IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2017, No. 1, pp. 129–155. DOI:10.13154/tosc.v2017.i1.129-155

Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices

Chaoyun Li[1] and Qingju Wang[1,2,3*]

[1] imec - Computer Security and Industrial Cryptography (COSIC) research group, Department of Electrical Engineering (ESAT), KU Leuven, Leuven, Belgium
chaoyun.li@esat.kuleuven.be
[2] Department of Applied Mathematics and Computer Science (DTU Compute), Technical University of Denmark, Kongens Lyngby, Denmark
[3] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
quwang@dtu.dk

Abstract. Near-MDS matrices provide better trade-offs between security and efficiency compared to constructions based on MDS matrices, which are favored for hardware-oriented designs. We present new designs of lightweight linear diffusion layers by constructing lightweight near-MDS matrices. Firstly generic $n \times n$ near-MDS circulant matrices are found for $5 \leq n \leq 9$. Secondly , the implementation cost of instantiations of the generic near-MDS matrices is examined. Surprisingly, for $n = 7, 8$, it turns out that some proposed near-MDS circulant matrices of order n have the lowest XOR count among all near-MDS matrices of the same order. Further, for $n = 5, 6$, we present near-MDS matrices of order n having the lowest XOR count as well. The proposed matrices, together with previous construction of order less than five, lead to solutions of $n \times n$ near-MDS matrices with the lowest XOR count over finite fields $\mathbb{F}_{2^m}$ for $2 \leq n \leq 8$ and $4 \leq m \leq 2048$. Moreover, we present some involutory near-MDS matrices of order 8 constructed from Hadamard matrices. Lastly, the security of the proposed linear layers is studied by calculating lower bounds on the number of active S-boxes. It is shown that our linear layers with a well-chosen nonlinear layer can provide sufficient security against differential and linear cryptanalysis.

Keywords: lightweight cryptography · diffusion layer · near-MDS matrix · branch number

1 Introduction

Symmetric-key cryptographic primitives including block ciphers, stream ciphers and hash functions, form the backbone of secure communication in modern society. *Confusion* and *diffusion* introduced by Shannon [Sha49] are widely used twin fundamental principles in the design of symmetric-key primitives. Most modern block ciphers and hash functions have well-designed confusion and diffusion layers. Among many design methods, substitution-permutation networks (SPN) have been popular in the design of block ciphers and hash functions. The best understood structure of an SPN round function consists of a brick layer of local nonlinear permutations (usually S-boxes) followed by a multiplication with a diffusion matrix over a finite field (linear diffusion). Diffusion layers play an crucial role in providing resistance against the two most powerful statistical attacks: differential cryptanalysis [BS91] and linear cryptanalysis [Mat94].

*Corresponding authors.

Received: 2016-11-23, Accepted: 2017-01-23, Published: 2017-03-08

In 1994, Vaudenay [Vau95] proposes multipermutations as perfect diffusion layers. It is worth noting that the linear multipermutations are exactly Maximum Distance Separable (MDS) matrices, which are defined from MDS codes [MS77]. AES [DR02], the most prominent example of an SPN, uses an MDS matrix in the MixColumns operation together with the ShiftRows operation to achieve diffusion. In the context of the wide-trail strategy, the *branch number* of a linear diffusion layer is defined to bound the probabilities of the best differential and linear trails. Furthermore, linear diffusion layers based on MDS matrices have been shown to provide optimal diffusion properties in the wide-trail strategy for any AES-like ciphers [DR02].

The development of ubiquitous computing such as the Internet of Things (IoT) brings new security requirements to the fore. This leads to the research area of lightweight cryptography. Recently, the study on lightweight diffusion matrices have been the focus of attention. Many constructions of lightweight MDS and involutory MDS matrices have been proposed [BKL16, CJK15, GR15, JV04, KPPY14, LW16, LS16, SDMO12, SS16, SKOP15]. Note that any element of an MDS matrix over a finite field must be nonzero. Thus MDS matrices are very dense and hence costly in hardware implementation. To further reduce the hardware cost, Guo *et al.* [GPP11, GPPR11] proposed a novel design approach of recursive (or serial) MDS matrices, which have a substantially lower hardware area at the cost of additional clock cycles [KPPY14, SKOP15]. Notable examples include the block cipher LED [GPPR11] that has low area in hardware and the hardware-oriented lightweight hash function PHOTON [GPP11] which has been standardized in ISO/IEC 29192-5:2016.

However, MDS and recursive MDS matrices might not offer an optimal trade-off between security and efficiency. Near-MDS have sub-optimal branch numbers while they require less area than MDS matrices and they do not need additional clock cycles. Indeed, some diffusion layers constructed from near-MDS matrices outperform those based on MDS or recursive MDS matrices in terms of the FOAM framework proposed by Khoo *et al.* [KPPY14]. Recently, near-MDS matrices have been adopted in some lightweight block ciphers, including PRINCE [BCG+12], FIDES [BBK+13], PRIDE [ADK+14], Midori [BBI+15] and MANTIS [BJK+16]. On the one hand, low-power, low-energy or low-latency lightweight symmetric-key primitives is becoming increasingly important, and near-MDS matrices are widely used in the design of dedicated lightweight block ciphers. On the other hand, there is insufficient research on the construction and security properties of near-MDS matrices. These motivate us to present novel results on linear diffusion layers constructed from near-MDS matrices.

Related work. First, we briefly introduce some previous work on the construction of lightweight (involutory) MDS matrices. Recursive MDS matrices are an important class of lightweight MDS matrices. The main idea of recursive MDS matrices is to represent an MDS matrix as a power of a very sparse matrix such as a companion matrix. In this way, the MDS matrix can be implemented by iterating the sparse matrix many times. Following this idea, much work has been done to further reduce the hardware cost and improve the performance of recursive MDS matrices [SDMS12, WWW13, AF13, Ber13, AF15]. Another common way is to generate efficient MDS matrices from some special types of matrices. Circulant matrices and their variants such as left-circulant matrices are popular candidates for lightweight MDS matrices [JV04, GR15, LS16, LW16, BKL16]. Involutory MDS matrices are useful in SPN structures as the same circuit can be used for both encryption and decryption. Many lightweight involutory MDS matrices have been constructed from Hadamard [SKOP15, LW16], Cauchy [YMT97, CJK15], Vandermonde [SDMO12] and left-circulant matrices [LS16]. More detailed surveys on the construction of lightweight (involutory) MDS matrices are given in [LS16, BKL16].

Next, we recall some pioneering work about near-MDS matrices which is the main focus

of this paper. In 2008, Choy and Khoo [CK08] define the *almost-MDS matrices* as diffusion matrices attaining a suboptimal differential branch number. In [KPPY14] Khoo *et al.* adopt the term almost-MDS matrices to denote diffusion matrices with both suboptimal differential and linear branch numbers. Notice that the almost-MDS matrices in [CK08] match the *almost MDS codes* introduced in [dB96], whereas the almost-MDS matrices in [KPPY14] correspond to *near-MDS codes* proposed in [DL95]. To link the matrices and the corresponding linear codes, the matrices yielding both suboptimal differential and linear branch numbers are called *near-MDS matrices* in this paper (more details in Sect. 2.1). Indeed, the theoretical results on near-MDS codes [DL95] form the basis of study on near-MDS matrices. In particular, the characterization of near-MDS matrices shown in [VR06] will play an important role in the present paper.

Almost-MDS $\{0,1\}$*-matrices* of order less than or equal to four have been proposed in [CK08]. Note that these almost-MDS matrices in [CK08] are symmetric and hence near-MDS matrices. Then near-MDS $\{0,1\}$-matrices of order less than or equal to four are obtained. Further, it is shown that the $\{0,1\}$-matrices of order larger than four cannot be almost MDS and hence cannot be near-MDS [CK08]. In practice, the $\{0,1\}$-matrix of order four has been widely employed by many block ciphers including PRINCE [BCG+12], FIDES [BBK+13], PRIDE [ADK+14], Midori [BBI+15] and MANTIS [BJK+16]. In [KPPY14], some instances of near-MDS matrices of order 4 and 8 over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ are presented.

Our contributions. The main purpose of this paper is to construct lightweight near-MDS matrices. Recall that near-MDS matrices of order less than five have been investigated in [CK08], hence we will focus on the matrices of order larger than four. For $5 \leq n \leq 9$, we present generic constructions of near-MDS matrices of order n over $\mathbb{F}_{2^m}$, where m is a positive integer. Our work gives an answer to an open problem proposed by Daemen and Rijmen [DR09] and Dodunekov [Dod09] in 2008. To our end, we first propose an algorithm for checking the near-MDS property of a matrix and generating the near-MDS conditions for a near-MDS matrix. Circulant matrices are introduced to reduce the search space. By computer search, we obtain some generic $n \times n$ near-MDS circulant matrices with optimal parameters for $5 \leq n \leq 9$.

To illustrate the efficiency of our generic constructions, some instantiations of the generic near-MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ and their XOR count are provided. A comparison shows that the XOR count of near-MDS matrices proposed in this paper can be around 65% of the XOR count of the best known lightweight MDS matrices constructed in [BKL16, LS16]. Based on experimental results, for $n \geq 8$, we also show some nonexistence results on near-MDS matrices with a small number of distinct entries. This demonstrates that generic near-MDS matrices of order larger than eight have more complicated forms.

We further investigate the total XOR count of the constructed near-MDS matrices in comparison with all other near-MDS matrices over finite fields. First, the exact value of the maximum occurrences of entries 0 and 1 are presented. Based on these results, for $n = 7, 8$, it turns out that some instantiations of generic near-MDS circulant matrices of order n proposed in Sect. 3 have the lowest XOR count among all near-MDS matrices of the same order. Similarly, for $n = 5, 6$, we present some near-MDS matrices of order n having the lowest XOR count. Note that most previous diffusion matrices are optimal among some subclasses rather than the whole space of the matrices with prescribed diffusion properties. It is worth noticing that the near-MDS matrices in Sect. 4 are *global optimal solutions*, that is, they have the lowest XOR count among all near-MDS matrices of the same order. Indeed, for $2 \leq n \leq 4$, it is readily seen that the near-MDS matrices in [CK08] are global optimal solutions since they are composed of 0 and 1 with maximum occurrences. Thus, for $2 \leq n \leq 8$ the global optimal solution for $n \times n$ near-MDS matrices are obtained over finite fields $\mathbb{F}_{2^m}$ for $4 \leq m \leq 2048$.

