Analysis of Toeplitz MDS Matrices

Sumanta Sarkar and Habeeb Syed

TCS Innovation Labs
Hyderabad, INDIA
Sumanta.Sarkar1@tcs.com Habeeb.Syed@tcs.com

Abstract. This work considers the problem of constructing efficient MDS matrices over the field $\mathbb{F}_{2^m}$. Efficiency is measured by the metric XOR count which was introduced by Khoo et al. in CHES 2014. Recently Sarkar and Syed (ToSC Vol. 1, 2016) have shown the existence of 4×4 Toeplitz MDS matrices with optimal XOR counts. In this paper, we present some characterizations of Toeplitz matrices in light of MDS property. Our study leads to improving the known bounds of XOR counts of 8×8 MDS matrices by obtaining Toeplitz MDS matrices with lower XOR counts over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$.

Keywords: Toeplitz matrix, MDS matrix, XOR count, lightweight block cipher, diffusion layer.

1 Introduction

Internet of Things (IoT) is a network of interconnected devices that can share data with each other and process when required. IoT applications range from health monitoring and traffic management to several other daily life activities; this is one of the reasons that it also has drawn attention from the industry. The devices used in IoT are mostly RFIDs and sensors, which have very low resources. Thus for ensuring privacy and confidentiality of the data in IoT, classical cryptosystems like AES, RSA are not suitable. To bridge this gap the topic lightweight cryptography has emerged. Lightweight cryptography is mostly based on symmetric key. The eSTREAM finalists `Grain` v1 [7], `MICKEY` 2.0 [1], and `Trivium` [18] are examples of lightweight stream ciphers. `CLEFIA` [16], `PRESENT` [5], `PRINCE` [6] are some of the existing lightweight block ciphers.

In this paper we are interested in lightweight block ciphers. Confusion and diffusion layers are the two important building blocks of a block cipher. While confusion layer is responsible for making the relation between key and ciphertext as complex as possible, the diffusion layer spreads the plaintext statistics through the ciphertext. Maximum distance separable (MDS) matrices are a popular choice to build diffusion layer as these matrices achieve the maximum diffusion power. However, constructing an MDS matrix with low implementation cost (as to suit lightweight cryptosystems) is a nontrivial task.

In CHES 2014, [9] introduced the metric XOR count that measures the cost of implementation of a diffusion matrix. A matrix filled with field elements having low Hamming weight may not necessarily result in low hardware cost for the implementation of the matrix, which was shown in [9]. This paper 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. Then several works [17, 14, 11, 10, 15] followed to find MDS matrices with low XOR counts. Search effort 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. Recently [15] settled the question of the minimum XOR counts of 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. They showed that matrices achieving the minimum XOR count exist in the class of Toeplitz matrices. This motivates us to study Toeplitz MDS matrices further and analyze several properties of such matrices.

Our Contributions Since a Toeplitz MDS matrix cannot be involutory [15], there is no scope of getting involutory MDS matrices in the class of Toeplitz matrices. In this work we restrict our study to MDS matrices only. In a Toeplitz matrix, several submatrices repeat. We count the number of distinct $d \times d$, $(1 \leq d \leq n)$ submatrices in Proposition 1; later Theorem 1 shows how many of these distinct submatrices are indeed Toeplitz. One can take the advantage of this redundancy while checking the MDS property of a Toeplitz matrix (see Remark 1). We also study Toeplitz matrices in the class of Cauchy matrices, and prove that a Cauchy-Toeplitz matrix cannot be MDS for dimension greater than 2.

In Section 4, we improve the XOR count of 8×8 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. As the class of all MDS 8×8 matrix is huge, we search in the subclass formed by the Toeplitz matrices. However, it is not easy to exhaust the full class of Toeplitz matrices for these fields. We develop a pruning based search algorithm which enables us to find Toeplitz MDS matrices with lower XOR counts. For $\mathbb{F}_{2^4}$ the lowest XOR count that we obtain is $170 + 8 \cdot 7 \cdot 4$ (earlier known value was $208 + 8 \cdot 7 \cdot 4$), whereas for $\mathbb{F}_{2^8}$ the improved XOR count is $232 + 8 \cdot 7 \cdot 8$ (earlier known value was $240 + 8 \cdot 7 \cdot 8$). Thus we improve the bounds of XOR counts of 8×8 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$.

2 Preliminaries

We denote by $\mathbb{F}_{2^m}$ the finite field with 2^m elements, and by $\mathbb{F}_2^m$ we denote the m-dimensional vector space over $\mathbb{F}_2$. MDS codes are the class of linear codes over the field $\mathbb{F}_{2^m}$ that achieve the Singleton bound, that is for an $[N, K]$ MDS code the minimum distance is $N - K + 1$. An $n \times n$ matrix M over $\mathbb{F}_{2^m}$ is MDS if the $n \times 2n$ matrix $G = [I_n \, M]$ is a generator of a $[2n, n]$ MDS code, where I_n is the $n \times n$ identity matrix. Another characterization of MDS matrices is as follows: M is MDS if and only if every submatrix of M is nonsingular. For details on this

one may consult [12]. MDS matrices are popular choice for building diffusion layers of block ciphers, as they attain the maximum diffusion power.

2.1 XOR Counts

The field $\mathbb{F}_{2^m}$ can be identified to the vector space $\mathbb{F}_2^m$, by choosing some basis. There are several kinds of bases for a finite fields, and the mostly used one is the polynomial basis of the form $\{1, \alpha, \ldots, \alpha^{m-1}\}$. To measure the implementation cost of field multiplication [9] proposed the metric XOR count defined as follows.

