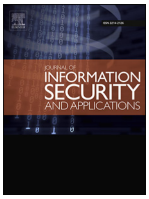
Journal of Information Security and Applications 38 (2018) 65–70

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa



Searching for perfect diffusion matrices with lightweight coefficients[☆]

Zhang Guoqiang, Zhang Wenying[*]

School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China

ARTICLE INFO

Article history:

Keywords:
Block cipher
MDS matrix
Circulant matrix
LFSRs
Lightweight coefficient
Hardware implementation

ABSTRACT

Diffusion layer is one of the main components of block ciphers and hash functions. MDS matrices are widely used to implement the diffusion layer. In this article, we first study the 4×4 MDS diffusion matrices constructed with linear feedback shift registers (LFSRs) of Fibonacci. For better hardware implementation, we focus on the low Hamming weight coefficients which are in the set $\{1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^3\}$ and there are not two identical elements in a row or column. In addition, we introduce a way to calculate the number of XORs. Then, we give the minimum of XORs required to implement a multiplication by a finite element x by using GF(2^8) defined by different irreducible polynomials and present some new lightweight coefficients that are lighter than the current known ones, such as the ones used in AES. These MDS matrices not only are lighter than AES diffusion matrix but also do not contain two identical elements in a row or column.

1. Introduction

Confusion and diffusion are two uppermost components of block ciphers and hash functions. The confusion layer is usually implemented by S-boxes which is a non-linear transformation. The diffusion layer is a linear transformation that can be implemented by multiplication by a matrix. The diffusion component has significant effect in resisting differential cryptanalysis (DC) [1], linear cryptanalysis(LC) [2] and other well-known attacks.

The security of resisting against DC and LC can be quantized by the branch number which was first proposed by Vaudenay [3,4] and named by Daemen [5].The larger the branch number is, the better the diffusion layer is. Maximum distance separable (MDS) diffusion layer is the most perfect diffusion layer with maximum branch numbers. Block ciphers like Advanced Encryption Standard (AES), Twofish [6], SQUARE [7], SHARK [8], CLEFIA [9] use MDS matrices as the core of their diffusion layers. MDS matrices also are widely used in the diffusion layer of many Hash functions like Maelstrom and PHOTON family of light weight hash functions.

MDS matrices can be constructed from Reed-Solomon code, random generating matrix and so on. However, these constructions are not usually efficient enough to implement. In the design of lightweight primitives PHOTON and LED, a strategy is put forward by Guo et al. to construct $s \times s$ MDS diffusion matrices with an s-stage linear feedback shift register (LFSR) over $F_{(2^n)}$. Wu et al. [10] further studied the MDS matrices with linear transformation with less number of XORs. The structure of linear diffusion layer proposed by Wu et al. seems to be more efficient in implementation among all of these constructions.

It is well known LFSRs have two fundamental architectures: Fibonacci and Galois structure. Xu et al. [11] presented a systematic analysis of 4 × 4 words diffusion layer constructed with those two structures. It is presented that it is not efficient enough to resist some well-known attacks if the diffusion matrix has identical element in a row or column.

The number of XORs can be used to measure the efficiency of hardware implementation. Thus, we can find hardware-optimal diffusion matrices by searching for lightweight coefficients.

This paper studied two problems. One is the conditions on f(x) to ensure M^4 been an MDS for the matrix M of LFSR of Fibonacci type. Another is the light coefficients for circulant matrices.

The rest of this paper is organized as follows. We first introduce some basic knowledge of diffusion layer in Section 2. Then some new 4 × 4 MDS diffusion matrices constructed by Fibonacci-LFSR are given in Section 3. Next we introduce a way to compute the number of XOR gates and calculate the minimum of XORs required to implement a multiplication by a finite field element x over $GF(2^8)$ defined by different irreducible polynomials and give the corresponding coefficient which is lighter than the AES matrix in Section 4. Finally, we give a short conclusion in Section 5.

[☆] This work is supported by the National Natural Science Foundation of China (no.61272434, 61672330, 61602287).

[*] Corresponding author.

E-mail addresses: 1073945816@qq.com (Z. Guoqiang), wenyingzh@sohu.com (Z. Wenying).

https://doi.org/10.1016/j.jisa.2017.11.009
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

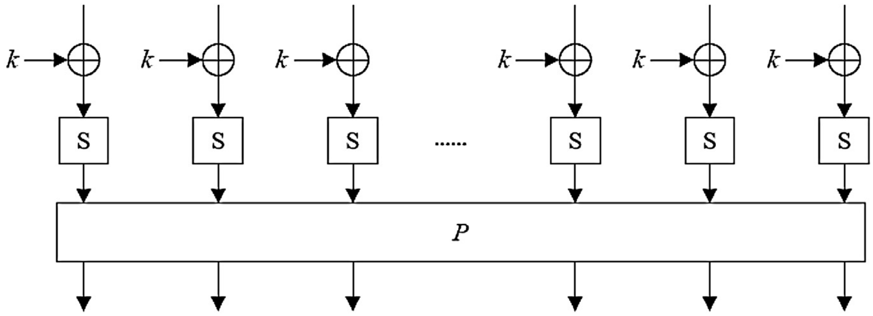


Fig. 1. One round SPN structure.

