SCIENCE CHINA
Information Sciences

• LETTER •

September 2016, Vol. 59 099101:1–099101:3
doi: 10.1007/s11432-015-0363-7

Construction of MDS block diffusion matrices for block ciphers and hash functions

Ruoxin ZHAO[1,2]*, Rui ZHANG[1]*, Yongqiang LI[1]* & Baofeng WU[1]*

[1] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2] *University of Chinese Academy of Sciences, Beijing* 100101*, China*

Received August 21, 2015; accepted March 7, 2016; published online June 2, 2016

Citation Zhao R X, Zhang R, Li Y Q, et al. Construction of MDS block diffusion matrices for block ciphers and hash functions. Sci China Inf Sci, 2016, 59(9): 099101, doi: 10.1007/s11432-015-0363-7

Dear editor,

Block ciphers are one of the most important building blocks in many cryptosystems. Modern block ciphers are often iterations with several rounds, where each round comprises a (nonlinear) confusion layer and a (linear) diffusion layer. The diffusion layer plays a significant role in block ciphers as well as in other cryptographic primitives such as hash functions. The security of a diffusion layer is measured by its differential branch number and the linear branch number. If the two branch numbers are larger, the diffusion layer is stronger at resisting differential cryptanalysis and linear cryptanalysis. The diffusion layers with the optimal branch numbers are referred to as maximum distance separable (MDS) (refer to [1–3]). Constructing diffusion layers with large branch numbers is a challenge for cryptosystem designers.

There are two types of diffusion layer according to the underlying fields, where the first is over extension fields of the finite field $GF(2)$, and the second type comprises block matrices over $GF(2)$. In fact, the former is a special case of the latter. In [4] and [5], the second type of diffusion layer was considered, i.e., block matrices where every block is a polynomial in a certain block L. Unfortunately, these previous studies only presented approaches for determining the forms of external matrices and failed to specify how to determine the internal block L.

In this letter, we also focus on the construction of block MDS diffusion layers where the blocks are all polynomials in a given block A. In contrast to previous studies, our approach starts from the internal block A. We propose a new method based on the minimal polynomials of matrices (refer to [6]) to test whether a diffusion layer is MDS. More significantly, we then present a new type of operation on matrices, which leads to an equivalence relation that can exponentially reduce the computational effort required when we search for MDS matrices. Thus, we describe a definite algorithm for finding block MDS diffusion layers. Using this algorithm, we find a large number of MDS diffusion layers with certain parameters. We give the detailed proofs and experimental results in the supplementary file associated with this letter.

Methodology. Suppose

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix}$$

*Corresponding author (email: zhaoruoxin@iie.ac.cn, r-zhang@iie.ac.cn, liyongqiang@iie.ac.cn, wubaofeng@iie.ac.cn)
The authors declare that they have no conflict of interest.

is an $(n \times n)$ polynomial matrix where every entry $f_{i,j}(x)$ is a polynomial in $\mathbb{F}_2[x]$ and $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ is a $(b \times b)$ matrix over the finite field $\mathbb{F}_2$ where $\mathcal{M}_{n\times n}(R)$ denotes the set of $(n \times n)$ matrices over a ring R. Then, $H(A)$ is a $(bn \times bn)$ matrix over $\mathbb{F}_2$. In this letter, we focus on diffusion layers with this form as $H(A)$. If the diffusion layer $L = H(A)$, we refer to $H(x)$ as the external matrix of L.

For an external matrix $H(x)$, to calculate $\det(H(A))$, we may assign A to x in each block of $H(x)$ and we can then calculate it directly as a $(bn \times bn)$ determinant. However, according to Lemma 1 in the supplementary file, we can choose another route. First, we calculate $h(x) = \det(H(x))$ (note that this is a polynomial), which is called the symbolic determinant of L. Next, we assign x with A and calculate $\det(h(A))$. In fact, we do not have to calculate directly $\det(h(A))$ because A has a minimal polynomial $m_A(x)$. To calculate $h(A)$, we simply need to obtain the residue $r(x)$ of $h(x)$ modulo $m_A(x)$ and calculate $r(A)$.