Definition 1. *Let $P(X)$ be an irreducible polynomial that defines $\mathbb{F}_{2^m}$ and let $\mathcal{B}$ be a basis of $\mathbb{F}_{2^m}$. The XOR count of an element $a \in \mathbb{F}_{2^m}$ with respect to $\mathcal{B}$ is the number of XORs required to implement the multiplication of a with an arbitrary element $b \in \mathbb{F}_{2^m}$. We denote by XOR(a) the XOR count of a.*

Note that XOR$(0) = 0 =$ XOR(1). It is mentioned in [9] that low XOR count is strongly correlated to the minimization of hardware area (GE). Thus finding MDS matrices with low XOR count is an active research topic in the context of lightweight cryptography. The set of XOR counts of all the elements of $\mathbb{F}_{2^m}$ is termed as the XOR count distribution which depends on $P(X)$ and $\mathcal{B}$ [17, 14]. Note that polynomial basis is a conventional choice for implementation and as noted in [15], we will only be considering polynomial basis. Recently [4] has relooked at XOR count of an element and allowed reuse of repeating terms in the product vector. However, we do not consider such optimization and regard XOR count in its simplified form as given by [9] and many subsequent works [17, 14, 15].

In [9] the formula for the XOR count of a row of a matrix was derived, later [15] extended it to the full $n \times n$ matrix M defined over $\mathbb{F}_{2^m}$ as

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

where γ_{ij} is the XOR count of the j-th entry of the i-th row of the matrix, and ℓ_i is the number of nonzero entries in that row. 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 $C(M) + n \cdot (n-1) \cdot m$, and $C(M)$ is the part that varies with the matrices.

3 Toeplitz MDS Matrices

In this section we study Toeplitz MDS matrices in details.

Definition 2. *A matrix is called Toeplitz if every descending diagonal from left to right is constant.*

The following is the general form of an $n \times n$ Toeplitz matrix.

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

A Toeplitz matrix is defined by its first row and first column, henceforth we will use

$$\texttt{Toep}(a_0, a_1, \dots, a_{n-1}, a_{-1}, a_{-2}, \dots, a_{-(n-1)}) \tag{3}$$

to describe an $n \times n$ Toeplitz matrix of the form (2). This matrix can also be defined as follows:

$$\mathrm{T} = [m_{i,j}], \quad \text{where} \quad m_{i,j} = a_{j-i}. \tag{4}$$

3.1 Properties of a Toeplitz Matrix

To check the MDS property of an $n \times n$ matrix, one has to check if all the submatrices are nonsingular. The total number of such submatrices are $\sum_{i=1}^{n} \binom{n}{i}^2$. However, it is easy to see that in a Toeplitz matrix several sub matrices are duplicates and hence can be ignored while checking MDS property. In this section we compute the number of distinct submatrices of a Toeplitz matrix. Following is a result in this regard proof of which is given in Appendix A.

Lemma 1. *Suppose T is a Toeplitz matrix as given in* (2)*. Every $d \times d$ submatrix of T is equal to a $d \times d$ submatrix T_{sub} such that*

1. *the first row of T_{sub} belongs to the first row of T. Or,*
2. *the first column of T_{sub} belongs to the first column of T.*

Example 1. Consider the following 4×4 Toeplitz matrix T.

$$T = \begin{bmatrix} \boxed{a_0} & a_1 & \boxed{a_2} & a_3 \\ a_{-1} & \textcircled{a_0} & a_1 & \textcircled{a_2} \\ \boxed{a_{-2}} & a_{-1} & \boxed{a_0} & a_1 \\ a_3 & \textcircled{a_{-2}} & a_{-1} & \textcircled{a_0} \end{bmatrix}.$$

The 2×2 submatrix formed by the 2nd and 4th row, and 2nd and 4th column (marked by circles) is equal to the 2×2 submatrix formed by the 1st and 3rd row, and 1st and 3rd column (marked by rectangles).

Let us now count the number of distinct submatrices of a Toeplitz matrices considering that all the a_i's are distinct.

Proposition 1. *Let $T = \texttt{Toep}(a_0, \dots, a_{-(n-1)})$ be a Toeplitz matrix in which all a_i's are distinct. Then the number of distinct $d \times d$ submatrices is*

$$\binom{n-1}{d-1}^2 + 2\binom{n-1}{d-1}\binom{n-1}{d} = \binom{n-1}{d-1}^2 \left(\frac{2n-d}{d}\right). \tag{5}$$

Consequently, the total number of distinct submatrices are

$$\binom{2n-2}{n-1} + 2\binom{2n-2}{n-2}. \tag{6}$$

Proof. We will count the distinct submatrices as per Lemma 1, i.e., submatrices having elements from the first row or first column. Let $T[0,0]$ be the $(0,0)$-th element of T. We count the number of submatrices with and without $T[0,0]$ separately.

Case 1: When $T[0,0]$ is absent. In this case there are two kinds of submatrices: submatrices that have elements from the first row, but not from the first column, or submatrices that have elements from the first column, but not from the first row. The number of distinct $d \times d$ submatrices that have elements from the first row is $\binom{n-1}{d-1}\binom{n-1}{d}$, and the number of submatrices that have elements from the first column is $\binom{n-1}{d-1}\binom{n-1}{d}$.

Case 2: When $T[0,0]$ is present. In this case the number of distinct $d \times d$ submatrices is $\binom{n-1}{d-1}\binom{n-1}{d-1}$.

