Constructing effectively MDS and recursive MDS matrices by Reed-Solomon codes

Trần Thị Lượng

Abstract− **Maximum Distance Separable (MDS) codes have been studied widely in coding theory. Recently, MDS codes have been applied in cryptography. Many different methods have been proposed for finding MDS matrices. Among these methods, the method for constructing them from MDS codes is a common one. In this paper, some methods for constructing effectively MDS and recursive MDS matrices from Reed-Solomon (RS) codes are presented. The MDS and recursive MDS matrices generated from these codes are useful and efficient for cryptographic applications.**

Tóm tắt− **Mã khả tách có khoảng cách cực đại (mã MDS) đã được nghiên cứu rộng rãi trong lý thuyết mã sửa sai. Hiện nay, mã MDS đang được quan tâm và ứng dụng trong mật mã. Nhiều phương pháp khác nhau đã được nghiên cứu để xây dựng các ma trận MDS. Trong đó, phương pháp xây dựng các ma trận MDS từ mã MDS là một phương pháp được sử dụng phổ biến. Bài báo này trình bày các phương pháp xây dựng hiệu quả các ma trận MDS/MDS truy hồi từ mã Reed-Solomon (RS). Các ma trận MDS/MDS truy hồi được sinh ra từ các mã này đạt hiệu quả cao trong các ứng dụng mật mã.**

Keywords*− *MDS code; MDS matrix; recursive MDS matrices; RS codes.

Từ khóa*− *mã khả tách có khoảng cách cực đại; ma trận MDS; ma trận MDS truy hồi; mã RS.

I. INTRODUCTION

The viability of using MDS matrices in block ciphers was first introduced by Serge Vaudenay in FSE'95 [1] as a linear case of multipermutations. Multipermutations characterize the notion of perfect diffusion [2] which requires that the change of any t out of m input bits must affect at least $m-t+1$ output bits.

The branch number is one of the important criteria for design a diffusion layer in SPN structure [3, 4]. It has an important role for resistance against strong attacks (such as linear and differential attacks) on block ciphers. It is always to be expected to have the maximum branch number for block cipher designers. As MDS matrices give maximum branch numbers for the linear transformations corresponding with them, they have been used for diffusion in many block ciphers such as: AES [5, 6], SHARK [7], Square, Twofish [8], Anubis, Khazad, Manta, Hierocrypt and Camellia. They are also used in stream ciphers like MUGI and cryptographic hash functions like WHIRLPOOL.

Due to the usefulness of MDS matrices, there are lots of methods for constructing them such as building MDS matrices from *MDS codes* [7, 8, 10]; building MDS matrices from appropriate matrices, for example Cauchy matrices [10], Hadamard matrices [11, 12], Vandermonde matrices [13], Serial matrices [15], recursive MDS matrices and so on.

Reed-Solomon code (RS) [14] as a class of MDS code is used commonly to build MDS matrices because of the simplicity and the efficiency in building it. Moreover, one can generate MDS matrices of arbitrary sizes over an arbitrary finite field from some RS code. Therefore, there are some studies on the construction of the MDS matrices from the RS codes, for example in [7, 8]. The methods of these authors are finding an MDS matrix of size n over $GF(2^m)$ by constructing a RS $[2n, n, n+1]$ code over $GF(2^m)$.

Besides, the recursive MDS matrices (exponent of a serial matrix [15]) have been studied by many authors in the literature thank to its important applications in lightweight cryptography, for example in [16-20]. However, none of the studies has ever shown the method to build a recursive MDS matrix from the RS codes.

In this paper, the methods for constructing effectively MDS and recursive MDS matrices are presented. Some constraints related to the RS codes for building MDS and recursive MDS matrices of arbitrary sizes are also shown.

The paper is organized as follows. In Section 2, RS codes are introduced. Section 3 presents the method for constructing effectively MDS matrices from RS codes and some relevant constraints. Section 4 provides the method for constructing effectively recursive MDS matrices from RS codes and some relevant constraints. And conclusions of the paper is in Section 5.

II. RS CODE

A RS code over $GF(q) = GF(p^m)$ is a BCH code of length $n = q - 1$. A RS code of length $n = q - 1$ designed with distance d will have the corresponding generator polynomial of degree $d - 1$ as follow:

$$g(x) \\ = (x - a^b)(x - a^{b+1}) \dots (x - a^{b+d-2}) \quad (1)$$

where b is a pre-selected value ($b \geq 1$).

It was proven that for any n, d and for the polynomial with the form in (1) the $RS[n, k, d]$ code generated from this polynomial will be an MDS code [14], i.e. it satisfies the condition: $d = n - k + 1$.

