International Journal of Mathematics and
Computer Science, **17**(2022), no. 4, 1619–1637

On Orthogonal Circulant MDS Matrices

Ichlas Adhiguna, Izdihar Salsabila Noor Arifin, Fajar Yuliawan, Intan Muchtadi-Alamsyah

Algebra Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung
Bandung, Indonesia

email: ntan@math.itb.ac.id

(Received May 18, 2022, Accepted July 5, 2022)

Abstract

In 2019, Cauchois and Loidreau gave a necessary and sufficient condition for the existence of circulant MDS matrices over a field of given characteristic. In this paper, we prove the non-existence of certain orthogonal circulant MDS matrices. Then we give a necessary and sufficient condition for orthogonal θ-circulant matrices using q-polynomial rings. We also discuss orthogonal circulant MDS matrices over Galois rings.

1 Introduction

In interacting with the internet, we are often required to transfer data. Cryptography plays a role in keeping data confidential so that it cannot be changed or read by anyone other than the recipient. An algorithm for converting data from plaintext into ciphertext and back into plaintext is called a cipher. There are two ciphers; namely, block ciphers and stream ciphers. Block cipher consists of two algorithms; namely, encryption and decryption. Encryption is a process that converts plaintext into ciphertext. In contrast, decryption is a process that converts ciphertext to plaintext.

Key words and phrases: MDS matrices, q-polynomial ring, θ-circulant matrices, orthogonal matrices.
AMS (MOS) Subject Classifications: 20H25, 94B05, 16S36.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

Shannon [7] introduced the concept of confusion and diffusion in block ciphers. The algorithm's component that performs diffusion is called the diffusion layer, and the element of the algorithm that performs confusion is called the confusion layer. The confusion layer hides the relationship between the ciphertext and the key. In contrast, the diffusion layer hides the relationship between ciphertext and plaintext. In the diffusion layer, a linear mapping is represented by a matrix. The diffusion power of this matrix is measured based on its branch numbers. The larger the branch number, the better the matrix. One of the matrices classes with a maximum branch number is the MDS (maximum distance separable) matrix. Therefore, many ciphers use the MDS matrix in their diffusion layer.

In 1996 the MDS matrix was first used in the chiper SHARK [10] and then followed by SQUARE [2] and AES [3]. The AES encryption process has four steps; namely, `SubBytes`, `ShiftRows`, `MixColumns`, and `AddRoundkey` [3]. The MDS matrix is used in the `MixColumns`. Since the decryption process usually uses the inverse of the matrix used in the encryption process, it will be better to use a matrix whose inverse is easy to find. One of the choices is to use an orthogonal or involutory MDS matrix even though AES does not require that.

In addition to inverses that are easy to determine, orthogonal or involutory matrices also have another advantage. Khoo et al. [6] introduced a metric called XOR-count to measure the cost of the hardware implementation of the diffusion of a matrix. The smaller the XOR-count value of a matrix, the better the matrix in hardware implementation. A matrix with a small XOR count does not necessarily have an inverse with a small XOR count. However, orthogonal or involutory matrices have the same XOR count as the inverse so that if one finds an orthogonal or involutory MDS matrix with a small XOR count, then the XOR-count for the inverse of the matrix will also be small. Therefore, the orthogonal or involutory MDS matrix is preferable in some block ciphers.

AES use a circulant MDS matrix in the diffusion layer. One advantage of the circulant matrix is that the $n \times n$ circulant matrix has a maximum of n different components so that storing of n elements is better than keeping n^2 elements. Daemen et al. [2] proved that the probability of finding a circulant MDS matrix is more significant compared to a randomized square matrix. Nevertheless, the MDS circulant matrices have some limitations. As previously explained, orthogonal or involutory matrices are preferable. A construction of involutory MDS matrices is given in [5].

Gupta and Ray [4] proved that there is no orthogonal circulant MDS

matrix of size $2^n \times 2^n$ for characteristic 2 and no involutory circulant MDS matrix of size $n \times n$ with $n \geq 3$ for characteristic 2. For characteristic $p > 2$ no involutory MDS matrix of size $2n \times 2n$ for $n \geq 2$ [1]. Therefore, Cauchois and Loidreau [1] generalized the circulant matrix to θ-circulant matrix. A circulant matrix is a θ-circulant matrix with θ is an identity mapping. Like the circulant matrix, the θ-circulant matrix of size $n \times n$ needs to store at most n elements. Therefore, Cauchois and Loidreau provided a sufficient and necessary condition for obtaining MDS θ-circulant involutory matrix. However, they do not discuss the orthogonal θ-circulant matrix.

In this paper, we prove some results on the non-existence of orthogonal circulant MDS matrices by using q-polynomial approach. Then we determine whether the transpose of a θ-circulant matrix is also θ-circulant. We use this result to give a sufficient and necessary condition so that the θ-circulant matrix is an MDS orthogonal matrix. We also discuss orthogonal circulant MDS matrices over Galois rings.

2 MDS Matrices over Rings

Let R be a commutative ring with identity. The set of matrix rows of size $1 \times n$ whose components are in R is denoted by R^n. Moreover, R^n is a module over R. A linear code over the ring R is a submodule of R^n. A linear code of dimension k and length n is called an $[n, k]$ code. Elements of the $[n, k]$ code are called codewords.

Suppose C is a linear code with x and y are any members of C. If $x = (x_1, x_2, \cdots x_n)$ and $y = (y_1, y_2, \cdots, y_n)$, then define $d(x, y)$ as follows:

$$d(x, y) = \sum_{i=1}^{n} d(x_i, y_i),$$

with $d(x_i, y_i) = 1$ if $x_i \neq y_i$ and $d(x_i, y_i) = 0$ if $x_i = y_i$. The value of $d(x, y)$ is called the Hamming distance (or simply the distance) of the elements x and y. For any $x, y, z \in C$, the Hamming distance satisfies

1. $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y)$.

Therefore, Hamming distance is a metric and so the linear code C and Hamming distance form a metric space. The Hamming weight $w(x)$ of x is the number of nonzero components of the vector x.

