UDC 621.3.16

M. YU. RODINKO, K. E. LISITSKIY

THE WIDE TRAIL STRATEGY WITHOUT SEPARABLE CODES

1. Introduction

J. Daemen and V. Rijmen are considered as discoverers of the wide trail strategy [1]. However, in our opinion, the origins of this strategy actually can be seen in Feistel's work [2]. The SPN structure, which was proposed in this work, has presupposed that S-boxes of nonlinear layer have been included so that to activate as much as possible number of S-boxes of the next cycle by their outputs (though in this case activation was implemented at the bit layer). The merit of J. Daemen and V. Rijmen is seen in the fact that they were able to show that separable codes with the maximum minimum distance (specified by MDS matrix) provide a way of building the optimal linear transformations with branch number $n + 1$, where n – number of ligaments (the number of S-boxes which entered to MDS transformation). Today the linear transformation constructed using multiplication by MDS matrix is considered optimal [1].

The J. Daemen's idea, natural in the context of differential and linear cryptanalysis, was to analyze a round function piece by piece: the S-box transformation and the linear transformation – separately, to ensure that cryptanalysis attack can't "bypass" nonlinear aspects of the algorithm [3]. AES's developers actually managed to offer the design of cyclic transformation amenable to clear analysis.

2. Implementation of the wide trail strategy in Rijndael

We recall here the implementation of the wide trail strategy on the example of SL transformation used in Muhomor cipher [4,5]. It is represented in Fig. 1. A similar transformation is used in Rijndael, but it hasn't got a special name there.

The input 32-bit value is divided into 4 bytes, each of which is substituted according to the given S-box. There are four different tables, one for each byte, used in transformation of Muhomor cipher (one S-box is used in Rijndael).

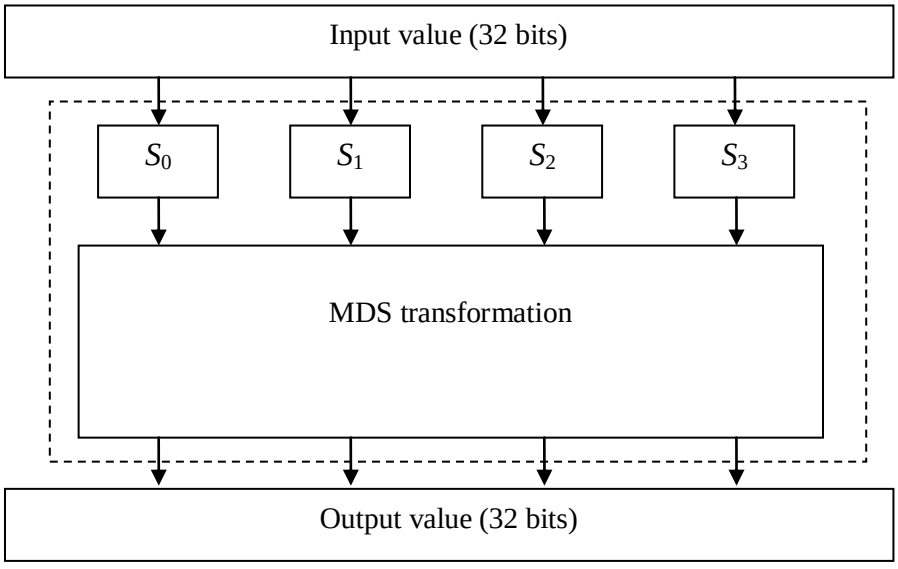

Fig. 1. SL transformation of Muhomor cipher

After substitution operation in S-boxes 4 bytes (a_0, a_1, a_2, a_3) are input to MDS transformation which performs the following matrix multiplication:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 \cdot a_0 \oplus 03 \cdot a_1 \oplus 01 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 02 \cdot a_1 \oplus 03 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 02 \cdot a_2 \oplus 03 \cdot a_3 \\ 03 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01 \cdot a_2 \oplus 02 \cdot a_3 \end{bmatrix}$$

The matrix of MDS transformation of Muchomor cipher match the matrix of Rijndael, but in calculating the product of vector's elements by matrix coefficients in Muchomor cipher another irreducible polynomial is used $m(x) = x^8 + x^4 + x^3 + x^2 + 1$ or {01}{1d} in hex. For further consideration kind of decomposable polynomial is not important.

