International Journal of Information & Network Security (IJINS)
Vol.2, No.4, August 2013, pp. 327~332
ISSN: 2089-3299

Optimum Dynamic Diffusion of Block Cipher Based on Maximum Distance Separable Matrices

Adham M. Elhosary *, Nabil Hamdy **, Ismail Abdel-Ghafar Farag †, Alaa Eldin Rohiem‡
* Departement of Communications, Military Technical College
** Misr International University
† Arab Academy for Science and Technology and Maritime Transport(AASTMT).
‡ Technical Research Center of the Armed Forces.

Article Info

Article history:

Received Jul 3rd, 2013
Revised Jul 15th, 2013
Accepted Aug 18th, 2013

Keyword:

Maximum Distance Separable
Optimal Diffusion
Branch Number
Involutory MDS
Punctured MDS

ABSTRACT

Maximum Distance Separable matrices became the state of the art as a diffusion component in block cipher design for example those MDS matrices used in algorithms such as AES and Twofish. This paper firstly reviews the relation between coding theory and cryptography in the context of providing optimal diffusion. Secondly, The Vandermonde and Cauchy based methodologies introduced by Mahdi Sajadieh et al. and J. Nakahara respectively for generating Involutory MDS matrices that are proposed to provide full block diffusion in order to decrease number of rounds of a block cipher were assessed. Finally Punctured MDS matrices are proposed to provide dynamicity of a block cipher, which guaranteed to provide optimum diffusion that should be considered in security proof against Linear and Differential Cryptanalysis of a block cipher.

Corresponding Author:

Adham M. Elhosary,
Departement of Communications,
Military Technical College, Egypt.
Email: adhosary@gmail.com

1. INTRODUCTION

In any block cipher there exist permutation components, which act as a confusion component on each input of the round function of a block cipher. These permutation components was usually presented as just an indexing matrix that was implemented as either a permutation matrix like the one used in DES [1] block cipher algorithm which was chosen with certain pattern, or as a displacement function like that one which was used in GOST [2] algorithm. Coding theory played an important role in that manor in a way that made a dramatic way turning point. Since Rijndael [3] , and its predecessor SHARK [4] block ciphers, which introduced the usage of Maximum Distance Separable (MDS) matrices that provide both permutation and diffusion simultaneously. This paper is organized in such a way that first a review on Diffusion of Block Cipher is introduced including the relation between coding theory and cryptography in term of branch number and Maximum Distance Separable matrices. Then comes a study and assessment of some methodologies for generating MDS and Hadamard Involutory MDS matrices are presented. Finally we introduce our proposal to achieve dynamicity using the proposed constructed MDS matrices to be used in block cipher design.

2. Diffusion of Block Cipher

Shannon [5] identified two properties of a perfect block cipher design, the first is confusion which refers to making the relationship between plaintext and key as complex as possible. Diffusion is the second property which refers to making the statistical relationship between plaintext and ciphertext as complex as

possible, in other words the redundancy of the plaintext should be spread and dissipated among each bit in the ciphertext, which we achieved by using highly nonlinear S-Boxes, and MDS matrices.

However, diffusion is just a concept. In order to measure diffusion, a metric was introduced that is called Branch number which is the sum of the input and output active bytes (nonzero difference in input/output blocks). The wide trail strategy provides a simplified technique to maximize the sum of the active bytes (trail of active bytes) over a few rounds. The lower bound on the sum of active bytes also provides a lower bound on the resistance offered by the cipher to many cryptanalytic attacks.

The wide trail strategy introduced by Rijmen [6] is based partially on the substitution permutation network, where the entire input block is transformed in every round. Although this approach makes each round of heavier computations compared to the Feistel structure, it helps in decreasing the number of rounds required for encryption. Block ciphers like Rijndael [3], Square [7] and Shark [4] are based on this strategy.

