Lightweight Diffusion Layer: Importance of Toeplitz Matrices

Sumanta Sarkar[1] and Habeeb Syed[2]

[1] TCS Innovation Labs, Hyderabad, INDIA, Sumanta.Sarkar1@tcs.com
[2] TCS Innovation Labs, Hyderabad, INDIA, Habeeb.Syed@tcs.com

Abstract. MDS matrices are used as building blocks of diffusion layers in block ciphers, and XOR count is a metric that estimates the hardware implementation cost. In this paper we report the minimum value of XOR counts of 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively. We give theoretical constructions of Toeplitz MDS matrices and show that they achieve the minimum XOR count. We also prove that Toeplitz matrices cannot be both MDS and involutory. Further we give theoretical constructions of 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ that have the best known XOR counts so far: for $\mathbb{F}_{2^4}$ our construction gives an involutory MDS matrix that actually improves the existing lower bound of XOR count, whereas for $\mathbb{F}_{2^8}$, it meets the known lower bound.

Keywords: No keywords given.

1 Introduction

Lightweight cryptography is about cryptosystems that require low implementation costs, and this topic has drawn huge attention over the last few years. Currently lightweight variants exist for many symmetric-key primitives. The eSTREAM finalists `Grain` v1 [11], `MICKEY` 2.0 [1], and `Trivium` [21] are examples of lightweight stream ciphers. Examples of lightweight block ciphers are `CLEFIA` [19], `PRESENT` [6], `LED` [9], `SIMECK` [22], etc., where the first two have been standardized by ISO/IEC 29192.

Confusion and diffusion are the two important cryptographic criteria of a block cipher. The confusion layer makes the relation between key and ciphertext as complex as possible, on the other hand the diffusion layer spreads the plaintext statistics through the ciphertext. In practice maximum distance separable (MDS) matrices are used as the diffusion layer as these matrices can achieve the maximum diffusion power. For instance `AES` [8] uses an MDS matrix for its diffusion layer. On top of the MDS property, if the diffusion matrix is an involution (self-inverse), then the implementation cost for its inverse is saved, which is certainly an advantage in the hardware implementation of lightweight cryptosystems. One may note that the diffusion matrix of `KHAZAD` [3] is an involution.

Choosing an MDS or MDS involution matrix that fits in a lightweight cipher is a challenging task as the designer has to keep in mind the constraints in the implementation cost. For software implementation of diffusion matrices clock cycle is important, if elements of an MDS matrix are of low Hamming weight, then multiplication takes lesser number of clock cycles. However, if we simply use look-up tables (like T-tables for AES), then software implementation can be very fast.

In 2014, [14] introduced the metric XOR count that measured the cost of hardware implementation of a diffusion matrix. One may think that by filling a matrix with field elements having low Hamming weight would result in low hardware cost for the implementation of the matrix. But [14] instead measured the number of XORs required

to compute the multiplication of a fixed field element, and showed that there are MDS diffusion matrices with higher Hamming weight than the `AES` diffusion matrix but needed lesser XORs to implement.

After the introduction of XOR count, several attempts have been made to find (involutory) MDS matrices with low XOR count. For example, [20] made a huge search effort to find lightweight diffusion matrices, and they also observed that XOR count distribution varies with different irreducible polynomial that generate the field. Later [18] showed that under the same irreducible polynomial, XOR count distribution still can be different under different choice of basis. However, considering different bases they did not get any improved (involutory) MDS matrix than [20]. The best known XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^8}$ is $32 + 4 \cdot 3 \cdot 8$, and over $\mathbb{F}_{2^4}$ it is $12 + 4 \cdot 3 \cdot 4$ which were obtained by [16]. Another attempt has been made by [15] to obtain efficient 4×4 MDS diffusion matrix when the matrices are defined over the general linear groups $GL(8, 2)$ and $GL(4, 2)$ instead of fields $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$. In [5], a slightly different notion of XOR count has been considered, and accordingly some matrices have been presented.

Search efforts for MDS matrices with low XOR count in the previous works have been made in some subclasses of matrices like Hadamard matrices and circulant matrices. Hadamard matrices have advantages in hardware implementation as one row of such a matrix defines all the rows. A circulant matrix has a similar property, precisely, all the rows are some cyclic shifts of the first row. The diffusion matrix of `AES` is circulant MDS. On top of circulant property, if an MDS matrix is involutory, then it is even more advantageous in the implementation. However, a circulant MDS matrix cannot be involution [10]. Thus one has to look beyond these special subclasses to find MDS involutory matrices. The total number of MDS matrices is so huge that it is difficult to exhaust.

1.0.1 Our contributions

In this paper, we aim to determine the minimum values of the XOR counts of MDS matrices of order 4×4 over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively, as MDS matrices with these dimensions are very common in practice.

In Section 2 we give the definition of XOR count of a field element and also discuss some of the properties of this metric. Then in Section 3, we consider Toeplitz matrices and prove that if a Toeplitz matrix is MDS then it cannot be involutory. We also give theoretical constructions of Toeplitz MDS matrices in Propositions 3 and 4. In Section 5 and 6, we determine the minimum value of the XOR counts of 4×4 MDS matrices over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$ respectively, through a search strategy described in Section 4. We are able to obtain 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ that have the **minimum** XOR counts. The values are $10 + 4 \cdot 3 \cdot 4$ and $27 + 4 \cdot 3 \cdot 8$ for $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively. This concludes the hunt for 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ with low XOR counts. Interestingly our theoretical construction of Toeplitz MDS matrix (Corollaries 2, 3) attain the minimum XOR count for $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$ respectively.

In Section 7, we give constructions of 4×4 involutory MDS matrices (Propositions 10 and 11). For $\mathbb{F}_{2^4}$ our construction gives an involutory MDS matrix (Example 3) with XOR count $16 + 4 \cdot 3 \cdot 4$ which improves the existing lower bound $24 + 4 \cdot 3 \cdot 4$. On the other hand for $\mathbb{F}_{2^8}$, our construction gives an involutory MDS matrix (Example 2) with XOR count $64 + 4 \cdot 3 \cdot 8$ that matches with the existing known lower bound.

2 Preliminaries

Let $\mathbb{F}_{2^m}$ be a finite field with 2^m elements, alternatively we will denote this by $\mathbb{F}_2[X]/(q(X))$, where $q(X)$ is an irreducible polynomial of degree m that generates the extension field $\mathbb{F}_{2^m}$. Throughout this paper α will denote a root of the irreducible polynomial $q(X)$.

The exclusive-or (XOR) sign $\oplus$ will specifically mean addition modulo 2, and we will use the $+$ sign to mean addition over any field (that applies to $\mathbb{F}_2$ as well).

An $n \times n$ matrix M is MDS if the $n \times 2n$ matrix $G = [I_n M]$ is a generator of an MDS code, where I_n is the $n \times n$ identity matrix. One necessary and sufficient condition for M to be MDS is that every submatrix of M is nonsingular. An MDS matrix attains the maximum diffusion power. If M is such that $M^2 = I_n$, then M is called involutory, and when $MM^t = I_n$, then it is orthogonal, where M^t is the transpose of M. Since an involutory matrix is self-inverse, thus implementation of its inverse comes for free, similarly for orthogonal matrices, its inverse can be implemented just by taking its transpose.

2.1 Basics of XOR counts

The field $\mathbb{F}_{2^m}$ can be identified to the vector space $\mathbb{F}_2^m$, which is the set of all m-tuple binary vectors, by choosing some basis of the field. For example $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a polynomial basis. In practice field elements are implemented by their corresponding binary vectors, and multiplication and addition of field elements can be realized by XOR operations. In [14] the metric XOR count was proposed as follows.

Definition 1. The XOR count of an element $\beta \in \mathbb{F}_{2^m}$ is the number of XORs required to implement the multiplication of β with an arbitrary element $b \in \mathbb{F}_{2^m}$. We denote the XOR count of β by $XOR(\beta)$.

This metric is very much useful in estimating the hardware implementation cost of the diffusion layer of a block cipher. The authors of [14] showed that low XOR count is strongly correlated to the minimization of hardware area (GE). Note that [14] implemented SPNs block ciphers considering circulant and serial type diffusion matrices to measure the hardware cost.

Usually MDS matrices are used as diffusion layer, as they have the highest diffusion power. For lightweight block ciphers, diffusion matrices with low XOR count are desired, thus finding MDS matrices with low XOR count is an interesting problem. The set of XOR counts of all the elements of $\mathbb{F}_{2^m}$ is termed as the XOR count distribution [18]. The authors of [18] have showed that XOR count distribution varies as the basis changes, however they did not find better MDS matrices (in terms of low XOR count) for any other bases than the polynomial basis. They observed that under the polynomial basis, fields elements tend to have low XOR counts. It is also to be noted that polynomial basis is a conventional choice for implementation. Therefore, we will only be considering polynomial basis.

