UDC 004.056.55
Doi: 10.31772/2587-6066-2019-20-2-183-190

For citation: Sokolov A. V., Zhdanov O. N. [Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength] *Siberian Journal of Science and Technology.* 2019, Vol. 20, No. 2, P. 183–190. Doi: 10.31772/2587-6066-2019-20-2-183-190

Для цитирования: Соколов А. В., Жданов О. Н. Строгий лавинный критерий функций четырехзначной логики как характеристика стойкости криптоалгоритмов // Сибирский журнал науки и технологий. 2019. Т. 20, № 2. С. 183–190. Doi: 10.31772/2587-6066-2019-20-2-183-190

STRICT AVALANCHE CRITERION OF FOUR-VALUED FUNCTIONS AS THE QUALITY CHARACTERISTIC OF CRYPTOGRAPHIC ALGORITHMS STRENGTH

A. V. Sokolov[1], O. N. Zhdanov[2]

[1]Odessa National Polytechnic University
1, Shevchenko Av., Odessa, 65044, Ukraine
[2]Reshetnev Siberian State University of Science and Technology
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
E-mail: onzhdanov@mail.ru

The S-box is the most important component of modern cryptographic algorithms which largely determines the quality of cryptographic transformation. The modern method of estimating the S-boxes quality employs their representation as component Boolean functions to which cryptographic quality criteria are applied. Such criteria include: nonlinearity, correlation immunity, an error propagation criterion, and a strict avalanche criterion. Nevertheless, it is obvious that a cryptanalyst is not constrained in the ways of representing the cipher components, in particular, using the functions of many-valued logic. The design features of modern cryptographic algorithms allow their representation in the form of 4-logic functions, which determines the need to research cryptographic properties of the S-boxes represented as component 4-functions. In the literature today there are methods for measuring the nonlinearity of 4-functions; nevertheless, there are no similar methods for researching the differential properties of 4-functions, in particular, involving their compliance with the strict avalanche criterion. In this paper the strict avalanche criterion is generalized to the case of 4-functions and the compliance of the S-boxes component 4-functions of the "Magma" cryptoalgorithm to the strict avalanche criterion has been researched. All balanced 4-functions of length N = 16 satisfying the strict avalanche criterion were synthesized using the restricted brute-force method. The basic properties of the constructed class of 4-functions are determined, and bijective S-boxes based on them are constructed. It has been established that S-boxes of length N = 16 satisfying the strict avalanche criterion, both in terms of component Boolean functions and in terms of 4-functions, also possess optimal nonlinear properties. This circumstance allows us to recommend S-boxes satisfying the strict avalanche criterion of component 4-functions for use in modern cryptographic algorithms.

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

СТРОГИЙ ЛАВИННЫЙ КРИТЕРИЙ ФУНКЦИЙ ЧЕТЫРЕХЗНАЧНОЙ ЛОГИКИ КАК ХАРАКТЕРИСТИКА СТОЙКОСТИ КРИПТОАЛГОРИТМОВ

А. В. Соколов[1], О. Н. Жданов[2]

[1]Одесский национальный политехнический университет
Украина, 65044, г. Одесса, просп. Шевченко, 1
[2]Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: onzhdanov@mail.ru

Важнейшим компонентом современных криптографических алгоритмов, который во многом определяет качество криптопреобразования, является S-блок. Современная методика оценки качества S-блоков предполагает их представление в виде компонентных булевых функций, к которым применяются критерии криптографического качества, такие как нелинейность, критерий распространения ошибки, строгий лавинный критерий, корреляционный иммунитет. Тем не менее очевидным является тот факт, что криптоаналитик не стеснен в способах представления компонент шифра, в частности и с помощью функций многозначной логики. Конструктивные особенности современных криптоалгоритмов допускают их представление в виде функций 4-логики, что диктует необходимость исследования криптографических свойств S-блоков, представленных *в виде компонентных 4-функций. В литературе сегодня имеются методы измерения нелинейности 4-функций, тем не менее отсутствуют подобные методы для изучения дифференциальных свойств 4-функций, в частности, их соответствия строгому лавинному критерию. В настоящей статье строгий лавинный критерий обобщен на случай 4-функций, проведены исследования соответствия строгому лавинному критерию компонентных 4-функций S-блоков криптоалгоритма «Магма». Методом ограниченного перебора синтезированы все сбалансированные 4-функции длины N = 16, удовлетворяющие строгому лавинному критерию. Определены базовые свойства построенного класса 4-функций, а также построены биективные S-блоки на их основе. Установлено, что S-блоки длины N = 16, удовлетворяющие строгому лавинному критерию как с точки зрения компонентных булевых функций, так и с точки зрения 4-функций, обладают также оптимальными нелинейными свойствами. Данное обстоятельство позволяет рекомендовать S-блоки, удовлетворяющие строгому лавинному критерию компонентных 4-функций, к использованию в современных криптоалгоритмах.*