It is easy to show that the Hamming weight of the element $x-y$ satisfies $w(x-y) = d(x,y)$. The minimum Hamming distance of the linear code C is a number d that satisfies

$$d = \min d(x,y) \qquad x, y \in C \text{ and } x \neq y$$

A linear code with length n, dimension k, and minimum Hamming distance d is called a linear code $[n,k,d]$. With almost a similar definition, the minimum Hamming weight of the linear code C is a number b that satisfies

$$b = \min w(x) \qquad x \in C \text{ and } x \neq \mathbf{0}$$

Hamming distance and Hamming weight of a linear code C are equal.

Theorem 2.1. *(Singleton limit)* [8] *Suppose C is a linear code $[n,k,d]$. Then $d \leq n-k+1$.*

Definition 2.2. *A linear code $[n,k,d]$ that satisfies $d = n-k+1$ is called an MDS code (maximum distance separable).*

We call a matrix G the generator matrix of $[n,k,d]$ code if its rows form a basis for the code. The generator matrix of $[n,k,d]$ code is always of size $k \times n$. The generator matrix of the form $G = [I \mid A]$ is called the generator matrix in standard form. If the linear code $[n,k,d]$ with the generator matrix $G = [I \mid A]$ is an MDS code, then A is called an MDS matrix. Another way to define the MDS matrix is by checking all of its minors. A matrix A is MDS if and only if all of its minors are unit elements in R.

The following theorem gives a restriction for the size of MDS matrices over a finite field.

Theorem 2.3. *Let A be an MDS $n \times n$ matrix over $\mathbb{F}_q$, where q is a prime power. Then $n \leq q-1$.*

Proof. Suppose on the contrary that $n \geq q$. Note that, since $A = (a_{ij})$ is MDS, $a_{ij} \neq 0$ for all i, j. Consider the n elements $a_{i,2}/a_{i,1}$, for $i = 1, 2, \cdots, n$ of $\mathbb{F}_q - \{0\}$. By the Pigeon Hole Principle, there exists $k < l$ such that $a_{k,2}/a_{k,1} = a_{l,2}/a_{l,1}$. It follows that the 2×2 submatrix $\begin{bmatrix} a_{k,1} & a_{k,2} \\ a_{l,1} & a_{l,2} \end{bmatrix}$ is not invertible, a contradiction to the fact that A is MDS.

□

Remark The above theorem can be proved using MDS codes. Denote by $M(k,q)$ the maximal length of an MDS code over $\mathbb{F}_q$ with dimension k. A square MDS matrix has a length of $2k$; therefore, $2k \leq q+k-1$, and we get $k \leq q-1$.

A matrix A of order m over R is called a circulant matrix if A has the following form.

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & \cdots & a_{m-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$$

with $a_i \in R$ for $i = 0, 1, \cdots, m-1$. We use the following notation: $A = circ(a_0, a_1, \cdots, a_{m-1})$. An orthogonal circulant MDS matrix over R is an orthogonal, circulant and MDS matrix.

3 Orthogonal Circulant MDS Matrices over Finite Fields

Let q be a prime power. In this section, a circulant matrix over $\mathbb{F}_q$ will be related to a polynomial in $\mathbb{F}_q[X]$.

Definition 3.1. [1] *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$ be a monic polynomial of degree m. The circulant matrix associated to h is the matrix defined by:*

$$C_h = \begin{bmatrix} h_0 & h_1 & \cdots & h_{m-1} \\ h_{m-1} & h_0 & \cdots & h_{m-2} \\ \vdots & \ddots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{bmatrix}$$

Theorem 3.2. [1] *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$ be a monic polynomial of degree m and C_h is the circulant matrix associated to h. Then C_h is the representation matrix with respect to the basis $\{1, X, X^2, \cdots, X^{m-1}\}$ of the map*

$$\begin{array}{rccc} \psi: & \mathbb{F}_q[X]/\langle X^m - 1\rangle & \to & \mathbb{F}_q[X]/\langle X^m - 1\rangle \\ & Q(X) & \mapsto & Q(X)h(X) \end{array}$$

We denote by $\mathbb{F}_{q,m-1}[X]$ the set of all polynomials in $\mathbb{F}_q[X]$ with degree smaller or equal to $m-1$.

Theorem 3.3. [1] *Let* $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$. *Suppose* C_h *is a circulant matrix associated to* h, *then* C_h *is an MDS matrix if and only if every nonzero* $Q_1(X) \in \mathbb{F}_{q,m-1}[X]$ *satisfies*

$$w(Q_1) + w(Q_1(X)h(X) \mod (X^m - 1)) \geq m + 1$$

In particular, an orthogonal or involutory MDS matrix is more desirable because it has an inverse that is easy to find. A sufficient and necessary condition for an involutory circulant matrix is described in the following theorem.

Theorem 3.4. [1] *Let* $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_1 X^i \in \mathbb{F}_q[X]$. *Suppose* C_h *is the circulant matrix associated to* h. *Then* C_h *is involutory if and only if* $h(X)^2 = 1 \mod (X^m - 1)$.

Suppose C_h and C_g are two circulant matrices associated to the polynomials h and g, respectively, and let I_m be the $m \times m$ identity matrix. The following proposition provides a sufficient and necessary condition for the two matrices to be inverses of each other.

Proposition 3.5. *Given the following polynomials*

$$h(X) = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1} X^{m-1} \in \mathbb{F}_q[X]$$

and

$$g(X) = (X^m - 1) + g_0 + g_1 X + \cdots + g_{m-1} X^{m-1} \in \mathbb{F}_q[X]$$

associated to C_h *and* C_g *respectively, then*

$$C_h C_g = I_m \quad \text{if and only if} \quad 1 = h(X)g(X) \mod (X^m - 1)$$

If $h(X) = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1} X^{m-1}$ is a polynomial associated to the matrix C_h then C_h^T is a matrix associated to $h'(X) = (X^m - 1) + h_0 + h_{m-1} X + h_{m-2} X^2 + \cdots + h_1 X^{m-1}$. If C_h is orthogonal then by Proposition (3.5) we get the following result.

