A Generalization of the Subfield Construction

Kamil Otal[1]

National Research Institute of Electronics and Cryptology, TÜBİTAK BİLGEM, Gebze, Kocaeli, Turkey
kamil.otal@gmail.com

Research Paper Received: 17.04.2022 Revised: 26.05.2022 Accepted: 27.05.2022

Abstract—The subfield construction is one of the most promising methods to construct maximum distance separable (MDS) diffusion layers for block ciphers and cryptographic hash functions. In this paper, we give a generalization of this method and investigate the efficiency of our generalization. As a result, we provide several best MDS diffusions with respect to the number of XORs that the diffusion needs. For instance, we give

- an involutory MDS diffusion $\mathbb{F}_{2^8}^3 \to \mathbb{F}_{2^8}^3$ by 85 d-XORs and
- an involutory MDS diffusion $\mathbb{F}_{2^8}^4 \to \mathbb{F}_{2^8}^4$ by 122 d-XORs

and hence present new records to the literature. Furthermore, we interpret the coding theoretical background of our generalization.

Keywords—maximum distance separable (MDS) matrices, subfield construction

1. Introduction

Block ciphers are the oldest and most common way of secure communication. In particular, The Advanced Encryption Standard (AES) [8] has been intensely utilized and analyzed all over the world since the day it was standardized. In the construction of a modern block cipher like AES, there are two main principles taken into account: confusion and diffusion. The confusion property is generally provided by S-boxes which are special nonlinear mappings on a finite dimensional vector space over $\mathbb{F}_2$, whereas the diffusion is often provided by a maximum distance separable (MDS) matrix which is the redundancy (check) part of a generator matrix of an MDS code.

In general, if r-bit to r-bit S-boxes are used during the construction of a block cipher, then an MDS matrix over $\mathbb{F}_{2^r}$ (or $\mathrm{GL}(r,\mathbb{F}_2)$ in general) is preferred for the maximum diffusion (see the wide trail strategy approach for further detail in [7]). Such a preference lets us easily count active S-boxes through rounds. Note that counting active S-boxes is an important process to show the resistance of the cipher against linear and differential attacks.

The subfield construction, which is introduced in [1], applies an unconventional usage of MDS matrices in case $r = 8$. In particular, a $k \times k$ MDS matrix over $\mathbb{F}_{2^4}$ is multiplied by the semi-columns of the input column, instead of multiplying a $k \times k$ MDS matrix over $\mathbb{F}_{2^8}$ by the input column (see Proposition 2 below). This procedure gives quite efficient MDS diffusions with respect to the number of XORs in some cases (see [14, Table 2] for example).

In this paper, we give a generalization of the subfield construction (Theorem 1) relaxing most of the parameters. We then examine the efficiency of our method with respect to the XOR counting procedure. As a result, we observe that our generalization gives the best MDS diffusions for many cases, see Tables 1, 2, 3, and 4.

The rest of the paper is organized as follows. We firstly recall some preliminary tools mostly from coding theory in Section 2. We state and prove our generalization, and examine its efficiency in Section 3. Lastly we present final remarks, containing the coding theoretical background, on our method in Section 4.

2. Preliminaries

In this section, we briefly recall the fundamental notions mostly coming from coding theory.

Let $\mathbb{F}_{2^r}^n$ denote the set of vectors of length n and with entries from the finite field $\mathbb{F}_{2^r}$ of size 2^r. The function $d : \mathbb{F}_{2^r}^n \times \mathbb{F}_{2^r}^n \to \mathbb{R}$ given by $d(u, v) := |\{i : i \in \{1, 2, \dots, n\}, u_i \neq v_i\}|$ satisfies the metric properties and is called the *Hamming distance*. A subset C of $\mathbb{F}_{2^r}^n$ endowed with the Hamming metric is called a *code*. We define the *minimum (Hamming) distance* of a code C by $d(C) := \min\{d(u, v) : u, v \in C, u \neq v\}$. There is an upper bound on $d(C)$ given by $d(C) \leq n + 1 - \log_{2^r}(|C|)$ and called the *Singleton bound*. A subset C of $\mathbb{F}_{2^r}^n$ satisfying the Singleton bound is called an *MDS code*.

The main parameters of a code C in $\mathbb{F}_{2^r}^n$ is denoted by $(n, |C|, d(C))_{2^r}$. In particular, if C is a k-dimensional subspace of $\mathbb{F}_{2^r}^n$ over $\mathbb{F}_{2^r}$, then we denote the main parameters of C by $[n, k, d(C)]_{2^r}$. MDS codes exist for many but not all parameters. In particular, the *MDS Conjecture*, which is stated below, formulates the existence of linear MDS codes with respect to their parameters (see also [22, Conjecture 11.16] for example).

Conjecture 1 (The MDS Conjecture) *The parameters of a linear MDS code $[n, k, n-k+1]_{2^r}$ of length n and dimension $k > 1$ over $\mathbb{F}_{2^r}$ satisfy the following.*

$$n \leq \begin{cases} 2^r + 1 & \text{if } k \in \{2\} \cup \{4, 5, \dots, 2^r - 2\}, \\ 2^r + 2 & \text{if } k \in \{3, 2^r - 1\}, \\ k + 1 & \text{if } k \geq 2^r. \end{cases}$$

A linear code corresponds to a rowspace of a $k \times n$ matrix over $\mathbb{F}_{2^r}$. Such a matrix is called a *generator matrix* of the code. In particular, linear MDS codes can be uniquely represented by a $k \times n$ matrix $[I : M]$ which is a concatenation of $k \times k$ identity matrix I and $k \times (n-k)$ matrix M over $\mathbb{F}_{2^r}$. Here, the redundancy (check) part M of the generator matrix is called an *MDS matrix*. The minimum distance of a given linear MDS code equips the corresponding MDS matrix as in the following well-known result.