Consider $\mathbb{F}_{2^3}$ with the underlying irreducible polynomial X^3+X+1. The multiplication of $\alpha^4 = \alpha + \alpha^2$ with an arbitrary element $b = b_0 + b_1\alpha + b_2\alpha^2$, where $b_i \in \{0, 1\}$ is

$$(b_0 + b_1\alpha + b_2\alpha^2)(\alpha + \alpha^2) = (b_1 + b_2) + (b_0 + b_1)\alpha + (b_0 + b_1 + b_2)\alpha^2.$$

Thus in vector form the above product looks like

$$(b_1 \oplus b_2, b_0 \oplus b_1, b_0 \oplus b_1 \oplus b_2),$$

in which there are 4 XORs.

It is obvious that the XOR count of the field element 0 is 0, and also $XOR(1) = 0$.

Remark 1. One may note that there might be repetitions of some terms in the coordinates of the product vector, which could be reused to reduce the total XOR count. In [20, 18] it is remarked that to get the advantage of reusing XORs might require additional cycle and memory which is likely to exceed the cost that is saved in the XOR count. However, this trade-off is more subtle and needs further explorations. Moreover, [20, 18] remarked that XOR count was a simplified metric, and we too follow the same consideration.

To measure the XOR count of a diffusion matrix one has to add the XOR counts of all the entries in that matrix. In [14] XOR count of a row of a matrix was derived as follows. The XOR count of the i-th row of an $n \times n$ matrix M over $\mathbb{F}_{2^m}$ is

$$\sum_{j=0}^{n-1} \gamma_{ij} + (\ell_i - 1) \cdot m,$$

where γ_{ij} is the XOR count of j-th element of i-th row, and ℓ_i is the number of nonzero entries in that row.

We extend this notion of XOR count of a row to the XOR count of the whole matrix by adding XOR counts of all the rows:

$$\sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \gamma_{ij} + (\ell_i - 1) \cdot m \right) = C(M) + \sum_{i=0}^{n-1} (\ell_i - 1) \cdot m \ . \tag{1}$$

The term $C(M)$ is the sum of XOR counts of all the entries of M. For an $n \times n$ MDS matrix over $\mathbb{F}_{2^m}$, $\ell_i = n$, so (1) becomes $C(M) + n \cdot (n-1) \cdot m$, note that $C(M)$ varies with the matrices.

2.1.1 Some properties of XOR count of field elements

In this section, we present some results on XOR counts.

Note that every irreducible polynomial of degree m always contains the terms X^m and 1, meaning that an irreducible polynomial can be written as $X^m + p(X) + 1$, where the highest and lowest possible degree terms of $p(X)$ are X^{m-1} and X respectively.

Proposition 1. *Suppose $q(X) = X^m + p(X) + 1$ is an irreducible polynomial of degree m over $\mathbb{F}_2$, where $p(X)$ has t nonzero coefficients. Then XOR count of $\alpha \in \mathbb{F}_2[X]/(q(x))$ is t, where $q(\alpha) = 0$.*

Proof. The XOR count of α is obtained from the product

$$\begin{aligned} (b_0 + b_1\alpha + \ldots + b_{m-1}\alpha^{m-1})\alpha &= b_0\alpha + b_1\alpha^2 + \ldots + b_{m-1}\alpha^m \\ &= b_{m-1} + b_0\alpha + b_1\alpha^2 + \ldots + b_{m-1}\ p(\alpha), \\ &\qquad \text{replacing } \ \alpha^m = p(\alpha) + 1. \end{aligned}$$

Clearly b_{m-1} will be XORed with b_i, if the coefficient of X^i in $p(X)$ is nonzero.

□

Proposition 2. *Suppose $q(X) = X^m + p(X) + 1$ is an irreducible polynomial of degree m over $\mathbb{F}_2$. Then XOR counts of $\alpha \in \mathbb{F}_2[X]/(q(x))$ and α^{-1} are the same, where $q(\alpha) = 0$.*

Proof. The XOR count of α^{-1} is obtained from the product

$$(b_0 + b_1\alpha + \ldots + b_{m-1}\alpha^{m-1})\alpha^{-1} = b_0\alpha^{-1} + b_1 + \ldots + b_{m-1}\alpha^{m-2}.$$

From $\alpha^m + p(\alpha) = 1$ we get $\alpha^{m-1} + \alpha^{-1}p(\alpha) = \alpha^{-1}$. Using this in the above relation

$$b_0\alpha^{-1} + b_1 + \ldots + b_{m-1}\alpha^{m-2} = b_0\alpha^{m-1} + b_0\alpha^{-1}p(\alpha) + b_1 + \ldots + b_{m-1}\alpha^{m-2}.$$

So b_0 will be XORed with b_i if coefficient of X^i is nonzero in $p(X)$. □

3 Toeplitz MDS Matrices

In this section we present some results on Toeplitz MDS matrices and show their importance with respect to XOR count.

Definition 2. A matrix, whose every row is a one cyclic shift of the previous row is called a circulant matrix.

This kind of matrices are useful in the hardware design as the full matrix can be generated from the first row. Following is an example of an $n \times n$ circulant matrix, where a row is generated by right cyclic shift of the previous row.

$$\texttt{Circ}(a_0, \ldots, a_{n-1}) = \begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix}.$$

Definition 3. A matrix is called Toeplitz if every descending diagonal from left to right is constant.

Following is an example of a Toeplitz matrix of order $n \times n$

$$\mathrm{T} = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} \\ a_{-1} & a_0 & a_1 & \ldots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{-(n-1)} & a_{-(n-2)} & a_{-(n-3)} & \ldots & a_{-1} & a_0 \end{bmatrix}. \tag{2}$$

Obviously circulant matrix is a special form of Toeplitz matrix. A Toeplitz matrix is defined by its first row and first column. For instance $\{a_0, a_1, \ldots, a_{n-1}, a_{-1}, a_{-2}, \ldots, a_{-(n-1)}\}$ defines the Toeplitz matrix T in 2. This matrix can also be defined as follows:

$$\mathrm{T} = [a_{ij}] \quad \text{where} \quad a_{ij} = a_{j-i}. \tag{3}$$

MDS circulant matrices have been used to build the diffusion layer of `AES` [8] and `WHIRLPOOL` [4]. One may refer to [10] for the construction of circulant MDS matrices, where they also proved that an MDS circulant matrix cannot be involutory. We prove that this is indeed true for the Toeplitz matrices as well.

Theorem 1. *Let T be an $n \times n$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and involutory.*

Proof. Let T be a Toeplitz matrix as in (2) which is both MDS and involutory. We treat the proof for odd and even n separately.

CASE 1 : When n is odd.
The $(n-2)$-th element in the 0-th row of T^2 is

$$\begin{aligned} [T^2]_{0,n-2} &= (a_0, a_1, \ldots, a_{n-1}) \cdot (a_{n-2}, a_{n-3}, \ldots, a_0, a_{-1}) \\ &= a_0 a_{n-2} + a_1 a_{n-3} + \ldots + a_{(n-1)/2} a_{(n-3)/2} + \ldots + a_{n-2} a_0 + a_{n-1} a_{-1} \\ &= a_{n-1} a_{-1}. \end{aligned}$$

Since T is involutory then

$$a_{n-1} a_{-1} = 0, \tag{4}$$

which implies that $a_{n-1} = 0$ or $a_{-1} = 0$, This contradicts that T is MDS, as being MDS every element of T is nonzero.

CASE 2 : When n is even. In this case

$$\begin{aligned}[T^2]_{0,n-2} &= (a_0, a_1, \ldots, a_{n-1}) \cdot (a_{n-2}, a_{n-3}, \ldots, a_0, a_{-1}) \\ &= a_0 a_{n-2} + a_1 a_{n-3} + \ldots + a_{(n-2)/2}^2 + \ldots + a_{n-2} a_0 + a_{n-1} a_{-1} \\ &= a_{(n-2)/2}^2 + a_{n-1} a_{-1}.\end{aligned}$$

Since T is an involution, so

$$a_{(n-2)/2}^2 + a_{n-1} a_{-1} = 0. \tag{5}$$

Consider the following 2×2 submatrix of T by taking the 0-th and $n/2$-th row, and $(n-2)/2$-th and $(n-1)$-th column,

$$\mathrm{A} = \begin{bmatrix} a_{(n-2)/2} & a_{n-1} \\ a_{-1} & a_{(n-2)/2} \end{bmatrix}$$

Since T is MDS matrix then determinant of A is

$$a_{(n-2)/2}^2 + a_{n-1} a_{-1} \neq 0,$$

which contradicts (5).