Now adding the above two counts we get the number of distinct $d \times d$ submatrices as (5).

Further note that for any positive integer t, $\sum_{i=0}^{t}\binom{t}{i}^2 = \binom{2t}{t}$ and $\sum_{i=0}^{t-1}\binom{t}{i}\binom{t}{i+1} = \binom{2t}{t} + \binom{2t}{t-1}$. Using these, the total number of distinct submatrices is obtained as

$$\sum_{d=1}^{n}\binom{n-1}{d-1}^2 + 2\sum_{d=1}^{n}\binom{n-1}{d-1}\binom{n-1}{d} = \binom{2n-2}{n-1} + 2\binom{2n-2}{n-2}.$$

□

Note that a submatrix of a Toeplitz matrix could also be Toeplitz. Denote by $\texttt{Row}(S) = (i_0, \ldots, i_{d-1})$, the ordered set of row indices of S and $\texttt{Col}(S) = (j_0, \ldots, j_{d-1})$ ordered set of column indices of S. We now present a characterization of a submatrix of a Toeplitz matrix to be Toeplitz also.

Proposition 2. *Let $T = \texttt{Toep}(a_0, \ldots, a_{-(n-1)})$ be a Toeplitz matrix in which all a_i's are distinct and S be a $d \times d$ submatrix of T for some $2 \le d \le n-1$. Then S is Toeplitz if and only if $\texttt{Row}(S) = (i_0, \ldots, i_{d-1})$, and $\texttt{Col}(S) = (j_0, \ldots, j_{d-1})$ satisfy*

$$i_{k+1} - i_k = j_{k+1} - j_k = \rho, \qquad k = 0, \ldots, d-2 \tag{7}$$

for some integer ρ such that

$$1 \le \rho \le \left\lfloor \frac{n-1}{d-1} \right\rfloor. \tag{8}$$

Proof. Recall that a square matrix $X = [x_{ij}]$ of order n is Toeplitz if and only if for all $0 \le i, j \le n-2$

$$x_{i,j} = x_{i+\theta, j+\theta}$$

for every $\theta \ge 1$ is such that $\max\{i+\theta, j+\theta\} \le n-1$. Now let's prove the lemma. Suppose that S is a $d \times d$ submatrix of T such that $\texttt{Row}(S)$ and $\texttt{Col}(S)$ satisfy

(7) with ρ as in (8). This implies that for any $i_k \in \texttt{Row}(S), j_t \in \texttt{Col}(S), 0 \leq k, t \leq d-2$ we have

$$S_{i_k,j_t} = T_{i_k,j_t} = T_{i_k+\theta,j_t+\theta} = S_{i_k+\theta,j_t+\theta}$$

as S is a submatrix of T which is a Toeplitz matrix. This shows that S is Toeplitz and hence the sufficiency part. Let us prove the necessary part. Suppose S is a $d \times d$ Toeplitz submatrix of T for some $2 \leq d \leq n-1$, then we show that $\texttt{Row}(S), \texttt{Col}(S)$ satisfy (7) with ρ as in (8). Observe that since (by hypothesis) all the elements of first row and column of T are distinct, it follows from the definition of a Toeplitz matrix that for any $0 \leq i, j, i', j' \leq n-1$,

$$T_{i,j} = T_{i',j'} \quad \text{if and only if} \quad j - i = j' - i'. \tag{9}$$

Using this in case of S (which is a Toeplitz submatrix), we have for every element of $\texttt{Row}(S)$, $\texttt{Col}(S)$

$$i_k - j_k = i_{k-1} - j_{k-1} \quad \Longrightarrow \quad i_k - i_{k-1} = j_k - j_{k-1},$$

which proves (7). Next suppose $\rho = i_k - i_{k-1}$ then the condition (8) is necessary to make sure that none of the indices of S grows bigger than indices of T. From (7) it follows that

$$i_{d-1} = i_{d-2} + \rho = \ldots = i_0 + \rho\,(d-1). \tag{10}$$

Using the facts $2 \leq d \leq (n-1)$, $\rho \geq 1$, and $1 \leq i_{d-1} \leq n-1$ in (10) we get

$$1 \leq 0 + \rho\,(d-1) \leq (n-1) \quad \Longrightarrow \quad 1 \leq \rho \leq \left\lfloor \frac{n-1}{d-1} \right\rfloor.$$

□

In the following we count the number of $d \times d$ Toeplitz submatrices of an $n \times n$ Toeplitz matrix.

Theorem 1. *Let T be an $n \times n$ Toeplitz matrix as given in* (2) *in which all the elements of first row and first column are distinct. Then the number of distinct $d \times d$ Toeplitz submatrices are*

$$\delta_{d,n} = \begin{cases} 2n-1 & \text{if } d = 1 \\ (n - d + \tau_{d,n} + 1) \cdot \lfloor \frac{n-1}{d-1} \rfloor & \text{if } d = 2, \ldots, n \end{cases}, \tag{11}$$

where $\tau_{d,n}$ is given by $n - 1 = \lfloor \frac{n-1}{d-1} \rfloor (d-1) + \tau_{d,n}$.

