DOI 10.15276/imms.v9.no3.111
УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 3, pp. 111-119

AVALANCHE CHARACTERISTICS OF NYBERG CONSTRUCTION S-BOXES REPRESENTED BY THE MANY-VALUED LOGIC FUNCTIONS

A.V. Sokolov, V.V. Radush

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: radiosquid@gmail.com

One of the most commonly used today cryptographic algorithms is the Advanced Encryption Standard (AES), in which the Nyberg construction is used as an S-box. The existing approach to estimating the cryptographic quality of S-boxes, in particular, the Nyberg construction, is based on its representation using the mathematical apparatus of Boolean functions. At the same time, one of the most important criteria of cryptographic quality is a strict avalanche criterion of component Boolean functions. Nevertheless, the cryptanalyst is not restricted in choosing a method for describing cipher components, which necessitates the research of the cryptographic properties of the Nyberg construction S-boxes represented using many-valued logic functions. This work is devoted to the research of the avalanche characteristics of the Nyberg construction S-boxes represented by Boolean functions, 4-functions, and 16-functions. In this case, we consider S-boxes of the Nyberg construction of practically valid length *N*=256 based on the full set of irreducible polynomials of eighth order. It has been established that the avalanche properties of the Nyberg construction S-box depend on the particular type of irreducible polynomial used to build it. The irreducible polynomials that provide the best avalanche characteristics of the Nyberg construction S-boxes in the sense of Boolean functions, 4-functions, and also 16-functions are determined. It was found that the S-box based on irreducible polynomial $f_{19}(x) = 319$ is characterized by the optimal deviation from the requirements of the strict avalanche criterion from the point of view of any possible representation by the functions of many-valued logic, thus, it can be recommended for practical use.

Keywords: S-box, Nyberg construction, strict avalanche criterion, many-valued logic.

Introduction and problem statement

Today, one of the most common block symmetric cryptographic algorithms is AES, which is used in many information protection systems. The AES cryptographic algorithm is characterized by a high level of cryptographic strength and the simplicity of software and hardware implementation. Nevertheless, the continuous development of cryptanalysis methods requires careful research of its cryptographic properties, as well as further improvement of its structure and the cryptographic primitives of which it consists.

The most important part of a block symmetric cryptographic algorithm is an S-box, which largely determines the general level of diffusion and confusion [1] of the cryptographic algorithm, as well as the simplicity of its technical implementation. Currently, there are many constructive methods for the synthesis of high-quality S-boxes, among which a special place is occupied by the Nyberg construction [2], on the basis of which the AES [3] cryptoalgorithm S-box is built. The Nyberg construction S-boxes are characterized by a high level of cryptographic quality, while today the quality of any cryptographic S-box is estimated using the following criteria [4, 5]:

- high nonlinearity distance;
- high algebraic degree of nonlinearity;
- compliance with the strict avalanche criterion (SAC);
- statistical independence of the output vectors of the S-box from its input vectors.

All of the listed criteria are based on representation of the S-box as a set of Boolean functions, and at the moment there are many researches devoted to the evaluation of these criteria for the S-box of the AES cryptographic algorithm [6, 7]. However, a cryptoanalysis attack can be carried out with help of any mathematical constructions used to represent the cryptographic algorithm, for example, using the apparatus of many-valued logic functions [8]. This circumstance requires more detailed research of the cryptographic quality of the many-valued logic functions that are part of the AES cryptographic algorithm S-box.

The purpose of this paper is to research the component q-functions of the full set of Nyberg construction S-boxes and also to determine the S-box with the best avalanche characteristics.

The choice of the Nyberg construction for the AES cryptographic algorithm was due to its high compliance with the main criteria of cryptographic quality, as well as the possibility of technical implementation both in a tabular and with help of calculations over the extended Galois field $GF(2^8)$. The Nyberg construction is a map defined by the multiplicatively inverse elements of Galois fields $GF(2^k)$

$$y = x^{-1}\mathrm{modd}(f(z), p),\ y, x \in GF(2^k), \tag{1}$$

combined together with the affine transform

$$b = Ay + a,\ a, b \in GF(2^k), \tag{2}$$

where $f(z)$ is the irreducible over the field $GF(2)$ polynomial of order k; $0^{-1} \equiv 0$ by definition; A is a nonsingular affine transform matrix; a is a shift vector; $p = 2$ is the characteristic of the extended Galois field; a, b, x, y are the elements of the extended Galois field $GF(2^k)$, they are considered as decimal numbers, binary vectors, and polynomials of order $k-1$.