Hence for both odd and even n, T cannot be both MDS and involution. This completes the proof. □

Theorem 2. *Let T be an $n \times n$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and orthogonal when $n = 2^r$.*

Proof. Let T be a Toeplitz matrix as in (2) which is both MDS and orthogonal. Suppose $T' = T \cdot T^t$ and let δ_i be the diagonal element of T' for $i = 0, \ldots, n-1$. We have

$$\delta_i = \sum_{j=0}^{n-1} a_{j-i}^2 = 1, \quad \text{for} \quad i = 0, 1, \ldots, n-1. \tag{6}$$

Considering the pair of equations (δ_i and δ_{i+1}) from the above system of equations we get

$$a_{-i} = a_{n-i} \quad \text{for} \;\; i = 1, \ldots, n-1, \tag{7}$$

that is T is indeed a circulant matrix. From [10, Lemma 2] it is known that any $2^r \times 2^r$ circulant matrix cannot be both orthogonal and MDS, this completes the proof. □

Therefore, to construct MDS involutory or MDS orthogonal (for order $2^r \times 2^r$) matrices, one has to look beyond the class of Toeplitz matrices.

3.1 Constructions of MDS Toeplitz matrix

We now give some theoretical constructions of Toeplitz MDS matrices. The idea behind these constructions is the following. Form several examples of Toeplitz MDS matrices by considering matrix entries with low XOR count, and then carefully check the relations between the elements and all the determinants of the submatrices.

As we see that XOR count of 1 is zero, so more presence of 1's in an MDS matrix is likely to keep the total XOR count of the matrix low. However, it is known from [12] that in a 4×4 MDS matrix, 1 cannot occur more than 9 times. In the following, we consider a special form of 4×4 Toeplitz matrix where 1 occurs 8 times, and analyze when this becomes MDS.

Proposition 3. *Let $T_1(x)$ be the following 4×4 Toeplitz matrix defined over $\mathbb{F}_{2^m}$:*

$$T_1(x) = \begin{bmatrix} x & 1 & 1 & x^{-2} \\ 1 & x & 1 & 1 \\ x^{-2} & 1 & x & 1 \\ x^{-2} & x^{-2} & 1 & x \end{bmatrix}.$$

If $x \in \mathbb{F}_{2^m}^*$ is such that the degree of its minimal polynomial over $\mathbb{F}_2$ is ≥ 5, then $T_1(x)$ is MDS.

Proof. As the minimal polynomial of x has degree > 4, so $x \neq 1$. Consider the set Δ_2 (respectively Δ_3) of all distinct determinants of submatrices of order 2×2 (respectively order 3×3):

$$\begin{aligned} \Delta_2(\mathrm{T}_1(x)) \quad = \quad & \{x^2+1, x+1, (x^3+1)/x^2, (x+1)/x, \\ & (x+1)/x^2, (x^4+1)/x^2, (x^5+1)/x^4, (x^2+1)/x^2, \\ & (x^6+1)/x^4, (x^2+1)/x^4\}, \end{aligned}$$

$$\begin{aligned} \Delta_3(\mathrm{T}_1(x)) \quad = \quad & \{(x^8+x^4+x^2+1)/x^6, (x^2+1)/x^2, x^2+1, (x^5+x^4+x^3+1)/x^4, \\ & (x^2+1)/x^4, (x^5+x^4+x^3+1)/x^3, (x^7+x^5+x^3+x^2+x+1)/x^4, \\ & (x^5+x^2+x+1)/x^2, (x^6+x^5+x^4+x^3+x^2+1)/x^4, (x^6+1)/x^4\}. \end{aligned}$$

All the numerators of the elements of $\Delta_2(\mathrm{T}_1(x))$ and $\Delta_3(\mathrm{T}_1(x))$ can be factored into irreducible polynomials over $\mathbb{F}_2$ of maximum degree 4 (refer to Appendix A.1). Therefore, none of these determinants are equal to zero.

Finally, the determinant of $\mathrm{T}_1(x)$ is $(x^{10}+x^8+x^6+1)/x^6 = (x+1)^4(x^3+x^2+1)^2/x^6$, which is also nonzero as the minimal polynomial of x has degree ≥ 5. □

Example 1. Consider the matrix $\mathrm{T}_1(\alpha)$ over $\mathbb{F}_{2^8}$ as given in Proposition 3 with the irreducible polynomial $X^8+X^6+X^5+X^2+1$ with α as its root. According to Proposition 3, this is an MDS matrix. The XOR counts of 1, α and α^{-2} are 0, 3 and 6 respectively, and there are 4 α's and 4 α^{-2}'s. For every row the additional XOR count is $3 \cdot 8$, therefore XOR count of $\mathrm{T}_1(\alpha)$ is $4 \cdot 3 + 4 \cdot 6 + 4 \cdot 3 \cdot 8 = 36 + 4 \cdot 3 \cdot 8$.

Note that in [14], a circulant matrix having the same XOR count was reported. To get a better XOR count for this kind of Toeplitz matrices, we try exhaustively by putting different values of x from $\mathbb{F}_{2^8}$ under the irreducible polynomial $X^8+X^6+X^5+X^2+1$. However, we do not get any improved matrix. So we look at some other form of Toeplitz matrices. Next we consider the following Toeplitz matrix.

Proposition 4. *Let $T_2(x)$ be the following 4×4 Toeplitz matrix defined over $\mathbb{F}_{2^m}$:*

$$T_2(x) = \begin{bmatrix} 1 & 1 & x & x^{-1} \\ x^{-2} & 1 & 1 & x \\ 1 & x^{-2} & 1 & 1 \\ x^{-1} & 1 & x^{-2} & 1 \end{bmatrix}.$$

If $x \in \mathbb{F}_{2^m}^*$ is such that

1. *the degree of the minimal polynomial of x is ≥ 4, and*
2. *x is not a root of the polynomial $X^6+X^5+X^4+X+1$,*

then $T_2(x)$ is MDS.

Proof. We show that all the square submatrices are nonsingular with this choice of x. The list of distinct determinants of 2×2 submatrices:

$$\begin{aligned}\Delta_2(\mathrm{T}_2)(x) \quad = \quad & \{\, (x^3+1)/x^2, (x^2+1)/x, (x+1)/x^2, (x+1)/x, \\ & 1+x, (x^3+1)/x, (x^3+1)/x^4, (x^3+1)/x^3, (x^2+1)/x^2, \\ & (x^4+1)/x^3, (x^4+1)/x^4 \,\}.\end{aligned}$$

Next we check the list of distinct determinants of 3×3 submatrices:

$$\begin{aligned}\Delta_3(\mathrm{T}_2)(x) \quad = \quad & \{\, (x^2+1)/x^3, (x^2+1)/x^4, (x^4+1)/x^3, (x^6+x^5+x^3+1)/x^5, \\ & (x^6+x^5+x^3+1)/x^6, (x^5+x^4+x^3+1)/x^3, \\ & (x^5+x^4+x^3+1)/x^4 \,\}.\end{aligned}$$

Notice that the elements of both $\Delta_2(\mathrm{T}_2(x))$ and $\Delta_3(\mathrm{T}_2(x))$ can be factored into irreducible polynomials over $\mathbb{F}_2$ of maximum degree 3 (refer to Appendix A.2). If the minimal polynomial of x is ≥ 4, then none of these determinants is zero.

Finally the determinant of the full matrix is

$$(x^9+x^7+x^6+1)/x^7 = (x+1)^3\,(x^6+x^5+x^4+x+1)/x^7.$$

This also does not vanish if x is not a root of $X^6+X^5+X^4+X+1$. Hence the proof. □

Remark 2. It is to be noted that the number of 1's in the MDS matrix $\mathrm{T}_2(x)$ is 9, which is the maximum possible occurrences of 1's in an MDS 4×4 matrix as pointed out in [12, Lemma 1].

We choose $x \in \mathbb{F}_{2^m}^*$ according to Proposition 4 to construct MDS matrices and determine their XOR counts. By choosing primitive α for x, it is likely that we would get an MDS matrix with low XOR count as $XOR(\alpha), XOR(\alpha^{-1})$ and $XOR(\alpha^{-2})$ tend to have low XOR counts (see Proposition 1 and 2).

