information

MDPI

Article

More Constructions of Light MDS Transforms Based on Known MDS Circulant Matrices

Jin-Bo Wang *, You Wu and Yu Zhou

Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China; doctor03@163.com (Y.W.); 18981672555@163.com (Y.Z.)
* Correspondence: wyou134@163.com

Abstract: Maximum distance separable (MDS) codes have the maximum branch number in cryptography, and they are generally used in diffusion layers of symmetric ciphers. The diffusion layer of the Advanced Encryption Standard (AES) uses the circulant MDS matrix with the row element of $\{2;3;1;1\}$ in $\mathbb{F}_{2^8}$. It is the simplest MDS matrix in $\mathbb{F}_{2^n}^4$, recorded as $\boldsymbol{A} = Circ(2;3;1;1)$. In this paper, we study the more extensive MDS constructions of $\boldsymbol{A}$ in $\mathbb{F}_{2^n}^4$. By transforming the element multiplication operation in the finite field into the bit-level operation, we propose a multivariable operation definition based on simple operations, such as cyclic shift, shift, and XOR. We apply this multivariable operation to more lightweight MDS constructions of $\boldsymbol{A}$ and discuss the classification of the MDS clusters. We also give an example of the MDS cluster of $\boldsymbol{A}$. Without changing the structure, elements, and the implementation cost of the known MDS matrix, the number of existing MDS transformations is expanded to $n^2/2$ times that of its original. The constructions in this paper provide rich component materials for the design of lightweight cryptographic algorithms.

Keywords: block cipher; MDS diffusion layers; circulant matrices; branch number; equivalence class

check for updates

Citation: Wang, J.-B.; Wu, Y.; Zhou, Y. More Constructions of Light MDS Transforms Based on Known MDS Circulant Matrices. *Information* **2022**, *13*, 347. https://doi.org/10.3390/info13070347

Received: 12 June 2022
Accepted: 14 July 2022
Published: 18 July 2022

1. Introduction

The design of modern cryptographic algorithms generally follows the principles of confusion and diffusion [1]. Diffusion layers are critical components of symmetric ciphers. It is an important means to achieve complex relationships between plaintexts and ciphertexts. By using the diffusion layer, each bit of the plaintext will affect multiple bits of the ciphertext, thus ensuring the security of the cryptographic algorithm. Maximum distance separable (MDS) codes have the maximum number of branches, so they are often used in cryptography to construct optimal diffusion layers of block ciphers, stream ciphers, and hash algorithms. For instance, the diffusion layer of the Advanced Encryption Standard (AES [2]) uses the simplest MDS matrix over $\mathbb{F}_{2^{4n}}$, which is a circulant MDS matrix with a row element of $\{2;3;1;1\}$ in $\mathbb{F}_{2^8}$, recorded as $\boldsymbol{A} = Circ(2;3;1;1)$. The diffusion layer of SM4 [3] uses the MDS transformation based on a 32-bit rotational-XOR operation. In cryptographic literature, numerous papers [4–17] have studied various aspects of MDS diffusion layers, including their structure, from mathematical viewpoints on rings and fields, as well as minimizing their implementation costs in software and/or hardware applications. For example, Mirzaee et al. [12] placed lightweight multiplication on MDS matrices in fields; Xiang et al. [14,15] proposed MDS matrices as the best implementations produced by various algorithms up to now and [16,17] provided some nonlinear MDS diffusion layers.

Currently, for known MDS matrices on $\mathbb{F}_{2^n}$, the operations and quantities are limited by irreducible polynomials in the finite field. In order to obtain more MDS diffusion layers from MDS matrices on fields, it is necessary to change the matrix form or component element, such by as replacing specific elements of the matrix with different primitive elements in the finite field so as to construct different MDS transformations [18]. For these simple MDS matrices, the manner by which to construct many more, and more extensive, MDS transformations, without changing their forms, component elements, and implementation costs, is of particular significance for the enrichment of the cognition of MDS and the improving of the adaptability of MDS diffusion layers.

This paper studies the more extensive MDS construction that is based on the circulant MDS matrix $Circ(2;3;1;1)$ (abbreviated as $\boldsymbol{A}$). With the aid of introducing a parametric map, defined by transforming the multiplication operation of $\boldsymbol{A}$ elements in $\mathbb{F}_{2^n}$ into bit-wise multivariable operation with cyclic shift and XOR, we extend the operation of matrix $\boldsymbol{A}$ to obtain more 4×4 MDS diffusion layers. We use the definition of the multivariable parametric map to obtain more MDS constructions based on $\boldsymbol{A}$, and we propose the connection between MDS clusters and the equivalence classification. Then, examples of the MDS cluster based on $\boldsymbol{A}$ over $\mathbb{F}_{2^8}^4$ are given. All such MDS constructions proposed in this paper have equally low-cost implementations, and the number of MDS is expanded to $n^2/2$ times that of the original construction. These constructions we proposed can be widely applied to the design of lightweight cryptographic algorithms which is for the purpose of constraining resources, such as IoTs and wireless communication environments.

This article is organized as follows: In Section 2, we give preliminary notations and definitions. Section 3 provides theoretical conclusions and examples for more extensive MDS constructions of $\boldsymbol{A}$, and Section 4 is devoted to the conclusion.

