Construction of MDS-matrix for linear transformation of symmetric block ciphers

Victor Ruzhentsev, Roman Oliynykov, Valeriy Stupak

Abstract – **The analysis of existing requirements for MDS matrices that are used in block ciphers is performed, the most important requirements are selected, and matrix corresponding to the selected requirements is constructed.**

Keywords – **symmetric block cipher, linear transformation, MDS-matrix.**

I. INTRODUCTION[1]

All modern block symmetric ciphers (BSC) are constructed according to classical principles of Shannon [1] and consist of linear transformations, which provide the diffusion, and nonlinear transformations, which provide confusion. The transformations on the basis of maximal distance separable codes (MDS-codes) are one of the most popular type of linear transformations. The main advantage of such linear transformations is the guaranteed level of dispersion for BSC. In other words, use of linear transformation on basis of MDS-codes guarantees enough large number of active S-boxes in the context of differential or linear cryptanalysis.

The objective of this work is a description and justification of our approach to the construction of MDS matrix over GF(2^8), which was used in the construction of a linear transformation in the cipher "Kalina".

II. ANALYSIS OF REQUIREMENTS TO MDS MATRICES

There are two basic requirements to MDS matrices of modern ciphers: the maximum distance properties and the effectiveness of implementation.

The first requirement is the **maximum distance separable (MDS) properties**. In accordance with Lemma 2 [2], if every square submatrix is nonsingular (its determinant is not equal to 0), then it is a necessary and sufficient condition to ensure that the matrix is MDS. Two approaches for the construction of MDS matrices are considered in [2]. The first approach is to construct a random matrix and then check necessary and sufficient condition. Second approach is to use an algebraic construction of the matrix, which is guaranteed to have the MDS property. During the computational experiments it was found that for matrices of size 10×10 bytes over GF(2^8) checks of necessary and sufficient conditions takes not long time, so it is possible to build such a matrix using the first approach. For large size of matrix, obviously, it should be used the second approach. The size of Kalina's matrix is 8×8 bytes, so it was decided to use the first approach.

The second requirement is **the effectiveness of the implementation of the multiplication of a byte vector on MDS matrix**. In accordance with this requirement MDS matrices are usually cyclical, that is, each row of the matrix is the previous row cyclically shifted by 1 byte. This structure of the matrix allows saving memory required to implementation of matrix multiplication.

Additional requirements associated with effective implementation, is to minimize the coefficients that are present in the direct and inverse matrix. The lower coefficients allows to minimize resources required to implement the transformation on 8-bit processors.

III. COMPUTATIONAL EXPERIMENTS

It was experimentally found out lower bounds for the coefficients of the cyclic MDS matrix with size 8×8 bytes over GF (2^8) with forming polynomial 0x11d. The results are presented in Table 1.

TABLE 1
LOWER BOUND FOR THE COEFFICIENTS OF DIRECT AND INVERSE MATRICES

		Example (the first row of a cyclic matrix)
The minimum number of significant bits in the direct coefficients	4	1 1 4 7 6 8 1 5
The minimum value of the maximum coefficient	8	
The minimum number of significant bits in the maximum inverse coefficient with 4 significant bits in the direct coefficients	6	Direct matrix: 1 1 6 1 9 C D E Inverse matrix: E 17 25 2B A 12 22 2C

The matrix with minimum value of the maximum direct coefficient was selected for the cipher "Kalina".

IV. CONCLUSION

The analysis of the existing requirements for MDS matrices was performed, the most essential requirements were selected, and in accordance with these requirements the MDS matrix for BSC "Kalina" was constructed.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949.
[2] A.M. Youssef, S.Mister, S.E.Tavares, On the design of linear transformations for substitution permutation encryption networks, available from http://citeseerx.ist.psu.edu/viewdoc/download.

Victor Ruzhentsev – Institute of Information Technologies, Kharkiv, Bakulina str. 12, 61166, Ukraine; e-mail: vityazik@rambler.ru