFRICACRYPT 2012, pp. 270–286, 2012.
8. J. Daemen, L. R. Knudsen and V. Rijmen, *The block cipher SQUARE*, In 4th Fast Software Encryption Workshop, LNCS 1267, pp. 149-165, Springer-Verlag, 1997.
9. J. Daemen and V. Rijmen, *The Design of Rijndael:AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.
10. G. D. Filho, P. Barreto and V. Rijmen, *The Maelstrom-0 Hash Function*, In Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security (2006).
11. P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer and S. Thomsen, *Grϕstl a SHA-3 Candidate.*, Submission to NIST (2008). Available at http://www.groestl.info.
12. J. Guo, T. Peyrin and A. Poschmann, *The PHOTON Family of Lightweight Hash Functions*, In CRYPTO 2011, pp. 222–239, Springer, 2011.
13. K. C. Gupta and I. G. Ray, *On Constructions of Involutory MDS Matrices*, In AFRICACRYPT 2013, pp 43–60, Springer 2013.
14. K. C. Gupta and I. G. Ray, *On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography*, In CD-ARES 2013 Workshops: MoCrySEn, pp. 29–43, Springer, 2013.
15. J. Nakahara Jr and E. Abrahao, *A New Involutory MDS Matrix for the AES*, International Journal of Network Security, Vol.9, No.2, PP.109-116, Sept. 2009.
16. 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.
17. P. Junod and S. Vaudenay, *FOX: a new family of block ciphers*, Selected Areas in Cryptography, SAC, 2004, pp. -114-119, Springer, LNCS
18. P. Junod and M. Macchetti, *Revisiting the IDEA philosophy*, Fast Software Encryption, 16th International Workshop (FSE), 2009, Lecture Notes in Computer Science, 5665, pp. 277-295, Springer, 2009
19. J. Lacan and J. Fimes, *Systematic MDS erasure codes based on vandermonde matrices*, IEEE Trans. Commun. Lett. 8(9), 570572 (2004) CrossRef
20. J. W. Lo, M. S. Hwang and C. H. Liu, *An efficient key assignment scheme for access control in a large leaf class hierarchy*, Journal of Information Sciences: An International Journal archive, Elsevier Science Inc. New York, NY, USA, Volume 181 Issue 4, February, 2011, Pages 917–925
21. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, 1986.
22. A. R. Rao and P. Bhimasankaram, *Linear Algebra*, Second Edition, Hindustan Book Agency.
23. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E. D. Win, *The cipher SHARK*, In 3rd Fast Software Encryption Workshop, LNCS 1039, pp. 99-112, Springer-Verlag, 1996.
24. M. Sajadieh, M. Dakhilalian, H. Mala and B. Omoomi, *On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$*, Design, Codes Cryptography 2012, pp.1–22, 2012.
25. M. Sajadieh, M. Dakhilalian, H. Mala and P. Sepehrdad, *Recursive Diffusion Layers for Block Ciphers and Hash Functions*, FSE 2012, pp. 385–401, Springer 2012.
26. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, *Twofish: A 128-bit block cipher*, In the first AES Candidate Conference. National Institute for Standards and Technology, 1998.
27. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, *The Twofish encryption algorithm*, Wiley, 1999.
28. C. Schnorr and S. Vaudenay, *Black Box Cryptanalysis of Hash Networks Based on Multipermutations*, In A. De Santis, editor, Advances in Cryptology - EUROCRYPT 94. Proceedings, volume 950 of LNCS, pp. 47–57. Springer-Verlag, 1995.
29. C. E. Shannon, *Communication Theory of Secrecy Systems*. Bell Syst. Technical J., 28, 656–715 (1949).
30. T. Shiraj and K. Shibutani, *On the Diffusion Matrix Employed in the Whirlpool Hashing Function*, Available at http://www.cosic.esat.kuleuven.be/nessie/reports/.../whirlpool-20030311.pdf
31. Sony Corporation, *The 128-bit Block cipher CLEFIA* Algorithm Specification (2007). Available at http://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf.

32. S. Vaudenay, *On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER*, In B. Preneel, editor, Fast Software Encryption 1995. Proceedings, volume 1008 of LNCS, pp. 286–297. Springer-Verlag, 1995.
33. D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi and B. Preneel *A new keystream generator MUGI*, FSE 2002, pp. 179–194. Springer Berlin/Heidelberg, 2002.
34. S. Wu, M. Wang and W. Wu, *Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions.*, SAC 2012, LNCS 7707, pp. 355–371, , Springer-Verlag Berlin Heidelberg, 2013.
35. A. M. Youssef, S. E. Tavares and H. M. Heys, *A New Class of Substitution Permutation Networks*, Workshop on Selected Areas in Cryptography, SAC '96, Workshop Record, pp. 132–147, 1996.
36. A. M. Youssef, S. Mister and S. E. Tavares, *On the Design of Linear Transformations for Substitution Permutation Encryption Networks*, In Workshop On Selected Areas in Cryptography, SAC 97, pp. 40–48, 1997.