2. Notations and Definitions

The binary digit 0 or 1 is called "1 bit" or "bit". Without losing generality, we specify that the most significant bit of data is always on the far left of its binary digits, and the lowest significant bit of data is always on the rightmost of its binary digits.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and $\mathbb{F}_2^n$ be the n-dimensional linear space over $\mathbb{F}_2$. We denote the multiplication in $\mathbb{F}_{2^n}$ by $\cdot$ and the addition in $\mathbb{F}_{2^n}$ by $\oplus$. The operation "$<<< t$" represents the left cyclic shift for t bits, and "&" denotes bitwise *and* operation. $x|_t$ denotes the t-th bit of x. "$\times$" is the ordinary multiplication function.

For any $\mathrm{X} = (\mathrm{x}_0, \mathrm{x}_1, \dots, \mathrm{x}_{\mathrm{n}-1}) \in \mathbb{F}_{2^\mathrm{n}}^\mathrm{m}$, the weight (denoted by $\mathrm{wt(X)}$) of X over $\mathbb{F}_{2^\mathrm{n}}$ is defined as

$$\mathrm{wt}(\mathrm{X}) = |\{\mathrm{i} : 1 \le \mathrm{i} \le \mathrm{m}, \mathrm{x}_\mathrm{i} \ne 0\}|.$$

Let F be a map on $\mathbb{F}_{2^\mathrm{n}}^\mathrm{m}$. The branch number (denoted by $\mathrm{Br_n(F)}$, or $\mathrm{Br(F)}$) of F over $\mathbb{F}_{2^\mathrm{n}}$ is defined as

$$\mathrm{Br_n(F)} = \min_{\mathrm{X,Y} \in \mathbb{F}_{2^\mathrm{n}}^\mathrm{m},\, \mathrm{X} \ne \mathrm{Y}} \{\mathrm{wt}(\mathrm{X} \oplus \mathrm{Y}) + \mathrm{wt}(\mathrm{F}(\mathrm{X}) \oplus \mathrm{F}(\mathrm{Y}))\}.$$

Definition 1. Let F be a map on $\mathbb{F}_{2^n}^m$. F is called MDS (over $\mathbb{F}_{2^n}$) if $Br(F) = m + 1$.

In this paper, we investigate the 4×4 circulant MDS matrix $Circ(2;3;1;1)$ used in the diffusion layer of AES, which is an MDS transformation with the simplest matrix form on $\mathbb{F}_{2^8}^4$. Its implementation cost is less than 92 XOR logic gates [14]. The circulant MDS matrix $Circ(2;3;1;1)$ on $\mathbb{F}_{2^n}^4$ is denoted as $\boldsymbol{A}$.

$$\boldsymbol{A} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Let $X = (x_0, x_1, \dots, x_3) \in \mathbb{F}_{2^n}^4$ be the input, and $Y = (y_0, y_1, \dots, y_3) \in \mathbb{F}_{2^n}^4$ be the output; then, the operation of $\boldsymbol{A}$ is expressed as follows:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

that is,

$$y_0 = 2{\cdot}x_0 \oplus 3{\cdot}x_1 \oplus 1{\cdot}x_2 \oplus 1{\cdot}x_3$$
$$y_1 = 1{\cdot}x_0 \oplus 2{\cdot}x_1 \oplus 3{\cdot}x_2 \oplus 1{\cdot}x_3$$
$$y_2 = 1{\cdot}x_0 \oplus 1{\cdot}x_1 \oplus 2{\cdot}x_2 \oplus 3{\cdot}x_3$$
$$y_3 = 3{\cdot}x_0 \oplus 1{\cdot}x_1 \oplus 1{\cdot}x_2 \oplus 2{\cdot}x_3$$

where both x_i and y_i are n-bit, and $3{\cdot}x_i = 2{\cdot}x_i \oplus x_i$, $i \in \{0,\ 1,\ 2,\ 3\}$.

According to the general understanding, the operations of matrix $\boldsymbol{A}$ are multiplication and addition in $\mathbb{F}_{2^n}$. For a map f on $\mathbb{F}_{2^n}$ up to the choice of the monic irreducible polynomial of degree n, the double multiplication on $\mathbb{F}_{2^n}$ recorded as $xtime_f(x) = 2{\cdot}x$ has a representation as follows:

Lemma 1. Suppose that $f = x^n + a_0x^{n-1} + a_1x^{n-1} + \cdots + a_{n-2}x + 1$ is a monic irreducible polynomial of degree n, where $a_i \in \mathbb{F}_2,\ i = 0,1,\ldots,n-2$. Let $a_{n-1} = 0$, and the corresponding coeffcient $(a_0,\ a_1,\ \cdots,a_{n-1}\ )$ is denoted as α in $\mathbb{F}_{2^n}$. Then,

$$xtime_f(x) = (x <<< 1) \oplus ((x <<< 1)\Big|_{n-1} \times \alpha),\ x \in \mathbb{F}_{2^n}. \tag{1}$$

According to Equation (1), the operation of matrix $\boldsymbol{A}$ can be written in the following Equation (2), with a left cyclic shift and XOR operations based on a parameter α.

