UDC 621. 3.06

I.V. Lisitskaya, D.Sc. K.E. Lisitsky
(*Kharkov National University, V.N. Karazine, Ukraine*)

About the minimum number of S-blocks activated on first SPN cycles

Using the example of the reduced model of the cipher Rijndael, real results are given for determining the dynamic parameters of the arrival of ciphers with various constructions of additional linear mixing transformations at its input to the state of random substitution. It is shown that these additional transformations are not effective for improving the randomness of Rijndel, ADE Kalina, Kuznechik and others.

INTRODUCTION

We have long been interested in activating the S-blocks of the first cycle of block symmetric ciphers [1-6, etc.] and studying the possibility of increasing their minimum number. Various schemes of linear pre-cycle mixing of data blocks were considered. However, as it now became clear, the randomness of the transforms is directly related to the use of the mechanisms of random mixing of the data segments participating in the transformations. They can be realized with the help of non-linear (substitution) transformations (mixing with S-blocks), which allow to ensure statistical independence of segments at the outputs of the transformation. In this paper, we present the results of estimating the differential parameters of the cyclic transformations of the mini versions of the Rijndael cipher with various designs of linear mixing transformations at the cipher input and compare the results obtained with the original development indicators. It is shown that linear transformations at the cipher input do not improve its randomness indicators.

1. STATUS OF THE QUESTION

Previous studies [1-3] have shown that the dynamic exponents of the arrival of ciphers to the state of a random environment depend significantly on the minimum number of S-blocks that are activated on the first cycles. Here, under the dynamic exponents of cipher arrival to the state of random substitution, the minimum number of encryption cycles is understood, after which the maximum values of differential and linear probabilities assume asymptotic values inherent in random permutations of the corresponding degree. This led to interest in studying the possibilities of increasing the number of activated S-boxes on the first cycles of encryption transformations. In our works [4-6], we considered the possibilities of increasing the number of activated S-blocks on the first cycles of ciphers due to the use of additional mixing linear transformations on their inputs. It was shown that really additional mixing transformations allow solving the problem of increasing the number of activated S-blocks. However, as it is now clear, linear transformations are not able to improve the randomness of ciphers. In this case, the random connection between the S-blocks is broken (there is no), and therefore the resulting probability of the first cycle is determined not by the product of the probabilities of S-block transitions, as is done in the cyclic transformations of most ciphers, but

rather by their sum. The purpose of this work is to first, using the reduced model of the cipher Rijndael, to give real results of determining the dynamic parameters of the arrival of this cipher with various designs of additional linear mixing transformations at its input to the state of random substitution and to show that indeed these additional transformations are not effective for improve the randomness of ciphers Rijndel, ADE, Kalina, Kuznechik several others.

2. RESULTS OF THE EXPERIMENTS

As an object of research, as noted above, a reduced model of the cipher Rijndael, taken from [7], was chosen. This is a cipher with a 16-bit size of the input data block and the key. It practically repeats the structure of the transformations of the original cipher design. First, whitening is performed using a 16-bit key, and then conversion cycles are performed, each of which involves passing the input data block through four S-boxes (the original SubBute development operation). In our mini-models they are the same. The S-blocks themselves are also taken from [7]. A separate S-block is specified by the string (10, 4, 3, 11, 8, 14, 2. 12, 5, 7, 6, 15, 0, 1, 9, 13) This S- the cipher block Rijndael and has the maximum values of the differential and linear probabilities equal to $DP^{\pi}_{\max} = LP^{\pi}_{\max} = 2^{-2}$.

The outputs of the S-boxes are fed to the MDS with a separable code matrix of 4×4; the activation of one S-block extends to all output nibbles of the loop (the MixColumn operation), and therefore the subsequent ShiftRow operation in the small version of the cipher is not required. The addition operation modulo 2 with the cyclic (round) key (AddRoundKey operation) completes the cyclic function.

Three constructions are considered as linear transformations:

1) Addition of the module 2 of all nibbles of the input 16-bit data block at the input of the first S-block. The remaining S-blocks receive the corresponding nibbles of the input data block (similar to the one used in the cipher. SHUP-1 [8]):

2)
```
d1= d1^d2^d3^d4;
d2 = d2;
d3 = d3;
d4 = d4.
```

3) Adding the input half-bytes to three at the inputs of the S-blocks of the cyclic function:

```
d1 = d1 ^ d3 ^ d4;
d2 = d2 ^ d1 ^ d4;
d3 = d3 ^ d2 ^ d1;
d4 = d4 ^ d3 ^ d1.
```

Use after the operation of the whitening of the half-byte operation MixColumn to the input data block.

In the first experiments, the distributions of the total differentials of the mini versions of the three-cycle Rijndael ciphers with various designs of linear mixing transformations at its input were calculated. The results of the experiments are shown in Table 1. Here in the first column the data for the original reduced version of the construction of the cipher are shown and in the other columns the results of

three-cycle encryptions are used for the application of the mini versions of the ciphers of the three variants of linear mixing transformations.

Table 1

Distribution of total differentials of the mini versions of the three-cycle Rijndael ciphers with different constructions of linear mixing transformations at its input

Clean Rijndael (without pre-cycle transformation)	Pre-cycle transformation 1)	Pre-cycle transformation 2)	Pre-cycle transformation 3)
0=2605083584	0=2605116431	0=2605059693	0=2605049242
2=1302347318	2=1302303977	2=1302393259	2=1302406612
4=325645417	4=325636237	4=325629048	4=325633997
6=54293282	6=54312219	6=54285939	6=54278384
8=6793579	8=6792690	8=6793103	8=6791931
10=677534	10=678900	10=679611	10=680739
12=56700	12=56937	12=56773	12=56578
14=4086	14=4078	14=4081	14=4000
16=246	16=275	16=243	16=259
18=14	18=16	18=8	18=17
0	0	0	20=1
0	0	0	0

As follows from the presented results, it turns out that the results presented earlier in [4-6] are erroneous in the sense that an increase in the number of activated S-blocks of the first cycle with linear pre-cyclic transformations does not lead to an increase in the randomness of ciphers.