Proposition 1 *Let u be a nonzero $k \times 1$ matrix and M be a $k \times k$ MDS matrix over $\mathbb{F}_{2^r}$. Then the number of minimum total nonzero entries in both u and Mu is at least $k + 1$.*

Construction of MDS matrices is an important and intensely studied area in mathematics and cryptography. We refer the reader to [9] which is a recent and comprehensive survey in this area.

Now we define a bijection between vector spaces $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^3} \times \mathbb{F}_{2^5}$ over $\mathbb{F}_2$: Let $\mathbb{F}_{2^8} = \mathbb{F}_2(\theta)$ where θ is a root of an irreducible polynomial of degree 8, $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$ where α is a root of an irreducible polynomial of degree 3, and $\mathbb{F}_{2^5} = \mathbb{F}_2(\beta)$ where β is a root of an irreducible polynomial of degree 5 over $\mathbb{F}_2$. Then, for

$$u = u_{0,0} + u_{0,1}\theta + u_{0,2}\theta^2 + \cdots + u_{0,7}\theta^7$$

where $u_{0,i} \in \mathbb{F}_2$ for $0 \leq i \leq 7$, we define

$$\begin{aligned} u_1 &= u_{0,0} + u_{0,1}\alpha + u_{0,2}\alpha^2 \\ u_2 &= u_{0,3} + u_{0,4}\beta + u_{0,5}\beta^2 + u_{0,6}\beta^3 + u_{0,7}\beta^4 \end{aligned}$$

and hence construct a bijection

$$u \leftrightarrow (u_1, u_2).$$

(We sometimes use notation $u_1||u_2$ to denote (u_1, u_2).) In that way, we obtain

$$1+\theta^2+\theta^3+\theta^4+\theta^6 \quad \leftrightarrow \quad (1+\alpha^2, 1+\beta+\beta^3)$$

for example. This bijection idea can be easily extended from $\mathbb{F}_{2^8} \leftrightarrow \mathbb{F}_{2^3} \times \mathbb{F}_{2^5}$ to

$$\mathbb{F}_{2^{r_1+r_2+\cdots+r_s}} \leftrightarrow \mathbb{F}_{2^{r_1}} \times \mathbb{F}_{2^{r_2}} \times \cdots \times \mathbb{F}_{2^{r_s}}$$

for arbitrary positive integers r_i $(1 \le i \le s)$, and to matrices directly. Remark that there always exists an irreducible polynomial of any degree over $\mathbb{F}_2$ (see [18] for further details).

We now give another method, first introduced in [1] and called the *subfield construction*, to satisfy the maximum byte-wise branching like in Proposition 1.

Proposition 2 *Let r be an even integer, u be a nonzero $k \times 1$ matrix over $\mathbb{F}_{2^r}$, u_1 and u_2 be $k \times 1$ matrices over $\mathbb{F}_{2^{r/2}}$ such that $u = u_1||u_2$, and M be a $k \times k$ MDS matrix over $\mathbb{F}_{2^{r/2}}$. Then the minimum total nonzero entries in both u and $Mu_1||Mu_2$ is at least $k+1$.*

We omit the proof of Proposition 2 since Theorem 1 in Section 3 covers Proposition 2, please see the proof of Theorem 1 for the verification of Proposition 2.

The efficiency of an MDS mapping is generally measured by the number of XORs that the mapping needs. In particular, we focus on the finite field multiplication between a constant finite field element and a variable. The number of XORs that the multiplication needs is determined with respect to the irreducible polynomial which defines the finite field. For example, consider the finite field $\mathbb{F}_{2^3} = \mathbb{F}(\alpha)$ where α is a root of $x^3+x+1 \in \mathbb{F}_2[x]$, the multiplication of $\alpha+\alpha^2$ and the arbitrary element $y = y_0 + y_1\alpha + y_2\alpha^2$ $(y_i \in \mathbb{F}_2$ for $0 \le i \le 2)$ is given by

$$\begin{aligned}(\alpha+\alpha^2)y &= (\alpha+\alpha^2)(y_0+y_1\alpha+y_2\alpha^2) \\ &= (y_1+y_2)+(y_0+y_1)\alpha \\ &\quad +(y_0+y_1+y_2)\alpha^2.\end{aligned}$$

which corresponds to the vector $(y_1+y_2,\ y_0+y_1,\ y_0+y_1+y_2)$. Here, the addition corresponds to the XOR operation and hence we need to apply $1+1+2=4$ XORs to execute the multiplication. That is, the multiplication by $\alpha+\alpha^2$ corresponds to the transformation

$$(y_0,\ y_1,\ y_2) \mapsto (y_1+y_2,\ y_0+y_1,\ y_0+y_1+y_2) \quad (1)$$

which requires 4 XORs. The XOR counting procedure given above is called the *direct XOR (d-XOR) counting* [13].