Let $z_0 = x_0 \oplus x_1$, $z_1 = x_1 \oplus x_2$, $z_2 = x_2 \oplus x_3$, $z_3 = x_3 \oplus x_0$; then, the operation of $\boldsymbol{A}$ is also expressed as follows:

$$\begin{aligned} y_0 &= (z_0 <<< 1) \oplus x_1 \oplus x_2 \oplus x_3 \oplus ((z_0 <<< 1)|_{n-1} \times \alpha) \\ y_1 &= (z_1 <<< 1) \oplus x_2 \oplus x_3 \oplus x_0 \oplus ((z_1 <<< 1)|_{n-1} \times \alpha) \\ y_2 &= (z_2 <<< 1) \oplus x_3 \oplus x_0 \oplus x_1 \oplus ((z_2 <<< 1)|_{n-1} \times \alpha) \\ y_3 &= (z_3 <<< 1) \oplus x_0 \oplus x_1 \oplus x_2 \oplus ((z_3 <<< 1)|_{n-1} \times \alpha) \end{aligned} \tag{2}$$

Whether the operation in Equation (2) is an MDS transformation depends on α.

Definition 2. The data $\alpha \in \mathbb{F}_{2^n}$ is called the MDS-generating element of $\boldsymbol{A}$ on $\mathbb{F}_{2^n}^4$, or for short, the MDS-generating element of $\boldsymbol{A}$, if α makes Equation (2) into an MDS transformation.

Obviously, the n-bit data $(a_0,\ a_1,\ \cdots,\ a_{n-2}\ ,0)$ corresponding to every monic irreducible polynomial $x^n + a_0x^{n-1} + a_1x^{n-1} + \cdots + a_{n-2}x + 1$ in $\mathbb{F}_{2^n}$ is the MDS-generating element of $\boldsymbol{A}$. It can be predicted that the number of MDS-generating elements of $\boldsymbol{A}$ is not less than the number of monic irreducible polynomials of degree n, which is indeed the case, as shown in Example 1.

Since the MDS-generating elements of $\boldsymbol{A}$ can be obtained according to the operations form of Equation (2), which is no longer limited to irreducible polynomials of degree n in $\mathbb{F}_{2^n}$, it is necessary to redefine $xtime_f(x) = 2{\cdot}x$, that is, to define the $xtime_\alpha(x)$ operation for parameter α in $\mathbb{F}_{2^n}$ as follows:

$$xtime_\alpha(x) = (x <<< 1) \oplus ((x <<< 1)|_{n-1} \times \alpha) \tag{3}$$

Next, we show how to generate more MDS transformations using each MDS-generating element of $\boldsymbol{A}$.

Let $h_{i,j}(\alpha):\ \mathbb{Z}\times\mathbb{Z}\times\mathbb{F}_{2^n}\rightarrow\mathbb{F}_{2^n}$ be a parametric function with two parameter variables (i,j) about the input $\alpha\in\mathbb{F}_{2^n}$. We parametrically extend the operation rule of the $xtime_\alpha(x)$ of Equation (3) and introduce $xtime_{h^\alpha_{i,j}}(x)$.

Definition 3. Let $t=(x<<<i)$ and $t_{n-1-j}=(x<<<i)|_{n-1-j}$, $x=(x_0x_1\ldots x_{n-1})\in\mathbb{F}_2^n$. $xtime_{h^\alpha_{i,j}}(x)$ is defined as

$$xtime_{h^\alpha_{i,j}}(x)=(x<<<i)\oplus\left((x<<<i)\Big|_{n-1-j}\times h_{i,j}(\alpha)\right) \tag{4}$$

where $0\le i\le n-1,\ 0\le j\le n-1$.

Now we use the $xtime_{h^\alpha_{i,j}}(x)$ operation defined in Equation (4) to replace the $2{\cdot}x$ operation in $\boldsymbol{A}$. Then, we obtain Equation (5), which is parametric with 3 parameter variables, $(i,j,\alpha)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{F}_{2^n}$ for $\boldsymbol{A}$, denoted by $A_{h^\alpha_{i,j}}$.

Let the input be $X=(x_0,x_1,x_2,x_3)\in\mathbb{F}^4_{2^n}$, and the output be $Y=(y_0,y_1,y_2,y_3)\in\mathbb{F}^4_{2^n}$; let

$$z_0=x_0\oplus x_1,\ z_1=x_1\oplus x_2,\ z_2=x_2\oplus x_3,\ z_3=x_3\oplus x_0.$$

Then, $Y=A_{h^\alpha_{i,j}}(X)$ is defined as follows:

$$\begin{array}{l} y_0=(z_0<<<i)\oplus x_1\oplus x_2\oplus x_3\oplus((z_0<<<i)\big|_{n-1-j}\times h_{i,j}(\alpha)) \\ y_1=(z_1<<<i)\oplus x_2\oplus x_3\oplus x_0\oplus((z_1<<<i)\big|_{n-1-j}\times h_{i,j}(\alpha)) \\ y_2=(z_2<<<i)\oplus x_3\oplus x_0\oplus x_1\oplus((z_2<<<i)\big|_{n-1-j}\times h_{i,j}(\alpha)) \\ y_3=(z_3<<<i)\oplus x_0\oplus x_1\oplus x_2\oplus((z_3<<<i)\big|_{n-1-j}\times h_{i,j}(\alpha)) \end{array} \tag{5}$$