Indeed, linear transformations at the input of the cipher allow increasing the number of activated S-blocks up to the maximum possible number, but due to the linear connection between the input segments, the probabilities of passing the S-blocks of the first cycle are not multiplied, as in the cyclic transformations of ciphers, but rather add up. Therefore, the influence of linear transformations at the input of the cipher is practically depreciated. This conclusion can be transferred to full-scale ciphers: Rijndel, ADE, Kalina, Kuznechik and other solutions close to them, in which the results of linear conversion of the input segments come directly to the S-block strokes.

The second series of experiments was performed by constructing the piecemeal laws for the distribution of the LAT displacement maxima of the mini versions of the Rijndael cipher with various designs of linear mixing transformations at its input. These results are presented in Table 2.

It can be seen that the randomness indicators, in the first and second cases, are practically independent of the presence of additional linear transformations at the input of the ciphers.

Using, for example, sets of S-blocks (as in the SL transformations of the SHUP ciphers [8]).

The distribution of the maxima of the LAT displacements of the mini version of the cipher Rijndael with various designs of linear mixing transformations at its input

Table 2

Number of encryption cycles	Clean Rijndael without pre-cycle transformation	Pre-cycle transformation		
		d1 = d1^d2^d3^d4 d2 = d2 d3 = d3 d4 = d4	d1 = d1^d3^d4 d2 = d2^d1^d4 d3 = d3^d2^d1 d4 = d4^d3^d1	Multiplication by MDS matrix separable code
1	16384	16384	16384	16384
2	2048	2048	2048	2048
3	824	824	824	792

However, simple considerations have shown that even in this case the minimum number of activated S-blocks of the first cycle is kept equal to one.

Indeed, if the design of the cipher is known, it is not difficult to calculate the result of passing the input difference through a separate S-block SL of the transformation and then forcefully realize the situation when the difference in the output of the current S-block coincides with the difference of the segments supplied to the adder by modulo 2 at the input the next S-block of the chain. Then, at the input of the next S-block of the chain, a zero difference is obtained, and the chain of mutually activated S-blocks is broken. As a result, we arrive at a situation where at least one S-block is activated at the input of the first cycle (chains of S-boxes).

It turns out that in the general case it is possible to increase the number of activated S-blocks of the first cycle only by applying a nonlinear pre-cycle transformation, as done, for example, in the Labyrinth cipher [9].

Another simple solution that allows increasing the minimum number of activated S-blocks of the first cycle is the use of a two-layer construction of the construction of the cycle function. This solution was also proposed in [8].

CONCLUSIONS

Summing up the existing results and the already existing convictions and conclusions, we can note the following:

1. The minimum number of activated S-blocks on the first cycles significantly affects the dynamic parameters of the arrival of ciphers to the state of random substitution.

2. Mixing linear transformations of any design on the inputs of the known algorithms for block symmetric encryption: Rijndel, ADE Kalina, Kuznechik linear transformations do not have a random mixing mechanism for segments of the input data block.

3. One possibility of increasing the number of activated S-blocks of the first cycles can be considered as replacing the first cycle with a more efficient construction, based on controlled substitutions [8]. This approach allows us to solve the problem of maximizing the number of activated S-blocks of the second cycle.

4. Another possibility of increasing the minimum number of activated S-blocks of the first cycle is to use a two-layer substitution transformation in the first cycle, as suggested in [8, etc.].

References

1. Лисицкая И. В. Экспериментальные данные по определению динамических показателей прихода блочных симметричных шифров к состояни. случайной подстановки / И. В. Лисицкая, К. Е. Лисицкий, М. Ю.Родинко и др. // Радиоэлектроника, информатика, управление Запорожье: ЗНТУ – 2017. – № 1(40) – С. 129-141.

2. Горбенко И.Д. Уточнённые показатели прихода шифров к состоянию случайной подстановки / И.Д. Горбенко, В.И. Долгов, Лисицкий К.Е. // Прикладная радиоэлектроника. – Харьков: ХНУРЭ. – 2014. Том. 13, № 3. С. 213-216.

3. Gorbenko I.D. On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov / Universal Journal of Electrical and Electronic Engineering, 2, 206-215.

doi: 10.13189/ujeee.2014.020409.

4. Долгов В.И. Усовершенствованный блочный симметричный шифр Калина / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // 0485-8972. – Радиотехника Всеукр. межвед. научн.-техн. сб. – 2016. – Вип.186. – С. 119-131.

5. Лисицкий К.Е. Усовершенствованный Rijndael / К.Е. Лисицкий, // Материалы VI Международной научно-технической конференции ″Захист інформації і безпека інформаційних систем″. – Львів – 1-2 червня 2017 р. С. 85-86.

6. Lisitskaya Iryna Impruvd Rijndael / Iryna Lisitskaya, Konstantin Lisitskiy, Mariya Rodinko // Science and Education Studies “Stanford University Press”Volume II – № 1(17), January- June – 2016. p. 608-618.

7. Долгов В.И. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / В.И. Долгов, И.В. Лисицкая. Монография – Харьков: Издательство “Форт”. – 2013. – 420 с.

8. Dolgov V.I. The new concept of block symmetric ciphers design / V.I. Dolgov, I.V. Lisitska, K.Ye. Lisitskyi // DOI: 10.1615 /TelecomRadEng. v. 76. i. 2. pages 157-184.

9.. Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» / С.А. Головашич // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 230-240.