About Circulant Involutory MDS Matrices

Victor Cauchois, Pierre Loidreau

About Circulant Involutory MDS Matrices

Victor Cauchois *
Pierre Loidreau †
DGA MI and Université de Rennes 1

Abstract

We give a new algebraic proof of the non-existence of circulant involutory MDS matrices with coefficients in fields of even characteristic. For odd characteristics we give parameters for the potential existence. If we relax circulancy to θ-circulancy, then there is no restriction to the existence of θ-circulant involutory MDS matrices even for fields of even characteristic. Finally, we relax further the involutory definition and propose a new direct construction of almost involutory θ-circulant MDS matrices. We show that they can be interesting in hardware implementations.

1 Introduction

MDS matrices offer the maximal diffusion of symbols for cryptographic applications. To reduce implementation costs, research focuses on circulant and recursive matrices, which need only a linear number of multipliers to compute the matrix-vector product. Additionally when considering a block-cipher based on the AES principle, decryption needs the computation of the inverse matrix. Therefore, for hardware implementations, it is interesting to consider involutory matrices or almost involutory matrices. All these problems were investigated in a large number of research papers:

- Concerning circulant matrices: Apart from the design of AES [DR02], circulant-like MDS matrix constructions were proposed by taking subsquare matrices of Hankel form, see [Aid86],[RS85]. In [RL89], the authors showed that generalised Cauchy matrices are redundant part of MDS codes. More recently, [SKOP15] considered lightweight Hadamard-Cauchy matrices. In [GR14], the authors proved that involutory circulant matrices do not exist. In [LW16], the authors showed that relaxing the definition of circulancy allows to build involutory matrices for some parameters. [LS16] found very low cost involutive matrices by replacing multiplication by field elements with invertible linear applications.
- Concerning recursive matrices: In [Ber13], the author used Gabidulin theory to propose a direct construction of recursive MDS matrices. Recursive MDS matrix constructions were also considered by [AF14] where they constructed

*victouf@hotmail.com
†Pierre.Loidreau@m4x.org

recursive matrices from shortened cyclic MDS codes. Such structures form the linear diffusion layer core of PHOTON family of hash function [GPP11] or LED block cipher [GPPR11]. The construction of involutory matrices with recursive structures was investigated in [CLM16] where the authors published a direct construction of MDS matrices, quasi-involutory and which can be recursively implemented with a derived version of a LFSR denoted SLFSR. An SLFSR is a logical structure built from a classical LFSR skewed via the action of a Frobenius automorphism.

Now from a complexity point of view, verifying if a matrix is MDS or not becomes quickly prohibitive, since one has to compute all the minors of the matrix. Therefore, it is worth knowing the parameters for which they may or may not exist. Additionally, if it were possible to obtain direct constructions by slightly relaxing the constraints, it would be a benefit for designers.

In the paper, we first introduce a general algebraic framework to study involutory properties of circulant and θ-circulant matrices which are the counterpart of circulant matrices if we relax the condition on the polynomial ring by considering the q-polynomial ring. In a second part we prove some results on the existence and non-existence of involutory circulant MDS matrices. In a third part we extend the results to the θ-circulant matrices and show that this increases the number of degrees of freedom for the choice of MDS matrices. In a final part by relaxing the involutory property we directly construct MDS θ-circulant matrices which are involutory modulo a permutation.

Our contribution

We provide a new simple proof that circulant involutory matrices do not exist in fields of even characteristic. For odd characteristics, we extend the result by using our algebraic framework. This gives some restrictions on the existence of the matrices. By generalising circulancy and considering θ-circulant matrices, the aforementioned restriction can be raised and involutory θ-circulant matrices may exist even for impossible parameters in the previous case. This approach does not provide a direct construction. To obtain a direct construction, we relax the condition on the matrix to be involutory, by authorising the action of the Frobenius automorphism and a permutation of the coordinates. These restriction do not impact much the hardware implementation costs.

2 An algebraic framework

2.1 Notations and definitions

Let q be some power of some prime p. We denote by $\mathbb{F}_q$ the field with q elements and $\mathbb{F}_q[X]$ the polynomial ring with coefficients in $\mathbb{F}_q$. We denote by $\mathcal{M}_{m,n}(\mathbb{F}_q)$ the set of matrices with m rows and n columns with coefficients in $\mathbb{F}_q$.