Corollary 3.6. *Let* $h(X) = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1} X^{m-1} \in \mathbb{F}_q[X]$ *be a polynomial associated to the* C_h *matrix. If* C_h^T *is the transpose of* C_h *and* C_h^T *is associated to the polynomial* $h' \in \mathbb{F}_q[X]$, *then*

$$C_h \text{ orthogonal} \quad \text{if and only if} \quad 1 = h(X)h'(X) \mod (X^m - 1)$$

Proof. The proof follows directly from Proposition (3.5) with $C_g = C_h^T$. □

Gupta and Ray [4] proved that an orthogonal circulant matrix of order 2^n with $n \geq 2$ over the field $\mathbb{F}_{2^r}$ cannot be MDS. Moreover, they also proved that an involutory circulant matrix of order n with $n \geq 3$ over the field $\mathbb{F}_{2^r}$ cannot be MDS. Not only in the field with characteristic 2, in the finite field with other characteristics have also limitations as described in the following theorem.

Theorem 3.7. [1] *Let $n \geq 2$. There is no involutory circulant MDS matrix of order $2n$ over a field of characteristic $p \geq 2$.*

In the following results, we use Cauchois and Loidreau's q-polynomial approach [1] to prove the non-existence of certain orthogonal MDS circulant matrices over a field of characteristic p.

Theorem 3.8. *Let p be a prime, $p > 2$ and $m = sp$ for some integer $s \geq 2$. Then there is no orthogonal circulant MDS matrix of order m over a field of characteristic p.*

Proof. Assume that there exists an $m \times m$ orthogonal circulant MDS matrix C_h in $\mathbb{F}_{p^r}$ with corresponding polynomial $h(X)$.
Let $h(X) = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1} X^{m-1}$. Define

$$\begin{aligned} a_1(X) &= h_0 + h_s X^s + h_{2s} X^{2s} + \cdots + h_{(p-1)s} X^{(p-1)s} \\ a_2(X) &= h_1 + h_{s+1} X^{s+1} + h_{2s} X^{2s+1} + \cdots + h_{(p-1)s+1} X^{(p-1)s+1} \\ &\vdots \\ a_s(X) &= h_{s-1} + h_{2s-1} X^{2s-1} + h_{3s-1} X^{3s-1} + \cdots + h_{m-1} X^{m-1} \end{aligned}$$

Notice that

$$a_1(X) + \cdots + a_s(X) \equiv h(X) \mod (X^m - 1).$$

Since C_h is an orthogonal matrix then

$$a_1(1) a_2(1) \cdots a_s(1) = 0.$$

Let $h'(X) = (X^m - 1) + h_0 + h_{m-1} X + h_{m-2} X^2 + \cdots + h_1 X^{m-1}$, the polynomial that corresponds to C_h^T. As we have $hh' \equiv 1 \mod (X^m - 1)$ then $h(1)h'(1) = 1$ and $h(1) = h'(1)$. This implies $h(1) = 1$ or $h(1) = -1$.

As $h(1) = \pm 1$, if $a_i(1) = 0$, then $X^s - 1$ divides $h(X) \mp X^{i-1}$. We also have

$$X^m - 1 = d(X)(X^s - 1)$$

for some $d(X)$ with $w(d(X)) = p$. Therefore

$$\begin{array}{lcl} h(X) \mp X^{i-1} & = & g(X)(X^s - 1) \text{ for some } g(X) \\ d(X)(h(X) \mp X^{i-1}) & = & g(X)d(X)(X^s - 1) \\ & = & g(X)(X^m - 1) \\ d(X)h(X) & \equiv & \pm X^{i-1}d(X) \mod (X^m - 1). \end{array}$$

Note that $w(d(X)h(X) \mod (X^m - 1)) = w(X^{i-1}d(X)) = p$. Therefore

$$w(d(X)) + w(d(X)h(X)) = 2p < m + 1.$$

This is a contradiction. □

Theorem 3.9. *1. Let $m = 4n, n \in \mathbb{N}$. Then there is no orthogonal circulant MDS matrix of order m over a field of characteristic 2.*

2. There is no orthogonal circulant MDS matrix of even order m over a field of characteristic $p > 2$.

Proof. Let $m = 4n$ if $p = 2$ and $m = 2n$ if $p \neq 2$, for some positive integer n. Assume that there exists an $m \times m$ orthogonal circulant MDS matrix C_h in $\mathbb{F}_{p^r}$ with corresponding polynomial $h(X)$.
Let $h(X) = (X^m - 1) + h_0 + h_1X + \cdots + h_{m-1}X^{m-1}$. Define

$$\begin{array}{lcl} a(X) & = & h_0 + h_2X^2 + \cdots + h_{m-2}X^{m-2} \\ b(X) & = & h_1 + h_3X^3 + \cdots + h_{m-1}X^{m-1} \end{array}$$

Notice that

$$a(X) + b(X) \equiv h(X) \mod (X^m - 1).$$

Since C_h is an orthogonal matrix then

$$a(1)b(1) = 0.$$

Let $h'(X) = (X^m-1)+h_0+h_{m-1}X+h_{m-2}X^2+\cdots+h_1X^{m-1}$, the polynomial that corresponds to C_h^T. As we have $hh' \equiv 1 \mod (X^m-1)$. Then $h(1)h'(1) = 1$ and $h(1) = h'(1)$. This implies $h(1) = 1$ or $h(1) = -1$. As $h(1) = \pm 1$,

1. if $a(1) = 1$, then $X^2 - 1$ divides $h(X) \mp 1$,

2. if $b(1) = 1$, then $X^2 - 1$ divides $h(X) \mp X$.

Hence

$$X^m - 1 = d(X)(X^2 - 1)$$

for some $d(X)$ with

$$w(d(X)) = \begin{cases} 2n & \text{if } p = 2 \\ n & \text{if } p \neq 2. \end{cases}$$

Therefore

$$w(d(X)) + w(d(X)h(X)) = m/2 + m/2 = m < m + 1.$$

This is a contradiction. □

We now explore the existence of circulant orthogonal matrices of odd orders.