Ключевые слова: функции многозначной логики, строгий лавинный критерий, S-блок.

Introduction and problem formulation. The problem of further improvement of modern cryptographic information protection systems is closely related to the tasks of constructing higher quality cryptographic primitives. In many ways the strength of a symmetric cryptographic algorithm is determined by a substitution box (*S*-box) [1].

Currently, the quality of *S*-boxes is determined by the following main criteria for cryptographic quality [2]:

1. The algebraic degree of nonlinearity.
2. The distance of nonlinearity.
3. The error propagation criterion, a particular case of which is the strict avalanche criterion (SAC), as well as the criterion of maximum avalanche effect.
4. The matrix of the correlation coefficients of the S-box output and input, as well as the associated criterion of the component Boolean functions correlation immunity.

All of these criteria are based on the representation of the *S*-box as a set of Boolean functions. However, other mathematical constructions describing a cryptoalgorithm, in particular, the apparatus of many-valued logic functions can be used to launch an attack.

This circumstance requires the research of all possible forms of *S*-boxes representation, in particular, using the component functions of many-valued logic.

The cryptoalgorithms used in practice often have S-boxes of length N multiple of 4, for example, $N = 16$ as in the “Magma” cryptoalgorithm [3] or $N = 256$ as in the Nyberg S-boxes [4; 5] in the AES cryptoalgorithm [6]. Thus, the research of the cryptographic quality of S-boxes represented as component 4-functions is of practical value.

The 4-nonlinearity criterion for S-boxes was introduced and a method for synthesizing S-boxes with a maximum 4-nonlinearity value was proposed in [7] on the basis of the Vilenkin–Chrestenson transformation. However, at present in the literature there is no definition of the strict avalanche criterion as applied to the representation of S-boxes as 4-logic functions.

This paper is devoted to the research of the strict avalanche criterion of 4-functions, as well as the synthesis of S-boxes whose component 4-functions satisfy the strict avalanche criterion.

The propagation criterion of the Boolean functions. The strict avalanche criterion is one of the main criteria which characterize resistance to differential cryptanalysis [8]. Methods for the synthesis of S-boxes that satisfy the strict avalanche criterion are practically in demand, and well-known [8–10].

The research of the Boolean function compliance with the strict avalanche criterion is based on the following definitions.

Definition 1 [11]. A derivative in the direction $u \in V_n$ of the Boolean function f is the Boolean function

$$D_u f(x) = f(x) \oplus f(x \oplus u), \qquad (1)$$

where V_n is the linear vector space of binary vectors of length n, $\oplus$ is the modulo 2 addition.

Definition 2 [11]. The Boolean function $f(x)$ satisfies the propagation criterion with respect to the vector $u \in V_n$ – $PC(u)$ if its derivative in the direction u is a balanced function, i. e.

$$p\{f(x) = f(x \oplus u)\} = 0{,}5. \qquad (2)$$

Definition 3 [11]. The Boolean function $f(x)$ satisfies the propagation criterion of the degree k – $PC(k)$ if it satisfies the propagation criterion $PC(u)$ with respect to all vectors u of weight $1 \le wt(u) \le k$, i. e.