We present some results on involutory near-MDS matrices in Sect. 5. First, involutory near-MDS of order $2, 3, 4$ are summarized. Then for $n > 4$ we show that there is no circulant involutory near-MDS matrix over finite fields. Next, the Hadamard matrices over finite fields are introduced and their properties are presented. This leads to our constructions of involutory near-MDS matrices of order 8 from Hadamard matrices.

To exploit near-MDS matrices in the design of linear layers, it is important to investigate the security properties of near-MDS matrices. Following the common strategy, we provide lower bounds on the number of differential and linear active S-boxes for SPN structures using near-MDS matrices and ShiftRows as diffusion layer. Our results indicate that the linear layers based on near-MDS matrices can provide sufficient security against differential and linear cryptanalysis.

The remainder of this paper is organized as follows. Section 2 introduces some basic concepts and results on near-MDS matrices. In Sect. 3, some generic near-MDS matrices and their instantiations are presented. In Sect. 4, we give some near-MDS matrices with the lowest XOR count among all near-MDS matrices of the same order. Results on involutory near-MDS are given in Sect. 5. A primary security analysis on near-MDS based linear layers are provided in Sect. 6. The final section concludes the paper.

2 Preliminaries

This section presents some background and results on linear diffusion layers, based on which we introduce the definition of near-MDS matrices. We also recall the notion of XOR count to measure the lightweight property of a diffusion matrix.

2.1 Linear diffusion layers

Most block ciphers and hash functions based on substitution-permutation network (SPN) structures have two layers in each round: the S-Box layer and the linear diffusion layer. The S-Box layer is usually composed of several (not necessarily identical) S-boxes, while the linear diffusion layer is implemented by using matrices over finite fields.

Let $\mathbb{F}_2 = \{0, 1\}$, and we denote by $\mathbb{F}_{2^m}$ a finite extension of $\mathbb{F}_2$ and $\mathbb{F}_{2^m}^n$ the n-dimensional vector space over $\mathbb{F}_{2^m}$, where m and n are positive integers. Indeed, for any linear mapping λ over $\mathbb{F}_{2^m}^n$, there exists a matrix M such that $\lambda(\mathbf{v}) = M \cdot \mathbf{v}$. Hereafter, we represent a linear diffusion layer by a diffusion matrix.

Given a vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})^\mathsf{T} \in \mathbb{F}_{2^m}^n$, its *bundle weight* $\mathrm{wt}_b(\mathbf{v})$ is equal to the number of non-zero components of $\mathbf{v}$. The branch numbers of a diffusion matrix can be defined in terms of the bundle weight of vectors.

Definition 1. ([Dae95, DR02]) Let M be an $n \times n$ matrix over $\mathbb{F}_{2^m}$. Then the *differential branch number* of an $n \times n$ matrix M over $\mathbb{F}_{2^m}$ is defined as

$$\mathcal{B}_d(M) = \min_{\mathbf{v} \neq 0} \{\mathrm{wt}_b(\mathbf{v}) + \mathrm{wt}_b(M\mathbf{v})\},$$

and the *linear branch number* of M over $\mathbb{F}_{2^m}$ is defined as

$$\mathcal{B}_l(M) = \min_{\mathbf{v} \neq 0} \left\{\mathrm{wt}_b(\mathbf{v}) + \mathrm{wt}_b(M^\mathsf{T}\mathbf{v})\right\}.$$

Recall that the branch number can be characterized by the minimum distance of linear codes.

Lemma 1. *([DR02]) Let M be an $n \times n$ matrix over $\mathbb{F}_{2^m}$. Suppose that C is a $[2n, n]$-linear code over $\mathbb{F}_{2^m}$ with generator matrix $(I_n | M^\mathsf{T})$, where I_n is the identity matrix of order n. Then the differential branch number of M equals the minimum distance of C, i.e., $\mathcal{B}_d(M) = d(C)$. Moreover, we have $\mathcal{B}_l(M) = d(C^\perp)$, where $C^\perp$ is the dual code of C.*

Let C be an $[n, k]$-linear code. We call C an maximum distance separable (MDS) code if the Singleton bound is attained, i.e., $d(C) = n - k + 1$ [MS77]. An $n \times n$ matrix M is called an *MDS matrix* if the linear code C_M with generator matrix $(I_n|M^{\mathsf{T}})$ is MDS. An MDS matrix M attains the upper bounds of the branch numbers simultaneously, i.e., $\mathcal{B}_d(M) = \mathcal{B}_l(M) = d(C_M) = n + 1$ [DR02].

In this paper, we focus on the diffusion matrices which attain the largest branch numbers among non-MDS matrices. Now the definition of a near-MDS matrix can naturally be given in terms of branch numbers.

Definition 2. An $n \times n$ matrix M is called a *near-MDS matrix* if $\mathcal{B}_d(M) = \mathcal{B}_l(M) = n$.

In [DL95], an $[n, k]$ near-MDS code C is defined by the conditions $d(C) = n - k$ and $d(C^{\perp}) = k$. Then by Lemma 1, for an $n \times n$ matrix M with $\mathcal{B}_d(M) = \mathcal{B}_l(M) = n$, the matrix $[I|M^T]$ is exactly a generator matrix of a $[2n, n, n]$ near-MDS code. This leads to the following characterization of a near-MDS matrix.

Lemma 2. *([VR06]) Let M be a non-MDS matrix of order n, where n is a positive integer with $n \geq 2$. Then M is near-MDS if and only if for any $1 \leq g \leq n - 1$ each $g \times (g + 1)$ and $(g + 1) \times g$ submatrix of M has at least one $g \times g$ non-singular submatrix.*

We conclude this section with a useful property of branch numbers which will be used in the sequel.

Lemma 3. *([LS16]) For any permutation matrices P_1 and P_2, the two matrices M and $P_1 M P_2$ have the same differential and linear branch numbers.*

2.2 XOR count

The hardware implementation efficiency of operations is typically measured by the area required. Note that the diffusion matrix can be implemented only with XOR gates, and this leads to the following definition.

Definition 3. ([KPPY14, SKOP15]) The *XOR count* of an element $\alpha \in \mathbb{F}_{2^m}$ is the number of XOR operations required to implement the multiplication of α with an arbitrary element $\beta \in \mathbb{F}_{2^m}$.

Given a basis of $\mathbb{F}_{2^m}$, the multiplication by α can be represented by multiplication with a binary matrix A of order m. An obvious upper bound of the XOR count of α is the number of ones in A minus m, and this bound is defined as the exact XOR count in [KPPY14, SKOP15]. It turns out that this bound can be improved in some cases [JPS, BKL16]. Now we recall the definition of XOR count in terms of the matrices.

Definition 4. ([BKL16]) An invertible matrix A has XOR count t, denoted by $\mathrm{wt}_{\oplus}(A) = t$, if t is the minimal number such that A can be written as

$$A = P \prod_{k=1}^{t} (I + E_{i_k, j_k}),$$

where $i_k \neq j_k$ for all k, P is a permutation matrix and E_{i_k, j_k} is a matrix over $\mathbb{F}_2$ with all entries zero except the (i_k, j_k)-entry.

Following Definition 4, Beierle *et al.* [BKL16] further consider the problem of optimizing the XOR count of a given element in finite fields. For $\alpha \in \mathbb{F}_{2^m}$, $m(x)$ is the *minimal polynomial of* α if $m(\alpha) = 0$ and α is not a root of any nonzero polynomial in $\mathbb{F}_2[x]$ of lower degree. With the above definitions, some results are shown below.

Lemma 4. *([BKL16]) Let $\alpha \in \mathbb{F}_{2^m}^*$. Then we have:*

(i) $\mathrm{wt}_{\oplus}(\alpha) = 0$ *if and only if* $\alpha = 1$ *while* $\mathrm{wt}_{\oplus}(\alpha) = 1$ *if and only if the minimal polynomial* $m(x)$ *of* α *is a trinomial of degree* m*;*

(ii) $\mathrm{wt}_{\oplus}(\alpha) = \mathrm{wt}_{\oplus}(\alpha^{-1})$*;*

(iii) $\mathrm{wt}_{\oplus}(\alpha^{\pm k}) \leq k \cdot \mathrm{wt}_{\oplus}(\alpha)$ *for* $k \geq 1$*.*

By Lemma 4(i), if there is no irreducible trinomial of degree m, then $\mathrm{wt}_{\oplus}(\alpha) \geq 2$ for any $\alpha \in \mathbb{F}_{2^m}^*$. Indeed, in these cases, there exists some $\beta \in \mathbb{F}_{2^m}^*$ and a basis B of $\mathbb{F}_{2^m}$ such that $\mathrm{wt}_{\oplus}(\alpha) = 2$ for all $m \leq 2048$ [BKL16]. Notice that there does not exist an irreducible trinomial of degree m if $8|m$ [Swa62]. Hence $\mathrm{wt}_{\oplus}(\alpha) = 2$ is optimal in $\mathbb{F}_{2^8}$, which will be used in the sequel.

3 Lightweight near-MDS circulant matrices

This section presents constructions of near-MDS circulant matrices over $\mathbb{F}_{2^m}$, where m is a positive integer. We propose an algorithm for checking the near-MDS property of a matrix and generating the near-MDS conditions for a near-MDS matrix. Circulant matrices are introduced to reduce the search space. By computer search, we obtain some generic near-MDS circulant matrices with optimal parameters. We also show some nonexistence results on near-MDS matrices with a small number of distinct entries. Finally, some instantiations of the generic near-MDS matrices and their XOR count are provided.

3.1 Approach to constructing generic near-MDS matrices

This section presents our main approach to constructing near-MDS matrices over $\mathbb{F}_{2^m}$, where m is a positive integer. An algorithm is proposed to check the near-MDS property of a candidate matrix and generate the near-MDS conditions if the matrix is near-MDS.

Main approach. To construct generic near-MDS matrices, the entries of the candidate matrices are supposed to be in the quotient field of $\mathbb{F}_2[x]$. Specifically, we suppose that the matrix contains 0 and nonzero entries in $\langle x \rangle$, where $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. Based on Lemma 2, we propose an algorithm for checking the near-MDS property and generating the near-MDS conditions via polynomials in $\mathbb{F}_2[x]$. Then one can substitute the indeterminate x with any $\alpha \in \mathbb{F}_{2^m}$ satisfying all the conditions for the matrices to be near-MDS. Consequently, lightweight near-MDS can be obtained by choosing the element α as light as possible.

