On the Counting of Involutory MDS Matrices

Susanta Samanta

Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata-700108, INDIA

susantas_r@isical.ac.in

Abstract

The optimal branch number of MDS matrices has established their prominence in the design of diffusion layers for various block ciphers and hash functions. Consequently, several matrix structures have been proposed for designing MDS matrices, including Hadamard and circulant matrices. In this paper, we first provide the count of Hadamard MDS matrices of order 4 over the field $\mathbb{F}_{2^r}$. Subsequently, we present the counts of order 2 MDS matrices and order 2 involutory MDS matrices over the field $\mathbb{F}_{2^r}$. Finally, leveraging these counts of order 2 matrices, we derive an upper bound for the number of all involutory MDS matrices of order 4 over $\mathbb{F}_{2^r}$.

1 Introduction

Claude Shannon, in his paper "Communication Theory of Secrecy Systems" [7], introduced the concepts of confusion and diffusion, which play a significant role in the design of symmetric key cryptographic primitives. The concept of confusion aims to create a statistical relationship between the ciphertext and message that is too intricate for an attacker to exploit. This is accomplished through the use of nonlinear functions such as Sboxes and Boolean functions. Diffusion, on the other hand, ensures that each bit of the message and secret key influences a significant number of bits in the ciphertext, and over several rounds, all output bits depend on every input bit.

Optimal diffusion layers can be achieved by employing *MDS matrices* with the highest branch numbers. As a result, various matrix structures have been suggested for the designing of MDS matrices, including *Hadamard* and circulant matrices. A concise survey on the various theories on the construction of MDS matrices is provided in [3]. In the context of lightweight cryptographic primitives, the adoption of *involutory matrices* allows for the implementation of both encryption and decryption operations using identical circuitry, thereby resulting in an equivalent implementation cost for both processes. So, it is of special interest to find efficient MDS matrices which are also involutory.

However, obtaining efficiently implementable involutory MDS matrices is a challenging task. Moreover, an exhaustive search for involutory MDS matrices over the finite field of higher order is not suitable due to the vast search space. A concise overview of the different constructions of MDS matrices, considering whether they possess the involutory property, is available in [3]. In 2019, Güzel et al. [4] demonstrated that there are $(2^r - 1)^2(2^r - 2)(2^r - 4)$ involutory MDS matrices of size 3×3 over the finite field $\mathbb{F}_{2^r}$. However, 4 and 8 are the most commonly used diffusion layer matrix sizes in the literature.

One of the most noteworthy advantages of Hadamard matrices lies in their capability to facilitate the construction of involutory matrices. If the matrix elements are selected such that the first row sums to one, the resultant matrix attains involutory properties [3]. Due to this advantageous characteristic, several block ciphers, such as Anubis [1], Khazad [2] and CLEFIA [8], have incorporated involutory Hadamard MDS matrices into their diffusion layers.

In this paper, the primary focus is to enumerate Hadamard MDS and involutory Hadamard MDS matrices of order 4 within the field $\mathbb{F}_{2^r}$. Subsequently, we provide counts for both order 2 MDS matrices and order 2 involutory MDS matrices in the field $\mathbb{F}_{2^r}$. Finally, by leveraging these counts of order 2 matrices, we establish an upper limit for the number of all involutory MDS matrices of order 4 over $\mathbb{F}_{2^r}$.

2 Definition and Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements, $\mathbb{F}_{2^r}$ be the finite field of 2^r elements and $\mathbb{F}^\star_{2^r}$ be the multiplicative group of $\mathbb{F}_{2^r}$. The set of vectors of length n with entries from the finite field $\mathbb{F}_{2^r}$ is denoted by $\mathbb{F}^n_{2^r}$.

A matrix D of order n is said to be diagonal if $(D)_{i,j} = 0$ for $i \neq j$. Using the notation $d_i = (D)_{i,i}$, the diagonal matrix D can be represented as $\operatorname{diag}(d_1, d_2, \ldots, d_n)$. It is evident that the determinant of D is given by $\det(D) = \prod_{i=1}^{n} d_i$. Therefore, the diagonal matrix D is nonsingular over $\mathbb{F}_{2^r}$ if and only if $d_i \neq 0$ for $1 \leq i \leq n$.