We consider the matrix $\mathrm{T}_2(x)$ over $\mathbb{F}_{2^m}$ for $x = \alpha$, where α is a primitive element of $\mathbb{F}_{2^m}$:

$$\mathrm{T}_2(\alpha) = \begin{bmatrix} 1 & 1 & \alpha & \alpha^{-1} \\ \alpha^{-2} & 1 & 1 & \alpha \\ 1 & \alpha^{-2} & 1 & 1 \\ \alpha^{-1} & 1 & \alpha^{-2} & 1 \end{bmatrix}. \tag{8}$$

Corollary 1. *Consider $\mathbb{F}_{2^8}$ generated by the primitive element α which is a root of $X^8+X^6+X^5+X^2+1$, then the matrix $\mathrm{T}_2(\alpha)$ as given in (8) is MDS and has XOR count $30 + 4 \cdot 3 \cdot 8$.*

Proof. Since the degree of the minimal polynomial of α is 8, so by Proposition 4, $\mathrm{T}_2(\alpha)$ is MDS.

Under this irreducible polynomial, $XOR(\alpha) = XOR(\alpha^{-1}) = 3$, and $XOR(\alpha^{-2}) = 6$. Therefore, the total sum of the XOR counts of the elements of $T_2(\alpha)$ is $C(T_2(\alpha)) = 4 \cdot 3 + 3 \cdot 6 = 30$. Moreover, every row has the additional XOR count $3 \cdot 8$. □

Here we get an improvement of the lower bound of the XOR count of 4×4 MDS matrices over $\mathbb{F}_{2^8}$. As pointed out in [20] that XOR counts differ as the underlying irreducible polynomial varies, we check for another irreducible polynomial, for which the same matrix T_2 has even lesser XOR count.

Corollary 2. *Consider $\mathbb{F}_{2^8}$ generated by the primitive element α which is a root of $X^8+X^7+X^6+X+1$, then the MDS matrix $\mathrm{T}_2(\alpha)$ as given in (8) has XOR count $27 + 4 \cdot 3 \cdot 8$.*

Proof. Since the degree of the minimal polynomial of α is 8, so by Proposition 4, $\mathrm{T}_2(\alpha)$ is MDS.

Under this irreducible polynomial, $XOR(\alpha) = XOR(\alpha^{-1}) = 3$, and $XOR(\alpha^{-2}) = 5$. Therefore, the sum of the XOR counts of the elements of $T_2(\alpha)$ is $C(T_2(\alpha)) = 4{\cdot}3{+}3{\cdot}5 = 27$. Per row the additional XOR count that is required is $3 \cdot 8$. □

This gives even better improved lower bound of XOR count of a 4×4 MDS matrices. But is there any MDS matrix that has better XOR count than $27 + 4 \cdot 3 \cdot 4$? We solve this question in Section 5.

Corollary 3. *Consider $\mathbb{F}_{2^4}$ generated by the primitive element α which is a root of $X^4 + X^3 + 1$, then the matrix $\mathrm{T}_2(\alpha)$ as given in (8) has XOR count $10 + 4 \cdot 3 \cdot 4$.*

Proof. Since the degree of the minimal polynomial of α is 4, and α can never be a root of $X^6 + X^5 + X^4 + X + 1$, therefore, by Proposition 4, $\mathrm{T}_2(\alpha)$ is MDS.

Under this irreducible polynomial, $XOR(\alpha) = XOR(\alpha^{-1}) = 1$, and $XOR(\alpha^{-2}) = 2$. Therefore, the sum of the XOR counts of the elements of $T_2(\alpha)$ is $C(T_2(\alpha)) = 4{\cdot}1{+}3{\cdot}2 = 10$. Per row the additional XOR count required is $3 \cdot 4$. □

This improves the previously known best XOR count: $12 + 4 \cdot 3 \cdot 4$ in [16], we will check if this can be improved further in Section 6.

4 Searching for MDS Matrix with the minimum XOR count

In this section, we consider matrices in general form to find the minimum value of XOR count of 4×4 matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. We would like to remind that we will only be considering polynomial basis as discussed in Section 2.1.

One can imagine the vastness of the search space as every single matrix is to be checked if that holds the MDS property. In order to be able to determine the minimum XOR count, we apply a search strategy which is a kind of "divide and conquer". Before describing the strategy, we first define some sets. For a $t \times n$ matrix Y, we define the set $\Delta_i(Y)$ as the set of determinants of all its $i \times i$ submatrices:

$$\Delta_i(Y) = \{\, \det(Z) \,:\, Z \text{ is an } i \times i \text{ submatrix of } A \,\}, \qquad i = 1, \ldots, \min\{t, n\}.$$

With this notation, necessary and sufficient condition for a square matrix A of order $n \times n$ to be MDS is that

$$0 \notin \Delta_i(A), \quad \text{for } i = 1, \ldots, n. \tag{9}$$

Given an $n \times n$ matrix A, for even n, it can be represented as

$$A = \left[\frac{A_u}{A_\ell} \right], \tag{10}$$

where A_u (respectively A_ℓ) is an $\frac{n}{2} \times n$ submatrix of A consisting of upper (respectively lower) $\frac{n}{2}$ rows of A.

FACT 1: With block representation of A as in (10) a necessary condition for A to be MDS matrix is that

$$0 \notin \Delta_i(A_u) \quad \text{and} \quad 0 \notin \Delta_i(A_\ell) \quad \text{for} \quad i = 1, \ldots, \frac{n}{2}. \tag{11}$$

Thus we see that every MDS matrix A of order $n \times n$ can be obtained from two matrices U, L of order $\frac{n}{2} \times n$ satisfying (11) by taking $A_u = U$ and $A_\ell = L$. In a nutshell, our search strategy consists of searching for A_u and A_ℓ and then constructing A.

The main advantage of halving A is that we need to search in a much smaller space. For example if the matrix A is defined over a set $S \subset \mathbb{F}_{2^m}$, exhaustive search would require $|S|^{\frac{n}{2} \times n}$ instead of $|S|^{n^2}$ effort. We will carefully choose the set S so that $|S|^{\frac{n}{2} \times n}$ becomes moderate which enables us to compute the set of matrices A_u faster.

Choosing the set S

As we just discussed, the set S plays central role in our search strategy and needs to be chosen carefully, that we will do by keeping in mind the known lower bound of XOR count of MDS matrices. One may note that $1 \in \mathbb{F}_{2^m}$ has the minimum XOR count, which is 0. For $m \leq 8$, one can check that the next minimum XOR count is associated with α and α^{-1} (refer to Proposition 1 and Proposition 2 for the exact value). Therefore, more presence of $\{1, \alpha, \alpha^{-1}\}$ in A is likely to keep XOR count low.

We now recall the notation $C(A)$ from (1) and define $\mathtt{C}$ that we will be frequently using in our search.

(i) $C(A)$: the sum of the XOR counts of all the entries of A.

(ii) $\mathtt{C}$: known lower bound of $C(A)$, where A is an $n \times n$ MDS matrix.

Recall from (1) that the XOR count of an $n \times n$ matrix A is $C(A) + n \cdot (n-1) \cdot m$. In our computation we ignore the constant $n \cdot (n-1) \cdot m$, and look for MDS matrices A with $C(A) < \mathtt{C}$, as that would improve the existing lower bound. Beginning with $\mathbb{F}_{2^m}$ and a $\mathtt{C}$ we choose the set S as follows. If there is any field element $\beta \in \mathbb{F}_{2^m}$ such that $XOR(\beta) \geq \mathtt{C}$, then β can never be an entry of a matrix A that has $C(A) < \mathtt{C}$.