It is known that the MDS property of L depends on the nonsingularity of all its submatrices, which comprise the blocks $f_{i,j}(A)$ for $i, j = 1, \ldots, n$. We can definitely calculate all the minor determinants that comprise the blocks $f_{i,j}(A)$ of L using the method given above. However, to avoid a large computation effort, we present a new efficient approach for checking the nonsingularity of the submatrices that comprise the blocks of L. Suppose that $M(x)$ is a submatrix of $H(x)$. Then, $M(A)$ is nonsingular if and only if $\det(M(x))$ is coprime to $m_A(x)$ (Lemma 2 in the supplementary file). According to this new technique, we do not need to assign x with A and calculate the big-size determinants. It should be noted that $m_A(x)$ can be factorized (e.g., with Berlekamp's factorization algorithm) after we fix A. Suppose that $m_A(x)$ has the standard factorization $m_A(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s}$, where $p_1(x), \ldots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$ and $e_1, \ldots, e_s$ are positive integers. Then, the following four statements are equivalent (Theorem 1 in the supplementary file).

(1) $H(A)$ is an MDS block matrix with block size $(b \times b)$.

(2) Every minor determinant of $H(x)$ is coprime with $m_A(x)$.

(3) Every minor determinant of $H(x)$ is coprime with $p_i(x)$ for $i = 1, \ldots, n$.

(4) Every minor determinant of $H(x)$ is not congruent to 0 modulo $p_i(x)$ for $i = 1, \ldots, n$.

According to the discussion above, for a given block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, whether an external matrix $H(x)$ makes $H(A)$ a block MDS diffusion layer in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ is determined absolutely by $m_A(x)$, but not by A itself or b. Thus, if $A, A' \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ have the same minimal polynomial (e.g., A' is similar to A), an external matrix $H(x) \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ makes $H(A)$ MDS if and only if it makes $H(A')$ MDS (Theorem 2 in the supplementary file).

In addition to this new approach for checking the MDS property of diffusion layers, we describe a new operation on $H(x)$ that can retain the MDS property of $H(A)$. Suppose that the given block A, the external matrix $H(x) = (f_{i,j}(x))$, and the minimal polynomial $m_A(x)$ are the same as above. Let $g(x) = p_1(x)p_2(x)\cdots p_s(x)$ and

$$H'(x) = H(x) + g(x) \begin{pmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ h_{n,1}(x) & h_{n,2}(x) & \cdots & h_{n,n}(x) \end{pmatrix},$$

where $h_{i,j}(x) \in \mathbb{F}_2[x]$ for $i, j = 1, \ldots, n$. Then, $H(A)$ is MDS if and only if $H'(A)$ is MDS (Theorem 3 in the supplementary file). This fact means that the MDS property of a diffusion layer will not change if we add a multiple of $g(x)$ to every entry in its external matrix. This gives us an approach for constructing new MDS diffusion matrices from a known one, but more importantly, it also leads to an equivalence relation γ on $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ (i.e., $\mathcal{M}_{n\times n}(\mathbb{F}_2[x]/\langle m_A(x)\rangle)$). $H(x)$ and $H'(x)$ are γ-related if every entry of $H(x) - H'(x)$ is a multiple of $g(x)$. Consequently, we can partition $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ into γ-classes and the MDS property (MDS or not MDS) is invariant in each class. This equivalence relation γ exponentially reduces the size of the space when we search for MDS matrices.

To summarize the statements above, for a given $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ and parameter n, we present Algorithm 1 to search for the external matrices of MDS diffusion layers. It should be noted that we only need to check the external matrices where the entries are the residues modulo $g(x)$.

Experiments. We conducted several experiments using our approach and found a large amount of MDS matrices belonging to several types. In this letter, we briefly describe one of them. More details are given in the supplementary file.

We conducted the experiments with Magma V2.12-16 on a computer with an Intel Core i5-2400 @ 3.10 GHz CPU and DDR3, 4 GBytes, 665.1 MHz RAM. The operating system was 32-bit Windows 7 Professional.