According to the definition of $A_{h^\alpha_{i,j}}$, set $(i,j)=(1,0)$, $h_{1,0}(\alpha)=\alpha$, then $A_{h^\alpha_{1,0}}$ is the operation of $\boldsymbol{A}$ in Equation (2). Note that the MDS diffusion layer of AES is the operation of $\boldsymbol{A}$ in $\mathbb{F}_{2^8}$ with the irreducible polynomial $f=0\times 11b$, that is, $h_{1,0}(\alpha)=0\text{x}1a$ in Equation (5).

In this paper, let $h_{1,0}(\alpha)$ be an identity transformation of α.

3. Extended Constructions and Theoretical Aspects of the Known MDS

In order to determine whether $A_{h^\alpha_{i,j}}$ generates an MDS transformation of $\boldsymbol{A}$ on $\mathbb{F}^4_{2^n}$, we have Theorem 1.

Theorem 1. *Let* $(i,j,\alpha)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{F}_{2^n}$, *where* $0\le i,\ j<n$. *If i is an even number, then* $A_{h^\alpha_{i,j}}$ *cannot generate an MDS.*

Proof of Theorem 1. According to the definition of $Y=A_{h^\alpha_{i,j}}(X)$, let $X=(x_0,x_1,x_2,x_3)\in\mathbb{F}^4_{2^n}$, $Y=(y_0,y_1,y_2,y_3)\in\mathbb{F}^4_{2^n}$, and $x_0\ne 0$, $x_1,x_2,x_3=0$. Suppose that $(x_0<<<i)|_{n-1-j}=0$; then, we have

$$y_0=(x_0<<<i),\ y_1=x_0,\ y_2=x_0,\ y_3=x_0\ \oplus\ (x_0<<<i).$$

For y_3, while i is an even number, if we can find some $x_0\ne 0$ satisfying $x_0\ \oplus\ (x_0<<<i)=0$, then $Br\left(A_{h^\alpha_{i,j}}\right)\le 4$. According to Definition 1, we know that $A_{h^\alpha_{i,j}}$ cannot generate an MDS.

Let $x_0=(x_{0,0},x_{0,1},\ldots,x_{0,n-1})\in\mathbb{F}_2^n$, $(x_0<<<i=(x_{0,i},x_{0,i+1},\ldots,x_{0,n-1},x_{0,0},\ldots,x_{0,i-1})$, we have

$$\begin{array}{c} x_0\ \oplus\ (x_0<<<i) \\ =(x_{0,0},x_{0,1},\ \ldots,\ x_{0,n-1-i},x_{0,n-i},\ x_{0,n-i+1},\ldots,x_{0,n-1})\oplus \\ (x_{0,i},x_{0,i+1},\ldots,x_{0,n-1},\ x_{0,0},\ \ x_{0,1},\ldots,x_{0,i-1}). \end{array}$$

Now, we define the following permutation (denoted by P) constructed by the corresponding bits' n positions of the binary sequence of the rightmost operand in the operation shown above.

$$P:\ (0,\ 1,\ \ldots, n-1) \to\ (i,\ i+1,\ \ldots,\ n-1,\ 0,\ 1,\ \ldots,\ i-1)$$

Because i is an even number, for P there exist two or more permutable subgroups with element $x_{0,\sigma} \neq x_{0,l}$, in which the subscripts σ and l mean that $x_{0,\sigma}$ and $x_{0,l}$ belong to different subgroups, respectively.

Suppose $(x_0 <<< i)\big|_{n-1-j} = x_{0,l} = 0$. For P, we choose the permutable subgroup which contains element $x_{0,l}$ and another permutable subgroup with element $x_{0,\sigma} \neq x_{0,l}$. Let us investigate the following two cases:

(1) If $l = 2$k and $x_{0,2t+1} = x_{0,\sigma}$, $0 \leq k \leq n/2$, $0 \leq t \leq \frac{n}{2} - 1$,

(2) If $l = 2k+1$ and $x_{0,2t} = x_{0,\sigma}$, $0 \leq k \leq \frac{n}{2} - 1$, $0 \leq t \leq n/2$.

Since $x_{0,l} = 0$, *if* $x_{0,2t+1} = x_{0,\sigma} = 1$, or $x_{0,2t} = x_{0,\sigma} = 1$, and let the other bits be 0, then $x_0 \neq 0$, and we have $y_3 = x_0 \oplus (x_0 <<< i) = 0$. □

According to the proof of Theorem 1, if i is an odd number, then the permutable subgroups of P degenerate into a full permutation which contains all elements $(x_{0,0}, x_{0,1}, \ldots, x_{0,n-1})$. In this case, if $x_0 \oplus (x_0 <<< i) = 0$, then we can derive that $x_{0,i} = x_{0,l} = 0$, or $x_{0,i} = x_{0,l} = 1$, where $i = 0,\ 1,\ \cdots,\ n-1$. Then, we have Corollary 1.