Let

$$\theta = \min \{C(H) : H \text{ is } \frac{n}{2} \times n \text{ matrix over } \mathbb{F}_{2^m} \text{ satisfying (11)}\}, \tag{12}$$

and suppose that we know the value of θ. It follows that any MDS matrix A satisfies $C(A_u) \geq \theta$ (respectively $C(A_\ell) \geq \theta$), whence we have $C(A_\ell) \leq \mathtt{C} - 1 - \theta$ (respectively $C(A_u) \leq \mathtt{C} - 1 - \theta$) so as to make $C(A) \leq \mathtt{C} - 1$. We now determine the possible XOR counts that elements of A_ℓ (respectively A_u) can take so that $C(A) \leq \mathtt{C} - 1$. Suppose β_0 is an element having the least nonzero XOR count, say τ. If there is any element β_1 in A_ℓ (respectively A_u) with $XOR(\beta_1) > \mathtt{C} - 1 - \theta - \tau$, then the only possible entries are 1's, otherwise $C(A) > \mathtt{C} - 1$. In this case there will be singular submatrices. Thus choices of elements for A_ℓ (respectively A_u) are

$$S = \{\beta \in \mathbb{F}_{2^m} : XOR(\beta) \leq \mathtt{C} - 1 - \theta - \tau\}.$$

Once we have $\mathtt{C}$ and a subset S of $\mathbb{F}_{2^m}^*$ we construct the following set by searching exhaustively:

$$\mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta) = \{\ H\ :\ H \text{ is } \frac{n}{2} \times n \text{ matrix over } S \text{ satisfying (11)} \text{ and } C(H) \leq \mathtt{C} - 1 - \theta\ \}.$$

Note that if A is an MDS matrix with $C(A) < \mathtt{C}$ then $A_u, A_\ell \in \mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta)$. On the other hand if $U, L \in \mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta)$, and

$$A = \left[\begin{array}{c} U \\ \hline L \end{array}\right]$$

as in (10) is an $n \times n$ MDS matrix with $C(A) < \mathtt{C}$ then our search succeeds in finding a new matrix with lower XOR counts, that improves the lower bound $\mathtt{C}$. Clearly during this step, we need to consider $|\mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta)|^2$ pairs. Thus the whole search requires

$$|S|^{\frac{n}{2} \times n} + |\mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta)|^2 \tag{13}$$

effort. The second term grows with both $S, (\mathtt{C} - \theta)$, and if these two values are moderate, then $|\mathcal{M}_{\frac{n}{2} \times n}(S, \mathtt{C}, \theta)|^2$ will be dominated by the initial search effort $|S|^{\frac{n}{2} \times n}$, as can be seen in Section 5 and 6.

5 MDS matrices over $\mathbb{F}_{2^8}$ with minimal XOR count

So far the best known XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^8}$ is $32+4\cdot3\cdot8$ as reported in [16]. Thanks to Corollary 1 and Corollary 2, we know that there exist MDS matrices with improved XOR counts as $30+4\cdot3\cdot8$ under primitive polynomial $X^8+X^6+X^5+X^2+1$, and $27+4\cdot3\cdot8$ under primitive polynomial $X^8+X^7+X^6+X+1$, respectively. Next we determine the minimum possible XOR count of these matrices using the search method described earlier.

5.1 Under the irreducible polynomial $X^8+X^7+X^6+X+1$

We consider the primitive polynomial $X^8+X^7+X^6+X+1$ of $\mathbb{F}_{2^8}$, and check whether there is any 4×4 MDS matrix A such that $C(A) < 27$, i.e., in our search strategy we set $\mathtt{C} = 27$.

First we need to know the value of θ as given in (12), i.e., the minimum value of a 2×4 matrix A_u (respectively A_ℓ) over $\mathbb{F}_{2^8}$ such that all its submatrices are nonsingular. We consider all possible 2×4 matrices H formed by elements with low XOR counts, in particular we take $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$, in which XOR count of every element is ≤ 5. The minimum $C(H)$ we obtain is 11. If there is a 2×4 matrix H that satisfies (11) and $C(H) < 11$, then an element β with $XOR(\beta) \geq 11$ can never be a part of it, in fact any β with $XOR(\beta) > 7$ can never be a part of it. The reason is the following: suppose $C(H) < 11$ and H has an element β with $7 < XOR(\beta) < 11$. Then $7 < C(H) < 11$, which implies all the other 7 elements of H are all equal to 1, as $XOR(1) = 0$, and the next minimum XOR count in $\mathbb{F}_{2^8}$ is 3. In this case H has singular submatrices. So to know the value of θ we form H with elements from $B = \{\beta : XOR(\beta) \leq 7\}$ and check whether H satisfies (11) and $C(H) < 11$. Note that $|B| = 6$, and this search is $6^8 \approx 2^{21}$. We do not find any such H, so we conclude that $\theta = 11$.

Now that we know $\theta = 11$, the maximum possible value of $C(A_\ell)$ (respectively $C(A_u)$) is 15 in order to make the total sum ≤ 26. In a 2×4 matrix A_u (respectively A_ℓ) if one element has XOR count 15, then rest of the 7 elements have to be 1, as $XOR(1) = 0$. But such a matrix has singular submatrices. So an element with XOR count 15 cannot be an entry of A_u (respectively A_ℓ). Using the same logic as used in determining θ, we conclude that the maximum possible XOR count of an element in A_u (respectively A_ℓ) could be 12, as the minimum nonzero XOR count value is 3. So we select the set $S = \{\beta \in \mathbb{F}_{2^8}^* : XOR(\beta) \leq 12\}$. The cardinality of S is 23, and hence the search space becomes $23^8 \approx 2^{36}$. Then we form all possible 2×4 matrices A_u such that $C(A_u) \leq 15$ and all its submatrices are nonsingular. The number of such matrices is 3360, and these form the possible choices for both A_u and A_ℓ. Combining A_u and A_ℓ to form A, we further check whether all the submatrices of A are nonsingular, if so, we check the value of $C(A)$. This requires to check $3360^2 \approx 2^{24}$ pairs of 2×4 matrices. Exhausting the search we do not find any MDS matrix A such that $C(A) \leq 26$. Therefore, our search completes with the conclusion that the minimum value of $C(A)$ is 27. We write it more formally below.

Proposition 5. *The minimum value of XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^8}$ under the irreducible polynomial $X^8+X^7+X^6+X+1$ is $27+4\cdot3\cdot8$.*

One may note that the initial search effort 2^{36} dominates in the whole search effort as the effort to combine the pairs is 2^{24}.

5.2 Under the irreducible polynomial $X^8+X^6+X^5+X^2+1$

We consider the primitive polynomial $X^8+X^6+X^5+X^2+1$ of $\mathbb{F}_{2^8}$, and check whether there is any 4×4 MDS matrix A such that $C(A) < 30$.

To do this search we consider $\mathtt{C} = 30$, and carefully look at possible values of $C(A_u)$ (respectively $C(A_\ell)$) of every 2×4 matrix A_u (respectively A_ℓ). As described in the previous search, we first determine the value of θ following the same technique. First we consider $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$, where the maximum XOR count attained is 6, and form all possible 2×4 matrices H satisfying (11). In this search, the minimum value of $C(H)$ is 12. As $XOR(1) = 0$ and the next minimum XOR count is 3, now we have to choose $B = \{\beta : XOR(\beta) \leq 8\}$ in order to determine if the minimum value of $C(H)$ is < 12 for all H satisfying (11). We notice that $B = \{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$. This concludes that $\theta = 12$.

Therefore when we half a matrix A into A_u and A_ℓ of order 2×4, the minimum value of $C(A_u)$ (respectively $C(A_\ell)$) is 12. Consequently, the maximum possible value of $C(A_\ell)$ (respectively $C(A_u)$) is 17 in order to make the total sum ≤ 29. In a 2×4 matrix A_u (respectively A_ℓ) if one element has XOR count 17, then rest of the 7 elements have to be 1, as 1 has XOR count zero. But such a matrix has singular submatrices. So an element with XOR count 17 cannot be an entry of A_u (respectively A_ℓ). Using the same logic as used in the previous search, we conclude that the maximum possible XOR count of an element in A_u (respectively A_ℓ) could be 14, as the minimum nonzero XOR count value is 3. So we select the set $S = \{\beta \in \mathbb{F}_{2^8} : XOR(\beta) \leq 14\}$. The cardinality of S is 22, and hence the search space becomes $22^8 \approx 2^{36}$. Then we form all possible 2×4 matrices A_u such that $C(A_u) \leq 17$ and all its submatrices are nonsingular. The number of such matrices is 3552, and these form the possible choices for both A_u and A_ℓ. Combining A_u and A_ℓ to form A, we further check whether all the submatrices of A are nonsingular, if so, we check the value of $C(A)$. This requires to check $3552^2 \approx 2^{24}$ pairs. Exhausting the search we do not find any MDS matrix A such that $C(A) \leq 29$. Therefore, our search completes with the conclusion that the minimum value of $C(A)$ is 30. We write it more formally below.

Proposition 6. *The minimum value of XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^8}$ under the irreducible polynomial $X^8 + X^6 + X^5 + X^2 + 1$ is $30 + 4 \cdot 3 \cdot 8$.*

As we see the initial search effort is 2^{36} and checking the pairs is 2^{24}, thus in this case also the initial search dominates in the whole search effort.

We check for all irreducible polynomials (up to reciprocals) that generate $\mathbb{F}_{2^8}$, and did not find any MDS matrix that improves the lower bound $27 + 4 \cdot 3 \cdot 8$.