An MDS matrix offers diffusion properties that find practical applications in the field of cryptography. This concept originates from coding theory, specifically from the realm of maximum distance separable (MDS) codes. An $[n, k, d]$ code is MDS if it meets the singleton bound $d = n - k + 1$.

Theorem 1. *[5, page 321] An $[n, k, d]$ code C with generator matrix $G = [I \mid M]$, where M is a $k \times (n-k)$ matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i = 1, 2, \ldots, min\{k, n-k\}$) of M is nonsingular.*

Definition 2. A matrix M of order n is said to be an MDS matrix if $[I \mid M]$ is a generator matrix of a $[2n, n]$ MDS code.

Another way to define an MDS matrix is as follows.

Fact 3. *A square matrix M is an MDS matrix if and only if every square submatrices of M are nonsingular.*

One of the elementary row operations on matrices is multiplying a row of a matrix by a nonzero scalar. MDS property remains invariant under such operations. Thus, we have the following result regarding MDS matrices.

Lemma 4. *[3] Let M be an MDS matrix, then for any nonsingular diagonal matrices D_1 and D_2, D_1MD_2 will also be an MDS matrix.*

Using involutory diffusion matrices is more beneficial for implementation since it allows the same module to be utilized in both encryption and decryption phases.

Definition 5. An involutory matrix is defined as a square matrix M that fulfills the condition $M^2 = I$ or, equivalently, $M = M^{-1}$.

Therefore, based on Lemma 4, we can deduce the following result.

Corollary 6. *For any nonsingular diagonal matrix D, the matrix DMD^{-1} is an involutory MDS matrix if and only if M is also an involutory MDS matrix.*

Definition 7. A matrix M of size $2^n \times 2^n$ in the field $\mathbb{F}_{2^r}$ is called a Finite Field Hadamard matrix, or simply a Hadamard matrix, if it can be represented in the following form:

$$\mathrm{M} = \begin{bmatrix} U & V \\ V & U \end{bmatrix}$$

where the submatrices U and V are also Hadamard matrices.

For example, a $2^2 \times 2^2$ Hadamard matrix is:

$$M = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_4 & a_3 & a_2 & a_1 \end{bmatrix}.$$

Note that Hadamard matrices are symmetric and can be represented by their first row. For simplicity, we will denote a Hadamard matrix with the first row as $a_1, a_2, \ldots, a_n$ as $\mathrm{Hada}(a_1, a_2, \ldots, a_n)$. Also, it is worth noting that if $a_1 + a_2 + \cdots + a_n = 1$, then the Hadamard matrix will be involutory [3, page 8].

3 Enumeration of 4×4 Hadamard MDS matrices

In this section, we enumerate 4×4 Hadamard MDS matrices, including involutory Hadamard MDS matrices, over the finite field $\mathbb{F}_{2^r}$. First, we present the conditions that the Hadamard matrix $\mathrm{Hada}(a, b, c, d)$ must satisfy to be considered an MDS matrix.

Lemma 8. *The Hadamard matrix $\mathrm{Hada}(a, b, c, d)$ over $\mathbb{F}_{2^r}$ is MDS if and only if the tuple $(a, b, c, d) \in \mathbb{F}_{2^r}^4$ satisfies the conditions: (i) $a, b, c, d \in \mathbb{F}_{2^r}^{\star}$, (ii) $\{a, b, c, d\}$ being a set of four distinct elements, (iii) $d \neq a^{-1}bc$, (iv) $d \neq ab^{-1}c$, (v) $d \neq abc^{-1}$, and (vi) $d \neq a+b+c$.*

Proof. The set of minors of $M = \mathrm{Hada}(a, b, c, d)$ is given by:

$$\{a, b, c, d, a^2 + b^2, bc + ad, ac + bd, c^2 + d^2, a^2 + c^2, ab + cd, b^2 + d^2, a^2 + d^2, b^2 + c^2,$$
$$a^3 + ab^2 + ac^2 + ad^2, a^2b + b^3 + bc^2 + bd^2, a^2c + b^2c + c^3 + cd^2, a^2d + b^2d + c^2d + d^3,$$
$$a^4 + b^4 + c^4 + d^4\}.$$