The output 32-bit vector of MDS transformation (b_0,b_1,b_2,b_3) is the output value of SL transformation.

As seen this transformation is the basic building block of cycle transformation of 128-bit Rijndael. Practically it's the basis of the wide trail strategy applied in the construction of this cipher.

The transformation's properties are shown in Table 1 which presents the distribution law of number of activated S-boxes because they become active S-boxes at the next cycle of transformations. The experiment was performed for 1000 texts for 16-bit input differences. Total turns $1000 \times 2^{16} = 65536000$ values. Here active bytes are considered as bytes with non-zero differences in the output.

Table 1

Number of active bytes at the output	Number of repeats in %
0	0
1	0,0000167
2	0,00861
3	1,51
4	98,480

Table 2 shows the results of experiments performed for SL transformations of Muhomor cipher where 28-bit differences have been used. The results almost haven't changed.

It's seen that indeed at the output of transformation with multiplication by MDS matrix with high probability (close to 0,9999) 3 or 4 output bytes are active in most cases.

Table 2

Number of active bytes at the output	Number of repeats in %
0	0,000000386
1	0,0000239
2	0,0091
3	1,548
4	98,44

3. The proposed implementation of the wide trail strategy

In this paper, it'll be shown that there is the possibility of joint implementation of the principles of confusion and diffusion within a single construction that does not allow its division into linear and nonlinear parts and we assume that the branch number per one input byte of MDS transformation can be obtained greater than at least one as compared with the construction of SL transformation with MDS matrix. Further, this assumption will be checked.

The construction of the proposed SL transformation is shown in Fig. 2.

As can be seen from the figure, 32-bit input data block is divided into four bytes, each of which is fed to a chain of S-block transformations included its outputs to inputs of the subsequent one. At the same time the input of the first S-box is fed the sum modulo two of the four byte segments. The second, third and fourth byte segments also receives on respective inputs of other S-

boxes, where they had previously joined through modulo two adders with the outputs of the previous S-boxes. In addition, the output of the last S-box added by modulo two with the outputs of all previous S-boxes, forming outputs of SL transformation.

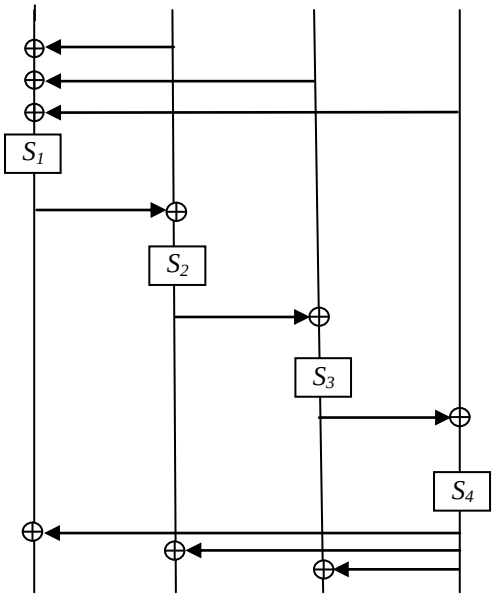

Fig. 2. Scheme of SL transformation using S-boxes

Obviously, due to the addition of four-byte segments at the input of first S-box we have four bytes pass through a chain of S-boxes and at the output of the fourth S-box it will be result (sum) of passage of each input byte through four S-boxes, wherein the first byte will pass through the four S-boxes, the second byte further pass through three S-boxes, third - through two S-boxes, fourth - through one S-box. But the output of the fourth S-box is also fed to the outputs (the sum modulo 2) of other S-boxes.