Definition 1. *Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_q$. Then $\mathcal{C}$ is* MDS *if its minimum distance d satisfies the Singleton Bound:*

$$d = n - k + 1.$$

In cryptography, we are more interested in the so-called MDS matrices defined by:

Definition 2. $\mathbf{M} \in \mathcal{M}_{k,n-k}(\mathbb{F}_q)$ *is* MDS *if and only if it satisfies one of the two following properties:*

- *All its minors are non zero.*
- *It is the redundant part of the generator matrix of an* MDS *code* $\mathcal{C}$ *under systematic form,* i.e. *this is the matrix* $\mathbf{M}$ *where*

$$\mathcal{C} = \langle (\mathbf{I} \mid \mathbf{M}) \rangle.$$

In the design of symmetric encryption schemes we usually need invertible matrices. This implies that we only consider square MDS matrices of order m. These matrices are redundant part of generator matrices under systematic form of MDS codes of length $2m$ and dimension m.

Definition 3. *A matrix* $\mathbf{M} \in \mathcal{M}_{m,m}(\mathbb{F}_q)$ *is involutory if it satisfies the following equation:*

$$\mathbf{M}^2 = \mathbf{I}_m$$

2.2 Circulant matrices and polynomial rings

For $g \in \mathbb{F}_q[X]$, we denote by $w_t(g)$ the weight of the polynomial g, corresponding to the number of non-zero coefficients of the polynomial g. We denote by $\mathbb{F}_{q,m}[X]$ the set of polynomials of degree less than or equal to m.
We introduce the following mapping between monic polynomials and circulant matrices:

Definition 4. *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 with* h *is the matrix defined by:*

$$\mathbf{C}_h = \begin{pmatrix} h_0 & h_1 & \dots & h_{m-1} \\ h_{m-1} & h_0 & \dots & h_{m-2} \\ \vdots & \ddots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}$$

Remark 1. *This mapping is* non-standard *in the sense that* h_0 *is not the constant term of the polynomial* h *but the constant term translated by* 1*.*

The following proposition sets the algebraic framework.

Proposition 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* $\mathbf{C}_h$ *be the circulant matrix associated with* h*. Then,* $\mathbf{C}_h$ *is the matrix in the basis* $\{1, X, \dots, X^{m-1}\}$ *of the mapping:*

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

2.3 θ-circulant matrices and q-polynomials rings

We extend the previous framework to *q-polynomial ring*. Let θ be a $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^m}$. Consider the set $\{\sum_i g_i X^i,\ g_i \in \mathbb{F}_{q^m}\}$ with the two following operations:

- *Addition*: usual addition of polynomials
- *Multiplication*: $X * a = a^{[1]} * X$ where $a^{[i]} = \theta^i(a), \forall i \in \mathbb{Z}$

extended by associativity and distributivity. It forms a ring called q-polynomial ring we denote by $\mathbb{F}_{q^m}[X;\theta]$. This ring is left and right Euclidean. To distinguish q-polynomials from classical polynomials, we use the notation $A\langle X\rangle$ to refer to an element $A \in \mathbb{F}_{q^m}[X;\theta]$.

For $h \in \mathbb{F}_{q^m}[X;\theta]$, we denote by $w_t(h)$ the Hamming weight of the q-polynomial h, which is its number of non-zero coefficients. We denote by $\mathbb{F}_{q^m,m}[X;\theta]$ the set of q-polynomials whose degree is less or equal to m.

Definition 5. *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. The θ-circulant matrix associated with h is the matrix defined by:*

$$\mathbf{C}_{h,\theta} = \begin{pmatrix} h_0 & h_1 & \dots & h_{m-1} \\ h_{m-1}^{[1]} & h_0^{[1]} & \dots & h_{m-2}^{[1]} \\ \vdots & \ddots & \ddots & \vdots \\ h_1^{[m-1]} & h_2^{[m-1]} & \dots & h_0^{[m-1]} \end{pmatrix}$$

Proposition 2. *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 $\mathbf{C}_{h,\theta}$ be the θ-circulant matrix associated with h. Then, the matrix $\mathbf{C}_{h,\theta}$ is the matrix in the basis $\{1, X, \dots, X^{m-1}\}$ of the application:*

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

3 Involutory circulant MDS matrices and polynomial rings

Gupta and Ray proved that circulant involutory MDS matrices do not exist in characteristic 2, [GR14]. Based on the framework introduced in section 2.2 we give a new simple proof of this result and we extend it to finite fields of any characteristic.

Based on definition 4, we are able to give an algebraic necessary and sufficient condition for such a matrix to be MDS.