Most cryptanalytic attacks make use of the imbalances in the mappings between the differences/correlation in the ciphertext to a particular difference/correlation in the plaintext or the round key. The wide trail strategy aims to spread the difference/correlation characteristics to the entire cipher state in a few rounds. This approach would prevent the cryptanalytic attacks that rely on the propagation of difference/correlation characteristics within sub-blocks of the input block. The spreading strength of the diffusion layer of a cipher is the key to achieve the wide trail strategy.

2.1. MAXIMUM DISTANCE SEPARABLE LINEAR CODES

A linear $[n, k]$-code C is a subspace of GF(2^n) of dimension k and represented by $k \times n$ matrix, where rows of it are linearly independent, which is called a Generating matrix. A Generating matrix is equivalent to a matrix of the form $[I_{k\times k}|P]$, where $I_{k\times k}$ is a $k \times k$ identity matrix, and P is a $k \times (n-k)$ matrix. The form $[I_{k\times k}|P]$ of a matrix is called the standard (or systematic) form of a Generating matrix [8]. The Hamming weight of a code word $c \in C$ is the number of nonzero components in c and denoted by $\mathcal{W}_H(c)$. The distance $d(C)$ of a linear code C is defined by

$$\begin{aligned} d(C) &= \min\{\mathcal{W}_H(c) \mid c \in C, c \neq 0\} \\ &= \min\{\mathcal{W}_H(c'|c'P) \mid c' \in GF(2^n), c' \neq 0\} \\ &= \min\{\mathcal{W}_H(c') + \mathcal{W}_H(c'P) \mid c' \in GF(2^n), c' \neq 0\} \end{aligned}$$

A linear [n, k, d]-code C represents a linear [n, k]-code whose distance is d. Equivalently the distance between any two code words c and c' in C is at least equals to d. If the minimum distance d reaches its maximum possible value which is called singleton bound (i.e. $d = n - k + 1$), the linear [n, k, d]-code C is said to be Maximum Distance Separable code. A Generating matrix is an MDS matrix if and only if all its possible square sub-matrices are non-singular (invertible) [9].

2.2. BRANCH NUMBER

The branch number of a permutation function is representing the diffusion rate and measures security against differential and linear cryptanalysis [10]. A diffusion layer in GF(2^n) over m-number of elements [11] is a linear transformation (A) noted by as follows $A(x) = (\{0,1\}^n)^m \longrightarrow (\{0,1\}^n)^m$:

$$A(x) = A.x^T = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

Where $x = (x_1, x_2, \ldots, x_m)^T$, $x_i \in \{0, 1\}^n$, $i = 1, \ldots, m$.

The Branch Number $\mathcal{B}$ of an $m \times m$ matrix A is defined by :

$$\mathcal{B}(A) = \min\{\mathcal{W}_H(x) + \mathcal{W}_H(A.x^T) \mid x \neq 0\}$$

Practically Branch Number $\mathcal{B}$ is the number of active S-Boxes in two successive rounds of an encryption algorithm, in case of using bijective S-Boxes over GF(2^n) [6]. MDS codes can be used for determining the maximum branch number of matrices in $GF(2^8)^{n\times n}$ and for finding a matrix with maximum branch number of any given finite field of any given dimension.

Theorem: Let C be an MDS $[2n, n, d]$-code over GF(2^8) and $[I_{n\times n}|P]$ be its standard form. Then,

$$d(C) = \mathcal{B}(P^T)$$

Proof: the proof can be derived from the definition above as follows:

$$\begin{aligned} n+1 &= d(C) \\ &= \min_{c' \in GF(2^8)^n, c' \neq 0} (\mathcal{W}_H(c') + \mathcal{W}_H(c'P)) \\ &= \mathcal{B}(P^T) \end{aligned}$$

Many constructions of MDS matrices over finite fields have been introduced in Coding Theory literature. Among them we find Reed Solomon MDS matrix construction which was used in Rijndael (AES) design. Reed Solomon is a Cyclic Linear Block Code, where any valid codeword is a cyclic shift of one another valid codeword. The Generator matrix of Reed Solomon code used in AES Mix Column (*MC*) is formed [8, 4, 5]-code over $GF(2^8)$ as follows

$$MC_{AES} = \begin{bmatrix} 02_x & 03_x & 01_x & 01_x \\ 01_x & 02_x & 03_x & 01_x \\ 01_x & 01_x & 02_x & 03_x \\ 03_x & 01_x & 01_x & 02_x \end{bmatrix}$$