Denoting the transformation of an input byte x by *i*-S-box as $S_i(x)$, the mathematical description of the scheme 2 can be represented as follows. In the first step scheme performs operations:

$$b'_0 = S_0(a_0 \oplus a_1 \oplus a_2 \oplus a_3);$$
$$b'_1 = S_1(b'_0 \oplus a_1);$$
$$b'_2 = S_2(b'_1 \oplus a_2);$$
$$b'_3 = S_3(b'_2 \oplus a_3),$$

or in expanded form for example

$$b'_3 = S_3(S_2(S_1(S_0(a_0 \oplus a_1 \oplus a_2 \oplus a_3) \oplus a_1) \oplus a_2) \oplus a_3).$$

And in the second step:

$$b_0 = b'_0 \oplus b'_3;$$
$$b_1 = b'_1 \oplus b'_3;$$
$$b_2 = b'_2 \oplus b'_3;$$
$$b_3 = b'_3.$$

As a result, the formation of the output of SL transformation for the first byte will be involved 4 + 1 = 5 S-boxes, for the second byte 1 + 4 + 3 = 8 S-boxes, for the third byte 1 + 2 + 4 = 7 S-boxes and 1 + 4 = 5 S-boxes will participate in the formation of the output of the fourth byte. Thus, our SL transformation allows activating at least five S-boxes by a single input byte (each byte goes through 5 S-blocks). The actual number of involved S-boxes is considerably higher (if not require

the passage of each byte the same number of S-boxes). Note that the same result - five S-boxes will be in the case when at the input of cycle transformation will be only one active byte. In principle, when bytes added at the input of the first S-box is possible that this sum will be equal to zero. However, we are interested in differences passing through the S-boxes. Obviously, if you consider the bits of the blocks are independent and equally probable, the probability of getting by chance a certain difference for addition of the 32-bit differences is 2^{-64}. It can be considered almost incredible event.

Table 3 shows the distribution law of the number of active S-boxes for the second type of transformation. In this case, the experiment was performed for 16-bit differences for 1000 texts. Total considered $1000 \times 2^{16} = 65536000$ values.

A comparison of the results Table 1 and Table 2 clearly shows that the second transformation almost repeats characteristics of the first transformation. Only according to our initial assumptions its effectiveness was expected even higher than effectiveness of the previous optimum transformation with multiplication by MDS matrix. In the latter case, as the material of the above, the input bytes pass through the total number of 25 S-boxes.

Table 3

Number of active bytes at the output	Number of repeats, %
0	0
1	0,0000198
2	0,0091
3	01,5458
4	98,445

Naturally, the increased number of activated S-boxes should influence on the dynamic indicators of arrival of the cipher to a random substitution. To check the validity of the above assumption experiments to determine the round by round distributions of maximums of transitions of differential and linear approximation tables of considered SL transformations were made.

Further, Table 4 ÷ Table 5 presents the results of a comparative analysis of the round by round distributions of the maximums of transitions of differential tables of considered SL transformation and round transformation of Rijndael. To avoid computational difficulties associated with the large dimension of input data blocks (32 bits) we have used a common methodology of evaluation of the properties of large ciphers on the basis of a study of reduced models [6-8]. Here we are talking about the fact that the experiment was carried out for reduced 16-bit constructions of SL transformations, in which instead of byte S-boxes were used nibble S-boxes. As a result, we came to the round function of reduced model of Rijndael, whose properties are well studied in a number of publications [9-11, etc.].

As follows from [8] SL transformation of reduced model of Rijndael (Rijndael round function) comes to indicators of a random substitution on linear and differential indicators for three rounds. Note that the full version of Rijndael comes to a random substitution on differential indicators for three rounds and on linear indicators for four rounds.

So the proposed transformation is completely identical to the original transformation of Rijndael on its properties.

You might also notice that the increase of the number of active S-boxes, we are trying to see earlier, was not confirmed.

Let us conclude on the performance indicators of the proposed design. Our experiments show that within the framework of generally accepted approaches of programming our version of transformation exceeds the cipher Rijndael, the rate on the order. An optimized version of the design Rijndael [12] of course much faster than proposed. But our design can be optimized. The idea is that instead of processing one-dimensional array of substitutions with the addition of their two inputs on the module, you can go to the processing of two-dimensional arrays by applying instead of

byte S-box substitutions as Latin squares. Such two-dimensional substitution can be obtained through the use of a single line is not the usual substitutions, and still use 255 lines, which are cyclic shifts of the original, although it will have to pay for the increase in the required memory 28 times (if you do the conversion to nibble S-blocks, the memory will be required is 128 bytes). Table 6 shows the performance indicators in yet another experiment for non-optimized and optimized versions.