Proposition 3. *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$. Let $\mathbf{C}_h$ be the circulant matrix associated with h. Then, $\mathbf{C}_h$ is MDS if and only if: $\forall Q_1 \in \mathbb{F}_{q,m-1}[X]$, let $Q_2 \in \mathbb{F}_{q,m-1}[X]$ such that $Q_2(X) = Q_1(X)h(x) \bmod X^m - 1$, we have:*

$$w_t(Q_1) + w_t(Q_2) \geq m + 1.$$

Proof.

$$\begin{array}{rcl} \mathbf{C}_h \text{ is MDS} & \Leftrightarrow & (I_m|\mathbf{C}_h) \text{ is the generator matrix of an MDS code} \\ & \Leftrightarrow & \forall (q_0,\dots,q_{m-1}) \in \mathbb{F}_q^m, w_t\left((q_0,\dots,q_{m-1})\cdot(I_m|\mathbf{C}_h)\right) \geq m+1 \\ & \Leftrightarrow & \forall (q_0,\dots,q_{m-1}) \in \mathbb{F}_q^m, w_t(q_0,\dots,q_{m-1}) + w_t((q_0,\dots,q_{m-1})\cdot\mathbf{C}_h) \geq m+1 \end{array}$$

If one considers $Q_1(X) = \sum_{i=0}^{m-1} q_i X^i$, then $w_t(q_0, \ldots, q_{m-1}) = w_t(Q_1)$. Since from proposition 1, $\mathbf{C}_h$ corresponds to the multiplication by $h(X)$ in $\mathbb{F}_q[X]/(X^m - 1)$, we have:

$$w_t((q_0, \ldots, q_{m-1}) \cdot \mathbf{C}_h) = w_t(Q_1(X)h(X) \bmod X^m - 1) = w_t(Q_2(X)),$$

which proves the proposition. □

Example 1. *Let $\mathbb{F}_{2^4}$ be defined by $X^4 + X + 1$ and α a root of this polynomial. The matrix $\mathbf{C}_h$ associated with $h(X) = (X^4 + 1) + \alpha^3 X^3 + \alpha X^2 + X + 1 \in \mathbb{F}_{2^4}[X]$ is a circulant MDS matrix.*

$$\mathbf{C}_h = \begin{pmatrix} 1 & 1 & \alpha & \alpha^3 \\ \alpha^3 & 1 & 1 & \alpha \\ \alpha & \alpha^3 & 1 & 1 \\ 1 & \alpha & \alpha^3 & 1 \end{pmatrix}$$

The involutory property for circulant matrices can be written under algebraic form:

Proposition 4. *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$. Let $\mathbf{C}_h$ be the circulant matrix associated with h. Then, $\mathbf{C}_h$ is involutory if and only if $h(X)^2 = 1 \bmod (X^m - 1)$.*

Proof. This proposition comes directly from proposition 1 and from the definition of involutory matrices. □

A natural question is to determine whether circulant matrices both MDS and involutory exist. A partial answer in characteristic 2 fields for even size matrices was given in [GR14]. The following theorem simplifies and extends the proofs to even size MDS matrices in finite fields of any characteristic.

Theorem 1. *Let $d \geq 2$. There exists no involutory circulant MDS matrix of size $2d$ over fields of characteristic $p \geq 2$.*

Proof. Suppose that $\mathbf{C}_h$ is an involutory circulant MDS matrix of size $2d$ with entries in $\mathbb{F}_q$. Let $h \in \mathbb{F}_q[X]$ be the polynomial associated with the circulant matrix $\mathbf{C}_h$. The proof is seperated into two parts depending on the characteristic of the field.

In even characteristics: We consider the settings of Proposition 1. Let $Q_1(X) = X^d - 1$. By hypothesis $h^2(X) - 1 = (h(X) - 1)^2 = 0 \bmod X^{2d} - 1$. Therefore $h(X) - 1 = 0 \bmod X^d - 1$ therefore $Q_2(X) = Q_1(X)h(X) \bmod X^{2d} - 1 = X^d - 1$. Hence $w_t(Q_1) + w_t(Q_2) = 4 \leq 2d + 1$ and $\mathbf{C}_h$ is not MDS.

In odd characteristics, notice that $X^{2d} - 1 = (X^2 - 1)B(X)$ where $B(X) = (X^{2(d-1)} + X^{2(d-2)} + \ldots + 1)$ has weight d. Hence $X^{2d} - 1$ is divisible by $X^2 - 1$ and we have:

$$\begin{aligned} \mathbf{C}_h \text{ involutory} &\Rightarrow h^2 = 1 \bmod (X^{2d} - 1) \\ &\Rightarrow h^2 = 1 \bmod (X^2 - 1) \\ &\Rightarrow h^2 = X^2 \bmod (X^2 - 1) \end{aligned}$$

Thus, $(h - 1)(h + 1) = A_1(X)(X^2 - 1)$ and $(h - X)(h + X) = A_2(X)(X^2 - 1)$ where $A_1, A_2 \in \mathbb{F}_q[X]$.

