Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 1237–1248
DOI : 10.47974/JDMSC-1715

On the direct building of 8 × 8 self-reciprocal recursive MDS Matrices effective for implementation over GF(q) using Reed-Solomon codes

Tran Thi Luong
Academy of Cryptography Techniques
No. 141 Chien Thang road
Tan Trieu, Thanh Tri
Hanoi
Vietnam

Abstract

MDS matrices are from the MDS codes in coding theory that are being used widely in cryptographic applications. Recursive MDS matrix is an matrix that is a power of some simple companion matrix. These matrices are so convenient for execution especially for hardware implementation using LFSRs. Therefore, these matrices have attracted the interest of many scientists. In this paper, we give a way to directly build 8 × 8 self-reciprocal recursive MDS matrices efficient for execution over the field $GF(q)$, ($q = p^r$, $p$is a prime number) using the Reed-Solomon codes. These matrices are significant in practice because they have the potential to be used in lightweight cryptographic algorithms.

Subject Classification: *(2010): 15Axx, 15Bxx.*

Keywords: *Companion matrix, Self-reciprocal MDS matrix, MDS matrix, Recursive matrix, Reed-solomon codes.*

1. Introduction

MDS matrices are important linear transforms used in many cryptographic applications. MDS matrices were first presented by Serge Vaudenay [1] for being used in cryptographic applications in FSE'95. Because of their ability to provide maximum diffusion, they are being used for the diffusion layer of many block ciphers and hash functions nowadays.

E-mail: luongtranhong@gmail.com

Since the implementation of MDS matrices is quite expensive, the researchers always expect to find good MDS matrices to ensure the lowest implementation cost for both encryption and decryption.

Recently, an approach using the recursive MDS matrices for lightweight applications is of interest. An MDS matrix $M = S_g^k$ where S_g is a companion matrix corresponding to a polynomial $g(X) \in F_q[X]$ is called a recursive MDS matrix [2, 4] which is a power of the matrix S_g. These matrices have the advantage that they can be implemented using LFSRs which can reduce implementation costs, especially for hardware implementation [2, 4].

Currently, there have been many studies in the literature to search for recursive MDS matrices as in [1, 2, 3, 4, 5, 6, 10,12]. However, these research methods are often based on exhaustive search [1], so only recursive MDS matrices of small size can be found. In [2, 4], the authors built recursive MDS matrices based on BCH codes, but the method based on BCH codes is quite complicated.

In [5], the authors mentioned regular recursive MDS matrices and symmetric recursive MDS matrices. In which, a symmetric recursive MDS matrix is attached with a self-reciprocal and monic polynomial. Symmetric recursive MDS matrices have the advantage that one can implement the same LFSR circuit for both encryption and decryption [5], so these recursive MDS matrices are very efficient for implementation, especially for hardware implementation. However, these matrices are not symmetric. Therefore, in this paper, we call a recursive MDS matrix attached with a self-reciprocal and monic polynomial *the self-reciprocal recursive MDS matrix*.

In [7], a simple and efficient method of building the recursive MDS matrices using Reed-Solomon (RS) codes was given. In [8], we presented a method to generate self-reciprocal recursive MDS matrices of size 4 efficient for implementation over $GF(q)$, $q = p^r$, using RS codes. However, in some cryptographic applications larger MDS matrices may be required because they provide higher diffusion and greater security for cryptographic algorithms. In this article, we give a way to directly construct self-reciprocal recursive MDS matrices of size 8 efficiently for implementation over $GF(q)$, $q = p^r$, using RS codes. The construction of RS codes has the advantage of being very simple so that such self-reciprocal recursive MDS ones can be easily found.

The paper is organized as follows. In Section 2, preliminaries and related works are given. Section 3 shows a method for the direct

construction of 8 × 8 self-reciprocal recursive MDS matrices efficient for implementation over $GF(q)$ using RS codes. Section 4 is the conclusion.