Checking the near-MDS property. By Lemma 2, a non-MDS matrix M is near-MDS if and only if for any $1 \leq g \leq n-1$ each $g \times (g+1)$ and $(g+1) \times g$ submatrix of M has at least one $g \times g$ non-singular submatrix. Then, to check the near-MDS property, one needs to compute the determinants of all the $g \times g$ submatrices of a given $g \times (g+1)$ or $(g+1) \times g$ submatrix of M. For the matrix composed of entries in $\langle x \rangle$, it is readily seen that the determinant of any submatrix is a quotient of two polynomials in $\mathbb{F}_2[x]$. Furthermore, the determinant of any submatrix is nonzero if and only if the numerator of the determinant is nonzero. Hence, for simplicity, we will consider the numerator of the determinant rather than the determinant itself.

After obtaining the numerators of the determinants of all $g \times g$ submatrices, it suffices to further check if there is at least one nonzero numerator. We introduce a result to simplify the process. Denote by $\gcd(f(x), g(x))$ the greatest common divisor of two polynomials $f(x), g(x)$ over $\mathbb{F}_2[x]$. By convention, let $\gcd(f(x), 0) = f(x)$. Let $n > 1$, we denote

$$\gcd(f_1(x), f_2(x), \cdots, f_n(x)) = \gcd(f_1(x), \gcd(f_2(x), \cdots, \gcd(f_{n-1}(x), f_n(x)) \cdots)).$$

Then the following lemma holds.

Lemma 5. *Let $f_1(x), f_2(x), \cdots, f_k(x)$ be k polynomials in $\mathbb{F}_2[x]$, where k is a positive integer. Then there exists at least one nonzero $f_i(x)$ if and only if* $\gcd(f_1(x), f_2(x), \cdots, f_k(x)) \neq 0$.

Proof. It is equivalent to prove that $f_1(x) = f_2(x) = \cdots = f_k(x) = 0$ if and only if $\gcd(f_1(x), f_2(x), \cdots, f_k(x)) = 0$, which is trivial. □

For any given $g \times (g+1)$ or $(g+1) \times g$ submatrix of M, Lemma 5 implies that it suffices to check the greatest common divisor of the numerators of the determinants of all $g \times g$ submatrices. If the greatest common divisor is nonzero, one can decompose the nonzero greatest common divisor into irreducible factors and collect the factors in a condition set S. Otherwise, the matrix is not near-MDS. The procedure is described in Algorithm 1.

Suppose that for the matrix M the condition set S is output by Algorithm 1. By substituting x with $\alpha \in \mathbb{F}_{2^m}$, the concrete matrix $M(\alpha)$ is near-MDS if and only if α is not a root of any polynomial in the set S.

Algorithm 1 Check near-MDS property and generate near-MDS conditions

Input: an $n \times n$ matrix M with entries in $\{0\} \cup \langle x \rangle$
Output: a condition set S if M is near-MDS and $\perp$ otherwise

```
S ← ∅
for g ∈ [1, n − 1] do                                   ▷ n is the order of M
    for all g × (g + 1) and (g + 1) × g submatrix A of M do
        f(x) ← 0, T ← ∅
        for all g × g submatrices B of A do             ▷ there are (g + 1) submatrices
            Compute the numerator p(x) of the fraction det(B)
            f(x) ← gcd(f(x), p(x))                      ▷ Compute the greatest common divisor
        if f(x) = 0 then
            return ⊥                                    ▷ M is not near-MDS
        else
            Compute the set T of the irreducible factors of f(x)
            S ← S ∪ T
return S
```

It should be pointed out that the main approach has been adopted in constructing recursive MDS matrices [WWW13, SDMS12, AF13]. In these works, the authors investigate matrices with entries of the form $\sum_i a_i L^i$, and deduce the MDS conditions by polynomials in L, where L is a sparse nonsingular $m \times m$ binary matrix and $a_i \in \mathbb{F}_2$. Recently, this method was exploited by Beierle *et al.* in [BKL16] to generate generic lightweight MDS matrices with entries in finite fields. These previous works motivate our approach to producing generic near-MDS matrices over finite fields. In this section, by Lemmas 2 and 5, Algorithm 1 are proposed to check the near-MDS property of a matrix and generate the near-MDS conditions for a near-MDS matrix.

3.2 Generic near-MDS circulant matrices

We describe the strategy for searching near-MDS circulant matrices. Some generic near-MDS circulant matrices with optimal parameters are shown. We also present some nonexistence results on near-MDS matrices with a small number of distinct entries.

Circulant matrices. Circulant matrices are widely adopted in the design of diffusion matrices. Following this approach, we will focus on circulant matrices in this section. First, the definition of a circulant matrix is recalled.

Definition 5. An $n \times n$ matrix M is *circulant* if its rows are generated by successive cyclic shifts of its first row. That is, there exist n elements $a_0, a_1, \cdots, a_{n-1}$ such that the (i,j)-entry of M can be represented by $M[i,j] = a_{(j-i) \bmod n}$. We denote the matrix M by $\mathrm{circ}(a_0, a_1, \cdots, a_{n-1})$.

The fact that each row of a circulant matrix is a cyclic shift of the first row enables one reuse the multiplication circuit to save implementation cost [KPPY14, LS16, SKOP15]. To construct the lightest diffusion matrices, it is natural to consider the circulant matrix with lightest field elements. It seems that the $\{0,1\}$-matrices are the best candidates. Choy and Khoo [CK08] proved the following results on $\{0,1\}$-matrices over finite fields.

Lemma 6. *([CK08]) Let n be a positive integer. For $n = 2, 3, 4$, the $n \times n$ circulant matrices*

$$\mathrm{circ}(0, 1, \cdots, 1) = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{pmatrix}$$

are near-MDS matrices over any finite field. For $n > 4$, any $\{0,1\}$-matrices of order n cannot be near-MDS.

It is readily seen that the matrices proposed in Lemma 6 are optimal near-MDS matrices in terms of XOR count. The 4×4 matrix $\mathrm{circ}(0,1,1,1)$ has been adopted in several lightweight block ciphers such as PRINCE [BCG+12], FIDES [BBK+13], PRIDE [ADK+14] and Midori [BBI+15], and MANTIS [BJK+16].

For $n \geq 5$, the nonexistence of near-MDS $\{0,1\}$-matrices leads to the study of circulant matrices with three or more distinct elements such as matrices with entries in the set $\{0, 1, \gamma\}$, where $\gamma \in \mathbb{F}_{2^m} \setminus \{0,1\}$. We use the criteria for efficient diffusion matrices proposed by Junod and Vaudenay [JV04] to maximize the occurrences of 0 and 1. Let $g = 1$ in Lemma 2, then there is at most one 0 in each row and each column of M. Hence, the following result can be obtained.

Proposition 1. *Suppose that $n \geq 5$ and $\mathrm{circ}(a_0, a_1, \cdots, a_{n-1})$ is near-MDS. Let N_δ be the number of δ in the multiset $\{a_0, a_1, \cdots, a_{n-1}\}$. Then, we have*

$$N_0 \leq 1\,.$$

Moreover, if $N_0 = 1$, then $N_1 \leq n - 2$.

Search strategy. Our main idea is to reduce the search space and explore the most efficient matrices first. By Proposition 1, we always assume that $N_0 = 1$. Lemma 3 indicates that the branch numbers of a circulant matrix are preserved by rotation of the first row. Hence, we will focus on circulant matrices of the form

$$\mathrm{circ}(0, a_1, a_2, \cdots, a_{n-1})\,, \tag{1}$$

where $a_i \in \langle x \rangle$ for $1 \leq i \leq n-1$ and $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. To explore the most efficient matrices first, we restrict the nonzero entries a_i's of the circulant matrices to elements in the set $\{1, x, x^{-1}\} \subseteq \langle x \rangle$.

We first exhaustively search the matrices with maximal N_1. Note that the XOR count of x and x^{-1} are identical, hence they will be treated equally. More specifically, N_1 is initialized as $n-2$ and $N_x + N_{x^{-1}}$ as 1. For any candidate matrix, we apply Algorithm 1 to check the near-MDS property and generate the condition set (*cf.* Algorithm 1) if it is near-MDS. If no near-MDS matrix is found, then $N_x + N_{x^{-1}}$ is increased by one and N_1 decreased by one. This exhaustive search process continues until all near-MDS with optimal parameters are found.

Table 1: Optimal parameters with maximum N_1 and minimum $N_x + N_{x^{-1}}$

n	N_0	N_1	N_x	$N_{x^{-1}}$	Number of Matrices
5	1	3	1	-	4
6	1	3	2	-	5
	1	3	1	1	18
7	1	4	1	1	12
8	1	4	1	2	8
	1	4	2	1	8
9	1	2	2	4	6
	1	2	4	2	6

Experimental results. We present some experimental results on near-MDS matrices of order n for $5 \leq n \leq 9$. In Table 1, the parameters $N_0, N_1, N_x, N_{x^{-1}}$ with maximum N_1 and minimum $N_x + N_{x^{-1}}$ are listed. We also show some good matrices and the corresponding near-MDS conditions in Table 2. A concrete near-MDS matrix is obtained by substituting x with $\alpha \in \mathbb{F}_{2^m}$ such that α is not a root of any polynomial listed in the Conditions column of Table 2. Moreover, the determinants of the constructed matrices are given. For the complete list, see Table 9 in Appendix B.

For $n = 7$, we also find near-MDS matrices consisting of three distinct elements $0, 1, x$ with $N_1 = 3$ and $N_x = 3$. For instance, the matrix $\mathrm{circ}(0, x, x, 1, x, 1, 1)$ is near-MDS under the following conditions

$$x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1\,.$$

However, for $8 \leq n \leq 10$, experimental results $0, 1, x$ do not suffice to construct near-MDS circulant matrices of order n. Indeed, this fact holds for all $n \geq 8$ and we summarize it in the following theorem, the proof of which is given in Appendix A.

Theorem 1. *For any $n \geq 8$, there is no near-MDS circulant matrix with three distinct entries $0, 1, x$, where $x \in \mathbb{F}_{2^m} \setminus \{0, 1\}$.*

It is worth noting that Theorem 1 partially generalizes the results of Lemma 6. Further, we pose the following conjecture based on experimental results.

Conjecture 1. *For any $n \geq 10$, there is no near-MDS circulant matrix with four distinct entries $0, 1, x, x^{-1}$, where $x \in \mathbb{F}_{2^m} \setminus \{0, 1\}$.*

3.3 Instantiations of generic near-MDS matrices

Considering the cryptographic applications of diffusion matrices, we focus on $\mathbb{F}_{2^m}$ with $m = 4$ and 8. It is readily seen that the discussion in this section also applies to any other m. For $5 \leq n \leq 8$, we list in Table 3 some $n \times n$ near-MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ from the generic matrices proposed in Table 2. The minimal polynomial of the nonzero elements of each matrix and XOR count of the first row are also presented.

