Universal Journal of Mathematics and Applications, 1 (1) (2018) 29-32

UJMA

Universal Journal of Mathematics and Applications

Journal Homepage: www.dergipark.gov.tr/ujma

An algorithm for constructing S-boxes for block symmetric encryption

Bakhtiyor Fayzievich Abdurakhimov[a] and Sattarov Alijon Bozorbayevich[a*]

[a]*Department of Applied Mathematics and Computer Analysis, National University of Uzbekistan, Uzbekistan*
[*]*Corresponding author E-mail: asb2602@mail.ru*

Article Info

Keywords: *S-box, algebraic cryptanalysis, algebraic immunity, nonlinearity*
2010 AMS: *94A60, 68P25, 11T71, 14G50*
Received: *10 February 2018*
Accepted: *27 February 2018*
Available online: *11 March 2018*

Abstract

This article presents an algorithm for the generation of S-boxes with the maximum algebraic immunity and high nonlinearity. The algorithm is founded method of the permutation of output element of S-box. On basis of the proposed method, $S(8\times 8)$-box created, with the algebraic immunity 3 (441) and nonlinearity 104. The algorithm given in this article can be used for oscillation of $S(8\times 8)$)-boxes with the increased resistance to algebraic, linear, differential and linear and differential methods of a cryptanalysis, for block symmetric algorithms of encryption.

1. Introduction

It is known that for determining the reliability of (cryptographic stability) encryption algorithms is required to assess their well-known modern methods of cryptanalysis. This shows that the emergence of a new method of cryptanalysis or development of existing methods of cryptanalysis can affect the cryptographic stability of the encryption algorithms used in practice. Today, algebraic method of cryptanalysis based on solving systems of equations over finite fields, is a modern and rapidly developing methods of cryptanalysis for block symmetric encryption algorithms [4]. As a result of research, experts, it has been proposed option "algebraic immunity" encryption algorithms that allows you to determine the stability (instability) it to the algebraic methods of cryptanalysis. Therefore, the use of encryption algorithms convert with high algebraic immunity, will serve as a basis for ensuring the reliability of its methods to algebraic cryptanalysis. After the introduction of the parameter has become an urgent task for research aimed at creating change, with the maximum algebraic immunity. In developing the new block symmetric encryption algorithms take into account the use of these transformations, with the maximum algebraic immunity, that is, its cryptographic stability to methods of algebraic cryptanalysis. For example, in algorithms of standard STB 34.101.31-2011, GOST R 34.11-2012 and GOST R 34.12-2015 used S-boxes with the maximum algebraic immunity. This article describes the algorithms for generating S-boxes, the maximum algebraic immunity and high degree of nonlinearity.

2. Generation of S-boxes

It should be noted that as a part of round function the modern block symmetric algorithms of enciphering two following main transformations are used: substitution (S-box) and permutation (P-box) [3, 5]. The main the purpose of the S-box is "hashing of bits" and their use as the main non-linear transformation in round function. P-box to serve "a dispelling of bits" and is the linear transformation.

Each S-box transformation is defined over some finite field. S-box represent a $S(n\times m)$ wherein the input bit length (n) and output bit length (m).

Below is a sample $S(4\times 4)$-box.

$$S=\left\{\begin{array}{rcccccccccccccccc} x=\{ & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ y=\{ & 15 & 14 & 13 & 11 & 6 & 12 & 9 & 2 & 5 & 10 & 4 & 8 & 0 & 1 & 3 & 7\} \end{array}\right\} \tag{2.1}$$

where: x - the input sequence in $S(4\times 4)$-box, y - output sequence with x respectively. For example: $S(6)=9$, $S(14)=3$.