2. Preliminaries and Related Works

2.1 *Recursive MDS Matrix*

An MDS matrix $M = S_g^k$ where S_g is a companion matrix corresponding to a polynomial $g(x) \in GF(q)[X]$ is called a recursive MDS matrix [2, 4] which is a power of the companion matrix S_g.

In [9], the definition of reciprocal polynomial is as follows:

Definition 1 [9] : The reciprocal g^* of a polynomial $g = a_0 + a_1X + \ldots + a_{k-1}X^{k-1} + a_kX^k \in \mathbb{F}_q[X]$ where $a_0, \ldots, a_k \in \mathbb{F}_q^*$, is defined by:

$$g^* = X^k g\left(\frac{1}{X}\right) = a_0X^k + a_1X^{k-1} + \ldots + a_{k-1}X + a_k.$$

A polynomial is self-reciprocal if it is the same as it's corresponding reciprocal polynomial.

A self-reciprocal polynomial g has $a_i = a_{k-i}$, $i = 0,1,\ldots,k$. If $\gamma(\neq 0)$ is a root of g and then so is γ^{-1}.

In [5] it is defined that: A symmetric recursive MDS matrix is an MDS matrix $M = S_g^m$ with its associated polynomial g being monic and self-reciprocal.

It is also shown in [5] that, combining a symmetric recursive MDS matrix (denoted by M) with a matrix that reverses the order of rows of M (denoted by R) forms the RM matrix, then RM is an involutory MDS matrix. So, the RM matrix can help use the same LFSR circuit for encryption and decryption processes.

Where

$$R = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{pmatrix}$$

However, to avoid confusion with regular symmetric matrices, we give another definition.

Definition 2 : A recursive MDS matrix $M = S_g^m$ (S is a companion matrix) associated with a monic and self-reciprocal polynomial g is called a self-reciprocal recursive MDS matrix.

Thus, we can see that self-reciprocal recursive MDS matrices are very efficient for implementation, especially for hardware implementation because we can use the above *RM* matrix.

Note that, in this article, there are a few places where we refer a self-reciprocal recursive MDS to a self-reciprocal MDS ones for brevity.

2.2 *RS code*

The RS code is a well-known cyclic code in error correcting code theory. The RS code is defined as follows:

A RS code [9, Ch. 10] is a BCH code of length $n = q-1$ over the field $GF(q)$ where $q = p^r, p$ is prime. Suppose that α is a root element of the field. Denote d, k the minimum distance and dimension of the code respectively. Then the RS code has a generating polynomial as follow:

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

Note that, $b \in N, b \geq 0$.

3. Use Reed-Solomon codes to build 8 × 8 self-reciprocal MDS matrices over *GF*(*q*)

Now we give a method to directly construct 8 × 8 self-reciprocal MDS matrices efficiently for execution over $GF(q)$ using RS codes.

Considering the general case, according to [7], we showed that to construct a recursive MDS matrix of size m the using RS code over $GF(q)$ where $q = p^r, p$ is the prime number, we need to build RS codes of length $n = q-1$, minimum distance $d = m+1$, dimension $k = n-d+1$ with the generating polynomial $g(x)$ (where $g(x)$ has degree $n-k = d-1$) has form (1), with $0 \leq b \leq q-1$, $b \in N$.

In [7], Proposition 2 showed that, to construct a recursive MDS matrix of size $n-k$ from an MDS code $C[n,k,d]$, the condition is $k \geq n-k$. This is equivalent to $n \leq 2k \leftrightarrow n \leq 2(n-d+1)$. This is equivalent to $n \geq 2d-2 \leftrightarrow q \geq 2d-1 \leftrightarrow q \geq 2m+1$. RS codes are also a case of MDS codes. We therefore have the following comment:

Comment 1: We can build a $m \times m$ recursive MDS matrix using a $RS[n,k,d]$ code if $q \geq 2m+1$.