Theorem 3.10. *If A is a circulant orthogonal matrix of order 3 over $\mathbb{F}_{2^r}$ without zero component, then A is MDS.*

Proof. A matrix $A = circ(a, b, c)$ is orthogonal if and only if $a^2 + b^2 + c^2 = 1$ and $ab + bc + ca = 0$. This implies $(a + b + c)^2 = 1$. In characteristic two, this is equivalent to $a + b + c = 1$.
Suppose that A is a circulant orthogonal matrix without zero component over a field of characteristic 2. If A is not MDS, then

- $a^2 = bc$, or $b^2 = ac$, or $c^2 = ab$, or
- $a^3 + b^3 + c^3 + a + b + c = 0$.

Without loss of generality, if $a^2 = bc$, then $ab+a^2+ca = 0$, i.e. $a(a+b+c) = 0$ and $a = 0$, contradiction.
If $a^3 + b^3 + c^3 + a + b + c = 0$, then $a^3 + b^3 + c^3 = 1$. But since

$$1 = (a + b + c)^3 = a^3 + b^3 + c^3 + a^2(b + c) + b^2(a + c) + c^2(a + b),$$

then $a^2(b + c) + b^2(a + c) + c^2(a + b) = 0$. This implies

$$\begin{aligned} 0 &= ab(a + b) + ac(a + c) + bc(b + c) \\ &= ab(1 + c) + ac(1 + b) + bc(1 + a) \\ &= ab + abc + ac + abc + bc + abc \\ &= abc. \end{aligned}$$

But this implies $a = 0$ or $b = 0$ or $c = 0$, contradiction. □

Based on the above theorem, to construct a 3×3 orthogonal circulant MDS matrix over $\mathbb{F}_{2^r}$, say $circ(a, b, c)$, we only need to solve the system of equations:

$$a + b + c = 1, \quad ab + bc + ca = 0$$

with $a, b, c \neq 0$ in $\mathbb{F}_{2^r}$. This can be done quickly by the following steps:

1. Choose any $a \neq 0$.
2. Choose b a root of the quadratic equation $b^2 + (a + 1)b + a(a + 1) = 0$
3. Compute $c = 1 + a + b$.

Example 3.11. *Suppose $\mathbb{F}_{2^4}$ is the field constructed from the irreducible polynomial $X^4 + X + 1$ and α is the root of the polynomial. Let $h(X) = (X^3 - 1) + (\alpha^2 + \alpha) + \alpha^3 X + (\alpha^3 + \alpha^2 + \alpha + 1)X^2 \in \mathbb{F}_{2^4}[X]$ be associated to the following circulant matrix*

$$\begin{aligned} C_h &= circ(\alpha^2 + \alpha, \alpha^3, \alpha^3 + \alpha^2 + \alpha + 1) \\ &= \begin{bmatrix} \alpha^2 + \alpha & \alpha^3 & \alpha^3 + \alpha^2 + \alpha + 1 \\ \alpha^3 + \alpha^2 + \alpha + 1 & \alpha^2 + \alpha & \alpha^3 \\ \alpha^3 & \alpha^3 + \alpha^2 + \alpha + 1 & \alpha^2 + \alpha \end{bmatrix} \end{aligned}$$

This matrix is an orthogonal circulant MDS matrix.

Now for $m \times m$ with m is odd and m divides $2^r - 1$, we will explain how to construct a circulant orthogonal MDS matrix. The main idea is to construct arbitrary circulant orthogonal matrix quickly, and then we check whether the matrix is also MDS or not.

Note that m divides $2^r - 1$ implies m divides the order of the cyclic group $\mathbb{F}_{2^r}^*$. Hence this group has an element of order m; namely, $\beta = g^{(2^k-1)/m}$ with g a primitive element in $\mathbb{F}_{2^r}$. In this case, $1, \beta, \beta^2, ..., \beta^{m-1}$ are roots of $X^m - 1$. The following theorem gives a criterion for orthogonal circulant matrices over $\mathbb{F}_{2^r}$.

Theorem 3.12. *Let $1, \beta, \beta^2, \beta^3, ..., \beta^{m-1}$ be roots of $X^m - 1$. A matrix $C_h = circ\,(h_0, h_1, ..., h_{m-1})$ is orthogonal circulant over $\mathbb{F}_{2^r}$ if and only if the polynomial*

$$h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i$$

satisfies $h(1) = 1$ and $h\,(\beta^j)\, h\left(\frac{1}{\beta^j}\right) = 1$ for all $j = 1, ..., m - 1$.

Proof. This is a consequence of Corollary 3.6: C_h is orthogonal if and only if $X^m - 1$ divides $h(X)\,h'(X) - 1$ with

$$\begin{aligned} h^{'}(X) &= (X^m - 1) + h_0 + h_{m-1}X + h_{m-2}X^2 + ... + h_1X^{m-1} \\ &\equiv h_0X^m + h_{m-1}X + h_{m-2}X^2 + ... + h_1X^{m-1} \bmod X^m - 1 \\ &\equiv X^m\left(h_0 + \frac{h_1}{X} + \frac{h_2}{X^2} + ... + \frac{h_{m-1}}{X^{m-1}}\right) \bmod X^m - 1, \end{aligned}$$

where $h'(X)$ is the polynomial corresponds to C_h^T. Note that $h'(X) = X^m h\left(\frac{1}{X}\right)$ mod $X^m - 1$. □

Example 3.13. *Suppose α is a root of $X^4 + X + 1$ in $\mathbb{F}_{2^4}$ as before. Then α is a primitive element and $\beta = \alpha^3$ is a root of $X^5 - 1$ with $\beta \neq 1$ in $\mathbb{F}_{2^4}$. We take arbitrary non-zero elements γ_1, γ_2 in $\mathbb{F}_{2^4}$ and then, use Lagrange Interpolation, or other methods to find a polynomial $g(X)$ of degree 4 such that*

$$g(1) = 1, g(\beta) = \gamma_1, g\left(\frac{1}{\beta}\right) = \frac{1}{\gamma_1}, g\left(\beta^2\right) = \gamma_2, g\left(\frac{1}{\beta^2}\right) = \frac{1}{\gamma_2}.$$

For example, for $\gamma_1 = \gamma_2 = \alpha^2 + \alpha + 1$ we find that

$$g(X) = 1 + \alpha X + (\alpha^2 + 1)X^2 + \alpha^2X^3 + (\alpha + 1)X^4.$$

The polynomial $h(X) = (X^5 - 1) + g(X)$ corresponds to the following 5×5 orthogonal circulant MDS matrix

$$C_h = circ(1, \alpha, \alpha^2 + 1, \alpha^2, \alpha + 1)$$

Unfortunately, this method does not work for the case m does not divide $2^r - 1$, for example when $m = 2d$ is even. The following theorem gives a necessary condition for a $2d \times 2d$ circulant matrix to be orthogonal.