It was established in [7] that the structure of the Nyberg construction S-box depends on the type of irreducible polynomial, while the number of irreducible polynomials [9] of order k is defined by the formula

$$|W_k| = \frac{1}{k} \sum_{\substack{d \\ d\,\square\mathrm{k}}} \mu(d) \cdot p^{(k/d)}, \tag{3}$$

where d are the divisors of the k, $\mu(d)$ is the Mobius function, the notation $d\,\square k$ means that d divides k. It is clear, that formula (3) also determines the cardinality of the Nyberg construction S-boxes class.

Designers of various cryptographic algorithms choose various irreducible polynomials for constructing S-boxes. For example, in the cryptographic algorithm AES the irreducible polynomial $f_1(z) = z^8 + z^4 + z^3 + z + 1$ is used. In this case, the choice of cryptographic constructions occurs only on the basis of the analysis of the cryptographic quality of their component Boolean functions. This circumstance necessitates a more reasonable choice of the irreducible polynomial $f(z)$ used to construct the S-box, taking into account the cryptographic properties of its component many-valued logic functions.

Avalanche characteristics of the functions of many-valued logic

We first introduce the definitions of avalanche characteristics of Boolean functions necessary for our research and then generalize them to the case of many-valued logic functions.

Definition 1 [10]. The function of q-valued logic of k variables is a mapping $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Definition 2 [11]. The derivative in the direction of $u \in V_k$ of the Boolean function is the Boolean function defined as

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{4}$$

where V_k is the linear vector space of binary vectors of length k, $\oplus$ is the summation modulo 2.

Definition 3 [11]. The Boolean function $f(x)$ satisfies the propagation criterion $PC(u)$ with respect to the vector $u \in V_k$ if its derivative in direction of u is a balanced function, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0{,}5. \tag{5}$$

Definition 4 [11]. A Boolean function $f(x)$ satisfies the propagation criterion $PC(m)$ of order m if it satisfies the propagation criterion with respect to all vectors u of Hamming weight $1 \le wt(u) \le m$, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0{,}5, \quad \forall u \in V_k, \quad 1 \le wt(u) \le m. \tag{6}$$

Definition 5 [11]. A Boolean function $f(x)$ satisfies the strict avalanche criterion (SAC) if it satisfies the propagation criterion $PC(1)$ of order 1

$$p\{f(x) = f(x \oplus u)\} = 0{,}5, \quad \forall u \in V_k, \quad wt(u) = 1. \tag{7}$$

Anyhow, modern S-boxes can be represented not only by the Boolean functions, but also by the functions of many-valued logic. So, for example, S-boxes of the commonly used today length $N = 256$, can be represented both using Boolean functions ($q = 2$), and using the 4-functions ($q = 4$) or 16-functions ($q = 16$). Each of the sets of these functions fully determines the quality of the S-box used.

The definition of a strict avalanche criterion for the functions of many-valued logic was introduced in [12]; however, a strict avalanche criterion of the functions of many-valued logic of the AES cryptographic algorithm was not researched. For completeness, we briefly describe the general scheme for researching the avalanche characteristics of many-valued logic functions, which is based on the following definitions.

Consider the q-function $f(x)$ of k variables, as well as the vector $u = (u_1, u_2, ..., u_k)$.

Definition 6 [12]. The weight $\varpi(u)$ of a q-valued vector is the number of its nonzero components.

Definition 7 [12]. The derivative of a q-function $f(x)$ in the direction of the vector u is the q-function

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \, (\text{mod}\, q), \tag{8}$$

where $\underset{q}{\oplus}$ denotes addition modulo q.

Definition 8 [12]. A q-valued logic function $f(x)$ satisfies the propagation criterion $PC(u)$ with respect to the vector $u \in V_k$ if its derivative in direction of u is a balanced function, i.e. values $0,1,...,q-1$ are taken with equal probabilities $p(D_u f(x) = i(\text{mod}\, q)) = 1/q$

for all $i = 0, 1, ..., q-1$. In other words $K^0 = K^1 = ... = K^{q-1}$, where K^i is the number of sets of variables on which the derivative takes a value i.