Suppose that $g(x) = g_0 + g_1 x + \dots + g_{n-k} x^{n-k}$ and the corresponding parity-check polynomial is $h(x) = h_0 + h_1 x + \dots + h_k x^k$. Then the generator matrix G and the parity check matrix H have the following forms:

$$G_{k\times n}= \\ \begin{bmatrix} g_0 & g_1 & g_2 & & \dots & g_{n-k} & 0 & 0 \dots 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_{n-k-1} & g_{n-k} & 0 \dots 0 \\ & & & \iddots & \cdots & \ddots & & \\ 0 & 0 & 0 & \dots & g_0\ g_1\ g_2 & \dots & & g_{n-k} \end{bmatrix} \quad (2)$$

$$H_{(n-k)\times n}= \\ \begin{bmatrix} 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & & h_0 & 0 \\ & & \iddots & & \cdots & & \ddots & & \\ h_k & h_{k-1} & & \dots & h_0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad (3)$$

III. CONSTRUCTING EFFECTIVELY MDS MATRICES FROM RS CODES

This section presents a method for constructing effectively MDS matrices from a generalized RS code.

Let $RS[n, k, d]$ be a generalized RS code over $GF(2^m)$, where $n = 2^m - 1$ is the length, $k = 2^m - d$ is the dimension and d is the minimum distance of the code. In order to create an MDS matrix of size l ($l \geq 1$) over $GF(2^m)$, it is to have constraints between m and l, between d and m, l. We have the following proposition:

Proposition 1. *If $l \times l$ MDS matrices can be generated from a $RS\,[2^m - 1\,, 2^m - d, d]$ code over $GF(2^m)$ then m, l and d must satisfy: $m \geq log_2(2l + 1)$ and $l + 1 \leq d \leq 2^m - l$.*

Proof.

Indeed, the length of the RS code is $n = 2^m - 1$, the dimension of the code is $k = 2^m - d$. From the generator matrix of this code, it is changed to echelon form $G_{k\times n} = [I \mid A]$, where A is a $k \times (n - k)$ matrix and I is the identity matrix of size k. Therefore, in order to derive MDS matrices of size $l \times l$ from the matrix A then k and n must satisfy the following conditions:

$$\begin{cases} k \geq l \\ n - k \geq l \end{cases}$$

The above conditions infer:

$$\begin{cases} k \geq l \\ n \geq 2l \end{cases} \rightarrow \quad 2^m - 1 \geq 2l \quad \leftrightarrow$$

$2^m \geq 2l + 1$ (or $l + 1 \leq 2^m - l$).

This yields: $m \geq log_2(2l + 1)$.

In addition, as $\begin{cases} k \geq l \\ n - k \geq l \end{cases} \rightarrow \quad l + 1 \leq \ d = n - k + 1 \leq n - l + 1$;

or $l + 1 \leq d \leq 2^m - l$ □

Applying Proposition 1, the following algorithm is given for building effectively MDS matrices from a generalized $RS[n, k, d]$ code.

Algorithm 1.

INPUTS: Size of the MDS matrices is l, the finite field is $GF(2^m)$ where $m \geq log_2(2l + 1)$.

OUTPUTS: $l \times l$ MDS matrices over $GF(2^m)$.

Detail of steps as follows:

Step 1: Constructing a $RS\,[n, k, d]$ code where $n = 2^m - 1$ by the following way:

- Select a value d satisfying: $l + 1 \leq d \leq 2^m - l$.
- Calculate the dimension of the code: $k = n - d + 1\ = 2^m - d, (\geq l\,)$.
- Find the generator matrix of the code.

Step 2: Change the generator matrix of the $RS\,[2^m - 1\,, 2^m - d, d]$ code to the echelon form $G = [I|A]$. Matrix A obtained is a $(2^m - d) \times (d - 1)$ one. Then, it can be taken any $l \times l$ submatrices of A. They are all MDS matrices of size l over $GF(2^m)$.

Complexity of Algorithm 1:

Step 1:

The selection d: $O\ (1)$.

The calculation k: $O\ (1)$.

Finding the generator matrix or the gene-rator polynomial $g(x)$ of the code has the com-plexity equal to: $O(d\ logd)$ where d is the min-imum distance of the code.