Theorem 3.14. *If $B = circ\,(b_0, b_1, ..., b_{2d-1})$ is an orthogonal matrix of size $2d \times 2d$ over a field of characteristic 2, then*

$$A = circ\,(b_0 + b_d, b_1 + b_{d+1}, ..., b_{d-1} + b_{2d-1})$$

is a $d \times d$ orthogonal matrix over the same field.

Proof. Let

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{2d-2} & b_{2d-1} \\ b_{2d-1} & b_0 & b_1 & \cdots & b_{2d-3} & b_{2d-2} \\ b_{2d-2} & b_{2d-1} & b_0 & \cdots & b_{2d-4} & b_{2d-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_{2d-1} & b_0 \end{bmatrix}$$

be orthogonal, then

$$A = \begin{bmatrix} b_0 + b_d & b_1 + b_{d+1} & \cdots & b_{d-1} + b_{2d-1} \\ b_{d-1} + b_{2d-1} & b_0 + b_d & \cdots & b_{d-2} + b_{2d-2} \\ \vdots & \vdots & \vdots & \vdots \\ b_1 + b_{d+1} & b_2 + b_{d+2} & \cdots & b_0 + b_d \end{bmatrix}$$

is also orthogonal because

$$(b_0 + b_d)^2 + (b_1 + b_{d+1})^2 + \cdots (b_{d-1} + b_{2d-1})^2 = \sum_{i=0}^{2d-1} b_i^2 = 1$$

Without loss of generality,

$$\begin{aligned} & \begin{bmatrix} b_0 + b_d & b_1 + b_{d+1} & \cdots & b_{d-1} + b_{2d-1} \end{bmatrix} \cdot \begin{bmatrix} b_{d-1} + b_{2d-1} & b_0 + b_d & \cdots & b_{d-2} + b_{2d-2} \end{bmatrix} \\ = \; & (b_0 + b_d)(b_{d-1} + b_{2d-1}) + (b_1 + b_{d+1})(b_0 + b_d) + \cdots + (b_{d-1} + b_{2d-1})(b_{d-2} + b_{2d-2}) \\ = \; & \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{2d-2} & b_{2d-1} \end{bmatrix} \cdot \begin{bmatrix} b_{2d-1} & b_0 & b_1 & \cdots & b_{2d-3} & b_{2d-2} \end{bmatrix} \\ & + \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{2d-2} & b_{2d-1} \end{bmatrix} \cdot \begin{bmatrix} b_{d-1} & b_d & b_{d+1} & \cdots & b_{d-3} & b_{d-2} \end{bmatrix} \\ = \; & 0 \end{aligned}$$

□

4 Orthogonal θ-circulant MDS Matrices over Finite Fields

As previously explained, the existence of a circulant MDS matrix in a certain order has limitations. Therefore, Cauchois and Loidreau in [1] generalize circulant matrix into θ-circulant matrix.

Suppose θ is an $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^m}$. Consider the set of polynomials

$$\left\{ \sum_i g_i X^i, g_i \in \mathbb{F}_{q^m} \right\}$$

with operations

1. ordinary addition of polynomials, and
2. multiplication defined as $X * a = a^{[1]}X$, where $a^{[i]} = \theta^i(a)$ for all i,

which are extended by associativity and distributivity. This set together with the two operations above forms a ring called the q-polynomial ring and is denoted by $\mathbb{F}_{q^m}[X, \theta]$. A subset of $\mathbb{F}_{q^m}[X, \theta]$ whose elements have degree less than or equal $m-1$ will be denoted by $\mathbb{F}_{q^m,m-1}[X, \theta]$. The element $f \in \mathbb{F}_{q^m}[X, \theta]$ is written as $f\langle X\rangle$ to distinguish it from the regular polynomial. The Hamming weight of the element $f\langle X\rangle \in \mathbb{F}_{q^m}[X, \theta]$ is denoted by $w(f)$, which is the number of nonzero coefficients of $f\langle X\rangle$.

Next we will define the θ-circulant matrix and give its relation to the q-polynomial ring.

Definition 4.1. [1] *Let $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_1 X^i \in \mathbb{F}_{q^m}[X, \theta]$ be a monic q-polynomial of degree m. Then the θ-circulant matrix associated to h is the matrix defined by:*

$$C_{h,\theta} = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{m-1} \\ h_{m-1}^{[1]} & h_0^{[1]} & h_1^{[1]} & \cdots & h_{m-2}^{[1]} \\ h_{m-2}^{[2]} & h_{m-1}^{[2]} & h_0^{[2]} & \cdots & h_{m-3}^{[2]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1^{[m-1]} & h_2^{[m-1]} & h_3^{[m-1]} & \cdots & h_0^{[m-1]} \end{bmatrix}$$

Next, we define $\mod_*$ as follows

$$r\langle X\rangle = c\langle X\rangle \mod_* g\langle X\rangle \quad \Leftrightarrow \quad c\langle X\rangle = b\langle X\rangle * g\langle X\rangle + r\langle X\rangle$$

with the degree of $r\langle X\rangle$ is less than the degree of $g\langle X\rangle$.