We can build a $m \times m$ recursive MDS matrix using a $RS[n,k,d]$ code

Here, we have some assumptions as follows:

$$\begin{cases} n = q-1 & (2) \\ q = p^r, p \text{ is prime} & (3) \\ d = m+1 & (4) \\ k = q-m-1 & (5) \\ 0 \le b \le q-1, b \in N & (6) \end{cases}$$

Since $k \ge 0$, so $q-m-1 \ge 0$ then $q-1 \ge m$. Combined with Comment 1, infer:

$$q \ge 2m+1 \quad (7)$$

The free coefficient of $g(x)$ has the form:

$$\alpha^{b+(b+1)+\ldots+(b+d-2)} = \alpha^{mb+\frac{m(m-1)}{2}} \quad (8)$$

Let $$e_m = mb + \frac{m(m-1)}{2}. \quad (9)$$

As α is the root element of the field $GF(q)$, $g(x)$ has its constant coefficient equal to 1 when:

$$(q-1) \mid e_m \quad (10)$$

Consider the case of matrices of size 8, that is m = 8.

In this case, we have:

$$g(x) = (x+\alpha^b)(x+\alpha^{b+1})\ldots(x+\alpha^{b+7}) \quad (11)$$

We have the following theorem:

Theorem 1: *Suppose* $g(x)$ *is a generating polynomial of the form (11) of the RS code over* $GF(q)$ *where* $q = p^r, r \ge 2$, p *is prime. Then,* $g(x)$ *is a self-reciprocal polynomial if and only if* $p = 2$, $r > 4$ *and* $b = 2^{r-1} - 4$.

Proof: From (7) it is deduced that $q \ge 17$ (12). From (9) it is to have $e_8 = 8b + 28$ (13).

In order for $g(x)$ to have the constant coefficient equal to 1, from (10) and (13), we have the condition is:

$$(q-1) \mid (8b+28) \quad (14)$$

From (11), we have:

$$
\begin{aligned}
g(x) &= (x+\alpha^b)(x+\alpha^{b+1})\ldots(x+\alpha^{b+7}) \\
&= [(x+\alpha^b)(x+\alpha^{b+7})]\ [(x+\alpha^{b+1})(x+\alpha^{b+6})] \\
&\ [(x+\alpha^{b+2})(x+\alpha^{b+5})]\ [(x+\alpha^{b+3})(x+\alpha^{b+4})] \\
&= [x^2+(\alpha^b+\alpha^{b+7})x+\alpha^{2b+7}][x^2+(\alpha^{b+1}+\alpha^{b+6})x+\alpha^{2b+7}] \\
&\ [x^2+(\alpha^{b+2}+\alpha^{b+5})x+\alpha^{2b+7}][x^2+(\alpha^{b+3}+\alpha^{b+4})x+\alpha^{2b+7}] \\
&= ([x^2+\alpha^b(1+\alpha^7)x+\alpha^{2b+7}][x^2+\alpha^{b+3}(1+\alpha)x+\alpha^{2b+7}]) \\
&\ ([x^2+\alpha^{b+1}(1+\alpha^5)x+\alpha^{2b+7}][x^2+\alpha^{b+2}(1+\alpha^3)x+\alpha^{2b+7}]) \\
&= [x^4+\alpha^b(1+\alpha^3)(1+\alpha^4)x^3+\alpha^{2b+3}(2\alpha^4+(1+\alpha)(1+\alpha^7))x^2 \\
&\ +\alpha^{3b+7}(1+\alpha^3)(1+\alpha^4)x+\alpha^{4b+14}\ ]. \\
&\ [x^4+\alpha^{b+1}(1+\alpha)(1+\alpha^4)x^3+\alpha^{2b+3}(2\alpha^4+(1+\alpha^3)(1+\alpha^5))x^2 \\
&\ +\alpha^{3b+8}(1+\alpha)(1+\alpha^4)x+\alpha^{4b+14}\ ]
\end{aligned}
$$

Let $coe(x^i)$ be the coefficient of x^i.