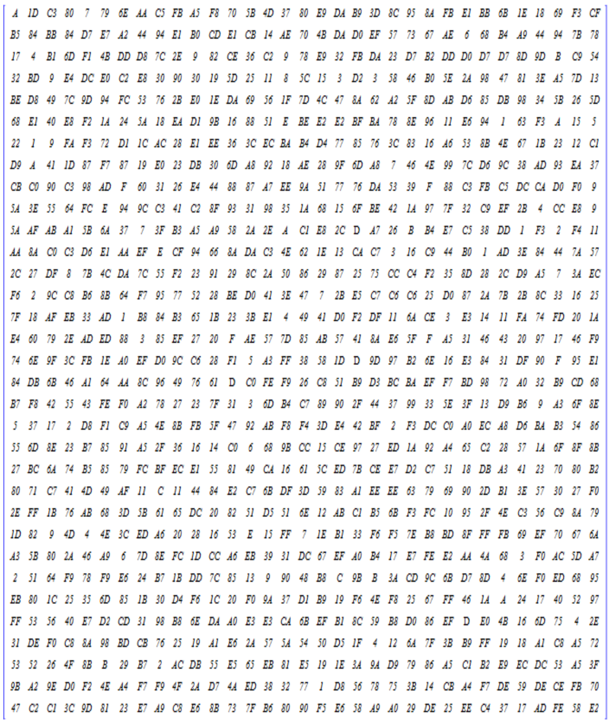
Step 2: Changing the generator matrix of the code to the echelon form has the complexity equal to: $O(k^3) = O((n-d+1)^3)$.

Thus the overall complexity of the Algorithm 1 is: $O(d\, logd) + O((n-d+1)^3)$. It can be reduced to $O(n^3)$.

Such as, one need a 16×16 MDS matrix over $GF(2^8)$. It is clear that $8 > log_2(2.16+1)$. Select $d = 34$ satisfying the condition $17 < d < 240$. Then, construct a $RS(255,222,34)$ code over $GF(2^8)$ with the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$, where $n = 255,\ d = 34,\ k = n - d + 1 = 222 > 16$.

(Maple is used to construct the RS code). After that, the generator matrix of this code is changed to the echelon form $G = [I|A]$. Matrix A achieved is a 222×33 one. Now, it can be taken any 16×16 submatrices of A, they are all MDS matrices of size 16 over $GF(2^8)$.

It is temporarily extracted a 33×33 submatrix A_1 of A (at 33 first rows of A). Matrix A_1 is in Figure 1.