Proof. Suppose S is a $d \times d$ a submatrix of T with $\texttt{Row}(S) = (i_0, \ldots, i_{d-1})$ and $\texttt{Col}(S) = (j_0, \ldots, j_{d-1})$. Let

$$\Gamma = \underbrace{\sum_{\theta=1}^{\lfloor \frac{n-1}{d-1} \rfloor} n - \theta\,(d-1)}_{(*)} + \underbrace{\sum_{\theta=1}^{\lfloor \frac{n-2}{d-1} \rfloor} (n-1) - \theta\,(d-1)}_{(**)}. \tag{12}$$

We will show that the distinct $d \times d$ Toeplitz submatrices of an $n \times n$ Toeplitz matrix T is given by Γ as in (12) and this simplifies to (11). To count distinct submatrices S we use Proposition 1 and consider only those submatrices S for which

$$(i_0 = 0) \text{ or } (i_0 > 0 \text{ and } j_0 = 0),$$

and for each case we count the exact number of Toeplitz submatrices using conditions of Proposition 2 which put together gives (11).

Case 1: When $i_0 = 0$.

This gives the term (*) in (12). In this case for every ρ satisfying (8), the only possibility for $\texttt{Row}(S)$ is $\texttt{Row}(S) = (0, \rho, \ldots, \rho\,(d-1))$. For every such possible $\texttt{Row}(S)$, the number of possibilities for $\texttt{Col}(S) = (j_0, \ldots, j_{d-1})$ satisfying (7) is $n - \rho\,(d-1)$. Varying ρ from 1 to $\lfloor \frac{n-1}{d-1} \rfloor$ and summing all the terms we get (*) in (12)

Case 2: When $i_0 > 0,$ and $j_0 = 0$

Let ρ_0 be a value of ρ satisfying (8). One can choose $\texttt{Row}(S) = (i_0, \ldots, i_{d-1})$ satisfying (7) for $\rho = \rho_0$ in exactly $(n-1) - \rho\,(d-1)$ ways. For every such chosen $\texttt{Row}(S)$ there exits a unique value $\texttt{Col}(S) = (0, j_1, \ldots, j_{d-1})$ (satisfying (7) for $\rho = \rho_0$) which together give a Toeplitz matrix S. Since $i_0 > 0$ total number of available rows is only $n-1$ and hence the total number of Toeplitz submatrices which do not involve 0 can be obtained by by adding the quantity $[(n-1) - \rho\,(d-1)]$ for $\rho = 1$ to $\lfloor \frac{n-2}{d-1} \rfloor$ we obtain (**) in (12).

To complete the proof we need to show that Γ in (12) simplifies to (11). This can be easily shown by considering the two cases $\tau_{d,n} > 0$ and $\tau_{d,n} = 0$ separately. □

Using this result, we compare the number of distinct submatrices of Toeplitz and general matrices in Table 2 in Appendix B.

Remark 1. Given an $n \times n$ matrix, to check the MDS property one needs to verify whether all the $\sum_{i=1}^{n} \binom{n}{i}^2 = \binom{2n}{n} - 1$ square submatrices are nonsingular. However, as we see in Lemma 1 that there are too many redundancies in a Toeplitz matrix, so we need to consider fewer submatrices as opposed to a general matrix. By Proposition 1, we need to consider $\binom{2n-2}{n-1} + 2\binom{2n-2}{n-2}$ submatrices in total for an $n \times n$ Toeplitz matrix.

3.2 Cauchy-Toeplitz Matrices

Cauchy matrices are interesting in the sense that it is easy to construct MDS matrices in this class. A Cauchy matrix over $\mathbb{F}_{2^m}$ is of the form

$$M = [a_{i,j}]_{n \times n}, \text{ where } a_{i,j} = \frac{1}{x_i + y_j}, \quad x_i \neq y_j, \quad 0 \leq i, j \leq n-1. \tag{13}$$

Fact 1 *The Cauchy matrix M is nonsingular if and only if $x_i \neq x_j$ and $y_i \neq y_j$, for all* $0 \leq i, j \leq n-1$.

There have been constructions of MDS matrices which are both Hadamard and Cauchy (see [17] for example). We now analyze the MDS property of matrices which are both Toeplitz and Cauchy. We call matrices which are both Toeplitz and Cauchy as Cauchy-Toeplitz. Example of such a matrix is given in Example 2 in Appendix A.

Theorem 2. *Let T be a $n \times n$ Cauchy-Toeplitz matrix over $\mathbb{F}_{2^m}$. Then the following hold.*

1. *T is symmetric.*
2. *T is singular if $n \geq 3$, and thus T is not MDS if $n \geq 3$.*

Proof. As T is Toeplitz, we must have $T_{i,i} = T_{j,j}$. Then

$$\frac{1}{x_i + y_i} = \frac{1}{x_j + y_j} \Longrightarrow \frac{1}{x_i + y_j} = \frac{1}{x_j + y_i},$$

that is $T_{i,j} = T_{j,i}$. So T is symmetric.
Next we prove that T is singular whenever $n \geq 3$. Consider a 3×3 Cauchy matrix

$$T_3 = \begin{bmatrix} \frac{1}{x_0+y_0} & \frac{1}{x_0+y_1} & \frac{1}{x_0+y_2} \\ \frac{1}{x_1+y_0} & \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} \\ \frac{1}{x_2+y_0} & \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} \end{bmatrix}.$$

By the definition of Cauchy matrix $x_i \neq y_j$ for $i, j = 0, 1, 2$ and from Fact 1 it follows that T_3 is nonsingular if and only if

$$x_i \neq x_j \quad \text{and} \quad y_i \neq y_j \quad \text{for } 0 \leq i < j \leq 2. \tag{14}$$

Suppose that T_3 is Toeplitz, then by Definition 2 we have the following.

$$\begin{aligned} x_0 + y_0 = x_1 + y_1 = x_2 + y_2 = C_0 \\ x_0 + y_1 = x_1 + y_2 = C_1 \\ x_1 + y_0 = x_2 + y_1 = C_2, \end{aligned} \tag{15}$$

for some C_0, C_1 and C_2 in $\mathbb{F}_{2^m}$. As it was proved above that T_3 is symmetric, $C_1 = C_2$ must hold. Using this in (15) we get $x_2 + y_1 = C_1$, and we also have $x_0 + y_1 = C_1$, which together imply $x_0 = x_2$. Then from (14) it follows that T_3 is singular matrix.