- Let $g(x)$ be a self-reciprocal polynomial then:

$$
\begin{cases}
coe(x^8) = coe(x^0) \\
coe(x^7) = coe(x) \\
coe(x^6) = coe(x^2) \\
coe(x^5) = coe(x^3)
\end{cases}
$$

+ The condition $coe(x^8) = coe(x^0) \leftrightarrow$ (14).
+ It is to have:

$$
\begin{aligned}
coe(x^7) &= \alpha^b(1+\alpha)^3(1+\alpha^4) \\
coe(x) &= \alpha^{7b+21}(1+\alpha)^3(1+\alpha^4)
\end{aligned}
$$

It is deduced that,

$$coe(x^7) = coe(x) \leftrightarrow \alpha^{6b+21} = 1 \leftrightarrow (q-1) \mid (6b+21). \tag{15}$$

+ It is to have:

$$
\begin{aligned}
coe(x^6) &= \alpha^{2b+1}[4\alpha^6+\alpha^2(1+\alpha^3)(1+\alpha^5)+\alpha^2(1+\alpha)(1+\alpha^7) \\
&\quad +(1+\alpha)(1+\alpha^3)(1+\alpha^4)^2] \\
coe(x^2) &= \alpha^{6b+15}[4\alpha^6+\alpha^2(1+\alpha)(1+\alpha^7)+\alpha^2(1+\alpha^3)(1+\alpha^5) \\
&\quad +(1+\alpha)(1+\alpha^3)(1+\alpha^4)^2]
\end{aligned}
$$

It is deduced that,

$$coe(x^6) = coe(x^2) \leftrightarrow \alpha^{4b+14} = 1 \leftrightarrow (q-1) \mid (4b+14). \tag{16}$$

+ It is to have:

$$coe(x^5) = \alpha^{3b+3}(1+\alpha^4)[3\alpha^4(1+\alpha^3)+3\alpha^5(1+\alpha)+\alpha(1+\alpha)^2(1+\alpha^7) + (1+\alpha^3)^2(1+\alpha^5)]$$

$$coe(x^3) = \alpha^{5b+10}(1+\alpha^4)[3\alpha^4(1+\alpha^3)+3\alpha^5(1+\alpha)+\alpha(1+\alpha)^2(1+\alpha^7) + (1+\alpha^3)^2(1+\alpha^5)]$$

It is deduced that,

$$coe(x^5) = coe(x^3) \leftrightarrow \alpha^{2b+7} = 1 \leftrightarrow (q-1) \mid (2b+7) \quad (17)$$

So for $g(x)$ to be a self-reciprocal polynomial then:

$$\begin{cases} (q-1) \mid (8b+28) & (14) \\ (q-1) \mid (6b+21) & (15) \\ (q-1) \mid (4b+14) & (16) \\ (q-1) \mid (2b+7) & (17) \end{cases} \leftrightarrow (q-1) \mid (2b+7) \quad (17)$$

because $6b+21 = 3(2b+7)$, $4b+14 = 2(2b+7)$ and $8b+28 = 4(2b+7)$.

Combining (17) with (3), (6) and (12), for $g(x)$ to be a self-reciprocal polynomial, the necessary and sufficient condition is:

$$\begin{cases} q = p^r, p \text{ is prime} & (3) \\ q \geq 17 & (12) \\ (q-1) \mid (2b+7) & (17) \\ 0 \leq b \leq q-1, b \in N & (6) \end{cases} \quad (*)$$

From (17): because $2b + 7$ is odd, so q – 1 must be odd $\rightarrow q$ must be even.

So q must be of the form $q = 2^r$ (that is, $p = 2$).

Then the condition (*) becomes:

$$\begin{cases} q = 2^r & (3a) \\ q \geq 17 & (12) \\ (q-1) \mid (2b+7) & (17) \\ 0 < b < q-1, b \in N & (6a) \end{cases} \quad (**)$$

Note that: If $b = 0$ or $b = q - 1$, from (17) it is to have $(q-1) \mid 7$ does not satisfy (12).