A	1D	C3	80	7	79	6E	AA	C5	FB	A5	F8	70	5B	4D	37	80	E9	DA	B9	3D	8C	95	8A	FB	E1	BB	6B	1E	18	69	F3	CF
B5	84	BB	84	D7	E7	A2	44	94	E1	B0	CD	E1	CB	14	AE	70	4B	DA	D0	EF	57	73	67	AE	6	68	B4	A9	44	94	7B	78
17	4	B1	6D	F1	4B	DD	D8	7C	2E	9	82	CE	36	C2	9	78	E9	32	FB	DA	23	D7	B2	DD	D0	D7	D7	8D	9D	B	C9	54
32	BD	9	E4	DC	E0	C2	E8	30	90	30	19	5D	25	11	8	5C	15	3	D2	3	58	46	B0	5E	2A	98	47	81	3E	A5	7D	13
BE	D8	49	7C	9D	94	FC	53	76	2B	E0	1E	DA	69	56	1F	7D	4C	47	8A	62	A2	5F	8D	AB	D6	85	DB	98	34	5B	26	5D
68	E1	40	E8	F2	1A	24	5A	18	EA	D1	9B	16	88	51	E	BE	E2	E2	BF	BA	78	8E	96	11	E6	94	1	63	F3	A	15	5
22	1	9	FA	F3	72	D1	1C	AC	28	E1	EE	36	3C	EC	BA	B4	D4	77	85	76	3C	83	16	A6	53	8B	4E	67	1B	23	12	C1
D9	A	41	1D	87	F7	87	19	E0	23	DB	30	6D	A8	92	18	AE	28	9F	6D	A8	7	46	4E	99	7C	D6	9C	38	AD	93	EA	37
CB	C0	90	C3	98	AD	F	60	31	26	E4	44	88	87	A7	EE	9A	51	77	76	DA	53	39	F	88	C3	FB	C5	DC	CA	D0	F0	9
5A	3E	55	64	FC	E	94	9C	C3	41	C2	8F	93	31	98	35	1A	68	15	6F	BE	42	1A	97	7F	32	C9	EF	2B	4	CC	E8	9
5A	AF	AB	A1	5B	6A	37	7	3F	B3	A5	A9	58	2A	2E	A	C1	E8	2C	D	A7	26	B	B4	E7	C5	38	DD	1	F3	2	F4	11
AA	8A	C0	C3	D6	E1	AA	EF	E	CF	94	66	8A	DA	C3	4E	62	1E	13	CA	C7	3	16	C9	44	B0	1	AD	3E	84	44	7A	57
2C	27	DF	8	7B	4C	DA	7C	55	F2	23	91	29	8C	2A	50	86	29	87	25	75	CC	C4	F2	35	8D	28	2C	D9	A5	7	3A	EC
F6	2	9C	C8	B6	8B	64	F7	95	77	52	28	BE	D0	41	3E	47	7	2B	E5	C7	C6	C6	25	D0	87	2A	7B	2B	8C	33	16	25
7F	18	AF	EB	33	AD	1	B8	84	B3	65	1B	23	3B	E1	4	49	41	D0	F2	DF	11	6A	CE	3	E3	14	11	FA	74	FD	20	1A
E4	60	79	2E	AD	ED	88	3	85	EF	27	20	F	AE	57	7D	85	AB	57	41	8A	E6	5F	F	A5	31	46	43	20	97	17	46	F9
74	6E	9F	3C	FB	1E	A0	EF	D0	9C	C6	28	F1	5	A3	FF	38	58	1D	D	9D	97	B2	6E	16	E3	84	31	DF	90	F	95	E1
84	DB	6B	46	A1	64	AA	8C	96	49	76	61	D	C0	FE	F9	26	C8	51	B9	D3	BC	BA	EF	F7	BD	98	72	A0	32	B9	CD	68
B7	F8	42	55	43	FE	F0	A2	78	27	23	7F	31	3	6D	B4	C7	89	90	2F	44	37	99	33	5E	3F	13	D9	B6	9	A3	6F	8E
5	37	17	2	D8	F1	C9	A5	4E	8B	FB	5F	47	92	AB	F8	F4	3D	E4	42	BF	2	F3	DC	C0	A0	EC	A8	D6	BA	B3	54	86
55	6D	8E	23	B7	85	91	A5	2F	36	16	14	C0	6	68	9B	CC	15	CE	97	27	ED	1A	92	A4	65	C2	28	57	1A	6F	8F	8B
27	BC	6A	74	B5	85	79	FC	BF	EC	E1	55	81	49	CA	16	61	5C	ED	7B	CE	E7	D2	C7	51	18	DB	A3	41	23	70	80	B2
80	71	C7	41	4D	49	AF	11	C	11	44	84	E2	C7	6B	DF	3D	59	83	A1	EE	EE	63	79	69	90	2D	B1	3E	57	30	27	F0
2E	FF	1B	76	AB	68	3D	5B	61	65	DC	20	82	51	D5	51	6E	12	AB	C1	B5	6B	F3	FC	10	95	2F	4E	C3	56	C9	8A	79
1D	82	9	4D	4	4E	3C	ED	A6	20	28	16	53	E	15	FF	7	1E	B1	33	F6	F5	7E	B8	BD	8F	FF	FB	69	EF	70	67	6A
A3	5B	80	2A	46	A9	6	7D	8E	FC	1D	CC	A6	EB	39	31	DC	67	EF	A0	B4	17	E7	FE	E2	AA	4A	68	3	F0	AC	5D	A7
2	51	64	F9	78	F9	E6	24	B7	1B	DD	7C	85	13	9	90	48	B8	C	9B	B	3A	CD	9C	6B	D7	8D	4	6E	F0	ED	68	95
EB	80	1C	25	35	6D	85	1B	30	D4	F6	1C	20	F0	9A	37	D1	B9	19	F6	4E	F8	25	67	FF	46	1A	A	24	17	40	52	97
FF	53	56	40	E7	D2	CD	31	98	B8	6E	DA	A0	E3	E3	CA	6B	EF	B1	8C	59	B8	D0	86	EF	D	E0	4B	16	6D	75	4	2E
31	DE	F0	C8	8A	98	BD	CB	76	25	19	A1	E6	2A	57	5A	54	50	D5	1F	4	12	6A	7F	3B	B9	FF	19	18	A1	C8	A5	72
53	52	26	4F	8B	B	29	B7	2	AC	DB	55	E5	65	EB	81	E5	19	1E	3A	9A	D9	79	86	A5	C1	B2	E9	EC	DC	53	A5	3F
9B	A2	9E	D0	F2	4E	A4	F7	F9	4F	2A	D7	4A	ED	38	32	77	1	D8	56	78	75	3B	14	CB	A4	F7	DE	59	DE	CE	FB	70
47	C2	C1	3C	9D	81	23	E7	A9	C8	E6	8B	73	7F	B6	80	90	F5	E6	58	A9	A0	29	DE	25	EE	C4	37	17	AD	FE	58	E2

Figure 1. A 33×33 MDS matrix from RS code

Now, it can be taken any 16×16 submatrices of A_1, they are all MDS matrices of size 16 over $GF(2^8)$.

Consequently, many different MDS matrices of different sizes can be generated by the Algorithm 1.