These minors have factors given by:

$$T = \{a, b, c, d, a+b, bc+ad, ac+bd, c+d, a+c, ab+cd, b+d, a+d, b+c, a+b+c+d\}.$$

Therefore, M is an MDS matrix if and only if each element in the set T is nonzero. This condition is satisfied if and only if $(a, b, c, d) \in \mathbb{F}_{2^r}^4$ satisfies the conditions: (i) $a, b, c, d \in \mathbb{F}_{2^r}^{\star}$, (ii) $\{a, b, c, d\}$ being a set of four distinct elements, (iii) $d \neq a^{-1}bc$, (iv) $d \neq ab^{-1}c$, (v) $d \neq abc^{-1}$, and (vi) $d \neq a+b+c$. This completes the proof. □

Theorem 9. *The count of* 4×4 *Hadamard MDS matrices over the finite field* $\mathbb{F}_{2^r}$ *is given by* $(2^r-1)(2^r-2)(2^r-4)(2^r-7)$.

Proof. According to Lemma 8, the number of 4×4 Hadamard MDS matrices over $\mathbb{F}_{2^r}$ is equal to the cardinality of the set S, defined as:

$$S = \{(a, b, c, d) \in (\mathbb{F}_{2^r}^{\star})^4 : \{a, b, c, d\} \text{ being a set of four distinct elements and } d \neq a^{-1}bc,$$
$$d \neq ab^{-1}c,\ d \neq abc^{-1},\ d \neq a+b+c\}.$$

Since $a \in \mathbb{F}_{2^r}^{\star}$, there are $2^r - 1$ possible choices for a. Furthermore, with $b \in \mathbb{F}_{2^r}^{\star}$ and $a \neq b$, there are $2^r - 2$ possible choices for b. Similarly, for c, there are $2^r - 3$ possible choices.

Now, we will demonstrate that $a^{-1}bc \notin \{b, c, ab^{-1}c, abc^{-1}, a+b+c\}$ for any choice of a, b and c.

Case 1: $a^{-1}bc = b$.
In this case, $a^{-1}bc = b$, which implies $a = c$. However, this contradicts our assumptions.

Case 2: $a^{-1}bc = c$.
In this case, $a^{-1}bc = c$, which implies $a = b$, and this is a contradiction.

Case 3: $a^{-1}bc = ab^{-1}c$.
Now,

$$\begin{aligned} & a^{-1}bc = ab^{-1}c \\ & \implies a^2 = b^2 \\ & \implies a = b \text{ [Since characteristic of } \mathbb{F}_{2^r} \text{ is 2]}, \end{aligned}$$

which is a contradiction.

Case 4: $a^{-1}bc = abc^{-1}$.
Now,

$$\begin{aligned} & a^{-1}bc = abc^{-1} \\ & \implies a^2 = c^2 \\ & \implies a = c \text{ [Since characteristic of } \mathbb{F}_{2^r} \text{ is 2]}, \end{aligned}$$

which is a contradiction.

Case 5: $a^{-1}bc = ab^{-1}c$.
Now,

$$\begin{aligned} a^{-1}bc &= a+b+c \\ \implies & a^2+ab+ac = bc \\ \implies & (a+b)(a+c) = 0 \\ \implies & a = b \text{ or } a = c. \end{aligned}$$

This again leads to a contradiction.

Therefore, we have $a^{-1}bc \notin \{b, c, ab^{-1}c, abc^{-1}, a+b+c\}$.

However, when $c = a^2b^{-1}$ (which is not equal to a and not equal to b), we have $a^{-1}bc = a$. In this case, there are $2^r - 7$ choices for d. For any other choices of a, b and c, there are $2^r - 8$.

Similarly, we can show the following:

(i) $ab^{-1}c \notin \{a, c, a^{-1}bc, abc^{-1}, a+b+c\}$ and when $c = b^2a^{-1}$ (which is not equal to a and not equal to b), we have $ab^{-1}c = b$. In this case, there are $2^r - 7$ choices for d. For any other choices of a, b and c, there are $2^r - 8$.