It is possible to define d-XOR in a slightly different way. Let $f(x) = f_rx^r + f_{r-1}x^{r-1} + \cdots + f_1x + f_0$ be an irreducible polynomial of degree r over $\mathbb{F}_2$, let α be a root of f, and define $\mathbb{F}_{2^r} = \mathbb{F}(\alpha)$. Here, considering α, define

$$M_\alpha = \begin{bmatrix} 0 & 0 & \dots & 0 & f_0 \\ 1 & 0 & \dots & 0 & f_1 \\ 0 & 1 & \dots & 0 & f_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & f_{r-1} \end{bmatrix}.$$

We call M_α the *companion matrix* of α over $\mathbb{F}_2$. There is a field isomorphism between $\mathbb{F}_{2^r}$ and $\{0\} \cup \{M_\alpha^i : 0 \le i \le 2^r-2\} \subseteq \mathbb{F}_2^{r\times r}$. Here, the number of ones in M_{α^i} for some $\alpha^i \in \mathbb{F}_2(\alpha)$ and $0 \le i \le 2^r-1$ is equal to r plus the d-XOR of α^i. For instance, taking $\mathbb{F}_{2^3} = \mathbb{F}(\alpha)$ where α is a root of $x^3+x+1 \in \mathbb{F}_2[x]$, we see that

$$M_\alpha = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Also see that the companion matrix of $\alpha^2+\alpha$ is

$$M_{\alpha^2+\alpha} = M_\alpha^2 + M_\alpha = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Here, the number of ones in $M_\alpha^2 + M_\alpha$ is 7 and $r=3$, hence the number of d-XORs of $\alpha^2+\alpha$ is $7-3=4$ (see also the d-XOR of Equation (1)).

The d-XOR counting process can be extended to matrices in $\mathbb{F}_{2^r}^{k\times k}$ directly: Let $A \in \mathbb{F}_{2^r}^{k\times k}$ and M_A denote the $rk \times rk$ companion matrix of A over $\mathbb{F}_2$ which is constructed by taking $(M_A)_{i,j} = M_{A_{i,j}}$ for all $1 \le i,j \le k$. Then the d-XOR of A is equal to the number of ones in M_A minus rk.

There are also some techniques to reduce the number of XORs in such mappings. For instance, the mapping in Equation (1) can be implemented as follows:

1 Compute $t_0 := y_1 + y_2$.
2 Return $(t_0,\ y_0 + y_1,\ y_0 + t_0)$.

In that way, it is possible to reduce the number of XORs to 3 from 4. However, we need to wait for t_0 to apply Step 2 in this time. In other words, the XOR depth here is 2 whereas the XOR depth in Equation (1) is 1. We hence observe a trade-off between the time and memory complexities. The lowest possible of XORs ignoring the XOR depth is called the *sequential XOR (s-XOR)* [11].

In general, for a fixed matrix having low d-XORs, mostly it is possible to reduce the number of XORs further considering the s-XOR procedure. Therefore, finding mappings with lower d-XORs is an important problem. We mean the d-XOR in the rest of the paper while mentioning the number of XORs unless otherwise stated. We refer the reader to [3], [4], [5], [6], [11], [16], [21], [26] for various types of optimization techniques.

An MDS matrix with less XORs is considered more efficient than the others. In general, an MDS mapping with less XORs provides similar efficiency benefits.

In the subfield construction introduced in Proposition 2, we multiply the number of XORs for the matrix by 2 since the matrix is applied on two different semi-columns.

In many block ciphers, MDS mappings are used for encryption and their inverses are used for decryption. Therefore, MDS mappings are considered together with their inverses in many usage areas in cryptography. Therefore, an MDS mapping whose inverse is itself, which is also called *involutory*, has a special interest in cryptography.

3. A Generalization of the Subfield Construction and Its Efficiency Analysis

In this section, we generalize Proposition 2 and then investigate the efficiency of this generalization with respect to the XOR counting.

Theorem 1 *Let u be a nonzero $k \times 1$ matrix over $\mathbb{F}_{2^{r_1+r_2+\cdots+r_s}}$, u_i be a $k\times 1$ matrix over $\mathbb{F}_{2^{r_i}}$ for $1 \le i \le s$, and $u = u_1||u_2||\ldots||u_s$. Let also M_i be a $k \times k$ MDS matrix over $\mathbb{F}_{2^{r_i}}$ for $1 \le i \le s$ and $v := M_1u_1||M_2u_2||\ldots||M_su_s$ be the $k\times 1$ matrix obtained by concatenating $M_1u_1, M_2u_2, \ldots, M_su_s$. Then the number of total nonzero entries in u and v is at least $k+1$.*

Proof: Assume that u has j nonzero entries for some $1 \le j \le k$. Then, there exists at least one $1 \le i \le s$ such that u_i has j_i nonzero entries for some $1 \le j_i \le j$. This implies that M_iu_i has at least $k+1-j_i$ nonzero entries, hence the number of nonzero entries in v must be greater than or equal to $k+1-j_i$. In other words, the number of nonzero entries in v is greater than or equal to $k+1-j$ since

$j_i \leq j$. As a result, the number of nonzero entries in both u and v is greater than or equal to $k+1$. □

We would like to highlight the differences between Theorem 1 and Proposition 2:

- We do not have to use the same MDS matrix M to multiply with u_1 and u_2 as in Proposition 2, we can use different MDS matrices M_1 and M_2 to satisfy the MDS branching.
- Similarly, M as in Proposition 2 does not have to be over $\mathbb{F}_{2^{r/2}}$, it can be over just a smaller field. That is, r does not have to be even (or a multiple of a certain fixed number).
- Additionally, we do not have to split u into two as u_1 and u_2, we can split it into more pieces.

The following example illustrates Theorem 1.