And (17) $\Leftrightarrow 2b+7 = t(q-1)$ for $t \geq 1; t \in N$.

It is deduced that

$$b = \frac{t(q-1)-7}{2} \tag{18}$$

From (6a), it is to have:

$$\frac{7}{q-1} < t < 2 + \frac{7}{q-1} \tag{19}$$

From (12) and (19), it is to have:

$$\left[\begin{array}{l} t=1 \\ t=2 \end{array}\right. \tag{20}$$

+ If $t = 1$, from (18) and (3a), it is to have: $b = \frac{q-8}{2} = 2^{r-1} - 4$

From (6a), the condition $b < q - 1$ is obviously true; the condition $0 < b \to r > 3$.

On the other hand, from (3a) and (12), it is deduced that $r > 4$

+ If $t = 2$, from (18) and (3a), so: $b = \frac{2q-9}{2} = 2^r - \frac{9}{2}$. In this case, b does not satisfy the condition $b \in N$.

Thus, for $g(x)$ to be self-reciprocal, the satisfying values are: $q = 2^r$ for $r > 4$ an $b = 2^{r-1} - 4$. ■

Note that, this $g(x)$ polynomial is monic.

Comment 2: There are $\phi(q-1)$ root elements in the field $GF(q)$, so it can be repeated the above process and then $\phi(q-1)$ self-reciprocal monic polynomials are obtained. On the other hand, if α is a root element of $GF(q)$, then so is α^u where u is co-prime with $q - 1$ and u is a positive integer.

Example: For $q = 2^5$, then $b = 12$; For $q = 2^6$, then $b = 28$;

For $q = 2^7$, then $b = 60$; For $q = 2^8$, then $b = 124$.

Table 1 shows some examples of self-reciprocal polynomials and the corresponding 8 × 8 self-reciprocal MDS matrices generated by Reed-Solomon codes.

Table 1

A few examples of self-reciprocal MDS matrices of size 8

No.	Field GF	Primitive polynomial	RS code, self-reciprocal generating polynomials	Corresponding self-reciprocal MDS matrices	Corresponding Companion matrix	b
1	$GF(2^5)$	x^5+x^2+1	RS(31, 23, 9), $g(x)=x^8+\alpha^{14}x^7+\alpha^{13}x^6$ $+\alpha^{25}x^5+\alpha x^4+\alpha^{25}x^3+\alpha^{13}x^2$ $+\alpha^{14}x+1$	$\begin{bmatrix} 1 & 1D & 1C & 19 & 2 & 19 & 1C & 1D \\ 1D & 17 & 16 & 11 & 6 & F & 12 & A \\ A & 11 & 11 & 17 & 5 & 7 & 9 & 1E \\ 1E & 1E & 1B & 12 & E & 6 & D & 1D \\ 1D & 8 & 15 & 16 & D & 3 & D & 1B \\ 1B & F & 1 & 4 & 5 & 1C & A & 1F \\ 1F & 12 & 19 & 1B & 1F & 1F & A & 3 \\ 3 & 1D & 13 & 17 & 1D & 11 & 1E & 8 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1D & 1C & 19 & 2 & 19 & 1C & 1D \end{bmatrix}$	$b=12$
2	$GF(2^5)$	$x^5+x^3+x^2+x$ $+1$	RS(31, 23, 9) $g(x)=x^8+\alpha^3x^7+\alpha x^6$ $+\alpha^{23}x^5+\alpha^{18}x^4+\alpha^{23}x^3$ $+\alpha x^2+\alpha^3x+1$	$\begin{bmatrix} 1 & 8 & 2 & 15 & D & 15 & 2 & 8 \\ 8 & 1F & 18 & 16 & C & 19 & 5 & 1C \\ 1C & A & 8 & 1 & 9 & 15 & E & 7 \\ 7 & B & 4 & 12 & D & 13 & 1B & 19 \\ 19 & 2 & 16 & 2 & 1B & B & E & 1E \\ 1E & B & 11 & A & 7 & 7 & 18 & 1C \\ 1C & 1C & 1C & 8 & 15 & 1E & 10 & 1A \\ 1A & 1 & 7 & A & 16 & 3 & 5 & D \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 8 & 2 & 15 & D & 15 & 2 & 8 \end{bmatrix}$	$b=12$
3	$GF(2^6)$	x^6+x+1	RS(63, 55, 9), $g(x)=x^8+\alpha^7x^7+\alpha^{50}x^6$ $+\alpha^{39}x^5+\alpha^{55}x^4+\alpha^{49}x^3$ $+\alpha^{50}x^2+\alpha^7x+1$	$\begin{bmatrix} 1 & 6 & 34 & 1A & 2E & 1A & 34 & 6 \\ 6 & 15 & 38 & 2B & 3B & 31 & 24 & 20 \\ 20 & 3 & 3B & 2F & 12 & 2C & 1F & 21 \\ 21 & 23 & 19 & 36 & 38 & 1F & 36 & 1C \\ 1C & 2A & B & D & A & 2C & 37 & 3D \\ 3D & 14 & 18 & 12 & 26 & 13 & 1E & 3F \\ 3F & 39 & D & 35 & 26 & B & A & 1A \\ 1A & 20 & 2F & 6 & 28 & 2D & 1D & 15 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 6 & 34 & 1A & 2E & 1A & 34 & 6 \end{bmatrix}$	$b=28$