Theorem 4.2. [1] *Let $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_{q^m}[X, \theta]$ be a monic q-polynomial of degree m and $C_{h,\theta}$ is the θ-circulant matrix associated to h. Then $C_{h,\theta}$ is the representation matrix with respect to basis $\{1, X, X^2, \cdots, X^{m-1}\}$ of the map*

$$\begin{array}{rccc} \phi: & \mathbb{F}_{q^m}[X;\theta]/\langle X^m - 1\rangle & \to & \mathbb{F}_{q^m}[X;\theta]/\langle X^m - 1\rangle \\ & Q\langle X\rangle & \mapsto & Q\langle X\rangle * h\langle X\rangle \end{array}$$

Theorem 4.3. [1] *Let $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X;\theta]$. Suppose $C_{h,\theta}$ is the θ-circulant matrix associated to h. Then $C_{h,\theta}$ is an MDS matrix if and only if every nonzero $Q_1\langle X\rangle \in F_{q,m-1}[X, \theta]$ satisfies*

$$w(Q_1\langle X\rangle) + w(Q_1\langle X\rangle * h\langle X\rangle \mod_* (X^m - 1)) \geq m + 1$$

Theorem 4.4. [1] *Suppose* $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_1 X^i \in \mathbb{F}_q[X;\theta]$. *Suppose* $C_{h,\theta}$ *is the* θ*-circulant matrix associated to* h*, then* $C_{h,\theta}$ *is involutory if and only if* $h\langle X\rangle * h\langle X\rangle \equiv 1 \mod {}_*(X^m - 1)$.

Theorem 4.4 gives a sufficient and necessary condition for an involutory θ-circulant matrix. Next, we will determine a sufficient and necessary condition for an orthogonal θ-circulant matrix. First, We need to consider the transpose of a θ-circulant matrix.

The θ-circulant matrix is determined based on the entries in the first row. Two θ-circulant matrices are equal if and only if they have the same first row. Using these facts, we can obtain a sufficient and necessary condition so that the transpose of a θ-circulant matrix is also a θ-circulant matrix.

Proposition 4.5. *The transpose of a* θ*-circulant matrix is* θ*-circulant.*

Proof. Let $C_{h,\theta}^T$ be the transpose of $C_{h,\theta}$ and A be a θ-circulant matrix whose first row is equal to the first row of $C_{h,\theta}^T$. Note that

$$C_{h,\theta}^T = \begin{bmatrix} h_0 & h_{m-1}^{[1]} & \cdots & h_1^{[m-1]} \\ h_1 & h_0^{[1]} & \cdots & h_2^{[m-1]} \\ h_2 & h_1^{[1]} & \cdots & h_3^{[m-1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m-2} & h_{m-3}^{[1]} & \cdots & h_{m-1}^{[m-1]} \\ h_{m-1} & h_{m-2}^{[1]} & \cdots & h_0^{[m-1]} \end{bmatrix} \text{ and } A = \begin{bmatrix} h_0 & h_{m-1}^{[1]} & \cdots & h_1^{[m-1]} \\ h_1^{[m]} & h_0^{[1]} & \cdots & h_2^{[m-1]} \\ h_2^{[m]} & h_1^{[m+1]} & \cdots & h_3^{[m-1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m-2}^{[m]} & h_{m-3}^{[m+1]} & \cdots & h_{m-1}^{[m-1]} \\ h_{m-1}^{[m]} & h_{m-2}^{[m+1]} & \cdots & h_0^{[m-1]} \end{bmatrix}$$

The set of all $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^m}$ forms a cyclic group generated by automorphism φ with $\varphi(a) = a^q$. Let $h\langle X\rangle = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1}X^{m-1} \in \mathbb{F}_{q^m}[X;\theta]$ be a a q-polynomial associated to $C_{h,\theta}$. Suppose θ is a $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^m}$ with $\theta(a) = a^{q^k}$ for a natural number k. Note that

$$\begin{aligned} h_i^{[m]} &= \theta^m(h_i) \\ &= (h_i)^{(q^k)^m} \\ &= (h_i)^{(q^m)^k} \end{aligned}$$

Since $\mathbb{F}_{q^m}$ has q^m members then $(h_i)^{q^m} = h_i$. Hence

$$h_i^{[m]} = (h_i)^{(q^m)^k} = h_i \text{ for every } 0 \le i \le m-1$$

so we get $C_{h,\theta} = A$. □

Before determining the sufficient and necessary condition such that a θ-circulant matrix is an orthogonal matrix, we will first prove the following proposition.

Proposition 4.6. *Given the following q-polynomials*

$$h\langle X\rangle = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1}X^{m-1} \in \mathbb{F}_{q^m}[X;\theta]$$

and

$$g\langle X\rangle = (X^m - 1) + g_0 + g_1 X + \cdots + g_{m-1}X^{m-1} \in \mathbb{F}_{q^m}[X;\theta]$$

associated to $C_{h,\theta}$ and $C_{g,\theta}$ respectively, then

$$C_{h,\theta}C_{g,\theta} = I_m \quad \Leftrightarrow \quad 1 = h\langle X\rangle * g\langle X\rangle \mod {}_*(X^m - 1)$$

Proof. Let $\mathcal{B} = \{1, X, X^2, \cdots, X^{m-1}\}$. Then the matrix $C_{h,\theta}$ is the matrix representation of the map

$$\begin{array}{ccc} \Phi_h : \mathbb{F}_{q^m}[X;\theta]/(X^m-1) & \to & \mathbb{F}_{q^m}[X;\theta]/(X^m-1) \\ U\langle X\rangle & \mapsto & U\langle X\rangle * h\langle X\rangle \end{array}$$

with respect to $\mathcal{B}$. While $C_{g,\theta}$ is the matrix representation of the map

$$\begin{array}{ccc} \Phi_g : \mathbb{F}_{q^m}[X;\theta]/(X^m-1) & \to & \mathbb{F}_{q^m}[X;\theta]/(X^m-1) \\ U\langle X\rangle & \mapsto & U\langle X\rangle * g\langle X\rangle \end{array}$$

also with respect to $\mathcal{B}$. Let $C_{h,\theta}C_{g,\theta} = I_m$. The image of $1 \in \mathbb{F}_{q^m}[X;\theta]$ by $\Phi_g \circ \Phi_h$ is

$$(\Phi_g \circ \Phi_h)(1) = 1 * h\langle X\rangle * g\langle X\rangle \mod {}_*(X^m - 1) \tag{4.1}$$