Example 1 *Let $k = 2$, $s = 3$, $r_1 = 2$, $r_2 = 3$, $r_3 = 3$, $\alpha \in \mathbb{F}_{2^{r_1}}$ be a root of $x^2+x+1 \in \mathbb{F}_2[x]$ and $\beta \in \mathbb{F}_{2^{r_2}} = \mathbb{F}_{2^{r_3}}$ be a root of $x^3+x+1 \in \mathbb{F}_2[x]$. Let also*

$$M_1 = \begin{bmatrix} \alpha & 1+\alpha \\ 1 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} \beta+1 & \beta^2+1 \\ 1 & \beta \end{bmatrix}, \quad M_3 = \begin{bmatrix} 1 & \beta \\ 1 & 1 \end{bmatrix}.$$

Note that M_1, M_2 and M_3 are MDS matrices. Remark that we can separate each nonzero $u \in \mathbb{F}_{2^8}^2$ by $u = u_1||u_2||u_3$ for some $u_1 \in \mathbb{F}_{2^2}^2, u_2 \in \mathbb{F}_{2^3}^2$, and $u_3 \in \mathbb{F}_{2^3}^2$. The transformation

$$u \mapsto v = M_1u_1||M_2u_2||M_3u_3$$

is an MDS diffusion, i.e. the number of nonzero bytes in both u and v is at least 3.

We call the method in Theorem 1 *generalized subfield construction*. We remark that the generalized subfield construction contains both the subfield construction (where $s = 2$, $M_1 = M_2$, and $r_1 = r_2$) and classical MDS matrix multiplication (where $s = 1$ and $r_1 = r$).

The generalized subfield construction has also the following nice property that we use in the rest of this section. We state it without proof since it is straightforward.

Theorem 2 *Consider the assumptions and notations of Theorem 1. Then, the MDS mapping is involutory if and only if the MDS matrix M_i is involutory for all $1 \leq i \leq s$.*

Remark 1 *We would like to emphasize some points on the generalized subfield construction: Theorem 1 seems a natural generalization of Proposition 2 but not a much promising method with respect to the XOR counting process. Interestingly, we observe that we can produce the best MDS diffusions using Theorem 1 in some cases. The following subsections are devoted to examine the efficiency of the generalized subfield construction for MDS diffusions.*

3.1. The $k = 2$ Case for Involutory MDS Diffusions

In this section, we focus on the involutory MDS diffusions $\mathbb{F}_{2^r}^2 \to \mathbb{F}_{2^r}^2$ using Theorem 1. We need the following generic result for this purpose.

Theorem 3 *Any 2×2 involutory MDS matrix over $\mathbb{F}_{2^r}$ is in the form of*

$$\begin{bmatrix} 1+(bc)^{2^{r-1}} & b \\ c & 1+(bc)^{2^{r-1}} \end{bmatrix} \tag{2}$$

for some nonzero $b, c \in \mathbb{F}_{2^r}$.

Proof: Assume that

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is an involutory MDS matrix over $\mathbb{F}_{2^r}$. Then, the property $M^2 = I$ implies the Equation system

$$\begin{aligned} a^2 + bc &= 1, & (3)\\ ab + bd &= 0, & (4)\\ ca + dc &= 0, & (5)\\ cb + d^2 &= 1. & (6) \end{aligned}$$

Here, Equations (3) and (6) implies $a = d$ since the characteristic of $\mathbb{F}_{2^r}$ is 2. The Equations (4) and (5) are then naturally satisfied. We obtain the required form combining (3) by the fact that $a = d$ and $\sqrt{bc} = (bc)^{2^{r-1}}$ since $(bc)^{2^r} = bc$ in $\mathbb{F}_{2^r}$. □

Example 2 *Let $r = 8$. We obtain the following results by a computer search trying all possible b and c in Theorem 3.*

- *Let $\mathbb{F}_{2^8} = \mathbb{F}_2(\alpha)$, α be a root of $x^8 + x^6 + x^5 + x^3 + 1$. The most efficient involutory MDS matrix over this field with respect to the number of XORs needs 32 XORs. One of such matrices is*
$$\begin{bmatrix} \alpha & 1 \\ \alpha^2+1 & \alpha \end{bmatrix}.$$
- *Let $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$, α be a root of $x^4 + x + 1$. The most efficient involutory MDS matrix over this field with respect to the number of XORs needs 13 XORs. One of such matrices is*
$$\begin{bmatrix} \alpha^2 & 1 \\ \alpha & \alpha^2 \end{bmatrix}.$$
Therefore, the classical subfield construction can be applied by 26 XORs.
- *Let $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, α be a root of $x^3 + x + 1$; $\mathbb{F}_{2^5} = \mathbb{F}_2(\beta)$, β be a root of $x^5 + x^2 + 1$. The most efficient involutory MDS matrices over these fields with respect to the number of XORs need 9 and 15 XORs, respectively. Samples of such matrices are*
$$\begin{bmatrix} \alpha & \alpha^2+1 \\ 1 & \alpha \end{bmatrix} \text{ and } \begin{bmatrix} \beta^4+\beta & 1 \\ \beta^3 & \beta^4+\beta \end{bmatrix}.$$
Therefore, the generalized subfield construction can be applied by 24 XORs.

This example shows that the generalized subfield construction provides better results in case $k = 2$ and $r = 8$.

In general, Table 1 contains computational results for different r values. As we observe from the table, Theorem 1 gives better results when r increases.

r	**Prop. 1** (r)	**Prop. 2** $\left(\frac{r}{2}+\frac{r}{2}\right)$	**Thm. 1** $\left(\sum_{i=1}^{s} r_i\right)$
2	**7**	NA	
3	**9**	NA	
4	**13**	14	
5	**15**	NA	16 (2+3)
6	19	**18**	20 (2+4)
7	**21**	NA	22 (3+4)
8	32	26	**24** (3+5)
9	**27**	NA	**27** (3+3+3)
10	33	**30**	**30** (3+7)

Table 1.
The least number of XORs for a 2×2 MDS diffusion over $\mathbb{F}_{2^r}$. (NA means "not applicable". The bold font indicates the best value in the row.)