Next, for $n > 3$, consider an $n \times n$ Cauchy-Toeplitz matrix T defined by the elements $(x_0, \ldots, x_{n-1})$ and $(y_0, \ldots, y_{n-1})$ of $\mathbb{F}_{2^m}$. Denote by T' the 3×3 submatrix of T consisting of first three rows and columns. Then T' is a Cauchy-Toeplitz matrix defined by the elements (x_0, x_1, x_2) and (y_0, y_1, y_2), and we just proved that $x_0 = x_2$. Consequently using Fact 1 it follows that T is singular. This also shows that T is not MDS. □

3.3 More Classes of Non-MDS Toeplitz Matrices

We now propose a characterization of Toeplitz matrices that are not MDS. Proofs of these lemmas can be found in Appendix A.

Lemma 2. *The $n \times n$ Toeplitz matrix T as given in (2) is not MDS if for some $i < j$ such that $i + j \leq n - 1$, $a_i = a_j$ and $a_{-i} = a_{-j}$ hold.*

Lemma 3. *The maximum number of occurrences of an element $\beta \in \mathbb{F}_{2^m}$ in a 8×8 MDS matrix is 24.*

4 Searching for MDS Matrices with Low XOR Count

In [15], authors have searched efficiently in the class of 4×4 MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ to obtain the least possible XOR count. However, the space of 8×8 MDS matrices is so vast that it is difficult to exhaust. In this section we search in the class of Toeplitz matrices as 4×4 MDS matrices with the optimal XOR counts in this class [15]. However, the class of 8×8 Toeplitz matrices is also large enough that searching for an improved matrix becomes a challenging task. To tackle this we apply a pruning strategy so that we get search results faster. First we form a search tree as follows.

Forming a Search Tree
A 8×8 Toeplitz matrix T can be defined as $T = \texttt{Toep}(a_0, \ldots, a_7, a_8, \ldots, a_{14})$. From (1) we have that for any 8×8 matrix M, over $\mathbb{F}_{2^m}$ the sum of XOR counts of all the elements of M is $C(M)$. We define $\texttt{C}$ as the lowest known value of $C(M)$. If we find a Toeplitz MDS matrix T such that

$$C(T) = \sum_{i=0, i\neq 7}^{13} (8 - (i \mod 7))\text{XOR}(a_i) + \text{XOR}(a_7) + \text{XOR}(a_{14}) < \texttt{C}, \quad (16)$$

we obtain a new MDS matrix with lower XOR count.

Suppose the matrix is defined over the set $U \subseteq \mathbb{F}_{2^m}$. Then every a_i has $|U|$ options to choose from. So the naive search complexity is $|U|^{15}$. Given a_i, for $i = 0, \ldots, 13$, next a_{i+1} will be one of $|U|$ choices, that is, we can view this as a tree where every node has $|U|$ children. As a_0 itself has $|U|$ choices, there will be $|U|$ such trees. Traveling from the root to a leaf will give us one tuple $(a_0, \ldots, a_7, a_8, \ldots, a_{14})$. If $\texttt{Toep}(a_0, \ldots, a_7, a_8, \ldots, a_{14})$ is MDS, and it also satisfies (16), we get an improved MDS matrix with respect to XOR count. However, if we see that for a choice of a_i, the tuple $(a_0, \ldots, a_i)$ cannot be a part of any $(a_0, \ldots, a_7, a_8, \ldots, a_{14})$ such that $\texttt{Toep}(a_0, \ldots, a_7, a_8, \ldots, a_{14})$ is not MDS or does not satisfy (16), then we can prune the whole subtree rooted at that a_i, as $\texttt{Toep}(a_0, \ldots, a_7, a_8, \ldots, a_{14})$ will not improve $\texttt{C}$ for such a choice of a_i. Next we discuss in detail the pruning criteria which we call as E1, E2, E3 and E4 .

E1: Occurrence of an element is more than 24 times

Suppose we are at the i-th level, that is with the subtuple $(a_0, \ldots, a_i)$. With this we have a submatrix where each a_r, $0 \leq r \leq i$ occurs $8 - (r \mod 7)$ times if $r \leq 13$ and only once if $r = 14$. We count the number of occurrences of the value of a_i in this submatrix, and if a_i occurs more than 24 times, then by Lemma 3, $(a_0, \ldots, a_i)$ cannot be a part of any Toeplitz MDS matrix $\texttt{Toep}(a_0, \ldots, a_i, \ldots, a_{14})$. So we prune the subtree rooted at this value of a_i, and switch to the next sibling. Figure 1 in Appendix B describes one such scenario.