We show that (X^2-1) divides necessarily one of the four polynomials:

$$\{h-1, h+1, h-X, h+X\}$$

Suppose X^2-1 does not divides neither $h(X)-1$ nor $h(X)+1$. Since 1 and -1 are the roots of X^2-1, then we have two cases:

- $h(1)=1$ and $h(-1)=-1$. This implies that $h(X)-X$ contains the roots of X^2-1 therefore is divisible by X^2-1;
- $h(1)=-1$ and $h(-1)=1$. This implies that $h(X)+X$ contains the roots of X^2-1 therefore is divisible by X^2-1.

The polynomial $(X^{2d}-1)$ divides one of the four polynomials:

$$\{B(X)(h-1), B(X)(h+1), B(X)(h+X), B(X)(h-X)\}$$

$\exists A(X) \in \mathbb{F}_q[X]$ such that:

- either $B(X)h(X) = \pm B(X) + A(X)(X^{2d}-1)$.
- or $B(X)h(X) = \pm XB(X) + A(X)(X^{2d}-1)$

Since the degree of $B(X)$ is less than $2d-2$, the $B(X)$ or $XB(X)$ corresponds to the remainder of $B(X)h(X)$ modulo $X^{2d}-1$. Moreover since $B(X)$ has weight d so has $XB(X)$ therefore

$$w_t(B(X)) + w_t(B(X)) = w_t(B(X)) + w_t(XB(X)) = 2d < 2d+1.$$

From proposition 1 this implies that $\mathbf{C}_h$ is not MDS, since by taking $Q_1(X) = B(X)$ we have $Q_2(X) = B(X)$ or $Q_2(X) = XB(X)$ and we have found a polynomial that does not satisfy the Hamming weight inequality.

□

In the particular case of odd characteristics, circulant involutory MDS matrices of odd sizes exist:

Example 2. *Consider $\mathbb{F}_{23}$ be the field with 23 elements. Then, $\mathbf{C}_h$, the circulant matrix associated with $h(X) = (X^3-1)+7X^2+7X+8$ is both involutory and MDS:*

$$C_g = \begin{pmatrix} 8 & 7 & 7 \\ 7 & 8 & 7 \\ 7 & 7 & 8 \end{pmatrix}$$

But there is no hope to find such matrices of odd sizes in even characteristics. This result was also shown in [GR14]. Here we give an alternative proof, which is an immediate consequence of previous results.

Theorem 2. *Let $\mathbb{F}_q$ be a finite field of characteristic 2. Let $m \geq 3$ be an odd integer. There are no involutory circulant MDS matrices of size m with entries in $\mathbb{F}_q$.*

Proof. Suppose that there exists an involutory circulant MDS matrix of size m, say $\mathbf{C}_h$ associated to the polynomial h. Let $g'(X)$ be the derivative of $g(X) = (X^m-1)$ that is:

$$g'(X) = mX^{m-1}.$$

The polynomial $g'(X)$ is prime with $g(X)$. Therefore $g(X)$ has exactly m distinct roots. By hypothesis we have that $h(X)^2 = 1 \bmod X^m - 1$ with h of degree m. Therefore there exist some polynomial $A(X)$ such that:

$$(h(X)+1)^2 = A(X)(X^m - 1).$$

Therefore, the m roots of $X^m - 1$ are also roots of $(h(X)+1)^2$ and since they are all simple roots, they are also roots of $h(X)+1$. Therefore, $h(X)+1 = 0 \bmod X^m - 1$. Since h is monic and of degree m necessarily $h(X) = X^m - 1$. Therefore C_h is not MDS since some of its entries are equal to 0. □

In even characteristics, the only involutory circulant MDS matrices are of size 1 or 2. The following example shows that some matrices of this type exist

Example 3. *Let $\mathbb{F}_{2^4}$ be defined by $X^4 + X + 1$ and α a root of this polynomial. The matrix $\mathbf{C}_h$ associated with $h(X) = (X^2+1) + \alpha^4 X + \alpha$ is both involutory and MDS.*

$$\mathbf{C}_h = \begin{pmatrix} \alpha & \alpha^4 \\ \alpha^4 & \alpha \end{pmatrix}$$

Namely, $h(X)^2 = X^4 + \alpha^8 X^2 + \alpha^8 = X^4 \mod (X^2+1) = X^2 \mod (X^2+1) = 1 \mod (X^2+1)$

Concerning odd characteristics, the following new theorem shows that there are strong constraints on the size of potential involutory circulant MDS matrices.