***Email addresses*:** **a_bakhtiyor@mail.ru (B. F. Abdurakhimov), asb2602@mail.ru (S. A. Bozorbayevich)**

Determination of [1, 6]. Let the following system of Boolean equations satisfies $S(n\times m)$-box:

$$G=\begin{cases} g_1(x_1,x_1,...,x_n,y_1,y_1,...,y_m)=0;\\ g_2(x_1,x_1,...,x_n,y_1,y_1,...,y_m)=0;\\ ...\\ g_r(x_1,x_1,...,x_n,y_1,y_1,...,y_m)=0. \end{cases} \tag{2.2}$$

Minimum degree algebraic equation (deg(g)) in the system (2.2) is called an algebraic immunity $S(n\times m)$-box ($AI(S)$). That is, it can be formally written as follows:

$$AI(S)=\min\{\ \deg(g)|g\in G\} \tag{2.3}$$

From this it follows that the high value of the parameter AI to S-box provides a high degree algebraic equation system.
After introducing the concept of the AI, it has become an urgent task of evaluating the maximum possible value of this parameter for the S-box of fixed length and a minimum number (N_{TS}) of possible equations in the system. As a result of investigations for solving this problem has been created in the following table indicating the maximum value of the AI and the minimum value of the N_{TS}, depending on the size of $S(n\times n)$-box.

n	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
AI	2	2	2	2	3	3	3	3	4	4	4	4
N_{TS}	14	21	24	15	342	441	476	327	7061	8855	9710	7774

Table 1: Optimal values of AI and N_{TS} for $S(n\times n)$-box

In general it should be noted that *if the values AI S-box is less than the possible maximum value or value N_{TS} is greater than the minimum possible value, the S-box does not provide maximum resistance to algebraic techniques of cryptanalysis*.

It is known that the linear and differential methods of a cryptanalysis are also the modern methods of a cryptanalysis, for block symmetric algorithms of encryption. For ensuring resistance of an algorithm to the linear cryptanalysis, it is required to use S-boxes with the maximal value of nonlinearity ($N(S)$), and for ensuring resistance of algorithms to a differential cryptanalysis, it is required to use S-boxes in which the maximal value (δ) in a matrix of differences is less. Therefore, in algorithms of encryption it is necessary to use those S-boxes in which not only AI value is maximal, but also $N(S)$ value is also maximal, and value δ minimum.
There are several methods of creation of the S-boxes having the maximal value of nonlinearity [2]. However, because of the made experiments it became of known that $AI(S)$ and $N(S)$ value for S-boxes would not be at the same time maximum (that is maximality of these values is mutually excluded). This condition demands to solve the following problem:
At what maximal values of the N(S) parameter value of the AI and N_{TS} parameters will be optimum?
Solution of this task nonlinearity demands to construct several S-boxes having some high (that is, smaller maximal) nonlinearity and to make the corresponding experiments with them. Because of the carried-out analysis, the following statement are more efficient approach for creation of S-boxes with high values of nonlinearity.
Statement [7]. Let, the following equalities for S_1(nxm) and S_2(nxm) of boxes are carried out.

$$\begin{cases} S_2(p_1)=S_1(p_2),\ \ p_1\neq p_2;\\ S_2(p_2)=S_1(p_1);\\ S_2(x)=S_1(x),\ \ x\neq p_1,p_2. \end{cases} \tag{2.4}$$

Then truly following expression.

$$N(S_1)-2\leq N(S_2)\leq N(S_1)+2 \tag{2.5}$$

It means, according to statements, as a result of permutation among themselves of two elements of the S-box of its value of nonlinearity either decreases on 2 or increases on 2 or does not change. At the same time the statement also follows from this statement the following: *if as a result of permutation between itself two different elements S_1-box having general degree nonlinearity N(S_1)=a, is present probability of the creation S_2-box with the common degree nonlinearity equal N(S_2)=a-2, that as a result of permutation different 4 elements S_1-box created S_3-box can have importance with the general degree nonlinearity equal N(S_3)=a-4.* This statement will be a basis for oscillation of S-boxes with different values of nonlinearity. That is, increasing quantity of mutually rearranged elements of the S-box it is possible to reduce value of nonlinearity sequentially. Put into practice experiments with S(8x8)-box it was revealed that at $N(S)$=104 values, δ=8 the AI and N_{TS} parameters can have optimum degree.