E2: XOR count of the submatrix $\geq$ C
First we sort U in ascending order with respect to XOR counts of its elements. Now suppose that we are at the subtuple $(a_0, \ldots, a_i)$ and if

$$\begin{aligned} &\sum_{r=0}^{i}(8 - (r \mod 7))\mathrm{XOR}\,(a_r) \geq \texttt{C}, \quad \text{for } i < 14, \text{ or} \\ &\sum_{r=0}^{13}(8 - (r \mod 7))\mathrm{XOR}\,(a_r) + \mathrm{XOR}\,(a_{14}) \geq \texttt{C}, \quad \text{for } i = 14 \end{aligned} \tag{17}$$

holds, then for the current value of a_i, $(a_0, \ldots, a_i)$ cannot be a part of any Toeplitz matrix $\texttt{Toep}(a_0, \ldots, a_i, \ldots, a_{14}), (a_i \neq 0, \forall i)$ whose XOR count is $< \texttt{C}$. Since a_i takes values from U which is sorted in increasing order, then all the next siblings will have equal or higher XOR counts, so they will also satisfy (17). Hence we prune the subtree rooted at the current value of a_i and all the other possible subtrees rooted at its next siblings having higher XOR counts. So we move back to a_{i-1} and update it by a new value from U. Figure 2 describes one such scenario.

E3: Submatrices satisfying Lemma 2
Suppose we are with a subtuple $(a_0, \ldots, a_7, \ldots, a_i)$. That is we are now dealing with a $(i - 6) \times 8$ Toeplitz submatrix. If $(a_0, \ldots, a_i)$ is such that the condition stated in Lemma 2 is satisfied, then $(a_0, \ldots, a_7, \ldots, a_i)$ cannot be a part of any Toeplitz MDS matrix defined $(a_0, \ldots, a_i, \ldots, a_{14})$. So we prune the subtree rooted at this value of a_i, and switch to the next sibling.

E4: One submatrix is singular
When we are dealing with a $(i - 6) \times 8$ Toeplitz submatrix T' formed by $(a_0, \ldots, a_7, \ldots, a_i)$, if one of the submatrices of T' is singular, then we prune the subtree rooted at a_i's current value, and replace it by a new value.

Finally when we land up having a tuple $(a_0, \ldots, a_{14})$ which has survived all the pruning criteria E1, E2, E3, E4 at every level, then we obtain a Toeplitz MDS matrix $T = \texttt{Toep}(a_0, \ldots, a_{14})$ with lower XOR count than C. Next we replace $\texttt{C} = C(T)$, and continue the search.

5 MDS Matrices over $\mathbb{F}_{2^4}$ with Improved XOR Count

Using the above mentioned search method we now search for 8×8 Toeplitz MDS matrices over $\mathbb{F}_{2^4}$. The lowest known XOR count of 8×8 MDS matrix is $208 + 7 \cdot 4 \cdot 8$ as reported in [17]. So we set $\mathtt{C} = 208$, and we look for Toeplitz MDS matrices over $\mathbb{F}_{2^4}$ with $C(T) < \mathtt{C}$. We consider $\mathbb{F}_{2^4}$ defined by primitive polynomial $X^4 + X + 1$ whose primitive element is denoted by α. We select $U = \mathbb{F}_{2^4}^*$ that is sorted in ascending order according to the XOR counts of its elements, $U = \{1, \alpha, \alpha^{14}, \alpha^2, \alpha^3, \alpha^{13}, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^{12}, \alpha^9, \alpha^{11}, \alpha^{10}\}$. The corresponding XOR counts are $\{0, 1, 1, 2, 3, 3, 5, 5, 5, 6, 6, 6, 8, 8, 9\}$. We apply our search strategy and obtain improved matrices. In fact we obtain several matrices T with $C(T) < 208$, we mention a matrix with least one. The matrix

$$\mathtt{Toep}(\alpha^1, 1, \alpha^4, 1, \alpha^5, \alpha^{14}, \alpha^7, \alpha^8, \alpha^3, \alpha^6, \alpha^{14}, \alpha^{14}, \alpha^8, \alpha^6, \alpha^3) \tag{18}$$

has XOR count $170 + 7 \cdot 4 \cdot 8$.

The naive search would require to consider $15^{15} = 2^{59}$ elements of $\mathbb{F}_{2^4}$. As our search is applying pruning, thus it ends up considering only

$$22275827417 \approx 2^{35}$$

possible $\mathbb{F}_{2^4}$ elements for the a_i's in total. This explains the effectiveness of our search strategy. As it is observed by [17] that change of irreducible polynomial has effect on the XOR count, so we consider other irreducible polynomials that define $\mathbb{F}_{2^4}$. Note that $X^4+X^3+X^2+X+1$ is the only such irreducible polynomial apart from $X^4 + X + 1$ up to reciprocal. However, we do not find any better matrix under this irreducible polynomial.

6 MDS Matrices over $\mathbb{F}_{2^8}$ with Lower XOR Count

Next we apply the same search strategy to obtain 8×8 Toeplitz MDS matrices over $\mathbb{F}_{2^8}$. The best known MDS matrix is reported in [11], which is a circulant matrix that has XOR count $240+8\cdot7\cdot8$. We consider $\mathbb{F}_{2^8}$ defined by the primitive polynomial $X^8 + X^7 + X^6 + X + 1$. We take Toeplitz matrices over a subset $U \subset \mathbb{F}_{2^8}$ of 15 elements[1], and sort it according to the XOR counts of the elements in increasing order. Precisely $U = \{x : \mathrm{XOR}(x) \leq 10\}$. In this case $|U| = 11$. Our search begins with $\mathtt{C} = 240$. When the search completes the lowest XOR count of Toeplitz MDS matrix that we obtain is $232 + 8 \cdot 7 \cdot 8$, example of such a matrix is

$$\mathtt{Toep}(1, 1, \alpha, \alpha^{253}, 1, \alpha^{253}, \alpha^{252}, \alpha^{157}, \alpha^{158}, \alpha^{253}, \alpha^{254}, \alpha, \alpha^{254}, \alpha^2, \alpha). \tag{19}$$