Theorem 3. *Let $m = 2d+1 \geq 3$. Let $\mathbb{F}_q$ be some field of odd characteristics. If there are circulant involutory MDS matrices of size m then there exists $A(X), B(X) \in \mathbb{F}_q[X]$ such that $A(X)$ has degree d, $gcd(A(X), B(X)) = 1$ and $X^m - 1 = A(X)B(X)$*

Proof. Suppose there exists an involutory circulant MDS matrix of size m, say $\mathbf{C}_h$ associated to the polynomial h. Suppose $X^m - 1$ does not admit a decomposition $X^m - 1 = A(X)B(X)$ with $A(X) \in \mathbb{F}_q[X]$ of degree d. By hypothesis, we have $h^2(X) = 1 \bmod X^m - 1$. Therefore there exists some polynomial $P(X)$ such that

$$(h(X) - 1)(h(X) + 1) = P(X)(X^m - 1)$$

In fields of odd characteristics, $(h(X) + 1)$ and $(h(X) - 1)$ are coprime. Thus, either $\gcd(X^m - 1, h(X) - 1)$ or $\gcd(X^m - 1, h(X) + 1)$ is of degree at least $d + 2$. There exist then either $B_1 \in \mathbb{F}_q[X]$ or $B_2 \in \mathbb{F}_q[X]$ of degree at most $d - 1$ such that $B_1(X)(h(X) + 1)$ or $B_2(X)(h(X) - 1)$ is divided by $X^m - 1$. In such a case $w_t(B_i(X)) \leq d$. Since $w_t(B_i(X)) + w_t(B_i(X)) \leq 2d < 2d+1$, for $i \in \{1, 2\}$ and since $B_1(X)h(X) = -B_1(X) \bmod (X^m - 1)$ or $B_2(X)h(X) = B_2(X) \bmod (X^m - 1)$, $\mathbf{C}_h$ is not MDS. □

Circulant involutory MDS matrices were found by exhaustive search whenever the previous factorisation exists. We conjecture then that for parameters not ruled out by the three last theorems, circulant involutory MDS matrices do exist.

Conjecture 1. *Let $m = 2d + 1 \geq 3$. Let $\mathbb{F}_q$ be some field of odd characteristic. If $X^m - 1$ can be decomposed as $A(X)B(X)$ with $A(X) \in \mathbb{F}_q[X]$ of degree d and $GCD(A(X), B(X)) = 1$, there exist circulant involutory MDS matrices.*

4 θ-circulant matrices and q-polynomial rings

As for classical polynomials, we establish algebraic conditions on q-polynomials to characterise those whose associated θ-circulant matrix is MDS since $\mathbb{F}_{q^m}[X;\theta]$ is right Euclidean. The proofs being similar to the classical polynomials case, we omit them.

We denote by $\mathrm{mod}_* g$ the operation of computing the remainder of the Euclidean division on the right by g:

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

Proposition 5. *Let $h\langle X\rangle = (X^m-1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_{q^m}[X;\theta]$. Let $\mathbf{C}_{h,\theta}$ be the θ-circulant matrix associated with h. Then, $\mathbf{C}_{h,\theta}$ is MDS if and only if:*

$\forall Q_1 \in \mathbb{F}_{q^m,m-1}[X,\theta]$, denoting by Q_2 the q-polynomial such that $Q_2 \in \mathbb{F}_{q^m,m-1}[X;\theta]$ and $Q_2\langle X\rangle = Q_1\langle X\rangle h\langle x\rangle \bmod_* (X^m-1)$, we have:

$$w_t(Q_1) + w_t(Q_2) \geq m+1$$

Example 4. *Let $\mathbb{F}_{2^4}$ be defined by X^4+X+1 and α a root of this polynomial. Let θ be the automorphism defined by $a \mapsto a^2$. The matrix $\mathbf{C}_{h,\theta}$ associated with $h\langle X\rangle = (X^4+1) + \alpha^{10}X^3 + \alpha X^2 + X + 1 \in \mathbb{F}_{2^4}[X;\theta]$ is a θ-circulant MDS matrix.*

$$\mathbf{C}_{h,\theta} = \begin{pmatrix} 1 & 1 & \alpha & \alpha^{10} \\ \alpha^5 & 1 & 1 & \alpha^2 \\ \alpha^4 & \alpha^{10} & 1 & 1 \\ 1 & \alpha^8 & \alpha^5 & 1 \end{pmatrix}$$

There is a simple algebraic condition on q-polynomials to characterise those whose associated θ-circulant matrix is involutory:

Proposition 6. *Let $h\langle X\rangle = (X^m-1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_{q^m}[X;\theta]$. Let $\mathbf{C}_{h,\theta}$ be the θ-circulant matrix associated with h. Then,*

$\mathbf{C}_{h,\theta}$ is an involutory matrix if and only if $g\langle X\rangle * g\langle X\rangle = 1 \bmod_* (X^m-1)$.