Algorithm 1 Search for MDS diffusion matrices

```
Require: two integers $b, n \in \mathbb{Z}^+$, a matrix $A \in M_{b\times b}(\mathbb{F}_2)$ together with its minimal polynomial $m(x) \in \mathbb{F}_2[x]$, $m(x)$'s standard factorization $m(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s}$ in $\mathbb{F}_2[x]$, $g(x) = p_1(x)p_2(x)\cdots p_s(x)$.
Ensure: some polynomial matrices, an integer $k$.
 1: define an integer $k$ and $k \leftarrow 0$;
 2: $d := \deg(g)$;
 3: define a set $PS(d) := \{h(x) \in \mathbb{F}_2[x] \mid \deg(h) < d, \mathrm{GCD}(h(x), p_i(x)) = 1, \forall i = 1, \ldots, s\}$;
 4: define a matrix $L \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and $L \leftarrow O_n$;
 5: define an integer $r$ and $r \leftarrow 0$;
 6: define $f_i(x) \in \mathbb{F}_2[x]/\langle p_i(x)\rangle$ and $f_i(x) \leftarrow 0$, $i = 1, \ldots, s$;
 7: print "The $(n \times n)$-size external matrices of MDS diffusion matrices in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ are:";
 8: for $L \in \mathcal{M}_{n\times n}(PS(d))$ do
 9:     for $i = 1, \ldots, s$ do
10:         transform $L$ into $L_i \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]/\langle p_i(x)\rangle)$ by a ring homomorphism $\eta : \mathbb{F}_2[x] \to \mathbb{F}_2[x]/\langle p_i(x)\rangle$ such that $\eta(h(x)) = h(x) + \langle p_i(x)\rangle$;
11:         $r \leftarrow n$;
12:         while $r \geqslant 2$ do
13:             define a matrix $B \in \mathcal{M}_{r\times r}(\mathbb{F}_2[x]/\langle p_i(x)\rangle)$ and $B \leftarrow O_r$;
14:             for $B$ runs over all the $(r\times r)-$size submatrices of $L_i$ do
15:                 $f_i(x) \leftarrow \det(B)$;
16:                 if $f_i(x) = 0$ then
17:                     goto Step 34;
18:                 else
19:                     if $r \geqslant 3$ then
20:                         compute $B^{-1}$;
21:                         for $f_i(x)$ runs over all the entries of $B^{-1}$ do
22:                             if $f_i(x) = 0$ then
23:                                 goto Step 34;
24:                             end if
25:                         end for
26:                     end if
27:                 end if
28:             end for
29:             $r \leftarrow r - 2$;
30:         end while
31:     end for
32:     print $L$;
33:     $k \leftarrow k + 1$;
34:     switch to the next $L$;
35: end for
36: print "where $x = A$.";
37: print "There are $k$ MDS diffusion matrices.".
```

We selected the parameters $b = 8$, $n = 4$, and the internal block

$$A = \begin{pmatrix} 0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \end{pmatrix} \in \mathcal{M}_{8\times 8}(\mathbb{F}_2).$$

We aimed to definitely find recursive MDS block matrices under these conditions.

After running a series of Magma codes, we finally obtained at least $5820 \times 2^{16} \times (8!)$ recursive block MDS diffusion layers in 9.516 s.

Conclusion. In this letter, we proposed a new method for checking MDS property of block diffusion matrices where the blocks are all polynomials in a certain block. We also described a new type of operation that retains MDS property of diffusion matrices and generates many new MDS matrices from a given one. Moreover, we obtained an equivalence relation from this kind of operation. MDS property is invariant with respect to this equivalence relation, which can greatly reduce the amount of computational effort when searching for MDS matrices. We expect that our proposed method will be helpful for designing diffusion layers of block ciphers and hash functions.

Acknowledgements This study was supported by the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant Nos. XDA06010703 and XDA06010701), and the National Natural Science Foundation of China (Grant Nos. 61472416, 61272478, 61379139 and 61303255).

Supporting information The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Blaum M, Roth R M. On lowest density MDS codes. IEEE Trans Inf Theory, 1999, 45: 46–59

2 Gupta K C, Ray I G. On constructions of MDS matrices from companion matrices for lightweight cryptography. In: Proceedings of CD-ARES 2013 Workshops. Berlin: Springer-Verlag, 2013. 29–43

3 Junod P, Vaudenay S. Perfect diffusion primitive for block ciphers. In: Proceedings of International Workshop, SAC 2004. Berlin: Springer-Verlag, 2005. 84–99

4 Sajadieh M, Dakhilalian M, Mala H, et al. Recursive diffusion layers for block ciphers and hash functions. In: Proceedings of International Workshop, FSE 2012. Heidelberg: Springer-Verlag, 2012. 385–401

5 Wu S B, Wang M S, Wu W L. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: Proceedings of International Conference, SAC 2012. Heidelberg: Springer-Verlag, 2013. 355–371

6 Burrow M D. The minimal polynomial of a linear transformation. Amer Math Monthly, 1973, 80: 1129–1131