As $|U| = 11$, the naive search would require to consider $11^{15} = 2^{43}$ elements from $\mathbb{F}_{2^8}$. Using our pruning strategy, we only need to consider

$$1427292833 \approx 2^{31}$$

[1] We do not consider full $\mathbb{F}_{2^8}$ as this leads to a huge search space which will be difficult to complete.

possible $\mathbb{F}_{2^8}$ elements for the a_i's in total. Further with a larger $U = \{x : \text{XOR}(x) \leq 12\}$, in which case $|U| = 18$, we do not find any improved matrix. In this case we need to consider approximately 2^{34} elements from $\mathbb{F}_{2^8}$ instead of $15^{18} \approx 2^{71}$ elements. Like $\mathbb{F}_{2^4}$, the search strategy is proving to be effective in case of $\mathbb{F}_{2^8}$ also.

We also consider other primitive polynomials (up to reciprocals) that define $\mathbb{F}_{2^8}$ with small a set U as above. However, we do not obtain any better matrices than the example above.

7 Comparisons

We summarize our findings and compare with the existing results in Table 1.

$\mathbb{F}_{2^8}$			
Irreducible polynomial	Reference	Matrix type	XOR Counts
$X^8 + X^7 + X^6 + X + 1$	Section 6	Toeplitz	$232 + 8 \cdot 7 \cdot 8$
$X^8 + X^7 + X^6 + X + 1$	[11]	Circulant	$240 + 8 \cdot 7 \cdot 8$
$X^8 + X^7 + X^6 + X + 1$	[17]	Hadamard	$320 + 8 \cdot 7 \cdot 8$
$X^8 + X^4 + X^3 + X^2 + 1$	[3]	Circulant	$392 + 8 \cdot 7 \cdot 8$
$\mathbb{F}_{2^4}$			
$X^4 + X + 1$	Section 5	Toeplitz	$170 + 8 \cdot 7 \cdot 4$
$X^4 + X + 1$	[17]	Hadamard	$208 + 8 \cdot 7 \cdot 4$
$X^4 + X + 1$	[2]	Hadamard	$264 + 8 \cdot 7 \cdot 4$

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

8 Conclusions

We have presented an extensive study on Toeplitz MDS matrices theoretically and also in the context of hardware implementation. We have developed an efficient search strategy that has helped find 8×8 Toeplitz MDS matrices with improved XOR count over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. As these matrices are in the Toeplitz class, it restates along with [15] the richness of this class of matrices with respect to containing efficient MDS matrices. On the other hand it will be interesting to have families of efficient (in terms of XOR count) 8×8 MDS matrices. As we have shown that Cauchy-Toeplitz matrices cannot be MDS in general, one has to consider more general matrices for such a construction.

References

1. Steve Babbage and Matthew Dodd. The stream cipher MICKEY 2.0, 2006. `http://www.ecrypt.eu.org/stream/mickeypf.html`.

2. Paulo S. L. M. Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser. Whirlwind: a new cryptographic hash function. *Des. Codes Cryptography*, 56(2-3):141–162, 2010.
3. Paulo S. L. M. Barreto and Vincent Rijmen. Whirlpool. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd Ed.*, pages 1384–1385. Springer, 2011.
4. Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices. In Matthew Robshaw and Jonathan 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.
5. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.
6. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. Prince: A low-latency block cipher for pervasive computing applications. In *Proceedings of the 18th International Conference on The Theory and Application of Cryptology and Information Security*, ASIACRYPT'12, pages 208–225, Berlin, Heidelberg, 2012. Springer-Verlag.
7. Martin Hell, Thomas Johansson, and Willi Meier. Grain : a Stream Cipher for Constrained Environments. *Int. J. Wire. Mob. Comput.*, 2(1):86–93, May 2007.
8. Pascal Junod and Serge Vaudenay. Perfect diffusion primitives for block ciphers. In Helena Handschuh and M. Anwar 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.
9. Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.
10. Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In Peyrin [13], pages 121–139.
11. Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In Peyrin [13], pages 101–120.
12. F. J. Macwilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes (North-Holland Mathematical Library)*. North Holland, January 1983.
13. Thomas 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.
14. Sumanta. Sarkar and Siang Meng 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.

15. Sumanta Sarkar and Habeeb Syed. Lightweight diffusion layer: Importance of Toeplitz matrices. *IACR Trans. Symmetric Cryptol.*, 2016(1):95–113, 2016.
16. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex 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.
17. Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin. Lightweight MDS Involution Matrices. In Gregor Leander, editor, *Fast Software Encryption*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer Berlin Heidelberg, 2015.
18. Yun Tian, Gongliang Chen, and Jianhua Li. On the Design of Trivium. Cryptology ePrint Archive, Report 2009/431, 2009. `http://eprint.iacr.org/`.