Therefore, if one relaxes the condition on the MDS matrix from being circulant to being θ-circulant, this is possible to find involutory matrices with implementation friendly (in a normal basis) properties.

Example 5. *Let $\mathbb{F}_{2^4}$ be defined by X^4+X+1 and α a root of this polynomial. Let θ be the automorphism defined by $a \mapsto a^2$. The matrix $\mathbf{C}_{h,\theta}$ associated with $h\langle X\rangle = (X^4+1) + \alpha^7 X^3 + \alpha^{14}X^2 + X + \alpha \in \mathbb{F}_{2^4}[X;\theta]$ is a θ-circulant involutory MDS matrix.*

$$\mathbf{C}_{h,\theta} = \begin{pmatrix} \alpha & 1 & \alpha^{14} & \alpha^7 \\ \alpha^{14} & \alpha^2 & 1 & \alpha^{13} \\ \alpha^{11} & \alpha^{13} & \alpha^4 & 1 \\ 1 & \alpha^7 & \alpha^{11} & \alpha^8 \end{pmatrix}$$

5 Direct Construction of θ-circulant almost involutory MDS matrices

From previous sections, we saw that involutory MDS θ-circulant matrices exist. To find them, we test the square of q-polynomials of degree m and check if it can be divided by $X^m - 1$ and then verify if they are MDS matrices. This can be algorithmically prohibitive for large m.

If we relax slightly the involutory condition, we can directly construct almost-involutory MDS matrices from Gabidulin codes for fields of even characteristic and matrices of even length. The first step of this relaxations is to consider instead of classical matrix product, the skewed matrix product $\mathbf{M}\mathbf{M}^{[1]}$, where if $\mathbf{M} = (m_{i,j})$ we have $\mathbf{M}^{[1]} = (m_{i,j}^{[1]})$ Since computing $\mathbf{M}^{[1]}$ is done by applying Galois automorphism individually on matrix coefficients, this can be done in hardware in normal basis with simple routing. The second step consists in allowing this product to equal a permutation matrix and not only the identity matrix. We say then this is almost-involutory since only one matrix and some additional routing is needed to compute both matrix product with $\mathbf{M}$ and with its inverse.

Let $m \geq 2$ be an integer. We consider $\mathbb{F}_{2^{2m}}$ and the Frobenius automorphism, $\theta(a) = a^{[1]} = a^2$.

Let α be a normal element in $\mathbb{F}_{2^{2m}}$. Let

$$\mathbf{G} = \begin{pmatrix} \alpha^{[0]} & \alpha^{[2]} & \cdots & \alpha^{[2m-1]} \\ \alpha^{[1]} & \alpha^{[3]} & \cdots & \alpha^{[0]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{[m-1]} & \alpha^{[m]} & \cdots & \alpha^{[m-2]} \end{pmatrix} \tag{1}$$

The matrix $\mathbf{G}$ is a generator matrix of a $[2m, m, m+1]$ Gabidulin code. Let $\mathbf{G}_1$ be the $m \times m$-left part of the matrix: $\mathbf{G}_1 = \left(\alpha^{[2j+i]}\right)_{i=0,j=0}^{m-1,m-1}$, and let $\mathbf{G}_2$ be the $m \times m$-right part of the matrix: $\mathbf{G}_2 = \left(\alpha^{[2j+i+1]}\right)_{i=0,j=0}^{m-1,m-1}$. We construct the matrix $\mathbf{M}$ as the redundant part of the generator matrix under systematic form without column permutations $(\mathbf{I} \mid \mathbf{M})$ of the Gabidulin code generated by $\mathbf{G}$. We have:

Theorem 4. *Let* $\mathbf{M} = \mathbf{G}_1^{-1}\mathbf{G}_2$*, then*

- $\mathbf{M}$ *is a* θ^2*-circulant MDS matrix*
- $\mathbf{M}\mathbf{M}^{[1]}$ *is a binary circulant permutation matrix,* i.e.

$$\mathbf{M}\mathbf{M}^{[1]} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

where $\mathbf{M}^{[1]}$ *consists of the matrix formed by the entries of* $\mathbf{M}$ *which are raised to the power* $[1]$*.*

We need the following lemma. We denote here by $\delta_{i,j}$ a number which is equal to 1 if $i = j$ and 0 otherwise.