Corollary 1. Let i be an odd number. If $x \neq 0 \in \mathbb{F}_2^n$ and $wt(x) \neq n$, then $x \oplus (x <<< i) \neq 0$.

Lemma 1. Let $i = 2k+1$, $0 \leq k \leq \frac{n}{2} - 1$, $0 \leq j \leq n-1$ in $h_{i,j}(\alpha)$. If $h_{i,j}(\alpha)$ makes $A_{h_{i,j}^{\alpha}}$ an MDS, for the input $x \neq 0 \in \mathbb{F}_{2^n}$ $0 \leq l \leq n-1$, let

$$t_0 = (x <<< i) \oplus ((x <<< i)\Big|_{n-1-j-l} \times (h_{i,j}(\alpha) <<< l))$$

$$t_1 = x \oplus (x <<< i) \oplus ((x <<< i)\Big|_{n-1-j-l} \times (h_{i,j}(\alpha) <<< l)),$$

then $t_0 \neq 0$ and $t_1 \neq 0$.

Proof of Lemma 1. Let $\beta = h_{i,j}(\alpha)$, where i is an odd number; then, we have Equation (6), $x \neq 0$.

$$\begin{aligned} t_0 &= (x <<< i) \oplus ((x <<< i)\Big|_{n-1-j-l} \times (\beta <<< l)) \\ t_1 &= x \oplus (x <<< i) \oplus ((x <<< i)\Big|_{n-1-j-l} \times (\beta <<< l)) \end{aligned} \tag{6}$$

According to Corollary 1, we know $x \oplus (x <<< i) \neq 0$ if $(x <<< i)\Big|_{n-1-j-l} = 0$. Then, we just need to prove Equation (7) if $(x <<< i)\Big|_{n-1-j-l} \neq 0$.

$$\begin{aligned} t_0 &= (x <<< i) \oplus (\beta <<< l) \neq 0 \\ t_1 &= x \oplus (x <<< i) \oplus (\beta <<< l) \neq 0 \end{aligned} \tag{7}$$

Note that $A_{h_{i,j}^{\alpha}}$ is an MDS; if $(x <<< i)\big|_{n-1-j} \neq 0$, then $(x <<< i) \oplus \beta \neq 0$ and $x \oplus (x <<< i) \oplus \beta \neq 0$. So, we have Equation (8).

$$\begin{aligned} t_0 <<< l &= (x <<< i+l) \oplus (\beta <<< l) \neq 0 \\ t_1 <<< l &= (x <<< l) \oplus (x <<< i+l) \oplus (\beta <<< l) \neq 0 \end{aligned} \tag{8}$$

Let $w = (x <<< l) \neq 0$, based on Equation (8), we can obtain Equation (9) if $(w <<< i)\big|_{n-1-j} \neq 0$ (that is $(x <<< i)\Big|_{n-1-j-l} \neq 0$).

$$\begin{aligned} t'_0 = t_0 <<< l = (w <<< i) \oplus \ (\beta <<< l) \neq 0 \\ t'_1 = t_1 <<< l = w \ \oplus \ (w <<< i) \oplus \ (\beta <<< l) \neq 0 \end{aligned} \quad (9)$$

In Equation (9), we can replace the input x with w.
Now, we have $t_0 \neq 0$ and $t_1 \neq 0$. □

According to Lemma 1, we have Theorem 2.

Theorem 2. *Let* $i = 2k + 1$, $0 \leq k \leq \frac{n}{2} - 1$, $0 \leq j \leq n - 1$ *in* $h_{i,j}(\alpha)$. *If* $h_{i,j}(\alpha)$ *makes* $A_{h^{\alpha}_{i,j}}$ *an MDS, for any* $0 \leq l \leq n - 1$, *assign* $h_{i,\ (j+l) mod\ n}(\alpha) = (h_{i,j}(\alpha) <<< l)$, *then* $A_{h^{\alpha}_{i,(j+l) mod\ n}}$ *is an MDS.*
Next, we give the construction of composite permutation φ based on the constructed permutation ϑ and inverse permutation ϑ^{-1}, and the transformational relations between $h_{i_0,j}(\alpha)$ and $h_{i_1,j}(\alpha)$.

Theorem 3. *Let* $i_e = 2k_e + 1$, $0 \leq k_e \leq \frac{n}{2} - 1$, $0 \leq j \leq n - 1$ *in* $h_{i_e,j}(\alpha)$ *with* $e \in \{0,1\}$. *If each of* $h_{i_e,j}(\alpha)$ *makes* $A_{h^{\alpha}_{i_e,j}}$ *an MDS, respectively, then there exists a map* φ: $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ *satisfying* $h_{i_1,j}(\alpha) = \varphi(\ h_{i_0,j}(\alpha))$.