2.3. VANDERMONDE BASED MDS MATRICES

A Vandermonde matrix $A = van_d(a_0, a_1, \cdots, a_{m-1})$ is an $m \times d$ matrix built from $a_0, a_1, \cdots, a_{m-1}$ as follows:

$$A = van_d(a_0, a_1, \cdots, a_{m-1}) = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{d-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{d-1} \\ \vdots & & \ddots & & \\ 1 & a_{m-1} & a_{m-1}^2 & \cdots & a_{m-1}^{d-1} \end{bmatrix}$$

The Vandermonde matrix of interest is a square matrix whose all elements are different (i.e. $i \neq j \; implies \; a_i \neq a_j$).

An MDS matrix can be constructed using two Vandermonde matrices $A = van_d(a_0, a_1, \cdots, a_{m-1})$ and $B = van_d(b_0, b_1, \cdots, b_{m-1})$ with different elements ($a_i \neq b_j$), then the matrix BA^{-1} is an MDS matrix [12] [9].

Example: for *m=3*, the Vandermonde matrix $A = van(01_x, 03_x, 7E_x)$, the finite field modulo polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, and Vandermonde matrix *B* such that ($a_i - b_i = EF_x$), so we have MDS matrix

$$BA^{-1} = \begin{bmatrix} 02_x & 07_x & 04_x \\ 03_x & 06_x & 04_x \\ 03_x & 07_x & 05_x \end{bmatrix}$$

2.4. HADAMARD INVOLUTORY MDS MATRICES

In General a function *f* is an Involutory function if *f* (*f* (*x*)) = *x*. Specifically, an Involutory matrix $M_{m \times m}$ is a matrix satisfying the property of $\boldsymbol{M^2_{m \times m} = I_{m \times m}}$. More MDS matrices constructions such as Cauchy based MDS matrices, and Vandermonde based MDS matrices have been introduced in literature. The later construction is of much interest because upon which an Involutory MDS matrix is proposed by Mahdi Sajadieh et al. [13]. They constructed an Involutory MDS matrix has been easily introduced by, which is very useful in fact in the sake of memory space instead of having two matrices one for encryption and its inverse in decryption, moreover it can be used to provide full block diffusion as stuied by J. Nakahara [14]. Rather than that J. Nakahara proposal of the Cauchy based Involutory MDS matrix have been practically proved to be non-MDS, as we found singular (non-invertible) square sub-matrices in it, which contradicts the MDS necessary condition, and the claim of Nakahara as follows.