Table 4

1 round		2 rounds		3 rounds		4 rounds	
The value of the table cell	Number of cells	The value of the table cell	Number of cells	The value of the table cell	Number of cells	The value of the table cell	Number of cells
16	65610000	2	1074832156	2	1296379111	2	1302460638
32	43740000	4	334541109	4	325976493	4	325619594
64	10935000	6	83459909	6	55297322	6	54280993
128	4131000	8	23507080	8	7141261	8	6787312
256	1508625	…	…	…	…	10	677609
512	243000	1024	92	108	1	12	56804
1024	62100	1152	9	110	2	14	3992
2048	16200	1280	2	112	1	16	236
4096	1350	1408	7	128	13	18	14
8192	360	1536	2	192	1		
16384	60	2048	8	256	2		

Table 5

1 round		2 rounds		3 rounds	
The value of the table cell	Number of cells	The value of the table cell	Number of cells	The value of the table cell	Number of cells
16	14776336	2	1094787733	2	1300464541
32	17159616	…	…	4	325708896
48	5719872	240	4	6	54625300
64	8426048	242	4	8	6920768
96	4981824	252	4	10	712746
128	3229952	256	152	12	64443
144	830304	260	8	14	5799
…	…	…	…	…	…
4608	432	488	4	32	12
6144	1368	500	4	34	4
8192	468	512	8	36	8
9216	216	576	52	38	4
12288	72	580	8	42	12
16384	78	648	8	44	4
24576	24	768	8	48	4
32768	4	864	8	66	8

Table 6

	Optimized cycle function with a multiplication by MDS matrix	The cycle function on the basis of managed substitutions	The cycle function on the basis of a Latin square
Time of encryption of 100 million different blocks, sec	0,4	1,7	0,5 for byte S-box (1,3 for half-byte S-box)

It is seen that performance indicators in optimized variant differ by less than twofold.

4. Conclusions

It was found that the cycle transformation with improved dynamic indicators to the arrival of the cipher to the state of random substitution can be constructed without separation of its linear and substitution parts into separate structures, as required by the wide trail strategy. It is possible to implement the principles of activation of bytes (and subsequently S-boxes) of cycle transformations of ciphers in a single structure that does not allow its division into linear and nonlinear parts that are not inferior by the number of active bytes (S-boxes) to the scheme with multiplication by MDS matrix used in Rijndael. This possibility consists of procedure of consistent activation of S-boxes of round function one by one by using managed substitutions. The proposed structure allows for the maximum branch number (when one S-box input activates the subsequent S-boxes of transformation).

References: 1. *Landau S.* Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard, February, 2004. 2. *Feistel H.* Cryptography and computer privacy, Scientific American, Vol. 228, No. 5, pp. 15-23, May 1973. *3. Daemen J., Rijmen V.* The Wide Trail Design Strategy, Lecture Notes in Computer Science, Springer-Verlag, Berlin, V. 2260, pp. 222-238, 2001. *4. Горбенко І.Д., Бондаренко М.Ф., Долгов В.І. та ін.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація // Прикладна радіоелектроніка. – Харків, Україна. – 2007. – Т. 6, №2. – С. 147-157. 5. *Долгов В.И.* Новый взгляд на шифр «Мухомор» / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Прикладная радиоэлектроника. – Харьков, Украина. – 2014. – Т. 13, №3. – С. 221-225. 6. *Лисицкая И.В.* Методология оценки стойкости блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123-133. 7. *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / І.Д. Горбенко, В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320. 8. *Долгов В. И.* Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа: монография / В.И. Долгов, И.В. Лисицкая. − Харьков : Форт, 2013. – 420 с. 9. *Долгов В.И.* Вариации на тему шифра Rijndael / В.И. Долгов, И.В. Лисицкая, А.В. Казимиров // Прикладная радиоэлектроника. – 2010. – Т.9, №3 – С. 321-325. 10. *Лисицкая И.В.* Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей / И.В. Лисицкая, А.А. Настенко, Лисицкий Е.К. // Автоматизовані системи управління та прибори автоматики. – 2012.– Вып. 159. – С. 13-21. 11. *Долгов В.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – 2009.– Т.8, №.3. – С. 252-257. 12. *Daemen J., Rijmen V.*, AES submission, Document on Rijndael, Version 2, September 1999, pp1-45.

Харьковский национальный
университет радиоэлектроники
Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 11.04.2015