We first explain how to choose the minimal polynomial of α in the case that $n = 5$. According to Table 2, the matrix $\mathrm{circ}(0, \alpha, 1, 1, 1)$ is near-MDS if and only if α is not a root of any of the following polynomials:

$$x, x + 1, x^2 + x + 1.$$

This implies that the minimal polynomial of α can be any irreducible polynomial except for the above three polynomials. For $m = 4$, one can take the minimal polynomial as $x^4 + x + 1$ or $x^4 + x^3 + 1$ since $\mathrm{wt}_{\oplus}(\alpha)$ is minimal, i.e., $\mathrm{wt}_{\oplus}(\alpha) = 1$ in these cases (see

Table 2: Examples of generic near-MDS circulant matrices of order $5 \leq n \leq 9$

n	Coefficients of the first row	Conditions to be near-MDS	Determinants
5	$(0, x, 1, 1, 1)$	x $x+1$ x^2+x+1	x^5+x^3+x+1
6	$(0, x, 1, 1, 1, x)$	x $x+1$ x^2+x+1	x^4
7	$(0, x, 1, x^{-1}, 1, 1, 1)$	x $x+1$ x^2+x+1 x^3+x+1 x^3+x^2+1 $x^4+x^3+x^2+x+1$	$x^7+x^5+x^{-1}+$ $x^{-3}+x^{-5}+x^{-7}$
8	$(0, x, 1, x, x^{-1}, 1, 1, 1)$	x $x+1$ x^2+x+1 x^3+x+1 x^3+x^2+1 $x^4+x^3+x^2+x+1$ $x^5+x^4+x^3+x^2+1$	x^{-8}
9	$(0, x, x^{-1}, x, x, x^{-1}, 1, 1, x)$	x $x+1$ x^2+x+1 x^3+x+1 x^3+x^2+1 x^4+x+1 x^4+x^3+1 $x^4+x^3+x^2+x+1$ x^5+x^2+1 x^5+x^3+1 $x^5+x^3+x^2+x+1$ $x^5+x^4+x^2+x+1$ $x^5+x^4+x^3+x+1$ $x^5+x^4+x^3+x^2+1$ $x^6+x^5+x^4+x^2+1$ $x^7+x^4+x^3+x^2+1$ $x^7+x^6+x^4+x+1$ $x^{12}+x^{11}+x^{10}+x^9+$ $x^8+x^7+x^6+x^2+1$	0

Table 3 in [BKL16]). Further, to make the matrix nonsingular, x^4+x+1 is selected as the minimal polynomial of α since

$$\det(\mathrm{circ}(0, \alpha, 1, 1, 1)) = \alpha^5+\alpha^3+\alpha+1 = (\alpha+1)(\alpha^4+\alpha^3+1).$$

For $m = 8$, as shown in Sect. 2.2, $\mathrm{wt}_{\oplus}(\alpha) = 2$ is best possible. One of the polynomials

Table 3: Near-MDS circulant matrices of order $5 \leq n \leq 8$ over finite field $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$

Finite fields	n	First row	Minimal polynomial of α	XOR counts
$\mathbb{F}_{2^4}$	5	$(0, \alpha, 1, 1, 1)$	$x^4 + x + 1$	$1 + 3 \times 4 = \mathbf{13}$
	6	$(0, \alpha, 1, 1, 1, \alpha)$	$x^4 + x + 1$	$2 + 4 \times 4 = \mathbf{18}$
	7	$(0, \alpha, 1, \alpha^{-1}, 1, 1, 1)$	$x^4 + x + 1$	$2 + 5 \times 4 = \mathbf{22}$
	8	$(0, \alpha, 1, \alpha, \alpha^{-1}, 1, 1, 1)$	$x^4 + x + 1$	$3 + 6 \times 4 = \mathbf{27}$
$\mathbb{F}_{2^8}$	5	$(0, \alpha, 1, 1, 1)$	$x^8 + x^4 + x^3 + x + 1$	$2 + 3 \times 8 = \mathbf{26}$
	6	$(0, \alpha, 1, 1, 1, \alpha)$	$x^8 + x^4 + x^3 + x + 1$	$4 + 4 \times 8 = \mathbf{36}$
	7	$(0, \alpha, 1, \alpha^{-1}, 1, 1, 1)$	$x^8 + x^4 + x^3 + x + 1$	$4 + 5 \times 8 = \mathbf{44}$
	8	$(0, \alpha, 1, \alpha, \alpha^{-1}, 1, 1, 1)$	$x^8 + x^4 + x^3 + x + 1$	$6 + 6 \times 8 = \mathbf{54}$

Table 4: Comparison of XOR counts of near-MDS circulant matrices and known (non-involutory) MDS matrices of order $5 \leq n \leq 8$ over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$

	$\mathbb{F}_{2^4}$		$\mathbb{F}_{2^8}$	
n	Near-MDS Table 3	MDS [LS16]	Near-MDS Table 3	MDS [BKL16]
5	13	20	26	40
6	18	32	36	54
7	-	-	44	64
8	-	-	54	82

attaining the minimal XOR count is $x^8 + x^4 + x^3 + x + 1$ (see Table 7 in [BKL16]). In this way, two efficient near-MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ are constructed respectively from one generic near-MDS matrix in Table 2. The other matrices in Table 3 are generated in the same manner.

To compute the XOR count of a circulant matrix, it is convenient to only consider the XOR count of the first row [KPPY14, LS16, BKL16]. For an $n \times n$ circulant matrix A over $\mathbb{F}_{2^m}$, the XOR count of the first row is

$$(c_0 + c_1 + \cdots + c_{n-1}) + (z - 1)m\,,$$

where c_i is the XOR count of the i-th entry in the row, z is the number of nonzero elements in the row. For instance, the XOR count of the first row of the matrix $\mathrm{circ}(0, \alpha, 1, 1, 1)$ is $1 + 3 \times 4 = \mathbf{13}$ since $\mathrm{wt}_{\oplus}(\alpha) = 1$ and $\mathrm{wt}_{\oplus}(0) = \mathrm{wt}_{\oplus}(1) = 0$.

Table 4 compares the efficiency of near-MDS matrices proposed in this paper with the best known lightweight MDS matrices constructed in [BKL16, LS16]. It is readily seen that the XOR counts of near-MDS matrices can be around 65% of the XOR counts of MDS ones of the same order. However, since the near-MDS matrices have slower diffusion than the MDS ones, a fair comparison should be carried out within a framework combining the security properties and implementation cost. A notable attempt in this direction is the new comparison metric *figure of adversarial merit (FOAM)* proposed by Khoo *et al.* in [KPPY14].

4 Near-MDS matrices with the lowest XOR count

It is not easy to define an optimal near-MDS matrix in terms of implementation cost, since the cost of the matrix largely depends on the implementation technologies. Among many criteria for efficient diffusion matrices, the XOR count of the matrix is a major feature in

various implementation methods [KPPY14, LS16, BKL16]. In this section, we concentrate on the total XOR count of **near-MDS matrices over finite fields**. First, the exact value of the maximum occurrences of special entries 0 and 1 are provided. Based on these results, one can prove that for $n = 7, 8$ the instantiations of generic near-MDS matrices in Sect. 3 have the lowest XOR count among all near-MDS matrices of the same order. Moreover, for $n = 5, 6$, we also present some near-MDS matrices of order n having the lowest XOR count.

Let M be a near-MDS matrix of order n over $\mathbb{F}_{2^m}$. Denote by $v_0(M)$ the number of entries in M equal to 0 and $v_1(M)$ the number of entries in M equal to 1. Let v_0^n be the maximum value of $v_0(M)$ for all M. Similarly, let v_1^n denote the maximum value of $v_1(M)$ for all M. Then, Proposition 1 and the results in Table 1 together show the following result on v_0^n for $5 \leq n \leq 8$.

Lemma 7. *Let M be a near-MDS matrix of order n. Then we have $v_0^n = n$ for $5 \leq n \leq 8$.*

Now we can present the upper bounds on v_1^n.

Proposition 2. *Let M be a near-MDS matrix of order n. For $5 \leq n \leq 8$, the upper bounds of v_1^n are shown in Table 5.*

Table 5: The upper bounds of v_1^n for near-MDS matrix M of order n with $5 \leq n \leq 8$

n	5	6	7	8
Upper bounds of v_1^n	16	21	28	32

Proof. We only prove the case that $n = 8$ since the other cases can be proved in the same manner. Suppose that M is a near-MDS matrix of order 8. Let k be the maximum occurrence of the entry 1 in a row of M. To derive the upper bound, we discuss five cases in terms of the value of k.

Case 1. Suppose that $k = 8$ and the first row has eight ones. We claim that there are at most two ones in any other row of M. Otherwise, assume that there are at least three ones in some row i with $i \neq 1$. For instance, M can be written as

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ * & 1 & * & * & 1 & 1 & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

It is easy to verify that M has a submatrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Then by Lemma 2, M is not near-MDS, which is a contradiction. Thus, the claim is correct and we have $v_1(M) \leq k + 2(n-1) = 22$.

Case 2. Assume that $k = 7$ and the first row contains seven ones. It follows from Lemma 3 that the near-MDS property is preserved under the permutation of columns of M. Without loss of generality, we can always assume that the first row is $(*1111111)$. Then we can claim that there are at most three ones in any other row of M. Otherwise, assume that there are at least four ones in some row i with $i \neq 1$. This implies that there are at least

three ones among the last four entries in row i, as shown below

$$\left(\begin{array}{c|cccccccc} * & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & 1 & * & 1 & 1 & 1 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right).$$

Similarly, we can derive a contradiction, which indicates the claim is correct. Hence, we have $v_1(M) \leq k + 3(n-1) = 28$.

Case 3. Let $k = 6$ and the first row contains six ones. Without loss of generality, we assume that the first row is $(**111111)$. The remaining seven rows are partitioned into two blocks A and B, as shown below

$$\left(\begin{array}{c|cccccc} ** & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline A & \multicolumn{6}{c}{B} \end{array}\right).$$

Similar to Case 1, there are at most two ones in each row of B. Note that the 2×7 block A cannot contain a submatrix of the form

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

This implies that the block A contains at most nine ones. Thus, we have $v_1(M) \leq k + 2(n-1) + 9 = 29$.