Proposition 7. *Over all irreducible polynomials of degree 8, the minimum XOR count of 4×4 MDS matrices over $\mathbb{F}_{2^8}$ is $27 + 4 \cdot 3 \cdot 8$.*

6 MDS matrices over $\mathbb{F}_{2^4}$ with minimal XOR count

Next we aim for finding MDS matrices with the least XOR count over $\mathbb{F}_{2^4}$. The currently known lower bound is $12 + 4 \cdot 3 \cdot 4$ [16]. In Corollary 3, we already have obtained an improved XOR count $10 + 4 \cdot 3 \cdot 4$. We consider $GF(2^4)$ generated by the primitive element α which is a root of $X^4 + X^3 + 1$. We search for general MDS matrices A with $C(A) < 10$. As previously done, we half the matrix A in two parts A_u and A_ℓ. First we find that the minimum possible value of A_u (respectively A_ℓ) by following the same strategy as used in the previous search. That is, we start with the set $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$ and follow the exact method as before to reach the conclusion that $\min C(A_u) = 4$. As the minimum nonzero XOR count value is 1, so using the same logic as done for $\mathbb{F}_{2^8}$, we set $S = \{\beta \in \mathbb{F}_{2^4} : XOR(\beta) \leq 4\}$, in this case $|S| = 6$. Thus the search space for A_u is 6^8. The total number of possible A_u (respectively A_ℓ) is 1344. Then combining A_u and A_ℓ we do not obtain any matrix A such that $C(A) < 10$.

Proposition 8. *The minimum value of the XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^4}$ under the irreducible polynomial $X^4 + X^3 + 1$ is $10 + 4 \cdot 3 \cdot 4$.*

There are 3 irreducible polynomials of degree 4: X^4+X^3+1 and X^4+X+1 are reciprocals of each other and the remaining one is $X^4+X^3+X^2+X+1$. We now check if there is any 4×4 MDS matrix A over $\mathbb{F}_{2^4}$ with $C(A)<10$ under $X^4+X^3+X^2+X+1$. Let us first find what is the minimum possible XOR count that a 4×4 MDS matrix can have under this polynomial. Under $X^4+X^3+X^2+X+1$, the minimum possible nonzero XOR count is 3, which is for α, a root of $X^4+X^3+X^2+X+1=0$, and we also have $XOR(1)=0$. We know from [12] that the maximum number of possible 1's in a 4×4 MDS matrix is 9. So if a 4×4 MDS matrix M has 1 in 9 places, and the rest 7 are elements with the least XOR counts, i.e., 3, then it shows that sum of the XOR counts of elements of M, is $C(M)\geq 7\times 3=21$. Thus we conclude the following.

Proposition 9. *Over all irreducible polynomials of degree 4, the minimum XOR count of 4×4 MDS matrices over $\mathbb{F}_{2^4}$ is $10+4\cdot 3\cdot 4$.*

7 Involutory MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$

We have seen in the previous sections that there are 4×4 Toeplitz MDS matrices that achieve the minimum XOR counts over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ respectively. As Theorem 1 suggests that involutory MDS Toeplitz matrices do not exist, we have to check beyond the space of Toeplitz matrices to get involutory MDS matrices. In the following we present results related to involutory MDS matrices and their XOR counts. We construct 4×4 involutory MDS matrices of the form

$$N=\begin{bmatrix} A & B \\ C & A \end{bmatrix}, \tag{14}$$

where A, B and C are 2×2 Hadamard matrices. One may note that [23] searched for involutory MDS matrices in a class, which is actually a subclass of (14). They considered matrices of the form

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

where A is an MDS matrix.

The intuition as mentioned in the constructions of MDS Toeplitz matrices at the beginning of Section 3.1 can similarly be applied for the constructions of involutory MDS matrices of the form (14). We are able to derive theoretical constructions of 4×4 involutory MDS matrices. First we present a class of 4×4 involutory MDS matrices over $\mathbb{F}_{2^m}$ as follows.

Proposition 10. *Suppose $N_1(x)$ is a 4×4 matrix over $\mathbb{F}_{2^m}$ such that*

$$N_1(x)=\begin{bmatrix} 1 & x & 1 & x^2+1 \\ x & 1 & x^2+1 & 1 \\ x^{-2} & 1+x^{-2} & 1 & x \\ 1+x^{-2} & x^{-2} & x & 1 \end{bmatrix}. \tag{15}$$

Then $N_1(x)$ is an involutory matrix for all nonzero $x\in\mathbb{F}_{2^m}$, and if the degree of the minimal polynomial of x over $\mathbb{F}_2$ is ≥ 4, then $N_1(x)$ is also MDS.

Proof. It is easy to check that $N_1(x)$ is involutory for any $x\in\mathbb{F}_{2^m}^*$. We now show that it is MDS.

Consider the set Δ_2 and Δ_3 of all distinct determinants of submatrices of $N_1(x)$ of order 2×2 and 3×3 respectively:

$$\begin{aligned}\Delta_2(\mathrm{N}_1(x)) &= \{x^2+1,(x^2+1)/x^2,x^2+x+1,x^3+x+1,1/x^2,1,x^4,\\ &\quad (x^3+x^2+1)/x^2,(x^4+1)/x^2,(x^4+x^2+1)/x^2,\\ &\quad (x^3+x+1)/x^2,(x^2+x+1)/x^2\},\end{aligned}$$

$$\Delta_3(\mathrm{N}_1(x)) = \{1,x^2+1,(x^2+1)/x^2,x,1/x^2\}.$$

Note that numerators of all the elements of $\Delta_2(\mathrm{N}_1(x))$ and $\Delta_3(\mathrm{N}_1(x))$ can be factored into irreducible polynomials over $\mathbb{F}_2$ of maximum degree 3 (refer to Appendix A.3). Therefore, none of these determinants is equal to zero as the degree of the minimal polynomial of x is ≥ 4. Since $N_1(x)$ is involutory so its determinant is 1. Thus $N_1(x)$ is MDS for such a given x. □

Next we present another class of 4×4 involutory MDS matrices over $\mathbb{F}_{2^m}$ as follows.

Proposition 11. *Suppose $N_2(x)$ is a 4×4 matrix over $\mathbb{F}_{2^m}$ such that*

$$N_2(x) = \begin{bmatrix} 1 & x^2+1 & x & 1 \\ x^2+1 & 1 & 1 & x \\ x^3+x & x^2+1 & 1 & x^2+1 \\ x^2+1 & x^3+x & x^2+1 & 1 \end{bmatrix}. \tag{16}$$

Then $N_2(x)$ is an involutory matrix for all $x \in \mathbb{F}_{2^m}$, and if the degree of the minimal polynomial of x over $\mathbb{F}_2$ is ≥ 4, then $N_2(x)$ is also MDS.

Proof. We skip the proof of the involutory property and only show that $N_2(x)$ is MDS.

Consider the set Δ_2 and Δ_3 of all distinct determinants of submatrices of $N_2(x)$ of order 2×2 and 3×3 respectively:

$$\begin{aligned}\Delta_2(\mathrm{N}_2(x)) &= \{x^2+1,x^4+x^3+x+1,x^4+x^2,x^2+x+1,x^3+x+1,\\ &\quad x^4+x^2+1,x^5+x^2+x+1,x^4,x^3+x^2+x+1,x^2,\\ &\quad x^6+x^4+x^2+1\},\end{aligned}$$

$$\Delta_3(\mathrm{N}_2(x)) = \{1,x^2+1,x,x^3+x\}.$$

All the elements of $\Delta_2(\mathrm{N}_2(x))$ and $\Delta_3(\mathrm{N}_2(x))$ can be factored into irreducible polynomials over $\mathbb{F}_2$ of maximum degree 3 (refer to Appendix A.4). Therefore, none of these determinants is equal to zero as the degree of the minimal polynomial of x is ≥ 4. Since $N_2(x)$ is involutory so its determinant is 1. Thus $N_2(x)$ is MDS for such a given x. □

We would like to point out that thanks to Propositions 10 and 11, it is very easy to construct involutory MDS matrices. For example, for $\mathbb{F}_{2^m}$, where $m \geq 4$, one can just take $x = \alpha$, where α is a root of the underlying irreducible polynomial of the field.

Remark 3. One may note that both the classes N_1 and N_2 contain many involutory MDS matrices over $\mathbb{F}_{2^m}$. For example over $\mathbb{F}_{2^8}$, the number of involutory MDS matrices that both N_1 and N_2 give is $|\mathbb{F}_{2^8}| - |\mathbb{F}_{2^2}| = 252$.