Contd...

4	$GF(2^7)$	x^7+x+1	RS(127, 119, 9), $g(x)=x^8+\alpha^{109}x^7+\alpha^{30}x^6$ $+\alpha^{28}x^5+\alpha^{117}x^4+\alpha^{28}x^3$ $+\alpha^{30}x^2+\alpha^{109}x+1$	$\begin{bmatrix} 1 & 32 & 44 & 11 & 2F & 11 & 44 & 32 \\ 32 & 1B & 52 & 5C & 4D & 37 & 71 & 5E \\ 5E & 9 & 14 & 71 & 45 & 6E & 38 & 4A \\ 4A & 4 & 48 & 65 & 28 & 34 & 2F & 62 \\ 62 & 51 & 5A & 1E & 3F & 7E & 6A & 34 \\ 34 & 57 & 2c & 24 & 23 & 41 & 3 & 5F \\ 5F & 3D & 1C & 1E & 12 & 11 & A & A \\ A & 2E & 1A & 35 & 3E & 3B & 36 & 7B \end{bmatrix}$ $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 32 & 44 & 11 & 2F & 11 & 44 & 32 \end{bmatrix}$	$b=60$
5	$GF(2^8)$	$x^8+x^6+x^5$ $+x^3+1$	RS(255,247,9) $g(x)=x^8+\alpha^{236}x^7+\alpha^{175}x^6$ $+\alpha^{11}x^5+\alpha^{115}x^4+\alpha^{11}x^3$ $+\alpha^{175}x^2+\alpha^{236}x+1$	$\begin{bmatrix} 1 & 1B & 45 & F3 & 8E & F3 & 45 & 1B \\ 1B & 2D & B3 & 62 & A6 & A9 & 5B & 69 \\ 69 & DC & 67 & AB & 3B & BE & E3 & 9C \\ 9C & D3 & E3 & 47 & 77 & 1B & 81 & 59 \\ 59 & 59 & 57 & 4D & 2B & D9 & 9F & 44 \\ 44 & EA & 82 & 26 & EB & 5A & 2 & 2C \\ 2C & 2B & 3E & 18 & 57 & 71 & 8E & 6D \\ 6D & 87 & 1C & 51 & AB & 38 & 46 & 25 \end{bmatrix}$ $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1B & 45 & F3 & 8E & F3 & 45 & 1B \end{bmatrix}$	$b=124$