Definition 9 [12]. A *q*-valued logic function $f(x)$ satisfies the propagation criterion $PC(m)$ of order m if it satisfies the propagation criterion $PC(u)$ with respect to all vectors u of weight $1 \le \varpi(u) \le m$.

Definition 10 [12]. The function $f(x)$ of *q*-valued logic satisfies the strict avalanche criterion (SAC) if it satisfies the propagation criterion $PC(1)$ of order 1.

Research of the avalanche characteristics of Nyberg construction S-boxes of length $N = 256$ based on the full class of irreducible polynomials. Consider a specific example. Let a Nyberg construction S-box based on an irreducible polynomial $f(z) = 283_{10} = z^8 + z^4 + z^3 + z + 1$ which is used in the AES cipher to be given in the form of its coding Q-sequence

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

As an example, we consider the process of finding avalanche characteristics of the S-box (9) represented by four component 4-functions $Ffour_i, i = 1, 2, ..., 4$, the first of which has the form

$$\begin{gathered}
Ffour_1 = \{01123231031001130023130303103022222111011201002201203122210\\
33311123311113033011110120033022010132233122303133313133101202002 12\\
1232302322321132102221020220301012302330102022232200331101122110233\\
0332003133030022323132203011003112322310233102333000230101012 10\}.
\end{gathered} \tag{10}$$

Using Definition 7, we find, for example, the derivative of the 4-function (10) in the direction of the vector $u = \{0, 0, 0, 1\}$ which has the form

$$\begin{gathered}
D_{0001}Ffour_1 = [1012312232301021021121323230120100310310 12\\
1002021120210133330202110200001300100331130301202031 22\\
0103101232210220202011202020131331131300330233330031 22\\
2223123113121011332200130003010310103032121300203320 11\\
10211313230331133032011201212101321201032110313113 31].
\end{gathered} \tag{11}$$

In accordance with the requirements of Definition 8, in order for the S-box (9) to satisfy the propagation criterion in direction of the vector $u = \{0, 0, 0, 1\}$, it is necessary that the number of characters “0”, “1”, “2” and “3” be equal to each other, i.e. $K^0 = K^1 = K^2 = K^3 = N/4 = 64$. However, this requirement is not satisfied for the derivative (11)

$$\left\{\begin{matrix} K^0_{D_{0001}Ffour} & K^1_{D_{0001}Ffour} & K^2_{D_{0001}Ffour} & K^3_{D_{0001}Ffour} \\ 69 & 73 & 55 & 59 \end{matrix}\right\}. \tag{12}$$

We find the deviation of the derivative (11) from the compliance with the requirements of Definition 8

$$\left\{\begin{matrix} \Delta K^0_{D_{0001}Ffour} & \Delta K^1_{D_{0001}Ffour} & \Delta K^2_{D_{0001}Ffour} & \Delta K^3_{D_{0001}Ffour} \\ \left|64-K^0_{D_{0001}Ffour}\right| & \left|64-K^0_{D_{0001}Ffour}\right| & \left|64-K^0_{D_{0001}Ffour}\right| & \left|64-K^0_{D_{0001}Ffour}\right| \end{matrix}\right\}= \\ =\left\{\begin{matrix} \Delta K^0_{D_{0001}Ffour} & \Delta K^1_{D_{0001}Ffour} & \Delta K^2_{D_{0001}Ffour} & \Delta K^3_{D_{0001}Ffour} \\ 5 & 9 & 9 & 5 \end{matrix}\right\}. \tag{13}$$