We check XOR counts of the involutory MDS matrices of type N_1 for all possible irreducible polynomials of degree 4 and 8 for $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ respectively. For $\mathbb{F}_{2^8}$, the minimum XOR count obtained for N_1 is $64 + 4 \cdot 3 \cdot 8$. On the other hand, for $\mathbb{F}_{2^4}$, the minimum XOR count obtained for N_1 is $30 + 4 \cdot 3 \cdot 4$. Note that the known lower bound of XOR count of 4×4 involutory MDS matrices over $\mathbb{F}_{2^8}$ is $64 + 4 \cdot 3 \cdot 8$, which was obtained

by searching over a huge space of Hadamard matrices [20]. However, we show that a theoretical construction is possible to get such a matrix.

Similarly we check XOR counts of the involutory MDS matrices of the N_2 for all possible irreducible polynomials of degree 4 and 8 for $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ respectively. For $\mathbb{F}_{2^8}$, the minimum XOR count obtained for N_2 is $70 + 4 \cdot 3 \cdot 8$. On the other hand for $\mathbb{F}_{2^4}$, the minimum XOR count obtained for N_1 is $16 + 4 \cdot 3 \cdot 4$. The best known XOR count of 4×4 involutory MDS matrix over $\mathbb{F}_{2^4}$ was $24 + 4 \cdot 3 \cdot 4$ obtained by a search [20]. Therefore, we are actually improving the lower bound of XOR count of 4×4 involutory MDS matrix over $\mathbb{F}_{2^4}$ with a theoretical construction.

Below we give examples of 4×4 involutory MDS matrices with XOR counts $64 + 4 \cdot 3 \cdot 8$ and $16 + 4 \cdot 3 \cdot 4$ over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$ respectively.

Example 2. The matrix

$$\begin{bmatrix} 1 & \alpha & 1 & \alpha^{211} \\ \alpha & 1 & \alpha^{211} & 1 \\ \alpha^{-2} & \alpha^{209} & 1 & \alpha \\ \alpha^{209} & \alpha^{-2} & \alpha & 1 \end{bmatrix}$$

is involutory and MDS over $\mathbb{F}_{2^8}$, where α is a root of the irreducible polynomial $X^8 + X^6 + X^5 + X^2 + 1$. As XOR counts of $1, \alpha, \alpha^{-2}, \alpha^{209}$ and α^{211} are $0, 3, 6, 10$ and 10 respectively, so the XOR count of this matrix is $64 + 4 \cdot 3 \cdot 8$.

Example 3. The matrix

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & 1 \\ \alpha & 1 & 1 & \alpha^2 \\ \alpha^3 & \alpha & 1 & \alpha \\ \alpha & \alpha^3 & \alpha & 1 \end{bmatrix}$$

is involutory and MDS over $\mathbb{F}_{2^4}$, where α is a root of the irreducible polynomial $X^4 + X + 1$. Since the XOR counts of $1, \alpha, \alpha^2$ and α^3 are $0, 1, 2$ and 3 respectively. with XOR count $16 + 4 \cdot 3 \cdot 4$.

8 Summary

In this section, we summarize our findings, and compare with the previous results.

$\mathbb{F}_{2^8}$			
Irreducible polynomial	Reference	Matrix type	XOR Counts
$X^8 + X^7 + X^6 + X + 1$	Corollary 2	Toeplitz	$27 + 4 \cdot 3 \cdot 8$ (Minimum)
$X^8 + X^7 + X^6 + X + 1$	[20]	Hadamard	$52 + 4 \cdot 3 \cdot 8$
$X^8 + X^4 + X^3 + X^2 + 1$	[14]	serial/circulant	$36 + 4 \cdot 3 \cdot 8$
$X^8 + X^7 + X^6 + X + 1$	[16]	left-circulant	$32 + 4 \cdot 3 \cdot 8$
$\mathbb{F}_{2^4}$			
$X^4 + X^3 + 1$	Corollary 3	Toeplitz	$10 + 4 \cdot 3 \cdot 4$ (Minimum)
$X^4 + X + 1$	[20]	Hadamard	$20 + 4 \cdot 3 \cdot 4$
$X^4 + X + 1$	`LED` [9]	serial	$16 + 4 \cdot 3 \cdot 4$
$X^4 + X + 1$	[14]	serial/circulant	$12 + 4 \cdot 3 \cdot 4$

Table 1: Comparison of the minimum XOR count of 4×4 MDS matrices over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$ with the previous known values.

Table 1 shows that the minimum possible XOR count of a 4×4 MDS matrix over $\mathbb{F}_{2^8}$ is $27 + 4 \cdot 3 \cdot 8$ and over $\mathbb{F}_{2^4}$ is $10 + 4 \cdot 3 \cdot 4$, the previously known values are $32 + 4 \cdot 3 \cdot 8$ and $12 + 4 \cdot 3 \cdot 4$, respectively [16].

$\mathbb{F}_{2^8}$			
Irreducible polynomial	Reference	Matrix type	XOR Counts
$X^8+X^6+X^5+X^2+1$	Example 2	As in (14)	$64+4\cdot 3\cdot 8$
$X^8+X^6+X^5+X^2+1$	[20]	Hadamard	$64+4\cdot 3\cdot 8$
$X^8+X^4+X^3+X^2+1$	[2]	Hadamard	$88+4\cdot 3\cdot 8$
$X^8+X^4+X^3+X+1$	[7]	Compact Cauchy	$216+4\cdot 3\cdot 8$
$\mathbb{F}_{2^4}$			
X^4+X+1	Example 3	As in (14)	$16+4\cdot 3\cdot 4$
X^4+X+1	[20]	Hadamard	$24+4\cdot 3\cdot 4$
X^4+X^3+1	[13]	Hadamard	$24+4\cdot 3\cdot 4$

Table 2: Comparison of the XOR counts of 4×4 involutory MDS matrices over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$.

In Table 2, we compare the XOR counts of 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ that we obtain in this paper with the previously known lower bound. For $\mathbb{F}_{2^4}$ we present a new lower bound of XOR count of a 4×4 MDS involutory matrix which is $16+4\cdot 3\cdot 4$.

9 Conclusions

In this paper we have obtained the minimum values of XOR counts of 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. We have considered the polynomial basis as this is a conventional choice in practice. Moreover, as in [18] we already have seen that all the best MDS matrices were found under polynomial basis, we are not attempting other bases. It is unlikely to get lower values of XOR counts on other bases. The interesting finding is that MDS matrix with the minimum XOR count belongs to the class of Toeplitz matrices. As the first row and the first column defines a Toeplitz matrix, these are efficiently implementable in hardware, and thus the Toeplitz matrix that have the minimum XOR count becomes a suitable candidate for lightweight diffusion matrix. However, we must remind that as our proof shows that Toeplitz matrix cannot be both involutory and MDS, hence the lightweight diffusion layer that demands the both of these properties, Toeplitz matrices do not apply there.

We also have improved the lower bounds of XOR counts of involutory MDS matrices over $\mathbb{F}_{2^4}$, and provide theoretical constructions of a class of involutory MDS matrices which contains such a matrix. For $\mathbb{F}_{2^8}$, we have another construction of involutory MDS matrices that yields a matrix with the best known XOR count.

At this moment it looks difficult to determine the minimum value of XOR count of 8×8 matrices. However, by using a more involved strategy based on our search method, this might be doable. We leave it for the future research.

References

[1] S. Babbage and M. Dodd. The stream cipher MICKEY 2.0, 2006. http://www.ecrypt.eu.org/stream/mickeypf.html.

[2] P. S. L. M. Barreto and V. Rijmen. The Anubis block cipher, 2000. http://www.cryptonessie.org.

[3] P. S. L. M. Barreto and V. Rijmen. The Khazad Legacy-Level Block Cipher, 2000. http://www.cryptonessie.org.

[4] P. S. L. M. Barreto and V. Rijmen. Whirlpool. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd Ed.*, pages 1384–1385. Springer, 2011.

[5] C. Beierle, T. Kranz, and G. Leander. Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices. In M. Robshaw and J. Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 625–653. Springer, 2016.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[7] T. Cui, C. Jin, and Z. Kong. On compact cauchy matrices for substitution-permutation networks. *IEEE Transactions on Computers*, 64(7):2098–2102, July 2015.

[8] J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[9] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED Block Cipher. In B. Preneel and T. Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.

[10] K. C. Gupta and I. G. Ray. On constructions of circulant MDS matrices for lightweight cryptography. In X. Huang and J. Zhou, editors, *Information Security Practice and Experience - 10th International Conference, ISPEC 2014, Fuzhou, China, May 5-8, 2014. Proceedings*, volume 8434 of *Lecture Notes in Computer Science*, pages 564–576. Springer, 2014.