Note that

$$[(\Phi_g \circ \Phi_h)(1)]_{\mathcal{B}} = [1]_{\mathcal{B}}C_{h,\theta}C_{g,\theta} = [1]_{\mathcal{B}} \quad \Rightarrow \quad (\Phi_g \circ \Phi_h)(1) = 1$$

Hence the equation (4.1) becomes

$$1 = h\langle X\rangle * g\langle X\rangle \mod {}_*(X^m - 1)$$

Conversely, suppose $1 = h\langle X\rangle * g\langle X\rangle \mod {}_*(X^m - 1)$, then there is an $f\langle X\rangle \in \mathbb{F}_{q^m}[X;\theta]$ that satisfies

$$h\langle X\rangle * g\langle X\rangle = f\langle X\rangle * (X^m - 1) + 1 \tag{4.2}$$

Take any $Q\langle X\rangle \in \mathbb{F}_{q^m,m-1}[X;\theta]$. If we multiply both sides of the equation (4.2) by $Q\langle X\rangle$ from the left we get

$$Q\langle X\rangle * h\langle X\rangle * g\langle X\rangle = Q\langle X\rangle * f\langle X\rangle * (X^m - 1) + Q\langle X\rangle$$

Since the degree of $Q\langle X\rangle$ is no more than $m-1$ then

$$Q\langle X\rangle = Q\langle X\rangle * h\langle X\rangle * g\langle X\rangle \mod {}_*(X^m - 1)$$

hence

$$[Q\langle X\rangle]_{\mathcal{B}} C_{h,\theta} C_{g,\theta} = [Q\langle X\rangle]_{\mathcal{B}}$$

Since $Q\langle X\rangle \in \mathbb{F}_{q^m,m-1}[X;\theta]$ is arbitrary then $C_{h,\theta}C_{g,\theta} = I_m$. □

If $h\langle X\rangle = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1}X^{m-1}$ is a q-polynomial associated to $C_{h,\theta}$, then $C_{h,\theta}^T$ is a matrix associated to $h'\langle X\rangle = (X^m - 1) + h_0 + h_{m-1}^{[1]}X + h_{m-2}^{[2]}X^2 + \cdots + h_1^{[m-1]}X^{m-1}$. If $C_{h,\theta}$ is orthogonal, then by using Theorem (4.6) we get the following result.

Corollary 4.7. *Let $h\langle X\rangle = (X^m - 1) + h_0 + h_1 X + \cdots + h_{m-1}X^{m-1} \in \mathbb{F}_{q^m}[X,\theta]$ be a q-polynomial associated to $C_{h,\theta}$. If $C_{h,\theta}^T$ is the transpose of $C_{h,\theta}$ and $C_{h,\theta}^T$ is associated to the q-polynomial $h' \in \mathbb{F}_{q^m}[X,\theta]$, then*

$$C_{h,\theta} \text{ orthogonal} \quad \Leftrightarrow \quad 1 = h\langle X\rangle * h'\langle X\rangle \mod {}_*(X^m - 1)$$

Proof. The proof follows directly from Proposition (4.6) by selecting $C_{g,\theta} = C_{h,\theta}^T$ and $g = h'$. □

Consequently, Corollary (4.7) gives a sufficient and necessary condition for an orthogonal θ-circulant matrix. To test that the matrix is an MDS matrix, we can use Theorem (4.3). By combining these two results, we have the next result.

Theorem 4.8. *Suppose $h\langle X\rangle$ is a q-polynomial associated to $C_{h,\theta}$. Then $C_{h,\theta}$ is an MDS orthogonal θ-circulant if and only if*

1. *Every nonzero $Q\langle X\rangle \in \mathbb{F}_{q^m,m-1}[X,\theta]$ satisfies*

$$w(Q\langle X\rangle) + w\left(Q\langle X\rangle * h\langle X\rangle \mod {}_*(X^m - 1)\right) \geq m + 1$$

2. *$h\langle X\rangle * h'\langle X\rangle \mod {}_*(X^m - 1) = 1$, where h' is associated to $C_{h,\theta}^T$.*

Example 4.9. *Suppose $\mathbb{F}_{2^4}$ is the field constructed from the irreducible polynomial $X^4 + X + 1$ and α is the root of the polynomial. Let $\theta(a) = a^2$ and $h\langle X\rangle = (X^4 - 1) + \alpha^{11} + \alpha X + \alpha^7 X^2 + \alpha^5 X^3 \in \mathbb{F}_{2^4}[X, \theta]$ is associated to the following θ-circulant matrix*

$$C_{h,\theta} = \begin{bmatrix} \alpha^{11} & \alpha & \alpha^7 & \alpha^5 \\ \alpha^{10} & \alpha^7 & \alpha^2 & \alpha^{14} \\ \alpha^{13} & \alpha^5 & \alpha^{14} & \alpha^4 \\ \alpha^8 & \alpha^{11} & \alpha^{10} & \alpha^{13} \end{bmatrix}$$

This matrix is an orthogonal θ-circulant MDS matrix.

5 Orthogonal Circulant MDS Matrices over Galois Rings

Let p be a prime number and let $\mathbb{Z}_{p^m}$ denote the ring of integers modulo p^m. Let $\mathbb{F}_p[X]$ and $\mathbb{Z}_{p^m}[X]$ be polynomial rings with coefficients in $\mathbb{F}_p$ and $\mathbb{Z}_{p^m}$ respectively. Define $f(X) := \sum_{i=0}^{t} a_i X^i \in \mathbb{Z}_{p^m}[X]$ and $\overline{f}(X) = \sum_{i=0}^{t} \overline{a}_i X^i \in \mathbb{F}_p[X]$, which $\overline{a}_i \equiv a_i \mod p$ for each i. Define an epimorphism $\overline{\mu}$ from $\mathbb{Z}_{p^m}[X]$ to $\mathbb{F}_p[X]$ by

$$\begin{array}{rccc} \overline{\mu} & : & \mathbb{Z}_{p^m}[X] & \longrightarrow & \mathbb{F}_p[X] \\ & & f(X) & \mapsto & \overline{f}(X) \end{array}$$