$$M_{16\times16} = \begin{bmatrix}
01_x & 03_x & 04_x & 05_x & 06_x & 07_x & 08_x & 09_x & 0a_x & 0b_x & 0c_x & 0d_x & 0e_x & 10_x & 02_x & 1e_x \\
03_x & 01_x & 05_x & 04_x & 07_x & 06_x & 09_x & 08_x & 0b_x & 0a_x & 0d_x & 0c_x & 10_x & 0e_x & 1e_x & 02_x \\
04_x & 05_x & 01_x & 03_x & 08_x & 09_x & 06_x & 07_x & 0c_x & 0d_x & 0a_x & 0b_x & 02_x & 1e_x & 0e_x & 10_x \\
05_x & 04_x & 03_x & 01_x & 09_x & 08_x & 07_x & 06_x & 0d_x & 0c_x & 0b_x & 0a_x & 1e_x & 02_x & 10_x & 0e_x \\
06_x & 07_x & 08_x & 09_x & 01_x & 03_x & 04_x & 05_x & 0e_x & 10_x & 02_x & 1e_x & 0a_x & 0b_x & 0c_x & 0d_x \\
07_x & 06_x & 09_x & 08_x & 03_x & 01_x & 05_x & 04_x & 10_x & 0e_x & 1e_x & 02_x & 0b_x & 0a_x & 0d_x & 0c_x \\
08_x & 09_x & 06_x & 07_x & 04_x & 05_x & 01_x & 03_x & 02_x & 1e_x & 0e_x & 10_x & 0c_x & 0d_x & 0a_x & 0b_x \\
09_x & 08_x & 07_x & 06_x & 05_x & 04_x & 03_x & 01_x & 1e_x & 02_x & 10_x & 0e_x & 0d_x & 0c_x & 0b_x & 0a_x \\
0a_x & 0b_x & 0c_x & 0d_x & 0e_x & 10_x & 02_x & 1e_x & 01_x & 03_x & 04_x & 05_x & 06_x & 07_x & 08_x & 09_x \\
0b_x & 0a_x & 0d_x & 0c_x & 10_x & 0e_x & 1e_x & 02_x & 03_x & 01_x & 05_x & 04_x & 07_x & 06_x & 09_x & 08_x \\
0c_x & 0d_x & 0a_x & 0b_x & 02_x & 1e_x & 0e_x & 10_x & 04_x & 05_x & 01_x & 03_x & 08_x & 09_x & 06_x & 07_x \\
0d_x & 0c_x & 0b_x & 0a_x & 1e_x & 02_x & 10_x & 0e_x & 05_x & 04_x & 03_x & 01_x & 09_x & 08_x & 07_x & 06_x \\
0e_x & 10_x & 02_x & 1e_x & 0a_x & 0b_x & 0c_x & 0d_x & 06_x & 07_x & 08_x & 09_x & 01_x & 03_x & 04_x & 05_x \\
10_x & 0e_x & 1e_x & 02_x & 0b_x & 0a_x & 0d_x & 0c_x & 07_x & 06_x & 09_x & 08_x & 03_x & 01_x & 05_x & 04_x \\
02_x & 1e_x & 0e_x & 10_x & 0c_x & 0d_x & 0a_x & 0b_x & 08_x & 09_x & 06_x & 07_x & 04_x & 05_x & 01_x & 03_x \\
1e_x & 02_x & 10_x & 0e_x & 0d_x & 0c_x & 0b_x & 0a_x & 09_x & 08_x & 07_x & 06_x & 05_x & 04_x & 03_x & 01_x
\end{bmatrix}$$

Obviously we see In J. Nakahara's matrix $\boldsymbol{M_{16\times16}}$ those matrices which were singular as proven as follows:

$$\text{for } Martix\ A = \begin{bmatrix} 03_x & 05_x \\ 07_x & 09_x \end{bmatrix};$$

$$|A| = \begin{vmatrix} 03_x & 05_x \\ 07_x & 09_x \end{vmatrix} = (03_x \times 09_x) - (05_x \times 07_x)$$

In $\mathrm{GF}(2^8)$

$$03_x = x + 1, \text{ and } 05_x = x^2 + 1, \text{ and } 07_x = x^2 + x + 1, \text{ and } 09_x = x^3 + 1$$

$$\therefore (03_x \times 09_x) = (x + 1) \times (x^3 + 1) = x^4 + x^3 + x + 1$$

$$\text{and, } \therefore (05_x \times 07_x) = (x^2 + 1) \times (x^2 + x + 1) = x^4 + x^3 + x + 1$$

$$\Rightarrow |A| = \begin{vmatrix} 03_x & 05_x \\ 07_x & 09_x \end{vmatrix} = 0$$

That's to mean *A* is singular (non-invertible) matrix.

Mahdi Sajadieh et al. introduced a successful construction of Hadamard Involutory MDS matrix based on Vandermonde matrices [13].

The construction states that, if *A* and *B* are two invertible Vandermonde matrices in the finite field $GF(2^q)$ satisfying the two properties $a_i = b_i + \Delta$, and $a_i \neq b_j, i, j \in \{0, 1, \cdots, m-1\}$, then BA^{-1} is an Involutory MDS matrix. An Involutory MDS matrix is quite sufficient for a cipher in sake for using one matrix in both ways encryption and decryption, but more optimization can be achieved by using Hadamard Involutory Matrix that only contains 2^n elements.