Comment 1. It can be seen that, in Algorithm 1 an MDS code is built from any general RS code $[\mathrm{n,k,d}]$ where $\mathrm{k = n - d + 1}$, however in [7, 8] a $\mathrm{RS}[2\mathrm{n},\mathrm{n},\mathrm{n}+1]$ code is built where the length of codewords is double of the dimension. Therefore, the method in this paper is more general than the ones in [7, 8].

III. CONSTRUCTING EFFECTIVELY RECURSIVE MDS MATRICES FROM RS CODES

This Section provides a method for constructing effectively recursive MDS matrices (exponent of serial matrices) from RS codes. First, from the theory of error correcting codes [14], the following proposition is shown.

Proposition 2. *Let C $[n,k,d]$ be an MDS code (i.e $d = n - k + 1$). If $k \geq n - k$ then a recursive MDS matrix of size $n - k$ can be generated from this code.*

Proof.

Denote the generator polynomial of C is $g(X)$. This polynomial has degree of $n - k$. Since C is a cyclic code, the result of multiplying $g(X)$ by any polynomial belongs to this code. Therefore, for any polynomial $P(X)$ of degree n, the polynomial $P(X) - (P(X)\, mod\, g(X))$ belongs to C. Using this property for $P(X) = X^i$ where $i \in [deg(g), n-1]$, an interesting echelon form of the generator matrix of this code is obtained as follow:

$$G_{k\times n} = [I_{k\times k}|A_{k\times(n-k)}] = \left[\begin{array}{c|c} \underbrace{\begin{matrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ & \cdots & & \\ 0 & 0 & 0 & 1\end{matrix}}_{k} & \underbrace{\begin{matrix}X^{n-k}\, mod\, g(X)\\ X^{n-k+1}\, mod\, g(X)\\ \cdots\cdots\\ X^{n-1}\, mod\, g(X)\end{matrix}}_{n-k}\end{array}\right] \tag{4}$$

where matrix A is a $k \times (n-k)$ MDS matrix.

Suppose the polynomial $g(X)$ has the following form:

$$g(X) = X^{n-k} + c_{n-k-1}X^{n-k-1} + \cdots + c_1X + c_0 \tag{5}$$

Let the serial matrix be:

$$S = Serial(c_0, c_1, c_2, \dots, c_{n-k-1}).$$

Obviously, S is a square submatrix of size $n-k$. According to the assumption, it is to have:

$$k \geq n-k \tag{6}$$

Then, performing exponent matrix S continuously for $n-k$ times will obtain a recursive matrix A_1 of size $n-k$ as follows:

$$S=\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 \\ X^{n-k} & & mod & & g(X) \end{bmatrix}$$

$$S^2=\begin{bmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ & & \cdots & & & \\ X^{n-k} & & mod & & g(X) & \\ X^{n-k+1} & & mod & & g(X) & \end{bmatrix} \tag{7}$$

$$\cdots$$

$$S^{n-k}=\begin{bmatrix} X^{n-k} & mod & g(X) \\ X^{n-k+1} & mod & g(X) \\ & \cdots\cdots & \\ X^{2(n-k)-1} & mod & g(X) \end{bmatrix}=A_1$$

As $k \geq n-k$ so $k+(n-k)-1 \geq 2(n-k)-1$ or $n-1 \geq 2(n-k)-1$. Thus, by (4) and (7) it easy to see that A_1 is a submatrix of matrix A and it follows that A_1 is also an MDS matrix. As a result, A_1 is a recursive MDS matrix of size $n-k$ (exponent of the serial matrix S)□

Comment 2. Thus, from an any MDS $[\mathrm{n,k,d}]$ code (where $\mathrm{d=n-k+1}$ and $\mathrm{k \geq n-k}$ or $\mathrm{k \geq d-1}$) having the echelon form generator matrix (4), a recursive MDS matrix of size $\mathrm{n-k}$ can be created by cutting the last positions in A part of the echelon form generator matrix of the code.

According to Proposition 1 and Algorithm 1 in Section 3, matrix A obtained from the echelon form generator matrix of a $RS\,[2^m-1\,,2^m-d,d]$ code (i.e $n=2^m-1$, $k=2^m-d$) is a $(2^m-d)\times(d-1)$ matrix. Thus, from this RS code, a recursive MDS matrix of size $n-k$ or $d-1$ can be generated. In other words, only one recursive submatrix of size $(d-1)\times(d-1)$ can be chosen from $d-1$ first rows of A.

The following algorithm shows how to achieve a recursive MDS matrix from a RS code.

Algorithm 2.

INPUTS: Size of the MDS matrices is l, the finite field is $GF(2^m)$ where $m \geq log_2(2l+1)$.

OUTPUTS: a $l \times l$ recursive MDS matrix over $GF(2^m)$.