Case 4. Let $k = 5$ and the first row contains five 1. Without loss of generality, we assume that the first row is $(***11111)$. The remaining rows are partitioned into two blocks, as shown below

$$\left(\begin{array}{c|ccccc} *** & 1 & 1 & 1 & 1 & 1 \\ \hline C & \multicolumn{5}{c}{D} \end{array}\right).$$

Similar to Case 1, there are at most two 1's in each row of D. Since M is near-MDS, the 3×7 block C cannot contain a submatrix having one of the two forms:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

By considering the maximum occurrence of 1 in a row of C, one can deduce that C contains at most 13 ones. Then we have $v_1(M) \leq k + 2(n-1) + 13 = 32$ for $k = 5$.

Case 5. For $k \leq 4$, we have $v_1(M) \leq kn \leq 32$.

By combining the above five cases, we have $v_1(M) \leq 32$ for any M. This gives $v_1^8 \leq 32$. □

The explicit near-MDS matrices shown in Table 1 give lower bounds for v_1^n. These together with Proposition 2 yield the following result.

Corollary 1. *We have* $v_1^7 = 28$ *and* $v_1^8 = 32$.

By Corollary 1, one can show that the instantiations of the generic near-MDS matrices proposed in Sect. 3.2 are optimal in terms of XOR counts.

Theorem 2. *Let* $\mathcal{C}$ *be the set of generic near-MDS matrices proposed in Sect. 3.2. For* $n = 7, 8$ *and* $m \geq 4$*, if* α *is a lightest element in* $\mathbb{F}_{2^m}$ *and* α *satisfies the near-MDS conditions, then the respective instantiations of the matrices in* $\mathcal{C}$ *have the lowest XOR count among all near-MDS matrices of the same order.*

Proof. Let M be a near-MDS matrix of order n. The XOR count of the matrix M can be written as

$$(n(n-1) - v_0(M))m + \sum_{\beta \neq 0,1} \mathrm{wt}_{\oplus}(\beta)\,,$$

where the sum is over all entries of M not equal to 0 or 1. It follows that

$$\begin{aligned}(n(n-1) - v_0(M))m + \sum_{\beta \neq 0,1} \mathrm{wt}_{\oplus}(\beta) \geq \quad & (n(n-1) - v_0^n)m \\ & + (n^2 - v_0^n - v_1^n) \min_{\gamma \neq 0,1} \mathrm{wt}_{\oplus}(\gamma)\,.\end{aligned}$$

The lower bound holds if and only if M satisfies the following conditions:

1. both v_0^n and v_1^n are attained
2. any entry of M not equal to 0 or 1 has the lowest XOR count, i.e., $\min_{\gamma \neq 0,1} \mathrm{wt}_{\oplus}(\gamma)$.

For $n = 7, 8$, it is easy to see that each instantiation of a matrix in $\mathcal{C}$ of order n satisfies the first condition. If α is a lightest element in $\mathbb{F}_{2^m}$, then so is α^{-1} by Lemma 4(ii). Note that α and α^{-1} are the only entries of M not equal to 0 or 1. This leads to the second condition. Hence, the respective instantiations of the matrices in $\mathcal{C}$ achieve the lower bound of XOR count and have the lowest XOR count among all near-MDS matrices of the same order. Thus, the theorem is proved. □

By Theorem 2, for near-MDS matrices of order 7 and 8, the minimum XOR count can be achieved by circulant matrices. As circulant matrices have many desirable properties such as efficient serial implementations [LS16], it is interesting to study the existence of near-MDS circulant matrices attaining minimum XOR count for other orders. However, as shown by subsequent results, circulant matrices of order 5 and 6 cannot achieve minimum XOR count. For $n = 5$ and 6, we give further results on $n \times n$ near-MDS matrices with maximum occurrences of entries 0 and 1. Some experimental results are presented.

To determine v_1^5 and v_1^6, by Proposition 2, it suffices to study the existence of the near-MDS matrix achieving the upper bound in Table 5. We performed an exhaustive search for near-MDS matrices of order 5 and 6 satisfying the following conditions:

- entries from $\{0, 1, x\}$
- $v_1(M)$ taken as the upper bound in Table 5
- $v_0(M) = n$ and the main diagonal consists of zeros

Experimental results give an affirmative answer to the existence of generic near-MDS matrices of order 5 and 6 satisfying both $v_0(M) = n$ and the value $v_1(M)$ attains the upper bound in Table 5. For instance, the following 5×5 matrix

$$\begin{pmatrix} 0 & \alpha & 1 & 1 & 1 \\ 1 & 0 & \alpha & 1 & 1 \\ 1 & 1 & 0 & \alpha & 1 \\ \alpha & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{2}$$

is near-MDS for any $\alpha \neq 0, 1$ while the 6×6 matrix

$$\begin{pmatrix} 0 & \alpha & \alpha & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & 1 & 1 \\ 1 & 1 & 0 & 1 & \alpha & 1 \\ 1 & 1 & \alpha & 0 & 1 & \alpha \\ 1 & \alpha & 1 & 1 & 0 & \alpha \\ \alpha & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{3}$$

is near-MDS for any $\alpha \neq 0, 1$ and $\alpha^2 + \alpha + 1 \neq 0$. This implies $v_1^5 = 16$ and $v_1^6 = 21$. Since $v_1(M)$ must be a multiple of the order of M if M is circulant, circulant matrices of order 5 and 6 cannot achieve v_1^5 and v_1^6 respectively. Hence, they cannot attain minimum XOR count. The following corollary summarizes the above results.

Corollary 2. *We have $v_1^5 = 16$ and $v_1^6 = 21$. Moreover, circulant matrices of order 5 and 6 cannot attain minimum XOR count.*

Consequently, one can show following result similarly to Theorem 2.

Theorem 3. *For $n = 5, 6$ and $m \geq 3$, if α is a lightest element in $\mathbb{F}_{2^m}$ and α satisfies the near-MDS conditions, then the generic near-MDS matrices of order n given by (2) and (3) have instantiations with the lowest XOR count among all near-MDS matrices of the same order over $\mathbb{F}_{2^m}$.*

Lightest elements in $\mathbb{F}_{2^m}$. With the aid of Theorems 2 and 3, the problem of constructing near-MDS matrices with lowest XOR count over $\mathbb{F}_{2^m}$ can be reduced to choosing α as the lightest element in $\mathbb{F}_{2^m}$. Recall that the only restriction on α is that it cannot be a root of any polynomial in the corresponding condition set. Now we give a primary analysis of the existence of lightest α satisfying the near-MDS conditions.

Suppose that $m \geq 4$. If there exists an irreducible trinomial of degree m, then by Lemma 4 (i) the lightest α is obtained by taking its minimal polynomial as the irreducible trinomial. For example, there is irreducible trinomial of degree m for $m \leq 7$. However, there exist no irreducible trinomial of degree m for certain m, such as $m = 8$. In this case, we recall the following fact (more details can be found in Sect. 3.2 of [BKL16]).

Fact 1. *([BKL16]) For all $m \leq 2048$ for which no irreducible trinomial of degree m exists, there is $\gamma \in \mathbb{F}_{2^m}$ having the optimal XOR count, i.e., $\mathrm{wt}_{\oplus}(\gamma) = 2$. Moreover, the minimal polynomial of γ is irreducible pentanomial of degree m.*

It is readily seen that the lightest element γ in Fact 1 satisfies the near-MDS conditions over $\mathbb{F}_{2^m}$ for $8 \leq m \leq 2048$. For $4 \leq m \leq 7$, one can verify that there exists an α such that $\mathrm{wt}_{\oplus}(\alpha) = 1$ and α satisfies the near-MDS conditions. This leads to the following result.

Corollary 3. *Let m be a positive integer with $4 \leq m \leq 2048$. For $n = 5, 6$, the generic near-MDS matrices of order n given by (2) and (3) have instantiations with lowest XOR count over $\mathbb{F}_{2^m}$. For $n = 7, 8$, the matrices of order n in Table 2 have instantiations with lowest XOR count over $\mathbb{F}_{2^m}$.*

Notice that the condition set only excludes a small number of elements in a large field $\mathbb{F}_{2^m}$ when $m > 2048$. So it seems that the lightest α satisfying the near-MDS conditions exists for all $m > 2048$. Further study of the existence of α for $m > 2048$ is left as an open problem.

Discussions. A long-standing problem in the study of lightweight diffusion matrices over finite fields is to find the *global optimal solutions*, i.e., matrices of a given order with prescribed branch numbers and lowest XOR count. Very recently, Sarkar and Syed in [SS16] propose 4×4 MDS matrices with lowest XOR count over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. However, the construction of global optimal solutions for MDS matrices with other parameters remains an open problem [JV04, BKL16]. Junod and Vaudenay in [JV04] present some exact values of the maximum occurrences of 1 in an MDS matrix. However, maximum occurrence of 1 does not directly ensure the lowest XOR count property. Recently, Beierle *et al.* in [BKL16] characterize elements in finite fields with lowest XOR count. Some very efficient MDS matrices are proposed based on these optimal elements. However, it is still

unknown whether these *local optimal solutions* can lead to global optimal solutions for MDS matrices.

This section shows that local optimal solutions can lead to global optimal solutions for near-MDS matrices. By Theorems 2 and 3, the near-MDS matrices with lowest XOR count are constructed with the lightest elements in the finite filed. Moreover, the explicit near-MDS matrices can be generated systematically from generic matrices rather than by an *ad hoc* method for a specific finite field. This also enables one to find global optimal solutions for near-MDS matrices over a large number of fields.

It is worth noticing that for $2 \leq n \leq 4$, the near-MDS matrices given in Lemma 6 are global optimal solutions over any finite field since they are composed of 0 and 1 and attain v_0^n and v_1^n simultaneously. This together with Corollary 3 shows that for $2 \leq n \leq 8$ the $n \times n$ near-MDS matrices with lowest XOR count are obtained over $\mathbb{F}_{2^m}$ with $4 \leq m \leq 2048$.

5 Involutory near-MDS matrices

This section presents some results on involutory near-MDS matrices. First, we summarize involutory near-MDS of order $2, 3$ and 4. Then for $n > 4$ we give a nonexistence result of circulant involutory near-MDS matrices. Hence, the Hadamard matrices over finite fields are introduced and their properties are provided. This allows us to find involutory near-MDS Hadamard matrices of order 8.

Cases $n = 2, 3$ and 4. It is easy to verify that the near-MDS matrices of order 2 and 4 given in Lemma 6 are involutory. However, for $n = 3$ the matrix $\mathrm{circ}(0, 1, 1)$ is not involutory. Furthermore, direct computation show that a $\{0, 1\}$-matrix of order 3 cannot be involutory.