A matrix *H* is Finite Field Hadamard (FFHadamard) [13] matrix in $GF(2^q)$ if its dimension is in the form $2^n \times 2^n$, and represented as follows:

$$H = \begin{bmatrix} U & V \\ V & U \end{bmatrix}, \quad \text{Where the two sub-matrices } U \text{ and } V \text{ are FFHadamard.}$$

Mahdi Sajadieh et al. Construction mentioned that by choosing certain elements in constructing the fundamental $2^n \times 2^n$ Vandermonde matrices *A* and *B*, the resulting $2^n \times 2^n$ matrix BA^{-1} is FFHadamard Involutory Matrix, which have been practically verified. The conditions are simply

$$a_i + b_i = a_0 + b_0 = \Delta, \quad \text{Where } \Delta \neq 0, and\ \Delta \in \mathrm{GF}(2^q), \text{ and}$$

$$a_i + b_j = a_l + b_{l \oplus i \oplus j}\text{ , For all } i, j, l \in \{0,1, \cdots, 2^n - 1\}.$$

Vandermonde based FFHadamard Involutory MDS matrices have been successfully constructed and tested that may be used instead of Nakahara's Matrix to provide a full block diffusion, which he proved to minimize number of rounds to only 5 rounds of the AES algorithm

$$F = \begin{bmatrix} 23_x & 46_x & 71_x & 2C_x & 95_x & 1E_x & AB_x & 5A_x & 87_x & 04_x & 48_x & 9E_x & 0E_x & 0D_x & 0A_x & 1F_x \\ 46_x & 23_x & 2C_x & 71_x & 1E_x & 95_x & 5A_x & AB_x & 04_x & 87_x & 9E_x & 48_x & 0D_x & 0E_x & 1F_x & 0A_x \\ 71_x & 2C_x & 23_x & 46_x & AB_x & 5A_x & 95_x & 1E_x & 48_x & 9E_x & 87_x & 04_x & 0A_x & 1F_x & 0E_x & 0D_x \\ 2C_x & 71_x & 46_x & 23_x & 5A_x & AB_x & 1E_x & 95_x & 9E_x & 48_x & 04_x & 87_x & 1F_x & 0A_x & 0D_x & 0E_x \\ 95_x & 1E_x & AB_x & 5A_x & 23_x & 46_x & 71_x & 2C_x & 0E_x & 0D_x & 0A_x & 1F_x & 87_x & 04_x & 48_x & 9E_x \\ 1E_x & 95_x & 5A_x & AB_x & 46_x & 23_x & 2C_x & 71_x & 0D_x & 0E_x & 1F_x & 0A_x & 04_x & 87_x & 9E_x & 48_x \\ AB_x & 5A_x & 95_x & 1E_x & 71_x & 2C_x & 23_x & 46_x & 0A_x & 1F_x & 0E_x & 0D_x & 48_x & 9E_x & 87_x & 04_x \\ 5A_x & AB_x & 1E_x & 95_x & 2C_x & 71_x & 46_x & 23_x & 1F_x & 0A_x & 0D_x & 0E_x & 9E_x & 48_x & 04_x & 87_x \\ 87_x & 04_x & 48_x & 9E_x & 0E_x & 0D_x & 0A_x & 1F_x & 23_x & 46_x & 71_x & 2C_x & 95_x & 1E_x & AB_x & 5A_x \\ 04_x & 87_x & 9E_x & 48_x & 0D_x & 0E_x & 1F_x & 0A_x & 46_x & 23_x & 2C_x & 71_x & 1E_x & 95_x & 5A_x & AB_x \\ 48_x & 9E_x & 87_x & 04_x & 0A_x & 1F_x & 0E_x & 0D_x & 71_x & 2C_x & 23_x & 46_x & AB_x & 5A_x & 95_x & 1E_x \\ 9E_x & 48_x & 04_x & 87_x & 1F_x & 0A_x & 0D_x & 0E_x & 2C_x & 71_x & 46_x & 23_x & 5A_x & AB_x & 1E_x & 95_x \\ 0E_x & 0D_x & 0A_x & 1F_x & 87_x & 04_x & 48_x & 9E_x & 95_x & 1E_x & AB_x & 5A_x & 23_x & 46_x & 71_x & 2C_x \\ 0D_x & 0E_x & 1F_x & 0A_x & 04_x & 87_x & 9E_x & 48_x & 1E_x & 95_x & 5A_x & AB_x & 46_x & 23_x & 2C_x & 71_x \\ 0A_x & 1F_x & 0E_x & 0D_x & 48_x & 9E_x & 87_x & 04_x & AB_x & 5A_x & 95_x & 1E_x & 71_x & 2C_x & 23_x & 46_x \\ 1F_x & 0A_x & 0D_x & 0E_x & 9E_x & 48_x & 04_x & 87_x & 5A_x & AB_x & 1E_x & 95_x & 2C_x & 71_x & 46_x & 23_x \end{bmatrix}$$