Lemma 1. *Let $\beta_0, \ldots, \beta_{m-1}$, be the first row of $\mathbf{G}_1^{-1}$, then*

1. $\mathbf{G}_1^{-1} = \left(\beta_j^{[2i]}\right)_{i=0,j=0}^{m-1,m-1}$
2. $\sum_{u=0}^{m-1} \beta_u \alpha^{[u+2j]} = \delta_{0,j}$, *for all* $j = 0, \ldots, m-1$
3. $\sum_{u=0}^{m-1} \alpha^{[2u+i]} \beta_j^{[2u]} = \delta_{i,j}$, *for all* $i, j = 0, \ldots, m-1$

Proof. Let $\beta_0, \ldots, \beta_{m-1}$, be the first row of $\mathbf{G}_1^{-1}$, it satisfies trivially the second item of the lemma. Raising this equation to the power [2], we obtain:

$$\begin{array}{lcll} \sum_{u=0}^{m-1} \beta_u^{[2]} \alpha^{[u+2(j+1)]} & = & \delta_{0,j}^{[2]} & = \delta_{0,j}, \quad \forall j = 0, \ldots, m-1 \\ \sum_{u=0}^{m-1} \beta_u^{[2]} \alpha^{[u+2j]} & = & \delta_{0,j-1}^{[2]} & = \delta_{1,j}, \quad \forall j = 0, \ldots, m-1 \end{array}$$

where for $j = m-1$, since $\alpha^{[2m]} = \alpha$, the equality comes from $\alpha^{[u+2(j+1)]} = \alpha^{[u]}$. Therefore $\beta_0^{[2]}, \ldots, \beta_{m-1}^{[2]}$ is the second line of $\mathbf{G}_1^{-1}$. By induction we prove the first item of the lemma. The last item stems from the obvious relation $\mathbf{G}_1^{-1}\mathbf{G}_1 = \mathbf{I} = \mathbf{G}_1\mathbf{G}_1^{-1}$. □

Now we prove the theorem

Proof. Let $\mathbf{M} = \mathbf{G}_1^{-1}\mathbf{G}_2$. By construction, $\mathbf{M}$ is the redundant part of some generator matrix under systematic form of a Gabidulin code of length $2m$ and of dimension m and is then MDS. From previous lemma, the generic term $m_{i,j}$ of $\mathbf{M}$ satisfies:

$$\begin{array}{lcll} m_{i,j} & = & \sum_{u=0}^{m-1} \beta_u^{[2i]} \alpha^{[u+1+2j]}, & \text{for all } i,\ j = 0, \ldots, m-1 \\ m_{i,j}^{[2]} & = & \sum_{u=0}^{m-1} \beta_u^{[2(i+1)]} \alpha^{[u+1+2(j+1)]}, & \text{for all } i,\ j = 0, \ldots, m-1 \end{array}$$

This implies that $m_{i+1,j+1} = m_{i,j}^{[2]}$, therefore $\mathbf{M}$ is a θ^2-circulant MDS matrix. It remains to prove the last item of the theorem. The generic $(i,j)th$ term of $\mathbf{M}\mathbf{M}^{[1]}$ is:

$$\sum_{k=0}^{m-1} \sum_{u,u'=0}^{m-1} \beta_u^{[2i]} \alpha^{[u+2k]} \beta_{u'}^{[2(k+1)]} \alpha^{[u'+2(j+1)]} \tag{2}$$

Note that the only term in the equation depending on k is $\alpha^{[u+1+2k]} \beta_{u'}^{[2(k+1)]}$. Therefore by summing on k and from the third item of lemma, we obtain:

$$\sum_{k=0}^{m-1} \alpha^{[u+2k]} \beta_{u'}^{[2(k+1)]} = \delta_{u',u+1}$$

Therefore, equation (2) becomes

$$\sum_{u=0}^{m-1} \beta_u^{[2i]} \alpha^{[u+2(j+1)]} = \left(\sum_{u=0}^{m-1} \beta_u \alpha^{[u+2(j-i+1)]} \right)^{[2i]} = \delta_{0,(j-i+1)}.$$

□

The previous theorem establishes that the inverse of $\mathbf{M}$ is $\mathbf{M}^{[1]}\mathbf{P}$, where $\mathbf{P}$ is a permutation matrix. From a hardware implementation point of view, permuting bits consists in routing them, so implies no additional cost. If the chosen basis is normal, then the product with $\mathbf{M}^{[1]}$ can be implemented easily with the multipliers implemented for $\mathbf{M}$.