Similarly, we can find the deviations of the derivative of the 4-function (10) from the compliance to the strict avalanche criterion in each direction of weight $\varpi(u)=1$

$$\begin{array}{lcccc} & \Delta K^0_{DFfour_1} & \Delta K^1_{DFfour_1} & \Delta K^2_{DFfour_1} & \Delta K^3_{DFfour_1} \\ \Delta K_{D_{0001}Ffour_1} & 5 & 9 & 9 & 5 \\ \Delta K_{D_{0010}Ffour_1} & 10 & 6 & 2 & 2 \\ \Delta K_{D_{0100}Ffour_1} & 2 & 9 & 4 & 7 \\ \Delta K_{D_{1000}Ffour_1} & 3 & 12 & 3 & 6 \\ \Delta K_{D_{0002}Ffour_1} & 0 & 2 & 4 & 2 \\ \Delta K_{D_{0020}Ffour_1} & 0 & 6 & 12 & 6 \\ \Delta K_{D_{0200}Ffour_1} & 14 & 6 & 2 & 6 \\ \Delta K_{D_{2000}Ffour_1} & 2 & 2 & 2 & 2 \\ \Delta K_{D_{0003}Ffour_1} & 5 & 5 & 9 & 9 \\ \Delta K_{D_{0030}Ffour_1} & 10 & 2 & 2 & 6 \\ \Delta K_{D_{0300}Ffour_1} & 2 & 7 & 4 & 9 \\ \Delta K_{D_{3000}Ffour_1} & 3 & 6 & 3 & 12 \end{array}\ . \tag{14}$$

It is clear that the overall quality of the component 3-function is determined by the largest value among the deviations (14), which is equal in our case to $\Delta_{\max}K_{DFfour_1}=14$, while the overall quality of the S-box will be determined by the maximum among the maximum deviations of its component functions, in our case $\Delta_{\max}K_{DFfour_i}=\max\{14,14,16,16\}=16$, $i=1,2,...,4$.

Another way to characterize the integral deviation of the derivative (11) from the compliance with the conditions of the propagation criterion (Definition 8) is to use the quantity

$$\Delta K_{D_{0001}Ffour_1}=\sum_{i=0}^{3}\Delta K^i_{D_{0001}Ffour_1}=5+9+9+5=28. \tag{15}$$

Similarly, we can find the sum of deviations in all directions of the weight $\varpi(u)=1$ of the component 4-function (10) of the S-box (9), as required by Definition 10 of the strict avalanche criterion

$$\Delta K_{DFfour_1}=\sum_{j=1}^{12}\sum_{i=0}^{3}\Delta K^i_{D_jFfour_1}=256. \tag{16}$$

We can also calculate the sum of deviations from the SAC for each of the four component 4-functions of the S-box

$$\Delta K_{DFfour} = \sum_{l=1}^{4}\sum_{j=1}^{12}\sum_{i=0}^{3} \Delta K^{i}_{D_j Ffour_l} = 1040\,. \qquad (17)$$

In the Table 1 we represent the data on the avalanche characteristics of Nyberg construction S-boxes built on the basis of a full set of irreducible polynomials of order $k = 8$ represented in the form of Boolean functions, 4-functions, and 16-functions

Table 1.

Deviation from the SAC criterion values for the component functions of Nyberg construction S-boxes

No.	Polynomial	Case of Boolean functions		Case of 4-functions		Case of 16-functions	
		$\Delta_{\max}K_{DFbin}$	ΔK_{DFbin}	$\Delta_{\max}K_{DFfour}$	ΔK_{DFfour}	$\Delta_{\max}K_{DFhex}$	ΔK_{DFhex}
1	285	**12**	516	16	1040	11	2848
2	299	16	428	17	992	11	2836
3	301	16	488	13	764	14	2644
4	333	16	464	16	924	12	2704
5	351	16	556	18	952	11	2820
6	355	16	408	13	848	12	2724
7	357	16	404	18	896	15	2844
8	361	16	480	18	892	**10**	2916
9	369	**12**	388	14	768	13	2732
10	391	**12**	432	16	960	12	2992
11	397	16	456	**12**	960	12	2772
12	425	16	444	16	868	14	2948
13	451	**12**	408	**12**	**684**	15	2856
14	463	16	496	15	820	13	2924
15	487	**12**	**360**	14	964	11	2700
16	501	16	440	16	944	13	2872
17	283	**12**	376	**12**	748	12	2724
18	313	16	424	20	924	11	2836
19	319	16	*376*	14	*760*	14	*2676*
20	375	16	364	16	796	11	2668
21	379	16	512	20	988	**10**	2764
22	395	**12**	416	16	888	11	2920
23	415	**12**	416	15	796	12	2716
24	419	16	536	14	1040	15	2900
25	433	16	520	**12**	1028	14	2872
26	445	16	464	16	860	13	2628
27	471	**12**	472	18	912	13	2840
28	477	16	504	14	820	12	**2556**
29	499	**12**	440	20	976	14	2744
30	505	16	412	18	912	12	2984