To construct generic near-MDS matrices of order 3, we performed an exhaustive search for matrices with elements in the set $\{0, 1, x, x^{-1}, x^2, 1+x\}$. Our experimental results show that there is no 3×3 generic near-MDS matrices composed of elements $\{0, 1, x, x^{-1}, x^2\}$. Indeed, there are 12 generic involutory near-MDS with entries in $\{0, 1, x, 1 + x\}$. For instance, the following matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ \alpha & 1+\alpha & \alpha \\ 1+\alpha & 1+\alpha & \alpha \end{pmatrix}$$

is involutory near-MDS for any $\alpha \neq 0, 1$. Consequently, for $n = 2, 3$ and 4, we list some lightweight involutory near-MDS matrices of order n in Table 6.

Table 6: Involutory near-MDS matrices of order less than or equal to 4

n	Entries Set	Examples	#Matrices	References
2	$\{0, 1\}$	$\mathrm{circ}(0, 1)$	4	[CK08]
3	$\{0, 1, \alpha, 1 + \alpha\}$ $\alpha \neq 0, 1$	$\begin{pmatrix} 0 & 1 & 1 \\ \alpha & 1+\alpha & \alpha \\ 1+\alpha & 1+\alpha & \alpha \end{pmatrix}$	12	This section
4	$\{0, 1\}$	$\mathrm{circ}(0, 1, 1, 1)$	10	[CK08, BKL16]

When $n > 4$, we have the following result analogous to the fact that there is no circulant involutory MDS matrix over finite fields [GR15].

Proposition 3. *For $n > 4$, any $n \times n$ circulant involutory matrices over $\mathbb{F}_{2^m}$ cannot be near-MDS.*

Proof. Consider the case $n = 2k$, where $k > 2$. Let $M = \mathrm{circ}(a_0, a_1, \cdots, a_{2k-1})$ be a $(2k) \times (2k)$ circulant involutory matrix over $\mathbb{F}_{2^m}$. Then $M^2 = I_n$. Direct computation shows that $M^2 = \mathrm{circ}(a_0^2 + a_k^2, 0, a_1^2 + a_{k+1}^2, 0, \cdots, a_{k-1}^2 + a_{2k-1}^2, 0)$. This implies that $a_0 + a_k = 1$ and $a_i = a_{k+i}$ for $1 \leq i \leq k-1$. Thus, the sum of the 0-th and k-th columns of M is $(1, 0, \cdots, 1, 0, \cdots, 0)^\mathsf{T}$. That is , $\mathcal{B}_d(M) \leq 4 < n$. Therefore, M is not near-MDS.

For $n = 2k+1$ we have $M^2 = \mathrm{circ}(a_0^2, a_{k+1}^2, a_1^2, a_{k+1}^2, \cdots, a_{2k}^2, a_k^2)$. It follows that $a_0 = 1$ and $a_i = 0$ for $1 \leq i \leq 2k$. Thus, M is not near-MDS. □

Proposition 3 inspires us to study other matrices than circulant matrices for $n > 4$.

Hadamard matrices. The definition of a Hadamard matrix is recalled below.

Definition 6. Let n be a power of 2. An $n \times n$ matrix H is *Hadamard* if there exist n elements $h_0, h_1, \cdots, h_{n-1}$ such that the (i, j)-entry of H can be represented by $H[i, j] = h_{i \oplus j}$. We denote the matrix H by $\mathrm{had}(h_0, h_1, \cdots, h_{n-1})$.

Analogously to circulant matrices, each row of a Hadamard matrix is a permutation of the first row. This allows one to implement the matrix efficiently [KPPY14, LS16, SKOP15]. The other desirable property is that it is easy to construct involutory matrices from Hadamard matrices.

Lemma 8. *([SKOP15]) An $n \times n$ Hadamard matrix $H = \mathrm{had}(h_0, h_1, \cdots, h_{n-1})$ is involutory, i.e., $H^2 = I_n$ if and only if $h_0 + h_1 + \cdots + h_{n-1} = 1$.*

By Lemma 2, a non-MDS matrix M is near-MDS if and only if for any $1 \leq g \leq n-1$ each $g \times (g+1)$ and $(g+1) \times g$ submatrix of M has at least one $g \times g$ non-singular submatrix. Note that a Hadamard matrix is symmetric, i.e., $H = H^\mathsf{T}$. This implies that there is a one-to-one corresponding between the $g \times (g+1)$ submatrices of a Hadamard matrix H and the $(g+1) \times g$ submatrices of H. Hence we have the following corollary.

Corollary 4. *Let H be a non-MDS Hadamard matrix of order n, where n is a positive integer with $n \geq 2$. Then H is near-MDS if and only if for any $1 \leq g \leq n-1$ each $g \times (g+1)$ (or $(g+1) \times g$) submatrix of H has at least one $g \times g$ non-singular submatrix.*

Corollary 4 halves the number of operations in checking the near-MDS property for Hadamard matrices. Consequently, Hadamard matrices are good candidates for constructing involutory near-MDS matrices.

Involutory near-MDS Hadamard matrices of order 8. Since we focus on the case $n > 4$ and the order of a Hadamard matrix is a power of 2, it is natural to consider the case $n = 8$. Similar to the search strategy in Sect. 3.1, we limit the entries of the Hadamard matrix to elements in the set $\{0, 1, x, x^{-1}, x^2\}$. For $\mathrm{had}(h_0, h_1, \cdots, h_{n-1})$, let N_δ be the number of times δ occurs in the multiset $\{h_0, h_1, \cdots, h_{n-1}\}$. Lemma 8 implies that

$$N_1 + N_x x + N_{x^{-1}} x^{-1} + N_{x^2} x^2 = 1 \pmod 2 . \tag{4}$$

We also have a trivial counting formula

$$N_0 + N_1 + N_x + N_{x^{-1}} + N_{x^2} = 8 . \tag{5}$$

We perform an exhaustive search for Hadamard matrices with parameters satisfying Eqs. (4) and (5). Experimental results show that any Hadamard matrix with four or less distinct entries from $\{0, 1, x, x^{-1}, x^2\}$ cannot be an involutory near-MDS matrix. Indeed, there are 2688 involutory near-MDS matrices from Hadamard matrices with five distinct entries $0, 1, x, x^{-1}, x^2$. Moreover, each of the matrices satisfies $N_0 = N_1 = 1$ and $N_x = N_{x^{-1}} = N_{x^2} = 2$.

To further analyze the properties of the involutory near-MDS matrices, the equivalence classes of Hadamard matrices are recalled from [SKOP15]. Let $H = \mathrm{had}(h_0, h_1, \cdots, h_{n-1})$ and denote $H^\sigma = \mathrm{had}(h_{\sigma(0)}, h_{\sigma(1)}, \cdots, h_{\sigma(n-1)})$, where σ is an index permutation. Two Hadamard matrices H and H^σ are equivalent if $\sigma(i) = i \oplus \alpha$ for $\alpha = 0, 1, \cdots, n-1$ or σ is a linear permutation with respect to the XOR operation, i.e., $\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j)$. This equivalent relation divides the set of Hadamard matrices into equivalence classes.

By Lemma 3 and Theorem 3 in [SKOP15], the following lemma holds.

Lemma 9. *([SKOP15]) Let s be a positive integer. Given the index set $\{0, 1, \cdots, 2^s - 1\}$, there are exactly $2^s \prod_{i=0}^{s-1}(2^s - 2^i)$ distinct index permutations generated by composition of linear permutations with respect to XOR operation and permutations having the form $\sigma(i) = i \oplus \alpha$.*

By Lemma 9 there are exactly $2^3 \prod_{i=0}^{2}(2^3 - 2^i) = 1344$ permutations for $n = 8$. We compute the equivalence classes of the 2688 involutory near-MDS Hadamard matrices with five distinct entries $0, 1, x, x^{-1}, x^2$. The experimental results are summarized in the following fact.

Fact 2. *The* 2688 *involutory near-MDS Hadamard matrices with five distinct entries $0, 1, x, x^{-1}, x^2$ can be classified into two different equivalence classes. Two representatives of the equivalence classes are*

$$\mathrm{had}(0, x^2, x^{-1}, x^2, x^{-1}, x, x, 1) \text{ and } \mathrm{had}(0, x^2, x^{-1}, x^{-1}, x^2, x, x, 1).$$

Moreover, each equivalence is exactly the set of matrices obtained by applying the 1344 *permutations to the corresponding representative.*

The representatives of the equivalence classes and the corresponding condition sets are listed in Table 7.

Table 7: Involutory near-MDS Hadamard matrices of order 8

Represntatives	Conditions to be near-MDS	Size of Equivalence Classes
$\mathrm{had}(0, x^2, x^{-1}, x^2, x^{-1}, x, x, 1)$	x $x+1$ x^2+x+1 x^3+x+1 x^3+x^2+1 x^4+x+1 $x^5+x^4+x^2+x+1$	1344
$\mathrm{had}(0, x^2, x^{-1}, x^{-1}, x^2, x, x, 1)$	x $x+1$ x^2+x+1 x^3+x+1 x^3+x^2+1 x^4+x+1 $x^4+x^3+x^2+x+1$ x^5+x^3+1	1344

Example 1. By taking the minimal polynomial of α as $x^4 + x^3 + 1$ and $x^8 + x^4 + x^3 + x + 1$, the matrix $\mathrm{had}(1, \alpha, \alpha, \alpha^2, 0, \alpha^2, \alpha^{-1}, \alpha^{-1})$ is involutory near-MDS over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively. The XOR count is 32 in $\mathbb{F}_{2^4}$ and 64 in $\mathbb{F}_{2^8}$.

Table 8: The minimum number of active S-boxes for SPN structures with ShiftRows and near-MDS matrices of order n

n	# Rounds															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	0	4	7	16	17	20	23	32	33	36	39	48	49	52	55	64
5	0	5	9	25	26	30	34	50	51	55	59	75	76	80	84	102
6	0	6	11	36	37	42	47	72	73	78	83	108	109	114	119	144
7	0	7	13	49	50	56	62	98	99	105	111	147	148	154	160	196
8	0	8	15	64	65	72	79	128	129	136	143	192	193	200	207	256

6 Security analysis

This section provides a primary analysis on the security property of near-MDS matrices. It is well known that resistance against linear and differential cryptanalysis is a standard design criterion for new designs. For the AES [Dae95, DR02], provable security against linear and differential cryptanalysis follows from the wide trail design strategy. We apply a similar proof strategy: after proving a lower bound on the number of active S-boxes for both differential and linear cryptanalysis, we use the maximum differential/linear probability of the S-boxes to derive an upper bound for the probability of the best characteristic. As is commonly done, the probability of the differential/linear hull is estimated by the probability of the best characteristic. Therefore the main task is to calculate the minimum number of active S-boxes.