Remark 2 *It is important to note that the irreducible polynomial used to construct the finite field affects the number of XORs. In general, the irreducible polynomials of the lowest number of terms and highest gap[1], for example $x^5 + x^2 + 1$ for $\mathbb{F}_{2^5}$, is preferred. However, such polynomials do not guarantee the lowest number of XORs especially for matrices. For example, the lowest number of XORs*

[1] The difference between the degrees of the two highest-degree nonzero terms is called *gap*.

for matrices of the form (2) *in Theorem 3 is 35 when we use* $x^8 + x^4 + x^3 + x + 1$, *whereas it is 32 when we use* $x^8 + x^6 + x^5 + x^3 + 1$ *in case* $r = 8$.

3.2. The $k = 3$ Case for Involutory MDS Diffusions

In this section, we focus on the involutory MDS diffusions $\mathbb{F}_{2^r}^3 \to \mathbb{F}_{2^r}^3$ using Theorem 1. We need the following main result presented by Güzel et al. in [10]. (See also [12] and [20] as other resources on such MDS diffusions.)

Theorem 4 *[10] Any* 3×3 *involutory MDS matrix over* $\mathbb{F}_{2^r}$ *is in the form of*

$$\begin{bmatrix} a_1 & (a_1+1)b_0 & (a_1+1)b_1 \\ (a_2+1)b_0^{-1} & a_2 & (a_2+1)b_0^{-1}b_1 \\ (a_1+a_2)b_1^{-1} & (a_1+a_2)b_1^{-1}b_0 & a_1+a_2+1 \end{bmatrix}$$

for some nonzero $a_1, a_2, b_0, b_1 \in \mathbb{F}_{2^r}$ *satisfying* $a_1 \neq a_2$, $a_1 + a_2 \neq 1$, $a_1 \neq 1$, *and* $a_2 \neq 1$.

r	**Prop. 1** (r)	**Prop. 2** $\left(\frac{r}{2}+\frac{r}{2}\right)$	**Thm. 1** $\left(\sum_{i=1}^{s} r_i\right)$
3	**31**	NA	
4	**43**(ref. [10])	NA	
5	**54**	NA	
6	67	**62**	
7	79	NA	**74** (3+4)
8	108 (ref. [10])	86 (ref. [10])	**85** (3+5)

Table 2.
The least number of XORs for a 3×3 MDS diffusion over $\mathbb{F}_{2^r}$. (NA means "not applicable". The bold font indicates the best value in the row.)

Example 3 *Let* $r = 8$. *We obtain the following results by a computer search trying all possible* a_1, a_2, b_0 *and* b_1 *in Theorem 4.*

- *Let* $\mathbb{F}_{2^8}$ *be constructed over* $x^8 + x^7 + x^6 + x + 1$. *The most efficient involutory MDS matrix over this field with respect to the number of XORs needs 108 XORs (see [10]).*
- *Let* $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$, α *be a root of* $x^4 + x + 1$. *The most efficient involutory MDS matrix over this field with respect to the number of XORs needs 43 XORs (see [10] for example). Therefore, the classical subfield construction can be applied by 86 XORs.*
- *Let* $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, α *be a root of* $x^3 + x + 1$; $\mathbb{F}_{2^5} = \mathbb{F}_2(\beta)$, β *be a root of* $x^5 + x^2 + 1$. *The most efficient involutory MDS matrices over these fields with respect to the number of XORs need 31 and 54 XORs, respectively. Samples of such matrices are*
$$\begin{bmatrix} \alpha^2+1 & 1 & \alpha+1 \\ 1 & \alpha^2+\alpha & \alpha \\ \alpha^2 & 1 & \alpha \end{bmatrix}$$
and
$$\begin{bmatrix} \beta^2 & 1 & \beta^2 \\ 1 & \beta^4+\beta^2+\beta & \beta^4+\beta^2+\beta \\ \beta^2 & \beta^4+\beta^2+\beta & \beta^4+\beta+1 \end{bmatrix}.$$
Therefore, the generalized subfield construction can be applied by 85 XORs.

This example shows that the generalized subfield construction provides better results in case $k = 3$ *and* $r = 8$.

In general, Table 2 contains computational results for different r values. As we observe from the table, Theorem 1 gives better results when r increases.

3.3. The $k = 4$ Case for Involutory MDS Diffusions

In this section, we focus on the involutory MDS diffusions $\mathbb{F}_{2^r}^4 \to \mathbb{F}_{2^r}^4$ using Theorem 1. Note that such mappings are among the most intensely used MDS diffusions in cryptography. We use the following form of matrices, which is presented by Kurt Pehlivanoğlu et al. in [15], for our computer search: A 4×4 involutory MDS matrix over $\mathbb{F}_{2^r}$ of the form

$$\begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1b_1^{-1} & a_0 & a_3b_1^{-1}b_2 & a_2b_1^{-1}b_3 \\ a_2b_2^{-1} & a_3b_2^{-1}b_1 & a_0 & a_1b_2^{-1}b_3 \\ a_3b_3^{-1} & a_2b_3^{-1}b_1 & a_1b_3^{-1}b_2 & a_0 \end{bmatrix} \qquad (7)$$

for some nonzero $a_0, a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_{2^r}$ is called *Generalized Hadamard.*