Detail of steps as follows:

Step 1: Select $\mathrm{d=l+1}$ (satisfying the condition $\mathrm{l+1 \leq d \leq 2^m-l}$ of the Algorithm 1). Construct a $\mathrm{RS\,[2^m-1\,,2^m-l-1,l+1]}$ code (where $\mathrm{2^m-l-1 \geq l}$ or $\mathrm{2^m-1 \geq 2l}$ according to the Proposition 2).

Step 2: Change the generator matrix of this code to the echelon form $\mathrm{G=[I|A]}$ where A is a $\mathrm{(2^m-d)\times(d-1)=(2^m-l-1)\times l}$ matrix.

Step 3: Get the square submatrix A_1 of size l at l first rows of A.

Then A_1 is the $l \times l$ recursive MDS matrix over $GF(2^m)$ that we are looking for. In addition, denote the serial matrix corresponding with A_1 is S of size l. This matrix has the elements in the last row coinciding with the elements in the first row of A_1 and these matrices satisfy: $A_1=S^l$.Note that the Algorithm 2 only gives the output when the RS code satisfies the condition $2^m-1 \geq 2l$.

Complexity of Algorithm 2: It's similar to the Algorithm 1.

For example, to find a recursive MDS matrix of size 4 over $GF(2^8)$, it is first to construct a $RS(255,251,5)$ code. Obviously, this code satisfies the condition $255 > 8$. Then, change the generator matrix of this code to the echelon form $G=[I|A]$, where matrix A is a 251×4 one. After that, get the 4×4 submatrix at 4 first rows of A. The matrix obtained is a recursive one that is expected. More specifically, a $RS(255,251,5)$ code can be built over $GF(2^8)$ with the irreducible polynomial $x^8+x^4+x^3+x^2+1$. The 4×4 recursive MDS matrix A_1 (the submatrix of A) achieved is:

$$A_1=\begin{bmatrix} 74 & E7 & D8 & 1E \\ B1 & A1 & 82 & 91 \\ FF & 7E & 70 & DA \\ A8 & 10 & 50 & 29 \end{bmatrix}$$

Denote the serial matrix corresponding with A_1 is S_1, it is to have:

$$S_1=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 74 & E7 & D8 & 1E \end{bmatrix}$$

and

$$S_1{}^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 74 & E7 & D8 & 1E \\ B1 & A1 & 82 & 91 \end{bmatrix}$$

$$S_1{}^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 74 & E7 & D8 & 1E \\ B1 & A1 & 82 & 91 \\ FF & 7E & 70 & DA \end{bmatrix}$$

$$S_1{}^4 = \begin{bmatrix} 74 & E7 & D8 & 1E \\ B1 & A1 & 82 & 91 \\ FF & 7E & 70 & DA \\ A8 & 10 & 50 & 29 \end{bmatrix} = A_1$$

For finding 8×8 recursive MDS matrices over $GF(2^8)$, a $RS(255, 247, 9)$ code can be built over $GF(2^8)$ with the irreducible polynomial $x^8 + x^6 + x^5 + x^3 + 1$, for example. This code satisfies $255 > 16$. Change the generator matrix of this code to the echelon form $G = [I|A]$, where matrix A is a 247×8 one. Then the 8×8 recursive MDS matrix A_2 (the submatrix of A) achieved is in Figure 2.

$$A_2 = \begin{bmatrix} 50 & BF & EF & 2B & 57 & BE & 94 & 97 \\ F9 & A & 1C & F7 & 8C & 9A & FC & 6 \\ 89 & C0 & BA & E6 & 6C & B3 & 59 & 35 \\ FC & B9 & C & 9B & 91 & 69 & A2 & 17 \\ 7D & C2 & FA & BF & 83 & B8 & E4 & 16 \\ 2D & FC & 6E & 62 & F0 & 14 & A1 & C7 \\ 1F & FD & 33 & F5 & FA & E7 & 5F & CA \\ 34 & 2 & D4 & 1E & 65 & 2D & D7 & 58 \end{bmatrix}$$

Figure 2. A 8 × 8 recursive MDS matrix from RS code

The serial matrix S_2 corresponding with A_2 is in Figure 3.