(ii) $abc^{-1} \notin \{a, b, a^{-1}bc, ab^{-1}c, a+b+c\}$. Since, the characteristic of $\mathbb{F}_{2^r}$ is 2, $x \mapsto x^2$ is an isomorphism over $\mathbb{F}_{2^r}$. Hence, there exist a unique element $\alpha \in \mathbb{F}_{2^r}$ such that $\alpha^2 = ab$. Now for $c = \alpha$ (which is not equal to a and not equal to b), we have $abc^{-1} = c$. In this case, there are $2^r - 7$ choices for d. For any other choices of a, b and c, there are $2^r - 8$.

(iii) $a+b+c \notin \{a, b, c, a^{-1}bc, ab^{-1}c, abc^{-1}\}$. However, $a+b+c$ may equal zero, and when $c = a+b$, we have $a+b+c = 0$. In this case, there are $2^r - 7$ choices for d. For any other combinations of a, b, and c, there are $2^r - 8$ choices.

Therefore, there are 4 choices of c for which d has $2^r - 7$ choices, whereas for any of the remaining $2^r - 7$ choices of c, d has $2^r - 8$ choices. Hence, we have

$$\begin{aligned} |S| &= (2^r-1)(2^r-2)[4 \cdot (2^r-7) + (2^r-7)(2^r-8)] \\ &= (2^r-1)(2^r-2)(2^r-7)(4+2^r-8) \\ &= (2^r-1)(2^r-2)(2^r-4)(2^r-7). \end{aligned}$$

Hence, the number of 4×4 Hadamard MDS matrices over the finite field $\mathbb{F}_{2^r}$ is equal to $(2^r-1)(2^r-2)(2^r-4)(2^r-7)$. □

It is worth noting that the Hadamard matrix $\mathrm{Hada}(a, b, c, d)$ over $\mathbb{F}_{2^r}$ achieves involutory property if and only if the condition $a+b+c+d = 1$ is satisfied. In the following theorem, we provide the exact count of the 4×4 involutory Hadamard MDS matrices over $\mathbb{F}_{2^r}$.

Theorem 10. *The count of* 4×4 *involutory Hadamard MDS matrices over the finite field* $\mathbb{F}_{2^r}$ *is given by* $(2^r-2)(2^r-4)(2^r-7)$.

Proof. If $M = \mathrm{Hada}(a, b, c, d)$ is a Hadamard matrix, then any nonzero scalar multiple of M is also a Hadamard matrix. Now since M is MDS, we must have $a + b + c + d \neq 0$. Thus, for every $t \neq 0$, there exist an equal number of Hadamard matrices such that $a + b + c + d = t$, as one can freely scale them, resulting in a bijection. In particular, the number of Hadamard matrices with a row sum of 1 is exactly the total number of Hadamard matrices divided by $(2^r - 1)$. Therefore, according to Theorem 9, the count of 4×4 involutory Hadamard MDS matrices is given by $(2^r - 2)(2^r - 4)(2^r - 7)$. $\square$

From Theorems 9 and 10, one can easily find the number of non-involutory Hadamard MDS matrices over the finite field $\mathbb{F}_{2^r}$. We present the count in the following corollary.

Corollary 11. *The count of 4×4 non-involutory Hadamard MDS matrices over the finite field $\mathbb{F}_{2^r}$ is given by $(2^r - 2)^2(2^r - 4)(2^r - 7)$.*

4 $2n \times 2n$ involutory MDS matrices

In this section, we first present a general form for all $2n \times 2n$ involutory MDS matrices over $\mathbb{F}_{2^r}$. Then, we determine the exact count of 2×2 MDS and involutory MDS matrices over $\mathbb{F}_{2^r}$. Using these counts, we establish an upper bound for the enumeration of all 4×4 involutory MDS matrices over $\mathbb{F}_{2^r}$.