Example 4 *Let $r = 8$. We have the following results.*

- *The most efficient involutory MDS matrix over $\mathbb{F}_{2^8}$ with respect to the number of XORs in the literature needs 144 XORs and such matrices were given in [23].*
- *The most efficient involutory MDS matrix over $\mathbb{F}_{2^4}$ with respect to the XOR count in the literature needs 64 XORs and such matrices were given in [15, Example 5]. Therefore, the classical subfield construction can be applied by 128 XORs.*
- *Let $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$, α be a root of $x^3 + x + 1$; $\mathbb{F}_{2^5} = \mathbb{F}_2(\beta)$, β be a root of $x^5 + x^2 + 1$. The most efficient involutory MDS matrices over these fields with respect to the number of XORs need 50 and 72 XORs, respectively, according to our computer search on matrices of the form* (7). *Samples of such matrices are*

$$\begin{bmatrix} 1 & \alpha & \alpha^2+\alpha+1 & 1 \\ \alpha & 1 & 1 & \alpha^2+\alpha+1 \\ \alpha^2+1 & \alpha & 1 & \alpha \\ \alpha & \alpha^2+1 & \alpha & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & \beta^4+\beta & \beta^2 & 1 \\ 1 & 1 & \beta & \beta^2 \\ \beta^2 & 1 & 1 & \beta^4+\beta \\ \beta & \beta^2 & 1 & 1 \end{bmatrix}.$$

Therefore, the generalized subfield construction can be applied by 122 XORs.

This example shows that the generalized subfield construction provides better results in case $k = 4$ and $r = 8$.

r	**Prop. 1** (r)	**Prop. 2** $\left(\frac{r}{2} + \frac{r}{2}\right)$	**Thm. 1** $\left(\sum_{i=1}^{s} r_i\right)$
3	**50**	NA	
4	**64** (ref. [15])	NA	
5	**72**	NA	
8	144 (ref. [23])	128	**122** (3+5)

Table 3.
The least known number of XORs for a 4×4 MDS diffusion over $\mathbb{F}_{2^r}$ in the literature. (NA means “not applicable”. The bold font indicates the best value in the row.)

In general, Table 3 contains computational results for different r values. As we observe from the table, Theorem 1 gives better results when r increases.

3.4. The $k = 4$ and $k = 8$ Cases for Involutory and Non-Involutory MDS Diffusions

In this section, we focus on the involutory and non-involutory MDS diffusions $\mathbb{F}_{2^8}^4 \rightarrow \mathbb{F}_{2^8}^4$ and $\mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8$ using Theorem 1. In particular, we give an example below and hence update some parts of a comprehensive table ([14, Table 2]) that presents the efficiency of various methods for such MDS mappings in Table 4. We remark that the generalized subfield construction produces quite good (and sometimes best) MDS diffusions.

Example 5 *Kranz et al. compared the number of XORs of* 4×4 *and* 8×8 *MDS and involutory MDS matrices over* $\mathrm{GL}(4, \mathbb{F}_2)$ *and* $\mathrm{GL}(8, \mathbb{F}_2)$ *in [14, Table 2]. We update this table as Table 4 considering the following results.*

1 *In [14, Table 2], we see that there are* 4×4 *MDS matrices over* $\mathrm{GL}(4, \mathbb{F}_2)$ *with 58 XORs [24]. If we apply these matrices for two semi-columns as in Proposition 2 (or Theorem 1 in general), then we obtain a diffusion* $\mathbb{F}_{2^8}^4 \to \mathbb{F}_{2^8}^4$ *with 116 XORs.*

2 *As shown in Example 4, we can apply Theorem 1 and obtain an involutory diffusion* $\mathbb{F}_{2^8}^4 \to \mathbb{F}_{2^8}^4$ *with 122 XORs.*

3 *There are* 8×8 *MDS matrices over* $\mathrm{GL}(4, \mathbb{F}_2)$ *with 380 XORs [15]. If we apply these matrices for two semi-columns as in Proposition 2 (or Theorem 1 in general), then we obtain a diffusion* $\mathbb{F}_{2^8}^8 \to \mathbb{F}_{2^8}^8$ *with 760 XORs.*

4 *There are* 8×8 *involutory MDS matrices over* $\mathrm{GL}(4, \mathbb{F}_2)$ *with 407 XORs [15]. If we apply these matrices on two semi-columns as in Proposition 2 (or Theorem 1 in general), then we obtain 814 XORs.*

Method	**Ref.**	**#XORs**
MDS Branching on a 4×1 Column over $\mathrm{GL}(8, \mathbb{F}_2)$		
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Subfield)	[23]	136
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Circulant)	[20]	128
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$	[17]	**106**
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Circulant)	[2]	136
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Toeplitz)	[24]	123
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Subfield)	[11]	122
Example 5(1)	This paper	116
Involutory MDS Branching on a 4×1 Column over $\mathrm{GL}(8, \mathbb{F}_2)$		
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Subfield)	[23]	144
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Hadamard)	[17]	136
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Circulant)	[17]	132
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$ (Subfield)	[11]	136
Example 5(2)	This paper	**122**
MDS Branching on a 8×1 Column over $\mathrm{GL}(8, \mathbb{F}_2)$		
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Hadamard)	[23]	768
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Circulant)	[20]	688
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Circulant)	[2]	784
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Toeplitz)	[25]	**680**
Example 5(3)	This paper	760
Involutory MDS Branching on a 8×1 Column over $\mathrm{GL}(8, \mathbb{F}_2)$		
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Hadamard)	[23]	816
Matrix in $\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$ (Hadamard)	[11]	1152
Example 5(4)	This paper	**814**

Table 4.
Comparison of MDS branchings with respect to XOR counts. This table is indeed an updated version of the related parts of [14, Table 2] by adding our results.