For finding 16×16 recursive MDS matrices over $\mathrm{GF}(2^8)$, a $\mathrm{RS}(255, 239, 17)$ code can be built over $\mathrm{GF}(2^8)$ with the irreducible polynomial $\mathrm{x}^8 + \mathrm{x}^5 + \mathrm{x}^3 + \mathrm{x} + 1$, for example. This code satisfies $255 > 32$. Change the generator matrix of this code to the echelon form $\mathrm{G} = [\mathrm{I}|\mathrm{A}]$, where matrix A is a 239×16 one. Then the 16×16 recursive MDS matrix A_3 (the submatrix of A) achieved is in Figure 4.

$$S_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 50 & BF & EF & 2B & 57 & BE & 94 & 97 \end{bmatrix}$$

Figure 3. A 8 × 8 serial matrix from RS code

$$\begin{bmatrix}
2F & 33 & F7 & 2D & 72 & 9F & 2E & 83 & 15 & 5D & 12 & B6 & 64 & EC & FE & B0 \\
76 & C6 & 4 & CA & 4C & 66 & 59 & A5 & AB & 2 & 18 & AD & 4 & A1 & 6C & 9C \\
FE & 7A & B6 & E9 & 6C & 5D & 4 & BA & 87 & F3 & 89 & C2 & A6 & 2F & 1 & 83 \\
C6 & 95 & 22 & 5D & 26 & 21 & 18 & E4 & 20 & 8E & 9D & 75 & 39 & A7 & 40 & 8A \\
BA & 2D & 53 & A7 & D & A0 & 11 & CF & C3 & CA & 62 & E0 & B7 & 65 & 17 & 7C \\
E0 & D & 8D & 4B & 28 & 56 & 3C & 1D & 79 & AC & 23 & FA & 5D & 1F & 24 & AC \\
3F & 3B & 20 & C1 & D5 & EA & C5 & 1A & B2 & D8 & 3A & 4B & 14 & AD & 79 & D9 \\
A3 & D3 & 28 & 1A & 4F & 87 & 90 & D8 & BE & 9F & 25 & 4B & 21 & 11 & 55 & 88 \\
E4 & 2E & D0 & F7 & AE & DC & EB & 6A & D5 & EE & 57 & 1F & 41 & 8E & 76 & 22 \\
39 & 18 & 64 & AD & DA & C0 & C7 & 40 & B6 & C1 & DC & CC & 88 & 20 & DD & 21 \\
48 & 90 & 60 & 6E & 16 & 3E & A9 & C2 & A3 & 45 & C5 & B6 & F7 & F6 & 5A & 71 \\
20 & B3 & F & A2 & 9D & AC & 6F & C8 & 9D & 70 & 66 & 52 & 89 & CF & ED & C0 \\
79 & 1 & EC & DD & 42 & AC & 15 & 6 & AA & 4 & 4 & F8 & BB & 98 & AA & A5 \\
43 & 22 & B2 & CE & DC & 4B & 4A & 4 & 14 & E8 & 10 & ED & 2F & 16 & 21 & E0 \\
1E & F8 & F2 & 47 & E7 & 96 & B5 & A5 & 90 & 23 & 8A & 52 & 5B & AC & F7 & 75 \\
9C & 29 & C6 & 84 & 57 & 77 & 7F & 8E & AE & 1C & 48 & 93 & D6 & AE & 32 & FB
\end{bmatrix}$$

Figure 4. A 16 × 16 recursive MDS matrix from RS code

The serial matrix S_3 corresponding with A_3 is in Figure 5.

$$\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2F & 33 & F7 & 2D & 72 & 9F & 2E & 83 & 15 & 5D & 12 & B6 & 64 & EC & FE & B0
\end{bmatrix}$$

Figure 5. A 16 × 16 serial matrix from RS code

Comment 3. The methods of Algorithm 2 and in [20] are the same in that the recursive MDS matrix is constructed from a cyclic code, namely the BCH code in [20] and the RS code in this paper. However, in [20] a BCH $[2k+z,k+z,k+1]_q$ code is constructed then shorten on z positions to obtain MDS code. In this paper, it is considered more generally that from an any MDS $[n,k,d]$ code where $k \geq n-k$ a recursive MDS matrix can be generated (MDS codes in this paper are built from RS codes). In addition, the RS codes are built much simpler than the BCH codes.

V. CONCLUSION

In this paper, the methods for constructing effectively MDS and recursive MDS matrices from RS codes and some relevant constraints are presented. Advantages of the given methods include MDS and recursive MDS matrices of arbitrary sizes can be created and constructing RS codes is very simple and can be easily installed. The MDS and recursive MDS matrices generated from these methods are not only having an important role in improving the security of block ciphers and hash functions against developing cryptanalytic techniques but also improving the efficiency in implementation of the diffusion layers.

REFERENCES

[1]. S. Vaudenay, “On the need for multipermutations: cryptanalysis of MD4 and SAFER”, In B. Preneel, editor, Fast Software Encryption. Proceedings, vol 1008 of LNCS, pp. 286-297, Springer-Verlag, 1995.

[2]. C. Schnorr and S. Vaudena, “Black box cryptanalysis of hash networks based on multipermutations”, In A. De Santis, editor, Advances in Cryptology - EU-ROCRYPT ’94. Proceedings, vol. 950 of LNCS, pp. 47-57. Springer-Verlag, 1995.