Lemma 12. *Let $M = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$ be a $2n \times 2n$ involutory MDS matrix over $\mathbb{F}_{2^r}$, where A_i are $n \times n$ matrices. Then M can be expressed in the form $M = DHD^{-1}$, where $H = \begin{bmatrix} A_1 & I_n + A_1 \\ I_n + A_1 & A_1 \end{bmatrix}$ and D is the block diagonal matrix $\mathrm{diag}(I_n, A_3(I_n + A_1)^{-1})$.*

Proof. Since M is involutory we have

$$\begin{aligned} & A_1^2 + A_2A_3 = I_n, && A_1A_2 + A_2A_4 = \mathbf{0}, \\ & A_3A_1 + A_4A_3 = \mathbf{0}, && A_3A_2 + A_4^2 = I_n. \\ \Longrightarrow\ & A_2 = (I_n + A_1^2)A_3^{-1} && A_4 = A_3A_1A_3^{-1}. \end{aligned}$$

Now, as M is an MDS matrix, A_2 is nonsingular. Thus, we must have $I_n + A_1^2$ nonsingular. Further, since $I_n + A_1^2 = (I_n + A_1)^2$, it follows that $I_n + A_1$ is nonsingular as well. Also, $A_1 \neq I_n$. Therefore, M can be expressed as:

$$\begin{aligned} M &= \begin{bmatrix} A_1 & (I_n + A_1^2)A_3^{-1} \\ A_3 & A_3A_1A_3^{-1} \end{bmatrix} \\ &= \begin{bmatrix} I_n & \mathbf{0} \\ \mathbf{0} & A_3(I_n + A_1)^{-1} \end{bmatrix} \begin{bmatrix} A_1 & I_n + A_1 \\ I_n + A_1 & A_1 \end{bmatrix} \begin{bmatrix} I_n & \mathbf{0} \\ \mathbf{0} & (I_n + A_1)A_3^{-1} \end{bmatrix} \\ &= DHD^{-1}, \end{aligned}$$

where H is the block matrix $\begin{bmatrix} A_1 & I_n + A_1 \\ I_n + A_1 & A_1 \end{bmatrix}$ and D is the block diagonal matrix $\mathrm{diag}(I_n, A_3(I_n + A_1)^{-1})$. $\square$

Lemma 13. *The count of* 2×2 *MDS matrices over the finite field* $\mathbb{F}_{2^r}$ *is given by* $(2^r - 1)^3(2^r - 3)$.

Proof. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an MDS matrix over $\mathbb{F}_{2^r}$. Note that a, b, c, and d all belong to the nonzero elements of the finite field $\mathbb{F}_{2^r}$. Also, $\det(M) = ad + bc$ must be nonzero. This implies that $d \neq a^{-1}bc$. Consequently, each of the values a, b, and c can be chosen from $2^r - 1$ possibilities, as they are drawn from the nonzero elements of $\mathbb{F}_{2^r}$. On the other hand, d can be selected from $2^r - 2$ possibilities because it cannot be equal to $a^{-1}bc$. Hence, the total number of 2×2 MDS matrices can be calculated as $(2^r - 1)^3(2^r - 2)$. $\square$

Lemma 14. *The count of* 2×2 *involutory MDS matrices over the finite field* $\mathbb{F}_{2^r}$ *is given by* $(2^r - 1)(2^r - 2)$.

Proof. According to Lemma 12, any 2×2 involutory MDS matrix M can be represented as $M = DHD^{-1}$, where H is the 2×2 Hadamard matrix $\text{Hada}(\alpha, 1 + \alpha)$, and D is a nonsingular diagonal matrix $\text{diag}(1, (1 + \alpha)\beta^{-1})$, with $\alpha, \beta \in \mathbb{F}_{2^r}^{\star}$. Also, from Corollary 6, we can say that M is an involutory MDS if and only if H is an involutory MDS.

Regarding H, there are $2^r - 2$ possible choices since $\alpha \notin \{0, 1\}$. On the other hand, D provides $2^r - 1$ options. Therefore, the total number of 2×2 involutory MDS matrices is $(2^r - 1)(2^r - 2)$. $\square$

The count of 2×2 involutory MDS matrices over $\mathbb{F}_{2^r}$ is also provided in [6]. However, it is noteworthy that the enumeration of 2×2 involutory MDS matrices in this paper is based on the generic matrix form outlined in Lemma 12, whereas the count in [6] relies on the characterization of 2×2 involutory MDS matrices.

In Theorem 10, we provide the count of 4×4 involutory Hadamard MDS matrices. Next, we establish an upper bound for the enumeration of all 4×4 involutory MDS matrices.

Theorem 15. *The number of* 4×4 *involutory MDS matrices over the finite field* $\mathbb{F}_{2^r}$ *is upper bounded by* $2^r(2^r - 1)^3(2^r - 2)^2(2^r - 3)(2^r - 4)$.