The direct construction of the MDS matrix in $\mathcal{M}_m(\mathbb{F}_{2^{2^m}})$ is summed up here:

1. Choose α a normal element in $\mathbb{F}_{2^{2^m}}$.
2. Build the two matrices $\mathbf{G}_1 = \left(\alpha^{[2j+i]}\right)_{i=0,j=0}^{m-1,m-1}$ and $\mathbf{G}_2 = \left(\alpha^{[2j+i+1]}\right)_{i=0,j=0}^{m-1,m-1}$.
3. $\mathbf{M} = \mathbf{G}_1^{-1}\mathbf{G}_2$

Example 6. *Let $\mathbb{F}_{2^8}$ be defined by $X^8 + X^4 + X^3 + X^2 + 1$, and α a root of this polynomial. The element α^5 is normal and we consider the Gabidulin code over $\mathbb{F}_{2^8}$ with generator matrix*

$$\begin{pmatrix} \alpha^5 & \alpha^{10} & \alpha^{20} & \alpha^{40} & \alpha^{80} & \alpha^{160} & \alpha^{65} & \alpha^{130} \\ \alpha^{10} & \alpha^{20} & \alpha^{40} & \alpha^{80} & \alpha^{160} & \alpha^{65} & \alpha^{130} & \alpha^5 \\ \alpha^{20} & \alpha^{40} & \alpha^{80} & \alpha^{160} & \alpha^{65} & \alpha^{130} & \alpha^5 & \alpha^{10} \\ \alpha^{40} & \alpha^{80} & \alpha^{160} & \alpha^{65} & \alpha^{130} & \alpha^5 & \alpha^{10} & \alpha^{20} \end{pmatrix}$$

The extraction of the even columns for $\mathbf{G}_1$ and the odd columns for $\mathbf{G}_2$ gives

$$\mathbf{M} = \mathbf{G}_1^{-1}\mathbf{G}_2 = \begin{pmatrix} \alpha^{98} & \alpha^{116} & \alpha^{132} & \alpha^{232} \\ \alpha^{163} & \alpha^{137} & \alpha^{209} & \alpha^{18} \\ \alpha^{72} & \alpha^{142} & \alpha^{38} & \alpha^{71} \\ \alpha^{29} & \alpha^{33} & \alpha^{58} & \alpha^{152} \end{pmatrix}$$

and finally

$$\mathbf{M}\mathbf{M}^{[1]} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

6 Conclusion

Together with a general framework of circulant matrices, we give a new algebraic proof of the non-existence of involutory circulant MDS matrices in fields of even characteristics.
Relaxing circulancy by considering q-polynomials, we draw general necessary and sufficient conditions for a q-polynomial to yield a MDS matrix or to yield an involutory matrix. We have seen that it may allow designers to build circulant layers that are MDS and involutory as in example 5.
Finally, relaxing also the involutory condition, we give a new direct construction of quasi-circulant quasi-involutory MDS matrices from Gabidulin codes.

References

[AF14] D. Augot and M. Finiasz. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In *Progress in Cryptology*, volume 8540, pages 3–17. FSE 2014, 2014.

[Aid86] A. K. Aidinyan. On matrices with nondegenerate square submatrices. In *Problems of Information Transmission*, volume 22, pages 106–108, 1986.

[Ber13] T. P. Berger. Construction of recursive MDS diffusion layers from Gabidulin codes. In *Progress in Cryptology-INDOCRYPT 2013*, volume LNCS 8250, pages 274–285. Springer, 2013.

[CLM16] V. Cauchois, P. Loidreau, and N. Merkiche. Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes. In *IACR Transactions on Symmetric Cryptology*, volume 2016 issue 2, pages 80–98, 2016.

[DR02] J. Daemen and V. Rijmen. *The Design of Rijndael - AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.

[GPP11] J. Guo, T. Peyrin, and A. Poschmann. The PHOTON family of lightweight hash functions. In *Advances in Cryptology*. CRYPTO 2011, 2011.

[GPPR11] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED block cipher. In *CHES 2011*, pages 326–341, 2011.

[GR14] K. C. Gupta and I. G. Ray. On constructions of circulant MDS matrices for lightweight cryptography. In *ISPEC 2014*, pages 564–576, 2014.

[LS16] M. Liu and S. M. Sim. Lightweight MDS generalized circulant matrices. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 101–120, 2016.

[LW16] Y. Li and M. Wang. On the construction of lightweight circulant involutory MDS matrices. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 121–139, 2016.

[RL89] R. M. Roth and A. Lempel. On MDS codes via Cauchy matrices. In *IEEE transactions on information theory*, volume 35, pages 1314–1319, 1989.

[RS85] R. M. Roth and G. Seroussi. On generator matrices of MDS codes. In *IEEE transactions on information theory*, volume IT-31, pages 826–830, 1985.

[SKOP15] S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin. Lightweight MDS involution matrices. In *FSE 2015*, 2015.