[3]. L. Keliher, “Linear cryptanalysis of substitution-permutation networks”, Queen's University, Kingston, Ontario, Canada, 2003.

[4]. M. R. Z’aba, “Analysis of linear relationships in block ciphers”, Ph.D. Thesis, Queensland University of Technology, Brisbane, Australia, 2010.

[5]. Daemen and V. Rijmen, “AES Proposal”, Rijndael (Version 2), NIST AES.

[6]. NIST, “Advanced Encryption Standard (AES)”, (FIP PUB 197), November 26, 2001.

[7]. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, “The cipher shark”, in Fast Software Encryption. Springer, pp. 99-111,1996.

[8]. J. Daemen, L. Knudsen, and V. Rijmen, “The block cipher square”, in Fast Software Encryption (FSE' 97). Springer, pp. 149-165, 1997.

[9]. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, Twofish: “A 128-bit block cipher, In the first AES Candidate Conference. National Journal of Network Security”, vol. 9, no. 2, pp. 109-116, 2009. Institute for Standards and Technology, 1998.

[10]. A. Youssef, S. Mister, and S. Tavares, “On the design of linear transformation for substitution permutation encryption networks,” in Workshop on Selected Areas in Cryptography (SAC96): Workshop Record, pp. 40-48, 1997.

[11]. R. Elumalai, A. R. Reddy, “Improving diffusion power of AES rijndael with 8x8 MDS matrix”, International Journal of Scientific & Engineering Research, vol. 2, pp. 1-5, 2011.

[12]. S. M. T. Sakallı, B. Aslan, “Algebraic construction of 16×16 binary matrices of branch number 7 with one fixed point”, Computer Engineering Department, Trakya University, Edirne, Turkey, 2012.

[13]. M. Sajadieh, M. Dakhilalian, H. Mala, and B. Omoomi, “On construction of involutory mds matrices from vandermonde matrices in GF (2^q)”, Design, Codes and Cryptography, vol. 64, no. 3, pp. 287-308, 2012.

[14]. F.J. MacWilliams, N.J.A. Sloane, “The theory of error-correcting codes”. Elsevier, 1977.

[15]. K. C. Gupta and I. G. Ray, “On constructions of MDS matrices from companion matrices for lightweight cryptography,” in Security Engineering and Intlligence Informatics. Springer, pp. 29-43, 2013.

[16]. M. Sajadieh, M. Dakhilalian, H. Mala, and P. Sepehrdad, “Recursive diffusion layers for block ciphers and hash functions”, in Fast Software Encryption. Springer, pp. 385-401, 2012.

[17]. S. Wu, M. Wang, and W. Wu, “Recursive diffusion layers for (lightweight) block ciphers and hash functions”, in Selected Areas in Cryptography. Springer, pp. 43-60, 2013.

[18]. D. Augot and M. Finiasz, “Exhaustive search for small dimension recursive mds diffusion layers for block ciphers and hash functions,” in 2013 IEEE International Symposium on Information Theory Proceedings (ISIT). IEEE, pp. 1551-1555, 2013.

[19]. S. Kolay, D. Mukhopadhyay, “Lightweight diffusion layer from the kth root of the mds matrix”, IACR Cryptology ePrint Archive, vol. 498, 2014.

[20]. D. Augot, M. Finiasz, “Direct construction of recursive mds diffusion layers using shortened BCH codes”, 21st International Workshop on Fast Software Encryption, FSE 2014, Springer, 2014.

ABOUT THE AUTHOR

MS. Trần Thị Lượng
Workplace: Academy of cryptography techniques.
Email: luongtranhong@gmail.com

She received Bachelor degree in Mathematics and Informatics from The Hanoi University of Science in 2006, Master degree in cryptographic technique from Academy of cryptographic technique in 2012.
Research today: Cryptogaphy and Database Security.

“Journal of Science and Technology on Information security”

(Version No. II of the *Information Security Journal*)

Information Security Journal publishes a periodical academic – scientific journal in the field of Information Security with the title "Research of Science and Technology in the field of Information Security". The Publication aims to create a forum for exchange of specialized scientific – technological issues in the field of Information Security, to support the research of science and technology, contributing to connecting research, trainning and applications deployement.

The Journal is published in Vietnamese and English, issued 2 editions / year in the whole territory of Vietnam, to the leaders, managers, scientific – technical staff, teachers, graduate students, the fellows,... such people who are conducting the activitiesin the field of Information Security in the country.

The papers that are published in journal are the scientific research works, applications of new technologies, scientific achievements, new techniques in the field of secrecy and information security, which have not been sent to any magazine to be published or to any conference proceedings and must be of scientific quality, which have been appraised and assessed by the experts in order to be counted points by the State’s scientific Councils for the converted scientific works.