Generally, the algorithm of creation of the S-boxes having such properties has the following sequence of steps:

Input: Certain $S(8\times 8)_{\ max}$ – box having maximal (that is: $N(S)$=112) nonlinearity.
Output: $S(8\times 8)$ – box satisfying to values: $N(S)$=104, δ=8, $AI(S)$=3 and N_{TS}=441.
1. $S(8\times 8)$=$S(8\times 8)_{\ max}$.
2. Permutation mutually 39 elements of the S(8x8)-box.
3. Determine value of the *N(S)* and δ parameters of the $S(8\times 8)$-box, created in 2 step.
4. If $N(S)$<104 or δ>8 that return to 1 step.
5. Define values of the $AI(S)$ and N_{TS} parameters of the $S(8\times 8)$-box, created 2 step.
6. If AI (S) $\neq$3 or N_{TS} $\neq$441 that return to 1 step.

7. Announce $S(8\times 8)$-box as output dates.
8. End.

Below the example of model $S(8\times 8)$-box created by means of the algorithm developed by the software is given (the output elements of the $S(8\times 8)$-box):
$S(8\times 8)_{\ example}$ = {173, 175, 17, 133, 114, 99, 57, 231, 126, 42, 247, 209, 230, 68, 181, 109, 248, 236, 115, 48, 188, 125, 18, 120, 53, 105, 4, 239, 32, 121, 76, 246, 6, 155, 13, 221, 254, 180, 226, 224, 36, 143, 196, 219, 78, 146, 227, 31, 96, 118, 92, 22, 249, 217, 49, 79, 67, 138, 198, 251, 93, 215, 60, 24, 69, 88, 50, 154, 253, 140, 206, 123, 184, 81, 160, 229, 98, 159, 139, 113, 233, 223, 238, 204, 153, 237, 107, 234, 225, 242, 14, 7, 183, 178, 72, 128, 203, 94, 124, 191, 84, 170, 205, 116, 29, 190, 150, 131, 103, 207, 97, 164, 51, 194, 65, 21, 37, 106, 58, 145, 212, 213, 172, 101, 100, 168, 163, 136, 9, 55, 86, 102, 195, 199, 15, 80, 132, 127, 61, 83, 176, 20, 122, 241, 38, 255, 82, 161, 171, 19, 89, 148, 220, 110, 8, 43, 3, 85, 66, 56, 142, 250, 40, 2, 59, 162, 134, 240, 182, 228, 141, 129, 211, 185, 179, 74, 11, 34, 62, 210, 193, 167, 197, 33, 156, 108, 30, 117, 95, 214, 187, 245, 35, 26, 27, 0, 252, 104, 202, 44, 208, 158, 147, 64, 157, 52, 192, 77, 5, 25, 152, 41, 12, 232, 87, 149, 119, 216, 165, 46, 75, 235, 169, 135, 222, 200, 39, 70, 91, 174, 112, 166, 54, 189, 243, 177, 218, 28, 10, 137, 144, 244, 16, 130, 45, 90, 73, 23, 201, 111, 47, 71, 151, 1, 63, 186}.
It is known that today in many algorithms of encryption $S(8\times 8)$-box is used. For comparison of the S(8x8)$_{example}$-box with some $S(8\times 8)$-boxes, created the table of assessment (Table 2).

Encrypting algorithm	**N(S)**	δ	**AI (N$_{TS}$)**	**IGS**
AES	112	4	2 (39)	0,886285
Camellia	112	4	2 (39)	0,886285
SQUARE	112	4	2 (39)	0,886285
UzDSt 1105:2009	112	4	2 (39)	0,886285
STB 34.101.31-2011	102	8	3 (441)	0,962426
GOST P 34.12-2015	100	8	3 (441)	0,956473
S(8x8)$_{example}$	**104**	**8**	**3(441)**	**0,968378**

Table 2: Comparative properties in algorithms of encryption $S(8\times 8)$-boxes.