Proof. From Lemma 12, we can deduce that any 4×4 involutory MDS matrix M can be expressed as:

$$M = \begin{bmatrix} A_1 & (I_n + A_1^2)A_3^{-1} \\ A_3 & A_3A_1A_3^{-1} \end{bmatrix},$$

where both A_1 and A_3 are 2×2 MDS matrices. Additionally, A_1 cannot be an involutory matrix. Therefore, by considering both Lemma 13 and Lemma 14, we can conclude that A_1 has a total of $(2^r - 1)^3(2^r - 2) - (2^r - 1)(2^r - 2) = 2^r(2^r - 1)(2^r - 2)^2$ possible choices.

Each row of A_3 must be linearly independent with the rows of A_1. Since A_3 is a 2×2 MDS matrix, there are $(2^r - 1)(2^r - 3)$ possible choices for the first row of A_3 and $(2^r - 1)(2^r - 4)$ possible choices for the second row. Thus, A_3 has a total of $(2^r - 1)^2(2^r - 3)(2^r - 4)$ possible choices. Hence, the number of 4×4 involutory MDS matrices over the finite field $\mathbb{F}_{2^r}$ is upper bounded by $2^r(2^r - 1)^3(2^r - 2)^2(2^r - 3)(2^r - 4)$. $\square$

Remark 16. It is essential to emphasize that the upper bound derived in Theorem 15 is very loose. For instance, while the count of all 4×4 involutory MDS matrices over $\mathbb{F}_{2^3}$ is 16464, our bound yields 1975680. This is because our calculation only considers cases involving 2×2 submatrices constructed from A_1 and A_3. To achieve a more precise bound, it is necessary to examine the other 2×2 submatrices as well as all 3×3 submatrices. However, currently, we are unable to exclude these potential cases from our analysis.

Remark 17. As stated in Lemma 12, we can represent any 4×4 involutory MDS matrix M as $M = DHD^{-1}$, where H is a 4×4 involutory matrix. However, it is important to note that in this context, D is not a standard diagonal matrix but rather a diagonal block matrix. Consequently, unlike Lemma 14 for 2×2 involutory MDS matrices, we cannot directly apply Corollary 6 to assert that M is MDS if and only if H is MDS. Furthermore, considering the specific form of H, it cannot be considered an MDS matrix.

5 Conclusion

This paper has concentrated on two main objectives. First, we have enumerated Hadamard MDS matrices with an order of 4 within the field $\mathbb{F}_{2^r}$ and then provide the count of involutory Hadamard MDS matrices over the same field. Additionally, we have established an upper limit for the number of involutory MDS matrices with an order of 4 over $\mathbb{F}_{2^r}$. However, it is important to note that the upper bound we have calculated is not a precise one. Consequently, determining the exact count of 4×4 involutory MDS matrices or achieving a tighter bound is a potential avenue for future research.

Acknowledgments

We are thankful to the anonymous reviewers for their valuable comments. We would also like to thank Lukas Koelsch for providing an idea in the proof of Theorem 10.

References

[1] Paulo S.L.M. Barreto and Vincent Rijmen. The ANUBIS Block Cipher. *Submission to the NESSIE Project, 2000.*, 2000.

[2] Paulo S.L.M. Barreto and Vincent Rijmen. The KHAZAD Legacy-Level Block Cipher. *Submission to the NESSIE Project, 2000.*, 2000.

[3] Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, and Susanta Samanta. Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results. *Advances in Mathematics of Communications*, 13(4):779–843, 2019.

[4] Gülsüm Gözde Güzel, Muharrem Tolga Sakallı, Sedat Akleylek, Vincent Rijmen, and Yasemin Çengellenmiş. A new matrix form to generate all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$. *Information Processing Letters*, 147:61–68, 2019.

[5] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[6] Fatma Buyuksaracoglu Sakalli, Ozlem Aydin, Gokhan Tuncay, Meltem Kurt Pehlivanoglu, Gulsum Gozde Guzel, and Muharrem Tolga Sakalli. On Lightweight 4×4 MDS Matrices over Binary Field Extensions. *International Journal of Information Security Science*, 9:94–103, 2020.

[7] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[8] 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*, pages 181–195, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.