2. Basic knowledge of diffusion layer

SPN structure is widely used in block ciphers. One round SPN structure (see Fig. 1) contains three operations: Addroundkey, Substition and Permutation. Firstly, the input is divided into m b-bit blocks. Each block is XORred with a b-bit roundkey. Then, each block is transformed by an b-bit S-box. Finally, the permutation operation is implemented by linear transformation.

Substition usually called confusion layer Plays a role of confusion. Permutation usually called diffusion layer Plays a role of diffusion.

2.1. Design principles of diffusion layer

The diffusion layer is usually implemented by linear transformation $\theta:(F_2^m)^n \rightarrow (F_2^m)^n$. The diffusion properties of diffusion layer can be measured by the branch number. The diffusion layer is called maximum distance separable (MDS) diffusion layer if and only if the linear transformation reached the maximum branch numbers. MDS diffusion layers are also called perfect diffusion layers.

Let x be an array of s n-bit elements $x = [x_0, x_1, \ldots, x_{(s-1)}]$, where x_i can be seen as an n-bit integer over the vector space F_2^n or the finite field $F_{(2^n)}$.

For a diffusion layer, we have the following definition:

Definition 1 [12]. The branch number of a linear diffusion layer θ is defined as

$$B(\theta) = \min_{x \neq 0}(\omega_b(x) + \omega_b(\theta(x)))$$

where θ can be represented as a linear transformation of $F_{(2^n)}$ and $\omega_b(x)$ denotes the number of non-zero elements in x.

Proposition 1 *[12]. For a diffusion layer acting on s-word inputs, the maximal branch number is s+1, known as the singleton bound.*

Definition 2 [13]. Let F be a finite field, and p and q be two integers. Let $x \rightarrow M \times x$ be a mapping from F_p to F_q defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs (x, $M \times x$) is an MDS code, that is, a linear code of dimension p, length p + q and minimal distance q + 1.

Proposition 2 *[13]. An [m, s, d] code C with generator matrix $G = [I|A]$, where A is an $s \times (m - s)$ matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i = 1, 2, \ldots, \min\{s, m - s\}$) of A is non-degenerate.*

The MDS matrix used in a diffusion layer is usually a square matrix. A square matrix is non-degenerate if and only if its determinant is non-zero.

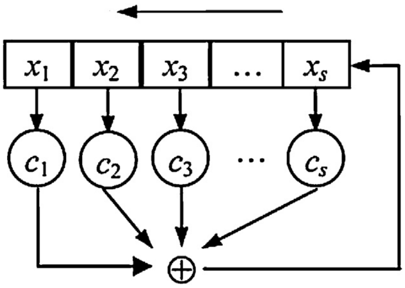


Fig. 2. Fibonacci-LFSR.

2.2. LFSRs with Fibonacci structure

It is well known LFSRs have two elementary structures: Fibonacci and Galois structure. We just do a simple introduction about Fibonacci structure. For an s-stage LFSR over $F_{(2^n)}$ with Fibonacci structure (see Fig. 2), in each step, only the last register is updated by a linear combination of all of the registers while other registers are obtained by shifting the state vector by one position to the left. That is, the state transition matrix of the LFSR can be given as

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_1 & c_2 & c_3 & \cdots & c_s \end{pmatrix} \tag{1}$$

where $c_i \in F_{(2^n)}$. For simplicity, we usually use the final row to represent the state transition matrix A, that is, $A^{(s)} = [c_1, c_2, \cdots, c_s]_{Fibonacci}$.

2.3. MDS matrices from LFSRs

Let M be the state transition matrix of a LFSR, then the d-step state transition matrix is M^d. If M^d is an MDS matrix, then we can obtain an MDS matrix over $F_{(2^n)}$ in this way. It is known that no better constructions can be obtained with $d \neq s$, so we only consider the case when $d \doteq s$.

For the MDS matrices constructed by Fibonacci-LFSRs, Guo et al. presented some examples of 4×4 MDS diffusion matrices M^4 constructed from LFSRs with the state transition matrix $M \doteq [1, \alpha, 1, \alpha^2]_{Fibonacci}$ or $[\alpha^2, 1, \alpha, \alpha]_{Fibonacci}$.

It is presented in [14] that it is not efficient enough to resist some well-known attacks if the diffusion matrix has the same element in a row or column.