It is clear that the indicator of the high quality of the cryptographic construction is the minimal value of $\Delta_{\max}K_{DF} \to \min$, as well as the value $\Delta K_{DF} \to \min$. Analysis of the data presented in Table 1 shows that the Nyberg construction S-box, which is built on the basis of a polynomial $f_{15}(x) = 487$, is characterized by the smallest deviation from the requirements of the strict avalanche criterion of component Boolean functions. At the same time, the Nyberg construction S-box based on a polynomial $f_{13}(x) = 451$ is characterized by the smallest deviation from the requirements of the strict avalanche criterion of component 4-functions. Moreover, Nyberg construction S-box based on polynomial $f_{28}(x) = 477$ is characterized by the smallest deviation from the requirements of the strict avalanche criterion of component 16-functions.

Note that from a practical point of view, the optimal S-box should converge the SAC requirements in the best way from the point of view of any possible representation of the many-valued logic functions. In the case of the Nyberg construction S-boxes, the S-box built on the basis of polynomial $f_{19}(x) = 319$, is the best in terms of satisfying the strict avalanche criterion from the point of view of any possible representation by many-valued logic functions and can be recommended for use in cryptographic applications.

References

The research of the S-boxes of AES cryptographic algorithm showed their unconformity with the conditions of strict avalanche criterion in terms of representations in the form of component Boolean functions, 4-functions, and 16-functions. It was established that the various irreducible polynomials used to construct the Nyberg construction S-boxes give different values of the deviation of the derivatives of the component *q*-functions from the requirements of the strict avalanche criterion.

We determined the irreducible polynomials that lead to the formation of Nyberg construction S-boxes, which are characterized by the smallest deviation of the derivatives of component *q*-functions from the compliance with the SAC requirements, both for the case of Boolean functions and for the case of 4-functions and 16-functions.

It has been established that the Nyberg construction S-box on the basis of the polynomial $f_{19}(x) = 319$ is characterized by the smallest deviation from the requirements of the strict avalanche criterion from the point of view of any possible representation by many-valued logic functions. Thus, the specified S-box can be recommended for practical use.

References

1. Shannon, C.E. A Mathematical Theory of Cryptography / C.E. Shannon. – Bell System Technical Memo MM 45-110-02., 1945. – 132 p.
2. Nyberg, K. Differentially uniform mappings for cryptography. Advances in cryptology / K. Nyberg. – Proc. of EUROCRYPT'93. Berlin, Heidelberg, Lecture Notes in Compuer Springer-Verlag, New York, 1994. – Vol.765. – Pp. 55-65.
3. FIPS 197. [Electronic resource] / Advanced encryption standard // Access mode: http://csrc.nist.gov/publications/
4. Жданов, О.Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. – М.: ИНФРА-М, 2013. – С. 90.
5. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров / А.В. Соколов. – Lap Lambert Academic Publishing, Germany, 2015. – 100 с.
6. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Радіотехніка: всеукр. міжвідом. наук.-техн. зб. – Харків, 2004 . – Т.126. – С. 132-138.
7. Мазурков, М.И. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов / М.И. Мазурков, А.В. Соколов // Одеський політехнічний університет. Праці. – 2012. – Т.39, №2. – С. 183-189.

8. Sokolov, A.V. Prospects for the Application of Many-Valued Logic Functions in Cryptography / A.V. Sokolov, O.N. Zhdanov. – International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018. – Pp. 331-339.
9. Мазурков, М.И. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / М.И. Мазурков, Е.А. Конопака // Радиоэлектроника. – 2005. – № 11. – С. 58-65.
10. Жданов, О.Н. О распространении конструкции Ниберг на поля Галуа нечетной характеристики / О.Н Жданов, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2017. – Т. 60, № 12. – С. 696-703.
11. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М: Издательство МЦНМО, 2004. – 472 с.
12. Sokolov, A.V. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength / A.V. Sokolov, O.N. Zhdanov // Siberian Journal of Science and Technology. – 2019. – Vol. 20, No. 2. – Pp. 183-190.