4. Concluding Remarks

We would like to state some of our observations on our generalization in this section. The parameters r, r_i, k, s mentioned below are from the notation of Theorem 1.

1. Observe that the classical usage of MDS matrices corresponds to the usage of linear MDS codes. In the literature, there are also some different diffusion layers that corresponds to the usage of nonlinear codes such as Kerdock codes (see [19] for example). Our method is between these two ideas: codes linear over $\mathbb{F}_2$ but nonlinear over $\mathbb{F}_{2^r}$. Particularly, our method uses codes which are linear over $\mathbb{F}_{2^{\gcd(r_1,\ldots,r_s)}}$ where $\gcd$ denotes the greatest common divisor. In other words, our method is an application of nonlinear but additive MDS codes in cryptog-

raphy.

2. The field $\mathbb{F}_{2^{r/2}}$ is a subfield of $\mathbb{F}_{2^r}$ in Proposition 2. However, $\mathbb{F}_{2^{r_i}}$ is not a subfield of $\mathbb{F}_{2^r}$ in Theorem 1 if r_i is not a divisor of r. Therefore, it may not be suitable to name our method as "generalized subfield construction" but we use such a term anyway since our method is the only generalization of Proposition 2 to the best of our knowledge.
3. Consider the $r = 8$ case. The most efficient irreducible polynomial of degree 8 over $\mathbb{F}_2$ is $x^8 + x^4 + x^3 + x + 1$ which needs 3 XORs for reduction. On the other hand, the most efficient irreducible polynomial of degree 4 over $\mathbb{F}_2$ is $x^4 + x + 1$ which needs 1 XOR for reduction. Therefore, it is expected that Proposition 2 outperforms Proposition 1 since $2 \times 1 < 3$. However, our computations show that the separation $r_1 = 3$ and $r_2 = 5$ is more efficient than the separation $r_1 = r_2 = 4$ for $r = 8$ in Theorem 1, even if it sensually seems the opposite. There are also many other such examples in our computations presented in Tables 1, 2, 3, and 4.
4. Our generalization gives better results when r increases especially for involutory MDS diffusions as we observe in Tables 1, 2 and 3.
5. The proper form of our generalization (i.e. the form covered in Theorem 1 but not in Propositions 1 and 2) is not applicable as k increases because of the MDS conjecture.
6. Our generalization seems promising when s increases as we observe in Table 1 for $r = 9$.
7. Our generalization indicates that it is important to study the MDS diffusions for not only $r = 4$ and $r = 8$ but also $r = 2, 3, 5, 6$ for daily life applications.
8. Our generalization seems promising especially for involutory MDS diffusions but we think that it is a powerful method for also non-involutory MDS diffusions as we observe in Table 4.
9. We remark that the results in this paper are only for d-XORs, i.e. the case where the XOR depth is 1. However, we also think that the generalized subfield construction is also useful for other cases in which the XOR depths are greater. Such cases are mainly based on various optimization techniques and intensely studied in those days (see for example [3], [4], [5], [6], [11], [16], [21], [26]). Therefore, the idea of utilizing the generalized subfield construction in such optimization techniques would be a possible future work.

References

[1] P. S. L. M. Barreto, V. Nikov, S. Nikova, V. Rijmen, and E. Tischhauser, "Whirlwind: a new cryptographic hash function," Designs, Codes and Cryptography, vol. 56, no. 2, pp 141–162, 2010. [Online]. Available: https://doi.org/10.1007/s10623-010-9391-y.

[2] C. Beierle, T. Kranz, and G. Leander, "Lightweight multiplication in GF(2^n) with applications to MDS matrices," In: CRYPTO 2016, Part I, Ed. by Matthew Robshaw and Jonathan Katz, Lecture Notes in Computer Science, vol. 9814, Springer, 2016, pp. 625–653. [Online]. Available: https://doi.org/10.1007/978-3-662-53018-4_23.

[3] J. Boyar, M. G. Find, and R. Peralta, "Small low-depth, low-size circuits for cryptographic applications," Cryptography and Communications, vol. 11, pp. 109–127, 2019. [Online]. Available: https://doi.org/10.1007/s12095-018-0296-3.

[4] J. Boyar, P. Matthews, and R. Peralta, "On the shortest linear straight-line program for computing linear forms," In: International Symposium on Mathematical Foundations of Computer Science (MFCS) 2008, Lecture Notes in Computer Science, vol. 5162, pp. 168–179, 2008. [Online]. Available: https://doi.org/10.1007/978-3-540-85238-4_13.

[5] J. Boyar, P. Matthews, and R. Peralta, "Logic minimization techniques with applications to cryptology," Journal of Cryptology, vol. 26, no. 2, pp. 280–312, 2013. [Online]. Available: https://doi.org/10.1007/s00145-012-9124-7.

[6] J. Boyar and R. Peralta, "A new combinational logic minimization technique with applications to cryptology," In: International Symposium on Experimental Algorithms (SEA) 2010, Lecture Notes in Computer Science, vol. 6049, pp. 178–189, 2010. [Online]. Available: https://doi.org/10.1007/978-3-642-13193-6_16.

[7] J. Daemen and V. Rijmen, “The wide trail design strategy,” In: IMA International Conference on Cryptography and Coding (IMACC) 2001, Lecture Notes in Computer Science, vol. 2260, Springer, pp. 222-238, 2001. [Online]. Available: https://doi.org/10.1007/3-540-45325-3_20.