The results of Theorem 1 show that, we can only build 8 × 8 self-reciprocal MDS matrices over on $GF(q)$, $q=p^r, p$ is a prime number, if and only if $p = 2$, and we can indicate the exact value of b, i.e. for $r > 4$ and $b=2^{r-1}-4$. Thus, it is possible for direct building self-reciprocal and monic generating polynomials of degree 8 of the corresponding RS codes. That means we can easily build 8 × 8 self-reciprocal MDS matrices from RS codes according to the results of Theorem 1. As analyzed in the introduction, from the self-reciprocal MDS matrices we can create involutory MDS matrices (form of *RM*) that are very convenient for implementation, especially for hardware implementation.

With our results, we can obtain many effective self-reciprocal MDS matrices for execution, especially for hardware execution. Comparing our results with [1, 2, 3, 4, 5, 6, 10,12], it can be seen that our method using RS codes is much simpler. Thanks to that, we can specify the self-reciprocal MDS matrices easily. From there, we can use these matrices for many lightweight applications nowadays.

4. Conclusion

Recursive MDS matrices are of great interest to researchers because of their efficient performance. Self-reciprocal MDS matrices are even more efficient because one can practice the same LFSR circuit for encryption and decryption processes. In this article, we propose an approach for direct building 8 × 8self-reciprocal MDS matrices that are efficient for performing over the field $GF(q)$, $q = p^r$ using the RS codes. We can take advantage of these matrices to be widely applied in today's lightweight cryptographic algorithms.

Funding

This work has been supported by Academy of Cryptography Techniques, Ha noi, Viet nam.

References

[1] Augot D. and Finiasz M., "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, 2013, pp.1551-1555.

[2] Augot D., Finiasz M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: FSE 2014, LNCS, vol. 8540, pp. 3–17. Springer (2015).

[3] Gupta K.C., Ray I.G.: On constructions of MDS matrices from companion matrices for lightweight cryptography. In: CD-ARES Workshops 2013, LNCS, vol. 8128, pp. 29–43. Springer (2013).

[4] Gupta K.C., Pandey S.K., Venkateswarlu A.: On the direct construction of recursive MDS matrices. Des. Codes Cryptogr. 82(1–2), 77–94 (2017).

[5] Gupta K.C., Pandey S.K., Venkateswarlu A., Almost involutory recursive MDS diffusion layers, *Design, Codes and Cryptography*, 87 (2018), 609-626.

[6] Kolay S., Mukhopadhyay D., "Lightweight diffusion layer from the k^{th} root of the mds matrix", *IACR Cryptology ePrint Archive*, vol. 498, 2014.

[7] Luong T. T., "Constructing effectively MDS and recursive MDS atrices by Reed-Solomon codes", *Journal of Science and Technology on Information Security of Viet Nam Government Information Security Commission*, vol.3, no. 2, pp. 10–16, 2016.

[8] Luong T. T., Cuong N. N., and Trinh B. D., *4 × 4 Recursive MDS Matrices Effective for Implementation from Reed-Solomon Code over GF(q) Field*. International Conference on Modelling, Computation and Optimization in Information Systems and Management Sciences – MCO 2021, pp 386-391, 2021.

[9] MacWiliams F.J, Sloan N.J. *The Theory of Error-Correcting Codes*, North-holland Publishing Company Amsterdam-New York- Oxford, Third Printing, 1981.

[10] Sajadieh M., Dakhilalian M., Mala H., Sepehrdad P.: Recursive diffusion layers for block ciphers and hash functions. In: FSE 2012, LNCS, vol. 7549, pp. 385–401. Springer (2012).

[11] Vaudenay S., On the need for multipermutations: cryptanalysis of MD4 and SAFER. In B. Preneel, editor, Fast Software Encryption. Proceedings, volume 1008 of LNCS, pages 286–297. Springer-Verlag, 1995.

[12] Wu S., Wang M., Wu W.: Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: SAC 2013, LNCS, vol. 7707, pp. 355–371. Springer (2013).