Values of the IGS parameter (the **I**ndex of the **G**eneral **S**tability, 0≤IGS≤1) specified in this table it is calculated by means of (2.6) formula, considering an indicator of resistance to the linear, differential and algebraic cryptanalysis of $S(8\times 8)$-box.

$$\mathrm{IGS} = \frac{\frac{\mathrm{N}\,(\mathrm{S})}{112} + \frac{\mathrm{AI}}{3} + \frac{258-\delta}{256}}{3} \tag{2.6}$$

Follows from this expression that for some $S(8\times 8)$-box there correspond the $N(S)$=112, δ=2 and AI=3 parameters, IGS values of this $S(8\times 8)$-box it will be maximal, that is IGS=1. Besides, the IGS value of the $S(8\times 8)_{\ example}$-box is higher than other $S(8\times 8)$-boxes given in the table.
In Figure 2.1 the comparative schedule on IGS value of the specified S-boxes is represented.

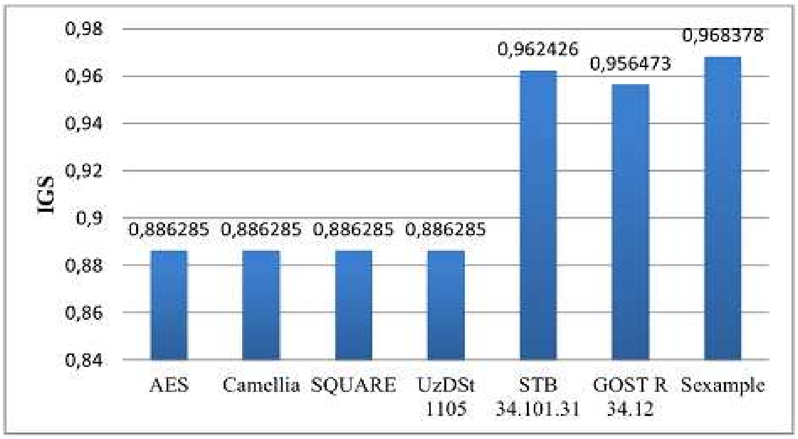

Figure 2.1: The comparative schedule on IGS value of the specified S-blocks.

3. Conclusions

The proposed method is based method of permutation of output element of S-box. It allows to find S-box with desired properties. Such S-box can be used in modern symmetric algorithms that demand high level of robustness against various types of attacks.

References

[1] A. Eilertsen, K. Kazymyrov, V. Kazymyrova, M. Storetvedt, *A Sage Library For Analysis Of Nonlinear Binary Mappings*, Selmer Center, Department of Informatics, University of Bergen, Norway. CECC'14, May 21, 2014.

[2] A. Sokolov, *New methods of synthesis of non-linear transformations of the modern encryptions,* LAP LAMBERT Academic Publishing house (Saarbrucken, Germany), 2015. ISBN: 978-3-659-67440-2.
[3] J. Daemen, *The design of Rijndael: AES-the advanced encryption standard,* Berlin; Heidelberg: Springer, 2002.
[4] N. Courtois, J. Pieprzyk, *Cryptanalysis of block ciphers with overdefined systems of equations,* ASIACRYPT, 2002. – P. 267-287.
[5] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko, S. Smyshlyaev, *Boolean functions in the theory of coding and cryptology,* Institute of problems of an inform.security of MSU. – 2nd prod., additional – M.: MTsNMO, 2012. – 583 pages.
[6] S. Fischer and W. Meier, *Algebraic Immunity of S-boxes and Augmented Functions*, FHNW, CH-5210 Windisch, Switzerland.
[7] Y. Yu, *Constructing Differentially 4 Uniform Permutations from Known Ones*, Chinese Journal of Electronics. – 2013. – Vol. 22, No. 3. – River 495–499.