[8] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Information Security and Cryptography, Springer, 2001. [Online]. Available: https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_2002.pdf.

[9] K. C. Gupta, S. K. Pandey, I. G. Ray, and S. Samanta, “Cryptographically significant MDS matrices over finite fields: a brief survey and some generalized results,” Advances in Mathematics of Communications, vol. 13, no. 4, pp. 779-843, 2019.

[10] G. G. Güzel, M. T. Sakallı, S. Akleylek, V. Rijmen, and Y. Çengellenmiş, “A new matrix form to generate all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$,” Information Processing Letters, vol. 147, pp. 61-68, 2019. [Online]. Available: https://doi.org/10.1016/j.ipl.2019.02.013.

[11] J. Jean, T. Peyrin, S. M. Sim, and J. Tourteaux, “Optimizing implementations of lightweight building blocks,” IACR Transactions on Symmetric Cryptology 2017, vol. 4, pp. 130-168, 2017. [Online]. Available: https://doi.org/10.13154/tosc.v2017.i4.130-168.

[12] P. Junod and S. Vaudenay, “Perfect diffusion primitives for block ciphers,” In: Selected Areas in Cryptography (SAC) 2004, Lecture Notes in Computer Science, vol. 3357, pp. 84-99, 2005. [Online]. Available: https://doi.org/10.1007/978-3-540-30564-4_6.

[13] K. Khoo, T. Peyrin, A. Y. Poschmann, and H. Yap, “FOAM: searching for hardware-optimal SPN dtructures and components with a fair comparison,” In: Conference on Cryptographic Hardware and Embedded Systems (CHES) 2014, pp. 433-450, 2014. [Online]. Available: https://doi.org/10.1007/978-3-662-44709-3_24.

[14] T. Kranz, G. Leander, K. Stoffelen, and F. Wiemer, “Shorter linear straight-line programs for MDS matrices,” IACR Transactions on Symmetric Cryptology 2017, vol. 4 pp. 188-211, 2017. [Online]. Available: https://doi.org/10.13154/tosc.v2017.i4.188-211.

[15] M. K. Pehlivanoğlu, M. T. Sakallı, S. Akleylek, N. Duru, and V. Rijmen, “Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography,” IET Information Security, vol. 12, no. 4, pp. 348-355, 2018. [Online]. Available: https://doi.org/10.1049/iet-ifs.2017.0156.

[16] S. Li, S. Sun, C. Li, Z. Wei, and L. Hu, “Constructing low-latency involutory MDS matrices with lightweight circuits,” IACR Transactions on Symmetric Cryptology 2019, vol. 1, pp. 84-117, 2019. [Online]. Available: https://doi.org/10.13154/tosc.v2019.i1.84-117.

[17] Y. Li and M. Wang, “On the Construction of lightweight circulant involutory MDS matrices,” In: Fast Software Encryption Workshop (FSE) 2016, Ed. by Thomas Peyrin, Lecture Notes in Computer Science, vol. 9783, Springer, pp. 121–139, 2016. [Online]. Available: https://doi.org/10.1007/978-3-662-52993-5_7

[18] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, UK: Cambridge University Press, 1994.

[19] Y. Liu, V. Rijmen, and G. Leander, “Nonlinear diffusion layers,” Designs, Codes and Cryptography, vol. 86, no. 11, pp. 2469-2484, 2018. [Online]. Available: https://doi.org/10.1007/s10623-018-0458-5

[20] M. Liu, S. M. Sim, “Lightweight MDS generalized circulant matrices,” In: Fast Software Encryption Workshop (FSE) 2016, Ed. by Thomas Peyrin, Lecture Notes in Computer Science, vol. 9783, Springer, pp. 101–120, 2016. [Online]. Available: https://doi.org/10.1007/978-3-662-52993-5_6

[21] C. Paar, “Optimized arithmetic for Reed-Solomon encoders,” In: IEEE International Symposium on Information Theory (ISIT) 1997, IEEE, pp. 250–250, 1997. [Online]. Available: https://doi.org/10.1109/ISIT.1997.613165

[22] R. M. Roth, *Introduction to Coding Theory*. Cambridge, UK: Cambridge University Press, 2006.

[23] S. M. Sim, K. Khoo, F. E. Oggier, and T. Peyrin, “Lightweight MDS involution matrices,” In: Fast Software Encryption Workshop (FSE) 2015, Ed. by Gregor Leander, Lecture Notes in Computer Science, vol. 9054, Springer, pp. 471–493, 2015. [Online]. Available: https://doi.org/10.1007/978-3-662-48116-5_23

[24] S. Sarkar and H. Syed, “Lightweight diffusion layer: importance of Toeplitz matrices,” Cryptology ePrint Archive, 2016/835, 2016. [Online]. Available: https://eprint.iacr.org/2016/835.pdf

[25] S. Sarkar and H. Syed, “Analysis of Toeplitz MDS matrices,” In: Australasian Conference on Information Security and Privacy (ACISP) 17, Part II, Ed. by Josef Pieprzyk and Suriadi Suriadi, Lecture Notes in Computer Science, vol. 10343, Springer, pp. 3–18, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-59870-3_1

[26] A. Visconti, C. V. Schiavo, and R. Peralta, “Improved upper bounds for the expected circuit complexity of dense systems of linear equations over GF(2),” Information Processing Letters, vol. 137, pp. 1-5, 2018. [Online]. Available: https://doi.org/10.1016/j.ipl.2018.04.010