3. DYNAMIC DIFFUSION

Punctured MDS code is also an MDS code. Puncturing is done by removing any row/column from the MDS generating matrix, accordingly the resulting matrix is yet another valid MDS matrix that satisfy the necessary condition of having all square sub-matrices non-singular (invertible), as shown below.

$$B_{5\times5} = \begin{bmatrix} 01_x & 7A_x & E0_x & DB_x & AA_x \\ 01_x & 45_x & DC_x & 92_x & 93_x \\ 01_x & B0_x & 7A_x & C3_x & E0_x \\ 01_x & 1F_x & 48_x & 6B_x & 8D_x \\ 01_x & F3_x & B2_x & 57_x & 7E_x \end{bmatrix}, \quad A_{5\times5} = \begin{bmatrix} 01_x & D8_x & 83_x & 7D_x & 16_x \\ 01_x & E7_x & BF_x & 7D_x & 2F_x \\ 01_x & 12_x & 19_x & BF_x & 5C_x \\ 01_x & BD_x & 2B_x & 65_x & 31_x \\ 01_x & 51_x & D1_x & 3E_x & C2_x \end{bmatrix}$$

$$A^{-1}{}_{5\times5} = \begin{bmatrix} 8B_x & 18_x & 55_x & 0E_x & C9_x \\ D6_x & B1_x & 4F_x & 1C_x & 34_x \\ 2A_x & 2C_x & DA_x & A4_x & 78_x \\ A1_x & 4C_x & B6_x & B9_x & E2_x \\ 33_x & 02_x & E8_x & 1C_x & C5_x \end{bmatrix}, \quad BA^{-1}{}_{5\times5} = \begin{bmatrix} DF_x & 54_x & 78_x & 02_x & F0_x \\ 31_x & A9_x & 91_x & 7B_x & 73_x \\ 53_x & 01_x & E9_x & 30_x & 8A_x \\ 78_x & B2_x & F3_x & DE_x & E6_x \\ 8E_x & D4_x & 13_x & 08_x & 40_x \end{bmatrix}$$

$\Longrightarrow$we arbitrarily choose any element

$$M_{5\times5} = \begin{bmatrix} DF_x & 54_x & 78_x & 02_x & F0_x \\ 31_x & A9_x & \boxed{91}_x & 7B_x & 73_x \\ 53_x & 01_x & E9_x & 30_x & 8A_x \\ 78_x & B2_x & F3_x & DE_x & E6_x \\ 8E_x & D4_x & 13_x & 08_x & 40_x \end{bmatrix}, \quad M'{}_{5\times5} = \begin{bmatrix} DF_x & 54_x & 02_x & F0_x \\ 53_x & 01_x & 30_x & 8A_x \\ 78_x & B2_x & DE_x & E6_x \\ 8E_x & D4_x & 08_x & 40_x \end{bmatrix}$$

When we eliminate its row and column, the resulting matrix is another MDS matrix

Corollary: If we have an MDS matrix $M_{m\times n}$, hence we can obtain $m \times n$ MDS matrices $M'_{m-1\times n-1}$ by omitting (puncturing) a row and a column indexed by each element in the original matrix at a time.