In this section we consider S-boxes with optimal cryptographic properties. We define a linear layer by combining our near-MDS matrices of order n with the ShiftRows operation of AES, i.e., the word in row i and column j $(0 \leq i, j \leq n-1)$ cyclically moves to position $(j - i) \bmod n$.

By applying the technique based on Mixed-Integer Linear Programming (MILP) [MWGP11], we obtain lower bounds on the number of differential and linear active S-boxes for SPN structures. The results are shown in Table 8. As described above, given a well-chosen S-box with maximum differential/linear probability, one can immediately compute the upper bounds for any differential/linear characteristics. From those, it shows that our linear layers can provide sufficient security against differential/linear cryptanalysis.

We note that the lower bounds also allow to evaluate the efficiency of matrices as well. For example, by specifying the nonlinear layers (e.g. S-boxes) and hardware architectures, one can compute the FOAM values of the primitives based on near-MDS matrices. Hence, our work will be useful for future design of lightweight ciphers based on near-MDS matrices.

Banik *et al.* in [BBI+15] show that the ShiftRows operation from AES is not always the best choice when near-MDS matrices are chosen in the MixColumns. It is an open problem to investigate how to design an efficient shuffle/permutation to speed up the diffusion with a near-MDS matrix.

7 Conclusion

This paper presents new designs of lightweight linear diffusion layer from lightweight near-MDS matrices. For $5 \leq n \leq 9$, some generic $n \times n$ near-MDS circulant matrices are found. The implementation cost of instantiations of the generic near-MDS matrices is also considered. This allows us to propose some near-MDS matrices of order n having the lowest XOR count among all near-MDS matrices of the same order, where $5 \leq n \leq 8$. Further, we provide some results on involutory near-MDS matrices of small orders and propose involutory near-MDS Hadamard matrices of order 8. Finally, we give a primary

analysis of the security of the proposed linear layers.

Acknowledgements

The authors would like to thank Bart Preneel and the anonymous reviewers of FSE for their comments and suggestions. This work was supported in part by the Research Council KU Leuven (C16/15/058). In addition, this work was partially supported by the Research Council KU Leuven (OT/13/071) and by the Flemish Government through FWO projects (G0842.13 and G.0130.13) and by the European Union's Horizon 2020 research and innovation programme under grant agreement H2020-MSCA-ITN-2014-643161 ECRYPT-NET, and the National Natural Science Foundation of China (No. 61472250, No. 61672347) and Major State Basic Research Development Program (973 Plan, No. 2013CB338004).

References

[ADK+14] Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçin. Block ciphers - focus on the linear layer (feat. PRIDE). In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 57–76. Springer, Heidelberg, August 2014.

[AF13] Daniel Augot and Matthieu Finiasz. Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 1551–1555, 2013.

[AF15] Daniel Augot and Matthieu Finiasz. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 3–17. Springer, Heidelberg, March 2015.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Heidelberg, November / December 2015.

[BBK+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES 2013*, volume 8086 of *LNCS*, pages 142–158. Springer, Heidelberg, August 2013.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, 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 - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, Heidelberg, December 2012.

[Ber13] Thierry P. Berger. Construction of recursive MDS diffusion layers from Gabidulin codes. In Goutam Paul and Serge Vaudenay, editors, *IN-*

DOCRYPT 2013, volume 8250 of *LNCS*, pages 274–285. Springer, Heidelberg, December 2013.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Heidelberg, August 2016.

[BKL16] 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, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 625–653. Springer, Heidelberg, August 2016.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Heidelberg, August 1991.

[CJK15] Ting Cui, Chenhui Jin, and Zhiyin Kong. On compact Cauchy matrices for substitution-permutation networks. *IEEE Trans. Computers*, 64(7):2098–2102, 2015.

[CK08] Jiali Choy and Khoongming Khoo. New applications of differential bounds of the SDS structure. In Tzong-Chen Wu, Chin-Laung Lei, Vincent Rijmen, and Der-Tsai Lee, editors, *ISC 2008*, volume 5222 of *LNCS*, pages 367–384. Springer, Heidelberg, September 2008.

[CLRS09] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms (3rd ed.)*. MIT Press, 2009.

[Dae95] Joan Daemen. *Cipher and Hash Function Design. Strategies based on linear and differential cryptanalysis.* PhD thesis, Katholieke Universiteit Leuven, 1995.

[dB96] Mario A. de Boer. Almost MDS codes. *Des. Codes Cryptography*, 9(2):143–155, 1996.

[DL95] Stefan M. Dodunekov and Ivan Landgev. On near-MDS codes. *J. Geom.*, 54(1):30–43, 1995.

[Dod09] Stefan M. Dodunekov. Applications of near MDS codes in cryptography. In *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pages 81–86. 2009.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.

[DR09] Joan Daemen and Vincent Rijmen. Codes and provable security of ciphers-extended abstract. In *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pages 69–80. 2009.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 222–239. Springer, Heidelberg, August 2011.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, Heidelberg, September / October 2011.

[GR15] Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptography and Communications*, 7(2):257–287, 2015.

[JPS] Jérémy Jean, Thomas Peyrin, and Siang Meng Sim.

[JV04] Pascal Junod and Serge Vaudenay. Perfect diffusion primitives for block ciphers. In Helena Handschuh and Anwar Hasan, editors, *SAC 2004*, volume 3357 of *LNCS*, pages 84–99. Springer, Heidelberg, August 2004.

[KPPY14] Khoongming Khoo, Thomas Peyrin, Axel York Poschmann, and Huihui Yap. FOAM: Searching for hardware-optimal SPN structures and components with a fair comparison. In Lejla Batina and Matthew Robshaw, editors, *CHES 2014*, volume 8731 of *LNCS*, pages 433–450. Springer, Heidelberg, September 2014.

[LS16] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 101–120. Springer, Heidelberg, March 2016.

[LW16] Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 121–139. Springer, Heidelberg, March 2016.

[Mat94] Mitsuru Matsui. Linear cryptoanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, pages 57–76, 2011.

[SDMO12] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Behnaz Omoomi. On construction of involutory MDS matrices from vandermonde matrices in GF(2^q). *Des. Codes Cryptography*, 64(3):287–308, 2012.

[SDMS12] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Recursive diffusion layers for block ciphers and hash functions. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 385–401. Springer, Heidelberg, March 2012.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28(4):656–715, 1949.

[SKOP15] Siang Meng Sim, Khoongming Khoo, Frédérique E. Oggier, and Thomas Peyrin. Lightweight MDS involution matrices. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 471–493. Springer, Heidelberg, March 2015.

[SS16] Sumanta Sarkar and Habeeb Syed. Lightweight diffusion layer: Importance of toeplitz matrices. Cryptology ePrint Archive, Report 2016/835, 2016. http://eprint.iacr.org/2016/835.

[Swa62] Richard G. Swan. Factorization of polynomials over finite fields. *Pacific J. of Math.*, 12(3):1099–1106, 1962.

[Vau95] Serge Vaudenay. On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 286–297. Springer, Heidelberg, December 1995.

[VR06] G. Viswanath and B. Sundar Rajan. A matrix characterization of near-MDS codes. *Ars Comb.*, 79:289–294, 2006.

[WWW13] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In Lars R. Knudsen and Huapeng Wu, editors, *SAC 2012*, volume 7707 of *LNCS*, pages 355–371. Springer, Heidelberg, August 2013.

[YMT97] A.M. Youssef, S. Mister, and S.E. Tavares. On the design of linear transformations for substitution permutation encryption networks. In Carlisle Adams and Mike Just, editors, *SAC 1997*, LNCS, pages 40–48. Springer, Heidelberg, August 1997.

A Proof of Theorem 1

Before presenting the proof we introduce some definitions of strings from [CLRS09]. A *string* over a finite set S is a sequence of elements of S. In the proof we focus on strings over set $\{1, x\}$. A *substring* s' of a string s is an ordered sequence of consecutive elements of s. Define a *run* of a string to be the maximal string of consecutive identical elements [MS77]. We call a string and a run of length k a k-string and a k-run respectively. For instance, the 8-string $11xxx1xx$ has four runs: 11, xxx, 1, xx.

Proof. Lemma 6 implies that there is no near-MDS circulant matrix with only two entries $0, 1$ or $0, x$. So we now assume that $N_1 N_x > 0$. Note that N_0 can be 0 or 1 by Proposition 1. We first consider the case $N_0 = 1$. As stated in Sect. 3.2, one only needs to consider the circulant matrices of the form $\mathrm{circ}(0, a_1, a_2, \cdots, a_{n-1})$.

To prove the result, it suffices to consider the strings of length three, i.e., $a_i a_j a_k$ with $1 \le i, j, k \le n-1$. A **matched pair** of strings $a_{i_1} a_{i_2} a_{i_3}$ and $a_{j_1} a_{j_2} a_{j_3}$ satisfies the following two conditions:

1. there exists an integer k such that $j_l - i_l \equiv k \pmod n$ and $k \not\equiv 0 \pmod n$ for $l = 1, 2, 3$;
2. $a_{i_1} a_{i_2} a_{i_3} = a_{j_1} a_{j_2} a_{j_3}$ as strings over $\{1, x\}$.

Indeed, the existence of a matched pair yields that the matrix $\mathrm{circ}(0, a_1, a_2, \cdots, a_{n-1})$ has the 2×3 submatrix

$$\begin{pmatrix} a_{i_1} & a_{i_2} & a_{i_3} \\ a_{j_1} & a_{j_2} & a_{j_3} \end{pmatrix} = \begin{pmatrix} a_{i_1} & a_{i_2} & a_{i_3} \\ a_{i_1} & a_{i_2} & a_{i_3} \end{pmatrix}$$

with three singular 2×2 submatrices. Then, by taking $g = 2$ in Lemma 2, we conclude that the matrix $\mathrm{circ}(0, a_1, a_2, \cdots, a_{n-1})$ is not near-MDS. Hence, to prove the theorem, we aim to find the matched pairs of the $(n-1)$-string $s = a_1 a_2 \cdots a_{n-1}$. One can divide the proof into four different cases in terms of the length of the longest runs (LLR) of s denoted by $\mathrm{LLR}(s)$.

Case 1. $\mathrm{LLR}(s) \ge 4$. In this case, there exists some i such that $a_i a_{i+1} a_{i+2} a_{i+3} = aaaa$ for $a \in \{1, x\}$. Hence, $a_i a_{i+1} a_{i+2} = a_{i+1} a_{i+2} a_{i+3} = aaa$, as required.