Proof of Theorem 3. Now, we construct a map ϑ on $\mathbb{F}_{2^n}$: for every α and $\tau_\alpha = \vartheta(\ h_{i_0,0}(\alpha))$, let parameters $(i, j, h_{i,j}(\alpha)) := (i_1, 0, \tau_\alpha)$ be related to Equation (5), which makes $Br\left(A_{h^{\tau_\alpha}_{i_1,0}}\right) = 5$ hold, and conversely, for every α and $\sigma_\alpha = \vartheta^{-1}(\ h_{i_1,0}(\alpha))$, let parameters $(i, j, h_{i,j}(\alpha)) := (i_0, 0, \sigma_\alpha)$ be related to Equation (5) which makes $Br\left(A_{h^{\sigma_\alpha}_{i_0,0}}\right) = 5$ hold.

Suppose $h_{i_k,0}(\alpha) = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}_2^n$ with $k \in \{0,1\}$; next, we construct a kind of map P_{i_k}: $\mathbb{F}_2^n \rightarrow \ \mathbb{F}_{2^n}^n$; this means

$$\begin{aligned} &(t_0, t_1, \ldots, t_{n-1}) \ \rightarrow \\ &(1 \times i_k \times t_0, (2 \times i_k) mod\ n) \times t_1, \ldots, ((n-1) \times i_k) mod\ n \times t_{n-2},\ 0) \end{aligned}$$

Then, we use P_{i_k} to define the following permutation $\vartheta(\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n})$ and its inverse permutation $\vartheta^{-1}(\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n})$ about data elements in $\mathbb{F}_2^n$:

(a) Let the binary digits of $h_{i_0,0}(\alpha)$ be the n-bit input element of P_{i_0}, the positions of the data in the sequence $\mathcal{H}_1 := (1 \times i_1, (2 \times i_1) mod\ n), \ldots, ((n-1) \times i_1) mod\ n),\ 0)$, which is the same with all non-zero data mapped from P_{i_0} to $\mathbb{F}_n$ marked as 1; the other positions are marked as 0, then we can obtain an n-bit position identification value about $\mathcal{H}_1$, denoted by $\tau_\alpha \in \mathbb{F}_{2^n}$, and define $\vartheta(h_{i_0,0}(\alpha)) = \tau_\alpha$;

(b) Let the binary digits of $h_{i_1,0}(\alpha)$ be the n-bit input element of $\ P_{i_1}$, the positions of the data in the sequence $\mathcal{H}_0 := (1 \times i_0, (2 \times i_0) mod\ n), \ldots, ((n-1) \times i_0) mod\ n),\ 0)$ which is the same with all non-zero data mapped from P_{i_1} to $\mathbb{F}_n$ marked as 1; the other positions are marked as 0; then we can obtain an n-bit position identification value for $\mathcal{H}_0$, denoted by $\sigma_\alpha \in \mathbb{F}_{2^n}$, and define $\vartheta^{-1}(h_{i_1,0}(\alpha)) = \sigma_\alpha$.

For all the $0 \leq j \leq n - 1$, by combining the permutation ϑ constructed above with the left cyclic shift operation of Theorem 2, the composite transformation φ from ϑ and "<<<" is obtained, and we have Theorem 3. □

Theorem 3 is the crucial theorem of the current paper. In the latter part, we provide some concrete instances based upon Theorem 3. By combining Theorem 2 and Theorem 3, we obtain Theorem 4.

Theorem 4. *For every parameter of each group* $(i, j\ ) \in \mathbb{Z} \times \mathbb{Z}$, $i = 2k + 1$, $0 \leq k \leq \frac{n}{2} - 1$, $0 \leq j \leq n - 1$, *there exists a mapping* $h_{i,j} :\ \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, *which maps each generating element* $\alpha \in \mathbb{F}_{2^n}$ *one by one to* $h_{i,j}(\alpha) \in \mathbb{F}_{2^n}$ *, such that* $A_{h^{\alpha}_{i,j}}$ *is an MDS.*

According to the previous conclusions, for every given parameter group $(i, j) := (I, J)$, $A_{h^{\alpha}_{i,j}}$ traverses all MDS-generating elements to make the MDS cluster partition of ***A*,** and we can obtain the MDS cluster $\{A_{h^{\alpha}_{i=I,j=J}}\}$ of $\boldsymbol{A}$. For every given parameter group $(i, \alpha) := (I, V)$. $A_{h^{\alpha}_{i,j}}$ traverses all $0 \leq j \leq n-1$ values to make the MDS cluster partition of ***A*,** and we can obtain the MDS cluster $\{A_{h^{\alpha=V}_{i=I,j}}\}$ of $\boldsymbol{A}$. Regarding the qualities, we have Proposition 1.

Proposition 1. Let $i = 2k+1$, $0 \leq k \leq \frac{n}{2} - 1$, $0 \leq j \leq n-1$, and α be an MDS-generating element of $\boldsymbol{A}$ in $\mathbb{F}_{2^n}$. For all α, the parameter variable (i, j) generates an MDS equivalence class division of $\boldsymbol{A}$.

We know that the number of n-order monic irreducible polynomials is $(n) = \frac{1}{n} \sum\limits_{d|n} \mu(d) 2^{\frac{n}{d}}$, $n \geq 1$, and $\mu(n)$ is an Mertens function. On the basis of Theorem 4, we have Corollary 2.