Definition 5.1. *Let $f \in \mathbb{Z}_{p^m}[X]$ and $\overline{f} \in \mathbb{F}_p[x]$ be the image of f from $\overline{\mu}$, that is $\overline{\mu}(f) = \overline{f}$. Then f is called basic irreducible if f is irreducible in $\mathbb{Z}_{p^m}[X]$ and $\overline{f}$ is irreducible in $\mathbb{F}_p[X]$.*

Suppose $f(X) \in \mathbb{Z}_{p^m}[X]$ is a basic irreducible polynomial of degree k. The Galois ring $GR(p^m, k)$ is defined as

$$GR(p^m, k) := \mathbb{Z}_{p^m}[X]/\langle f(X)\rangle.$$

Note that the finite field $\mathbb{F}_{p^k}$ may be constructed as $\mathbb{F}_{p^k} := \mathbb{F}_p[X]/\langle \overline{f}(X)\rangle$. In this section, we will focused on the existence of MDS Matrices over Galois ring $GR(2^m, k)$.

Let $f(X) \in \mathbb{Z}_{2^m}[X]$ be a basic irreducible polynomial of degree k, then $\overline{f}(X) \in \mathbb{F}_2[X]$ is an irreducible polynomial. Suppose that α and $\overline{\alpha}$ are roots of

$f(X)$ and $\overline{f}(X)$, respectively. Define an epimorphism $\mu : GR(2^m, k) \longrightarrow \mathbb{F}_{2^k}$ by,

$$\begin{array}{rcccc} \mu & : & GR(2^m,k) = \mathbb{Z}_{2^m}[x]/\langle f(X)\rangle & \longrightarrow & \mathbb{F}_{2^k} = \mathbb{F}_2[x]/\langle \overline{f}(X)\rangle \\ & & \sum_{i=0}^{k-1} a_i\alpha^i & \mapsto & \sum_{i=0}^{k-1} \overline{a}_i\overline{\alpha}^i \end{array}$$

where $\overline{a}_i \equiv a_i \mod 2$ for each i.

The following theorem provides a connection between MDS matrices over $\mathbb{F}_{2^k}$ and MDS matrices over $GR(2^m, k)$.

Theorem 5.2. *[9] Let μ be the above epimorphism from $GR(2^m, k)$ to $\mathbb{F}_{2^k}$ and $A = (a_{ij})$ be an $n \times n$ matrix over $GR(2^m, k)$. Suppose $\overline{A} := \mu(A) = (\mu(a_{ij}))$ is a matrix over $\mathbb{F}_{2^k}$. Then,*

1. *$\mu(\det(A)) = \det(\overline{A})$;*
2. *A is an MDS matrix over $GR(2^m, k)$ if and only if $\overline{A} = \mu(A)$ is MDS over $\mathbb{F}_{2^k}$.*

Gupta and Ray [4] proved that an orthogonal circulant matrix of order 2^n with $n \geq 2$ over the field $\mathbb{F}_{2^k}$ cannot be MDS, and in Theorem 3.9 we have proved the non-existence for orthogonal circulant matrix of oder $4n$. In the following result, we obtain the non-existence of circulant orthogonal MDS matrices over Galois ring $GR(2^m, k)$ with order $4n$ as a consequence of Theorem 3.9.

Theorem 5.3. *Let $circ(a_0, a_1, \ldots, a_{4n-1})$ be a circulant orthogonal matrix over $GR(2^m, k)$ of order $4n$, where $m, k, n \in \mathbb{N}$, then $circ(a_0, a_1, \ldots, a_{4n-1})$ cannot be MDS.*

Fortunately, for odd orders we still have the following examples.

Example 5.4. *Let $GR(2^2, 4) = \mathbb{Z}_{2^2}[x]/\langle x^4 + x + 1\rangle$ and α be a root of $X^4 + X + 1$ in $GR(2^2, 4)$. Then $A = circ(\alpha^2 + \alpha, \alpha^3, \alpha^3 + \alpha^2 + \alpha + 3)$, and $B = circ(1, \alpha, \alpha^2 + 1, 3\alpha^2, \alpha + 3)$. are orthogonal circulant MDS matrices over $GR(2^2, 4)$ of odd order.*

Acknowledgment. This research is supported by Hibah PPMI ITB 2022.

References

[1] V. Cauchois, P. Loidreau, On circulant involutory MDS matrices, *Des. Codes Cryptogr.,* **87**, (2019), 249–260. doi: 10.1007/s10623-018-0520-3.

[2] J. Daemen, L. R. Knudsen, V. Rijmen, The block cipher SQUARE, in 4th *Fast Software Encryption Workshop*, LNCS, **1267**, (1997), 149–165.

[3] J. Daemen, V. Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard, Springer-Verlag, Berlin, (2002), 20–21.

[4] K. C. Gupta, I. G. Ray, Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications, *Cryptography and Communications*, **7**, (2015), 257–287.

[5] Irwansyah, I. Muchtadi-Alamsyah, F. Yuliawan, A construction of MDS involutory matrices using MDS self-dual codes: a preliminary result, *Journal of Physics Conf. Series*, **1722**, (2021), 012030.

[6] K. Khoo, T. Peyrin, A. Y. Poschmann, H. Yap, FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison, *Cryptographic Hardware and Embedded Systems*, LNCS, **8731,** (2014), 433–450.

[7] C. E. Shannon, Communication Theory of Secrecy Systems, *Bell Syst. Technical J.,* **28**, (1949), 656–715.

[8] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Publishing Co., Amsterdam-New York-Oxford, (1997), 9–321.

[9] C. H. Tan, T. F. Prabowo, *Orthogonal MDS Diffusion Matrices over Galois Rings*, IMACC 2017, LNCS 10655, Springer, 2017, 307–330.

[10] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. D. Win, The cipher SHARK, In 3rd *Fast Software Encryption Workshop*, LNCS, **1039**, (1996), 99–111.