Accordingly we can manage to use these kinds of matrices for providing optimum diffusion and dynamicity simultaneously in any block cipher construction that use Static MDS matrices such as AES and Twofish.

4. CONCLUSION

This paper presented and practically validated Vandermonde based methodology of generating MDS matrices, Involutory MDS, and Hadamard Involutory MDS matrices that we suggest to be used in constructing diffusion components of block cipher algorithms. These matrices guarantee to provide optimum diffusion that should be considered in security proof against Linear and Differential Cryptanalysis of a block cipher. Moreover; We validated the success of Vandermonde based methodology that is proposed by Sajadieh [13] of generating Finite Field Hadamard Involutory MDS matrices, we agree with it in providing full block diffusion in order to decrease number of rounds of a block cipher, and on the contrary we proved the failure of Nakahara's [14] proposal of his Finite Field Hadamard Involutory MDS. We also contributed in proposing the puncturing method of MDS matrices in order to provide dynamicity of block cipher, pertaining optimum diffusion that should be considered in security proof against Linear and Differential Cryptanalysis of a block cipher.

REFERENCES

[1] Data Encryption Standard (DES). In : Fedral Information Processing Standard Publication 46. (1977)

[2] I. A. Zabotin, G.: GOST. In : Cryptographic Protection for Information Processing Systems. Government Committee of the USSR for Standards, 1989 In Russian, translated to English by Aleksandr Malchik with an EnglishPreface co-written with Whitfield Diffie, can be found at http://www.autochthonous.org/crypto/gosthash.tar.gz.

[3] Joan Daemen, Vincent Rijmen: The Block Cipher Rijndael. In : Smart Card Research and Applications, Lecture Notes in Computer Science vol. 1820. Springer Berlin / Heidelberg (2000) pp. 277-284

[4] Vincent Rijmen, J.: The Cipher SHARK. In : 3rd International Workshop on Fast Software Encryption. Cambridge: Springer-Verlag (1996) pp. 99–111

[5] Shannon, C. E.: Communication Theory of Secrecy System. In : Bell System Technical Journal 28. (1949) pp. 656-715

[6] Rijmen, J.: The wide trail design strategy. In : Proceedings of the 8th IMA International Conference on Cryptography and Coding. Springer-Verlag, London (2001) pp. 222–238

[7] Joan Daemen, L.: The Block Cipher Square. In : Lecture Notes in Computer Science - Fast Software Encryption (FSE) 1267. Springer-Verlag (1997) pp. 149–165

[8] Sloane, F.: The Theory of Error-Correcting Codes North-Holland Mathematical Library edn. 16. North-Holland Publishing Co., Amsterdam (1977)

[9] Jérôme Lacan, Jérôme Fimes: A Construction of Matrices with No Singular Square Submatrices. In : Finite Fields and Applications, Lecture Notes in Computer Science vol. 2948. Springer Berlin / Heidelberg (2004) pp. 145-147

[10] Daemen, J.: Cipher and Hash Function Design Strategies based on Linear and Differential Cryptanalysis. In : PhD thesis, K.U.Leuven. (1995)

[11] Rudolf Lidl, Harald Niederreiter: Finite Fields, Encyclopedia of Mathematics and its Applications (20) 2nd edn. Cambridge University Press (June 2008)

[12] J. Lacan, J.: Systematic MDS Erasure Codes Based on Vandermonde Matrices. In : IEEE Transactions Communications Letters 8. (2004) pp. 570- 572

[13] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, Behnaz Omoomi: On construction of involutory MDS matrices from Vandermonde Matrices inGF(2^q). Designs, Codes and Cryptography vol. 64(3), pp. 287-308 (2012-09-01)

[14] Nakahara, J., Abrahão, É.: A New Involutory MDS Matrix for the AES. In : International Journal of Network Security 9. (2009) pp. 109-116