Corollary 2. According to the number of all possible values of i and j, the number of the MDS (denoted by $M(n)$) constructed by $A_{h^{\alpha}_{i,j}}$ of $\boldsymbol{A}$ in $\mathbb{F}_{2^n}$ satisfies $M(n) \geq \frac{n}{2} \sum\limits_{d|n} \mu(d) 2^{\frac{n}{d}}$, where $n \geq 2$. Then, the number of existing MDSs is expanded to $n^2/2$ times that of the original.

Note that the number of the monic irreducible polynomials of degree 8 defined in $\mathbb{F}_{2^8}$ is equal to 30 by the formula $N(n)$. According to computer searching, there are 36 generating elements of $\boldsymbol{A}$ in $\mathbb{F}_{2^{\mathrm{n}}}$, which shows that Equations (2) and (5), defined by the bit-level operation, expand the operational connotation of $\boldsymbol{A}$ in $\mathbb{F}_{2^{\mathrm{n}}}$.

According to the MDS-generating elements of $\boldsymbol{A}$ in $\mathbb{F}_{2^8}$, by Theorem 4, we obtain that the total number of MDSs constructed by the operation $A_{h^{\alpha}_{i,j}}$ of $\boldsymbol{A}$ in $\mathbb{F}_{2^8}$ is 1152 (= 4 × 8 × 36).

Example 1. All 36 MDS-generating elements $\{h_{1,0}(\alpha)\}$ of $\boldsymbol{A}$ in $\mathbb{F}_{2^8}$ are listed below.
0x04, 0x16, 0x1a, 0x1c, 0x2a, 0x2c, 0x38, 0x3e, 0x40, 0x4c, 0x54, 0x5e,
0x62, 0x64, 0x68, 0x70, 0x76, 0x7a, 0x86, 0x8a, 0x8c, 0x9e, 0xa2, 0xa8,
0xb0, 0xba, 0xbc, 0xc2, 0xce, 0xd0, 0xd6, 0xdc, 0xe6, 0xf2, 0xf4, 0xf8.

Once we determine the generating elements of $\boldsymbol{A}$ in $\mathbb{F}_{2^n}$, for all operation $A_{h^{\alpha}_{i,j}}$ of $\boldsymbol{A}$ in $\mathbb{F}_{2^n}$, by Theorem 2 and Theorem 3, we can obtain the transformational relations between clusters of $\{h_{i,j}(\alpha)\}$, and derive the total number of MDSs from $\boldsymbol{A}$.

Example 2. Based on the 36 data points $\{h_{1,0}(\alpha)\}$ in Example 1, respectively, we can obtain the derived 36 data points $\{h_{3,0}(\alpha)\}$ in $\mathbb{F}_{2^8}$, as shown below:
0x40, 0x58, 0x1a, 0x52, 0x8a, 0xc2, 0x92, 0xda, 0x04, 0x46, 0x54, 0x5e,
0x8c, 0xc4, 0x86, 0x94, 0xdc, 0x9e, 0x68, 0x2a, 0x62, 0x7a, 0xa8, 0xa2,
0xb0, 0xba, 0xf2, 0x2c, 0x6e, 0x34, 0x7c, 0x76, 0xec, 0xbc, 0xf4, 0xb6.

Regarding the map ϑ definition of Theorem 3, one could verify the correctness of the derived data set shown in Example 2. Then, we show the verification process for the first 2 elements in Example 1, and the other cases are similar.

1. For the first element $\mathrm{h}_{1,0}(\alpha) = 0\mathrm{x}04$ in Example 1, let its binary bits $(0\ 0\ 0\ 0\ 0\ 1\ 0\ 0)$ be the input of map $\mathrm{P}_{\mathrm{i}_0}$; then, the output is $(0\ 0\ 0\ 0\ 0\ 6\ 0\ 0)$. For $\mathcal{H}_1 := (3\ 6\ 1\ 4\ 7\ 2\ 5\ 0)$, the same with all non-zero data (only "6") mapped from $\mathrm{P}_{\mathrm{i}_0}$ to $\mathbb{F}_8$ are marked as 1, the other positions are marked as 0; then, we can obtain the n-bit position identification value $(0\ 1\ 0\ 0\ 0\ 0\ 0\ 0)$ as $\mathrm{h}_{3,0}(0\mathrm{x}04) = \vartheta(\mathrm{h}_{1,0}(0\mathrm{x}04)) = 0\mathrm{x}40$.

2. For the second element $h_{1,0}(\alpha) = 0\text{x}16$ in Example 1, let its binary bits $(0\,0\,0\,1\,0\,1\,1\,0)$ be the input of map P_{i_0}; then, the output is $(0\,0\,0\,\mathbf{4}\,0\,\mathbf{6}\,\mathbf{7}\,0)$. For $\mathcal{H}_1 := (3\,\mathbf{6}\,1\,\mathbf{4}\,\mathbf{7}\,2\,5\,0)$, the same with all non-zero data "4, 6, 7" mapped from P_{i_0} to $\mathbb{F}_8$ are marked as 1; the other positions are marked as 0. Then, we can obtain the n-bit position identification value $(0\,\mathbf{1}\,0\,\mathbf{1}\,\mathbf{1}\,0\,0\,0)$ as $h_{3,0}(0\text{x}16) = \vartheta(h_{1,0}(0\text{x}16)) = 0 \times 58$.