Case 2. $\mathrm{LLR}(s) = 3$. Suppose that $a_i a_{i+1} a_{i+2} = aaa$. If there is another run with length greater than or equal to two, i.e., $a_j a_{j+1} = bb$, then we have $a_i a_{i+1} a_j = a_{i+1} a_{i+2} a_{j+1} = aab$, as desired. Otherwise, all remaining runs are 1-runs. According to the position of the 3-run aaa in s, s contains at least one of the following five substrings:

$$ababaaa \quad babaaab \quad abaaaba \quad baaabab \quad aaababa\,.$$

Direct verifications show that there is at least one matched pair.

Case 3. $\mathrm{LLR}(s) = 2$. The proof of this case can be split into four subcases.

Subcase 3.1 There are at least three distinct 2-runs. Suppose that $a_i a_{i+1}, a_j a_{j+1}$ and $a_k a_{k+1}$ are 2-runs. Then $a_i = a_{i+1}, a_j = a_{j+1}$, and $a_k = a_{k+1}$. This leads to a matched pair $a_i a_j a_k$ and $a_{i+1} a_{j+1} a_{k+1}$.

Subcase 3.2 There are exactly two 2-runs aa and bb with $a \ne b$. Note that all remaining runs are of length 1. It is readily seen that there can be 0, 2 or at least 4 elements between aa and bb in s.

First, suppose that there are at least four elements between aa and bb. This yields the substrings $ababa$ or $babab$ of s. Thus, a matched pair occurs.

Secondly, if there are exactly two elements between aa and bb, i.e., s has the substring $aababb$ (resp. $bbabaa$), then s contains the substrings $baababb$ or $aababba$ (resp. $abbabaa$ or $bbabaab$). In these cases, it is easy to find a matched pair. For instance, let $a_i a_{i+1} a_{i+2} a_{i+3} a_{i+4} a_{i+5} a_{i+6} = baababb$, then we have $a_i a_{i+1} a_{i+3} = a_{i+3} a_{i+4} a_{i+6} = bab$.

Finally, we suppose that *bbaa* or *aabb* is a substring of s. It suffices to consider *aabb*. In terms of the position of *aabb* in s, s contains at least one of the following four substrings:

$$aabbaba \quad babaabb \quad baabbab \quad abaabba\,.$$

For the latter two substrings, it is easy to find a matched pair while a verification of the first two substrings can be done by considering $n = 8$ and $n \geq 9$. We omit the details here.
Subcase 3.3 There are exactly two *aa* runs. The relative position of two *aa* runs in s implies that s contains at least one of the following four substrings:

$$aabaab \quad baabaa \quad aababaa \quad babab\,.$$

It is obvious that there is at least one matched pair.
Subcase 3.4 There are exactly one 2-run *aa*. Concerning the position of *aa* in s, it follows that s contains at least one of the following five substrings:

$$aababab \quad baababa \quad babaaba \quad bababaa \quad babab\,.$$

Direct verifications show that there is at least one matched pair.

The four subcases together yield Case 3.
Case 4. $\mathrm{LLR}(s) = 1$. It follows that one can always find the substring $x1x1x$. Thus, in this case, at least one matched pair exists.

Note that $\mathrm{LLR}(s) \geq 1$. Then the above four cases combine to give the result when $N_1N_x > 0$ and $N_0 = 1$. The case that $N_0 = 0, N_1N_x > 0$ can be proved in the same manner. Therefore, the theorem is proved. □

B Tables

In Table 9, we provide a list of generic near-MDS circulant matrices of order $5 \leq n \leq 9$ over the finite field $\mathbb{F}_{2^m}$. Based on a generic matrix, one can obtain a concrete near-MDS matrix by substituting x with $\alpha \in \mathbb{F}_{2^m}$ such that α is not a root of any polynomial in the corresponding condition set which is given in Table 10. The determinants of the generic matrices are given as well.

Note that A and A^{T} have exactly the same properties, including near-MDS property, determinant and XOR count. So we only list the matrix A when $A \neq A^{\mathsf{T}}$. For instance, both $\mathrm{circ}(0, x, 1, 1, 1)$ and $\mathrm{circ}(0, 1, 1, 1, x)$ are near-MDS under certain conditions, but we only present the former one in Table 9 since $\mathrm{circ}(0, x, 1, 1, 1) = \mathrm{circ}(0, 1, 1, 1, x)^{\mathsf{T}}$.

Table 9: List of generic near-MDS circulant matrices of order $5 \leq n \leq 9$

n	Coefficients of the first row	Condition sets (cf.Table 10)	Determinants
5	$(0, x, 1, 1, 1)$	S_0	$x^5 + x^3 + x + 1$
	$(0, 1, x, 1, 1)$		
6	$(0, x, 1, 1, 1, x)$	S_0	x^4
	$(0, x, 1, x, 1, 1)$	S_0	$x^4 + x^2 + 1$
	$(0, 1, x, x, 1, 1)$	S_2	$x^4 + x^2 + 1$
	$(0, x^{-1}, x, 1, 1, 1)$	S_1	$x^6 + x^4 + 1 + x^{-4} + x^{-6}$
	$(0, x, x^{-1}, 1, 1, 1)$	S_2	$x^6 + x^4 + 1 + x^{-4} + x^{-6}$
	$(0, x^{-1}, 1, x, 1, 1)$	S_1	$x^6 + 1 + x^{-2} + x^{-4} + x^{-6}$
	$(0, x, 1, x^{-1}, 1, 1)$	S_1	$x^6 + x^4 + x^2 + 1 + x^{-6}$
	$(0, x^{-1}, 1, 1, x, 1)$	S_4	$x^6 + x^2 + 1 + x^{-2} + x^{-6}$
	$(0, x, 1, 1, x^{-1}, 1)$	S_5	$x^6 + x^2 + 1 + x^{-2} + x^{-6}$
	$(0, x^{-1}, 1, 1, 1, x)$	S_0	$x^6 + x^4 + 1 + x^{-4} + x^{-6}$
	$(0, 1, x^{-1}, x, 1, 1)$	S_3	$x^6 + 1 + x^{-2} + x^{-4} + x^{-6}$
	$(0, 1, x, x^{-1}, 1, 1)$	S_3	$x^6 + x^4 + x^2 + 1 + x^{-6}$
7	$(0, x^{-1}, 1, x, 1, 1, 1)$	S_6	$x^7 + x^5 + x^3 + x + x^{-5} + x^{-7}$
	$(0, x, 1, x^{-1}, 1, 1, 1)$		$x^7 + x^5 + x^{-1} + x^{-3} + x^{-5} + x^{-7}$
	$(0, x^{-1}, 1, 1, 1, x, 1)$		$x^7 + x^5 + x^{-1} + x^{-3} + x^{-5} + x^{-7}$
	$(0, x, 1, 1, 1, x^{-1}, 1)$		$x^7 + x^5 + x^3 + x + x^{-5} + x^{-7}$
	$(0, 1, x^{-1}, x, 1, 1, 1)$		$x^7 + x^5 + x^{-1} + x^{-3} + x^{-5} + x^{-7}$
	$(0, 1, x, x^{-1}, 1, 1, 1)$		$x^7 + x^5 + x^3 + x + x^{-5} + x^{-7}$
8	$(0, x, x^{-1}, 1, x, 1, 1, 1)$	S_7	x^{-8}
	$(0, x, 1, x, x^{-1}, 1, 1, 1)$	S_8	x^{-8}
	$(0, x, 1, 1, x^{-1}, 1, 1, x)$	S_8	x^{-8}
	$(0, 1, x^{-1}, 1, x, x, 1, 1)$	S_7	x^{-8}
	$(0, 1, 1, x, x^{-1}, x, 1, 1)$	S_8	x^{-8}
	$(0, x^{-1}, x, 1, x^{-1}, 1, 1, 1)$	S_7	x^8
	$(0, x^{-1}, 1, x^{-1}, x, 1, 1, 1)$	S_8	x^8
	$(0, x^{-1}, 1, 1, x, 1, 1, x^{-1})$	S_8	x^8
	$(0, 1, x, 1, x^{-1}, x^{-1}, 1, 1)$	S_7	x^8
	$(0, 1, 1, x^{-1}, x, x^{-1}, 1, 1)$	S_8	x^8
9	$(0, x, x^{-1}, x, x, x^{-1}, 1, 1, x)$	S_9	0
	$(0, x, x, x, 1, x^{-1}, 1, x, x^{-1})$	S_9	
	$(0, x^{-1}, x, 1, x, x, x, x^{-1}, 1)$	S_9	
	$(0, x^{-1}, x, x^{-1}, x^{-1}, x, 1, 1, x^{-1})$	S_{10}	
	$(0, x^{-1}, x^{-1}, x^{-1}, 1, x, 1, x^{-1}, x)$	S_{10}	
	$(0, x, x^{-1}, 1, x^{-1}, x^{-1}, x^{-1}, x, 1)$	S_{10}	

Table 10: Condition sets in Table 9

Sets	Conditions
S_0	$x, x+1, x^2+x+1$
S_1	$x, x+1, x^2+x+1, x^3+x+1$
S_2	$x, x+1, x^2+x+1, x^3+x^2+1$
S_3	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1$
S_4	$x, x+1, x^2+x+1, x^3+x+1, x^4+x^3+1$
S_5	$x, x+1, x^2+x+1, x^3+x^2+1, x^4+x+1$
S_6	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x^3+x^2+x+1$
S_7	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$
S_8	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x^3+x^2+x+1, x^5+x^4+x^3+x^2+1$
S_9	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1$ $x^4+x^3+x^2+x+1, x^5+x^2+1, x^5+x^3+1, x^5+x^3+x^2+x+1$ $x^5+x^4+x^2+x+1, x^5+x^4+x^3+x+1, x^5+x^4+x^3+x^2+1$ $x^6+x^5+x^4+x^2+1, x^7+x^4+x^3+x^2+1, x^7+x^6+x^4+x+1$ $x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^2+1$
S_{10}	$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1$ $x^4+x^3+x^2+x+1, x^5+x^2+1, x^5+x^3+1, x^5+x^3+x^2+x+1$ $x^5+x^4+x^2+x+1, x^5+x^4+x^3+x+1, x^5+x^4+x^3+x^2+1$ $x^6+x^4+x^2+x+1, x^7+x^5+x^4+x^3+1, x^7+x^6+x^3+x+1$ $x^{12}+x^{10}+x^6+x^5+x^4+x^3+x^2+x+1$