ЛАВИННІ ХАРАКТЕРИСТИКИ S-БЛОКІВ КОНСТРУКЦІЇ НІБЕРГ, ПРИ ЇХ УЯВЛЕННІ ЗА ДОПОМОГОЮ ФУНКЦІЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

А.В. Соколов, В.В. Радуш

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Одним з найбільш поширених сьогодні криптографічних алгоритмів є криптоалгоритм Advanced Encryption Standard (AES), в якому в якості S-блока використовується конструкція Ніберг. Існуючий підхід до оцінки криптографічної якості S-блоків, зокрема, конструкції Ніберг, заснований на їх описі за допомогою математичного апарату булевих функцій. При цьому, одним з найважливіших критеріїв криптографічної якості є суворий лавинний критерій компонентних булевих функцій. Проте, криптоаналітик не обмежений у виборі способу опису конструкцій шифру, що обумовлює необхідність дослідження криптографічних властивостей S-блоків конструкції Ніберг, представлених за допомогою функцій багатозначної логіки. Дана робота присвячена дослідженню лавинних характеристик S-блоків конструкції Ніберг, представлених за допомогою булевих функцій, 4-функцій і 16-функцій. При цьому розглядаються S-блоки конструкції Ніберг практично цінної довжини N=256 на основі повної множини незвідних поліномів восьмого степеню. Встановлено, що лавинні властивості S-блока конструкції Ніберг залежать від конкретного виду використаного для його побудови незвідного полінома. Знайдено незвідні поліноми, що забезпечують найкращі лавинні властивості S-блоків конструкції Ніберг в сенсі булевих функцій, 4-функцій, а також 16-функцій. При цьому встановлено, що S-блок на основі незвідного полінома $f_{19}(x)=319$ характеризується оптимальним відхиленням від вимог суворого лавинного критерію з точки зору будь-якого можливого подання функціями багатозначної логіки, таким чином, може бути рекомендований до практичного застосування.

Ключові слова: S-блок, конструкція Ніберг, суворий лавинний критерій, багатозначна логіка.

ЛАВИННЫЕ ХАРАКТЕРИСТИКИ S-БЛОКОВ КОНСТРУКЦИИ НИБЕРГ ПРИ ИХ ПРЕДСТАВЛЕНИИ С ПОМОЩЬЮ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А.В. Соколов, В.В. Радуш

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Одним из наиболее распространенных сегодня криптографических алгоритмов является криптоалгоритм Advanced Encryption Standard (AES), в котором в качестве S-блока используется конструкция Ниберг. Существующий подход к оценке криптографического качества S-блоков, в частности, конструкции Ниберг, основан на их описании с помощью математического аппарата булевых функций. При этом, одним из важнейших критериев криптографического качества является строгий лавинный критерий компонентных булевых функций. Тем не менее, криптоаналитик не стеснен в выборе способа описания конструкций шифра, что обуславливает необходимость исследования криптографических свойств S-блоков конструкции Ниберг, представленных с помощью функций многозначной логики. Данная работа посвящена исследованию лавинных характеристик S-блоков конструкции Ниберг, представленных с помощью булевых функций, 4-функций и 16-функций. При этом рассматриваются S-блоки конструкции Ниберг практически ценной длины N=256 на основе полного множества неприводимых полиномов восьмой степени. Установлено, что лавинные свойства S-блока конструкции Ниберг зависят от конкретного вида использованного для его построения неприводимого полинома. Найдены неприводимые полиномы, обеспечивающие наилучшие лавинные свойства S-блоков конструкции Ниберг в смысле булевых функций, 4-функций, а также 16-функций. При этом установлено, что S-блок на основе неприводимого полинома $f_{19}(x)=319$ характеризуется оптимальным отклонением от требований строгого лавинного критерия с точки зрения любого возможного представления функциями многозначной логики, таким образом, может быть рекомендован к практическому применению.

Ключевые слова: S-блок, конструкция Ниберг, строгий лавинный критерий, многозначная логика.