4. Conclusions

The circulant MDS matrix used in the diffusion layer of the AES algorithm is simple and efficient. Based on the known lightweight MDS matrix on $\mathbb{F}_{2^n}^4$, by constructing permutation-based parameters, we can obtain a large number of lightweight parametrical MDS transformations, which expands the design idea of MDS from static to dynamic and increases the number of MDSs from a single one to a large batch at one time. The constructions in this paper provide rich component materials for the design of lightweight cryptographic algorithms, which have low-cost implementations for the purpose of constraining resources, such as IoT and wireless communication environments.

Author Contributions: Methodology, J.-B.W.; Writing—review & editing, Y.W. and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key R&D Program of China (Program number: No. 2020YFC1522900) and the Sichuan Science and Technology Program (Program numbers: Nos. 2020JDJQ0076 and 2021ZYD0011).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that there are no conflict of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Daemen, J.; Rijmen, V. *The Design of Rijndael: AES. The Advanced Encryption Standard. Information Security and Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002.
3. Specification of SMS4, Block Cipher for WLAN Products-SMS4 (In Chinese) [EB/OL]. Available online: https://sca.gov.cn/sca/c100061/201611/1002423/files/330480f731f64e1ea75138211ea0dc27.pdf, (accessed on 18 November 2016).
4. Cui, T.; Jin, C.; Kong, Z. On compact cauchy matrices for substitution-permutation networks. *IEEE Trans. Comput.* **2015**, *64*, 2098–2102. [CrossRef]
5. Gupta, K.C.; Pandey, S.K.; Venkateswarlu, A. Almost involutory recursive MDS diffusion layers. *Des. Codes Cryptogr.* **2019**, *87*, 609–626. [CrossRef]
6. Güzel, G.G.; Sakallı, M.T.; Akleylek, S.; Rijmen, V.; Çengellenmi, Ş. A new matrix form to generate all 3 × 3 involutory MDS matrices over. *Inf. Processing Lett.* **2019**, *147*, 61–68. [CrossRef]
7. Li, Y.; Wang, M. On the Constructions of Lightweight Circulant Involutory MDS Matrices. In Proceedings of the Fast Software Encryption—23rd International Conference, FSE 2016, LNCS 9783, Bochum, Germany, 20–23 March 2016; Springer: Berlin/Heidelberg, Germany, 2016; Volume 5, pp. 121–139.
8. Liu, M.; Sim, S.M. Lightweight MDS generalized circulant matrices. In Proceedings of the Fast Software Encryption 23rd International Conference. FSE 2016, Bochum, Germany, 20–23 March 2016; pp. 101–120, Revised Selected Papers.
9. Dong, X.; Hu, J. Design and Analysis of Lightweight Linear MDS Transformation. *Commun. Technol.* **2018**, *51*, 653–658.
10. Wang, J. The optimal permutation in cryptography based on cyclic-shift linear transform. *China Crypt.* **2007**, *c2007*, 306–307.
11. Sébastien, D.; Gaëtan, L. MDS Matrices with Lightweight Circuits. IACR Trans. *Symmetric Cryptol.* **2018**, *2018*, 48–78.
12. Christof, B.; Thorsten, K.; Gregor, L. *Lightweight Multiplication in GF(2n) with Applications to MDS Matrices*; CRYPTO 2016. LNCS 9814; Springer: Berlin/Heidelberg, Germany, 2016; pp. 625–653.
13. Shirai, T.; Shibutani, K. *Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices*; Roy, B., Meier, W., Eds.; FSE 2014, LNCS 3017; Springer: Berlin/Heidelberg, Germany, 2014; pp. 260–278.
14. Xiang, Z.; Zeng, X.; Lin, D.; Bao, Z.; Zhang, S. Optimizing Implementations of Linear Layers. *IACR Trans. Symmetric Cryptol.* **2020**, *2*, 120–145. [CrossRef]
15. Lin, D.; Xiang, Z.; Zeng, X.; Zhang, S. A Framework to Optimize Implementations of Matrices. In Proceedings of the CT-RSA 2021: Cryptographers' Track at the RSA Conference 2021, San Francisco, CA, USA, 17–20 May 2021; pp. 609–632.

16. Shamsabad, M.R.M.; Dehnavi, S.M.; Rishakani, A.M. Randomized Nonlinear Software oriented MDS Diffusion Layers. *Groups Complex. Cryptol.* **2019**, *11*, 123–131. [CrossRef]
17. Shanmsabad, M.R.M.; Dehnavi, S.M. A Family of Nonlinear MDS Diffusion Layers. *Groups Complex. Cryptol.* **2019**, *11*, 123–131. [CrossRef]
18. Wu, Y.; Dong, X.-F.; Wang, J.-B.; Zhang, W.-Z. Construction of MDS Matrices Based on the Primitive Elements of the Finite Field. In Proceedings of the 2021 International Conference on Networking and Network Applications (NaNA), Lijiang, China, 29 October 2021—1 November 2021; IEEE: Piscataway Township, NJ, USA, 2021; pp. 485–488.