[11] M. Hell, T. Johansson, and W. Meier. Grain : a Stream Cipher for Constrained Environments. *Int. J. Wire. Mob. Comput.*, 2(1):86–93, May 2007.

[12] P. Junod and S. Vaudenay. Perfect diffusion primitives for block ciphers. In H. Handschuh and M. A. Hasan, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, volume 3357 of *Lecture Notes in Computer Science*, pages 84–99. Springer, 2004.

[13] E. Kavun, M. Lauridsen, G. Leander, C. Rechberger, P. Schwabe, and T. Yalc. PRØST v1.1. Submission to the CAESAR competition (2014).

[14] K. Khoo, T. Peyrin, A. Y. Poschmann, and H. Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In L. Batina and M. Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.

[15] Y. Li and M. Wang. On the construction of lightweight circulant involutory MDS matrices. In Peyrin [17], pages 121–139.

[16] M. Liu and S. M. Sim. Lightweight MDS generalized circulant matrices. In Peyrin [17], pages 101–120.

[17] T. Peyrin, editor. *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*. Springer, 2016.

[18] S. Sarkar and S. M. Sim. A deeper understanding of the XOR count distribution in the context of lightweight cryptography. In D. Pointcheval, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2016.

[19] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In A. Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[20] S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin. Lightweight MDS Involution Matrices. In G. Leander, editor, *Fast Software Encryption*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer Berlin Heidelberg, 2015.

[21] Y. Tian, G. Chen, and J. Li. On the Design of Trivium. Cryptology ePrint Archive, Report 2009/431, 2009. http://eprint.iacr.org/.

[22] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong. The simeck family of lightweight block ciphers. In T. Güneysu and H. Handschuh, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*, pages 307–329. Springer, 2015.

[23] A. Youssef, S. Mister, and S. Tavares. On the design of linear transformations for substitution permutation encryption networks. Workshop on Selected Areas in Cryptography (SAC 1997).

A Factorizations of the determinants in Proposition 3, Proposition 4, Proposition 10 and Proposition 11

A.1 Determinants in Proposition 3

We only factor the terms having degree > 4.

$$\begin{aligned}\Delta_2(\mathrm{T}_1(x)) &= \{x^2+1, x+1, (x^3+1)/x^2, (x+1)/x,\\ &\quad (x+1)/x^2, (x^4+1)/x^2, (\mathbf{x^5+1})/\mathbf{x^4}, (x^2+1)/x^2,\\ &\quad (\mathbf{x^6+1})/\mathbf{x^4}, (x^2+1)/x^4\}\\ &= \{x^2+1, x+1, (x^3+1)/x^2, (x+1)/x,\\ &\quad (x+1)/x^2, (x^4+1)/x^2, (\mathbf{x+1})(\mathbf{x^4+x^3+x^2+x+1})/\mathbf{x^4},\\ &\quad (x^2+1)/x^2, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^2+x+1})^{\mathbf{2}}/\mathbf{x^4}, (x^2+1)/x^4\}.\end{aligned}$$

$$\begin{aligned}\Delta_3(\mathrm{T}_1(x)) &= \{(\mathbf{x^8+x^4+x^2+1})/\mathbf{x^6}, (x^2+1)/x^2, x^2+1, (\mathbf{x^5+x^4+x^3+1})/\mathbf{x^4},\\ &\quad (x^2+1)/x^4, (\mathbf{x^5+x^4+x^3+1})/\mathbf{x^3}, (\mathbf{x^7+x^5+x^3+x^2+x+1})/\mathbf{x^4},\\ &\quad (\mathbf{x^5+x^2+x+1})/\mathbf{x^2}, (\mathbf{x^6+x^5+x^4+x^3+x^2+1})/\mathbf{x^4}, (\mathbf{x^6+1})/\mathbf{x^4}\}\\ &= \{(\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x^2+1})^{\mathbf{2}}/\mathbf{x^6}, (x^2+1)/x^2, x^2+1,\\ &\quad (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x^2+1})/\mathbf{x^4}, (x^2+1)/x^4, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x^2+1})/\mathbf{x^3},\\ &\quad (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^2+x+1})(\mathbf{x^3+x^2+1})/\mathbf{x^4}, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x+1})/\mathbf{x^2},\\ &\quad (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^4+x^3+1})/\mathbf{x^4}, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^2+x+1})^{\mathbf{2}}/\mathbf{x^4}\}.\end{aligned}$$

A.2 Determinants in Proposition 4

We only factor the terms having degree > 3.

$$\begin{aligned}\Delta_2(\mathrm{T}_2)(x) &= \{(x^3+1)/x^2, (x^2+1)/x, (x+1)/x^2, (x+1)/x,\\ &\quad 1+x, (x^3+1)/x, (x^3+1)/x^4, (x^3+1)/x^3, (x^2+1)/x^2,\\ &\quad (\mathbf{x^4+1})/\mathbf{x^3}, (\mathbf{x^4+1})/\mathbf{x^4}\}\\ &= \{(x^3+1)/x^2, (x^2+1)/x, (x+1)/x^2, (x+1)/x,\\ &\quad 1+x, (x^3+1)/x, (x^3+1)/x^4, (x^3+1)/x^3, (x^2+1)/x^2,\\ &\quad (\mathbf{x+1})^{\mathbf{4}}/\mathbf{x^3}, (\mathbf{x+1})^{\mathbf{4}}/\mathbf{x^4}\}.\end{aligned}$$

$$\begin{aligned}\Delta_3(\mathrm{T}_2)(x) &= \{\,(x^2+1)/x^3, (x^2+1)/x^4, (\mathbf{x^4+1})/\mathbf{x^3}, (\mathbf{x^6+x^5+x^3+1})/\mathbf{x^5},\\ &\quad (\mathbf{x^6+x^5+x^3+1})/\mathbf{x^6}, (\mathbf{x^5+x^4+x^3+1})/\mathbf{x^3},\\ &\quad (\mathbf{x^5+x^4+x^3+1})/\mathbf{x^4}\}\\ &= \{\,(x^2+1)/x^3, (x^2+1)/x^4, (\mathbf{x+1})^{\mathbf{4}}/\mathbf{x^3}, (\mathbf{x+1})^{\mathbf{3}}(\mathbf{x^3+x+1})/\mathbf{x^5},\\ &\quad (\mathbf{x+1})^{\mathbf{3}}(\mathbf{x^3+x+1})/\mathbf{x^6}, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x^2+1})/\mathbf{x^3},\\ &\quad (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x^2+1})/\mathbf{x^4}\}.\end{aligned}$$

A.3 Determinants in Proposition 10

We only factor terms with degree > 3.

$$\begin{aligned}\Delta_2(\mathrm{N}_1(x)) &= \{x^2+1, (x^2+1)/x^2, x^2+x+1, x^3+x+1, 1/x^2, 1, x^4,\\ &\quad (x^3+x^2+1)/x^2, (\mathbf{x^4+1})/\mathbf{x^2}, (\mathbf{x^4+x^2+1})/\mathbf{x^2},\\ &\quad (x^3+x+1)/x^2, (x^2+x+1)/x^2\}\\ &= \{x^2+1, (x^2+1)/x^2, x^2+x+1, x^3+x+1, 1/x^2, 1, x^4,\\ &\quad (x^3+x^2+1)/x^2, (\mathbf{x+1})^{\mathbf{4}}/\mathbf{x^2}, (\mathbf{x^2+x+1})^{\mathbf{2}}/\mathbf{x^2},\\ &\quad (x^3+x+1)/x^2, (x^2+x+1)/x^2\}.\end{aligned}$$

A.4 Determinants in Proposition 11

We only factor terms with degree > 3.

$$\begin{aligned}\Delta_2(\mathrm{N}_2(x)) &= \{x^2+1, \mathbf{x^4+x^3+x+1}, \mathbf{x^4+x^2}, x^2+x+1, x^3+x+1,\\ &\quad \mathbf{x^4+x^2+1}, \mathbf{x^5+x^2+x+1}, x^4, x^3+x^2+x+1, x^2,\\ &\quad \mathbf{x^6+x^4+x^2+1}\}\\ &= \{x^2+1, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^2+x+1}), (\mathbf{x^2+x})^{\mathbf{2}}, x^2+x+1, x^3+x+1,\\ &\quad (\mathbf{x^2+x+1})^{\mathbf{2}}, (\mathbf{x+1})^{\mathbf{2}}(\mathbf{x^3+x+1}), x^4, x^3+x^2+x+1, x^2,\\ &\quad (\mathbf{x+1})^{\mathbf{6}}\}.\end{aligned}$$