A Proofs and Example

Proof of Lemma 1

Proof. Consider the following $d \times d$ submatrix A.

$$A = \begin{bmatrix} m_{i_0,j_0} & m_{i_0,j_1} & \dots & m_{i_0,j_{d-1}} \\ m_{i_1,j_0} & m_{i_1,j_1} & \dots & m_{i_1,j_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ m_{i_{d-1},j_0} & m_{i_{d-1},j_1} & \dots & m_{i_{d-1},j_{d-1}} \end{bmatrix}.$$

Applying (4), we get the form of this matrix as

$$A = \begin{bmatrix} a_{j_0-i_0} & a_{j_1-i_0} & \dots & a_{j_{d-1}-i_0} \\ a_{j_0-i_1} & a_{j_1-i_1} & \dots & a_{j_{d-1}-i_1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{j_0-i_{d-1}} & a_{j_1-i_{d-1}} & \dots & a_{j_{d-1}-i_{d-1}} \end{bmatrix}. \tag{20}$$

If $j_0 - i_0 \geq 0$, then A is equal to the following submatrix whose first row belongs to the first row of the main matrix T:

$$T_{sub} = \begin{bmatrix} m_{0,j_0-i_0} & m_{0,j_1-i_0} & \dots & m_{0,j_{d-1}-i_0} \\ m_{i_1-i_0,j_0-i_0} & m_{i_1-i_0,j_1-i_0} & \dots & m_{i_1-i_0,j_{d-1}-i_0} \\ \vdots & \vdots & \vdots & \vdots \\ m_{i_{d-1}-i_0,j_0-i_0} & m_{i_{d-1}-i_0,j_1-i_0} & \dots & m_{i_{d-1}-i_0,j_{d-1}-i_0} \end{bmatrix}.$$

On the other hand, if $j_0 - i_0 < 0$, then (20) is equal to the following matrix whose first column belongs to the first column of the main matrix T:

$$T_{sub} = \begin{bmatrix} m_{i_0-j_0,0} & m_{i_0-j_0,j_1-j_0} & \dots & m_{i_0-j_0,j_{d-1}-j_0} \\ m_{i_1-j_0,0} & m_{i_1-j_0,j_1-j_0} & \dots & m_{i_1-j_0,j_{d-1}-j_0} \\ \vdots & \vdots & \vdots & \vdots \\ m_{i_{d-1}-j_0,0} & m_{i_{d-1}-j_0,j_1-j_0} & \dots & m_{i_{d-1}-j_0,j_{d-1}-j_0} \end{bmatrix}.$$

□

Proof of Lemma 2

Proof. As $i + j \leq n - 1$, in the $(i + j)$-th row (row and column number starts from 0), a_{-j} appears in the i-th column, i.e., both a_i and a_{-j} are in the same column. Again in the $(i + j)$-th row, a_{-i} appears in the j-th column, i.e., a_{-i} and a_j are in the same column. Therefore, the 2×2 submatrix of T formed by the $0, (i+j)$-th row and i, j-th column is $\begin{bmatrix} a_i & a_j \\ a_{-j} & a_{-i} \end{bmatrix}$. The determinant of this is $a_i a_{-i} + a_j a_{-j} = 0$ by hypothesis. □

Proof of Lemma 3

Proof. It is easy to check that given an MDS matrix $M = [m_{i,j}]_{n \times n}$ and $\beta \in \mathbb{F}_{2^m}^*$ the matrix $\beta M = [\beta\, m_{i,j}]_{n \times n}$ is also MDS. From [8] it is known that in a 8×8 MDS matrix, 1 can occur at most 24 times. So if there is an element β in an 8×8 MDS matrix V that occurs more than 24 times, then $\beta^{-1}V$ contains 1 more than 24 times, a contradiction. □

Example 2. Suppose α is a primitive root of $X^4 + X + 1 = 0$ that generates $GF(2^4)$. Consider

$$\begin{aligned} x_0 &= 1, \quad y_0 = \alpha + 1, \\ x_1 &= \alpha, \quad y_1 = x_0 + y_0 + x_1, \\ x_2 &= x_0, \quad y_2 = y_0. \end{aligned}$$

Then the following is a Cauchy-Toeplitz matrix

$$\begin{bmatrix} a^3+1 & 1 & a^3+1 \\ 1 & a^3+1 & 1 \\ a^3+1 & 1 & a^3+1 \end{bmatrix}.$$

B Figures and Tables

Dimension	Submatrices of General matrix	Toeplitz matrix	
		General submatrices	Toeplitz submatrices
4×4	69	50	20
5×5	251	182	35
6×6	923	672	55
7×7	3431	2508	81
8×8	12869	9438	113
16×16	601080389	445962870	614

Table 2. Number of submatrices of general matrices, and number of general and Toeplitz submatrices of Toeplitz matrices.

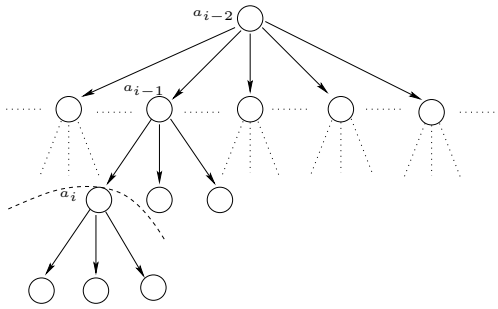

Fig. 1. If the value of a_i occurs more than 24 times then the whole subtree rooted at a_i is pruned.

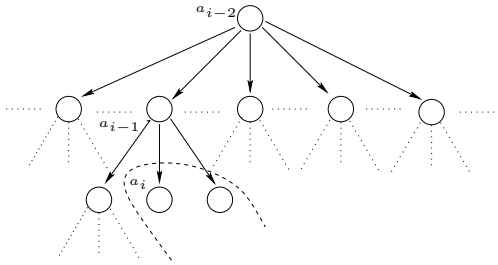

Fig. 2. If the value of a_i satisfies (17), all the subtrees rooted at this a_i and its subsequent siblings are pruned.