$$p\{f(x) = f(x \oplus u)\} = 0{,}5, \quad \forall u \in V_n, \quad 1 \le wt(u) \le k. \qquad (3)$$

Definition 4 [11]. The Boolean function f satisfies the strict avalanche criterion (SAC) if it satisfies the propagation criterion of the degree 1 – $PC(1)$

$$p\{f(x) = f(x \oplus u)\} = 0{,}5, \quad \forall u \in V_n, \quad wt(u) = 1. \qquad (4)$$

Let us consider the S-box synthesized in [10] and its decomposition into component Boolean functions

$$S = \left\{ \begin{array}{cccccccccccccccc} 4 & 7 & 2 & 14 & 1 & 13 & 8 & 11 & 15 & 12 & 6 & 10 & 5 & 9 & 3 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{array} \right\}. \qquad (5)$$

Let us give an example of researching the Boolean function of four variables which is the first component function of the S-box (5) on compliance with the strict avalanche criterion

$$f(x_1, x_2, x_3, x_4) = \\ = \{0 \;\; 1 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 0 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 0\}. \qquad (6)$$

Table 1

Example of finding derivatives of the Boolean function

$f(X)$	$f(X\oplus 0001)$	$D_{0001}f$	$f(X\oplus 0010)$	$D_{0010}f$	$f(X\oplus 0100)$	$D_{0100}f$	$f(X\oplus 1000)$	$D_{1000}f$
$f(0000)=0$	$f(0001)=1$	1	$f(0010)=0$	0	$f(0100)=1$	1	$f(1000)=1$	1
$f(0001)=1$	$f(0000)=0$	1	$f(0011)=0$	1	$f(0101)=1$	0	$f(1001)=0$	1
$f(0010)=0$	$f(0011)=0$	0	$f(0000)=0$	0	$f(0110)=0$	0	$f(1010)=0$	0
$f(0011)=0$	$f(0010)=0$	0	$f(0001)=1$	1	$f(0111)=1$	1	$f(1011)=0$	0
$f(0100)=1$	$f(0101)=1$	0	$f(0110)=0$	1	$f(0000)=0$	1	$f(1100)=1$	0
$f(0101)=1$	$f(0100)=1$	0	$f(0111)=1$	0	$f(0001)=1$	0	$f(1101)=1$	0
$f(0110)=0$	$f(0111)=1$	1	$f(0100)=1$	1	$f(0010)=0$	0	$f(1110)=1$	1
$f(0111)=1$	$f(0110)=0$	1	$f(0101)=1$	0	$f(0011)=0$	1	$f(1111)=0$	1
$f(1000)=1$	$f(1001)=0$	1	$f(1010)=0$	1	$f(1100)=1$	0	$f(0000)=0$	1
$f(1001)=0$	$f(1000)=1$	1	$f(1011)=0$	0	$f(1101)=1$	1	$f(0001)=1$	1
$f(1010)=0$	$f(1011)=0$	0	$f(1000)=1$	1	$f(1110)=1$	1	$f(0010)=0$	0
$f(1011)=0$	$f(1010)=0$	0	$f(1001)=0$	0	$f(1111)=0$	0	$f(0011)=0$	0
$f(1100)=1$	$f(1101)=1$	0	$f(1110)=1$	0	$f(1000)=1$	0	$f(0100)=1$	0
$f(1101)=1$	$f(1100)=1$	0	$f(1111)=0$	1	$f(1001)=0$	1	$f(0101)=1$	0
$f(1110)=1$	$f(1111)=0$	1	$f(1100)=1$	0	$f(1010)=0$	1	$f(0110)=0$	1
$f(1111)=0$	$f(1110)=1$	1	$f(1101)=1$	1	$f(1011)=0$	0	$f(0111)=1$	1

To do this, in accordance with ***Definition 3*** and ***Definition 4***, we need to find the derivatives of the Boolean function (6) in all directions of the Hamming weight $wt(u)=1$, i.e. in directions $\{001\}$, $\{010\}$ and $\{001\}$. The results are shown in tab. 1.

The presented results lead to the conclusion: all derivatives $D_i f$ are balanced, i.e. $wt(D_i f)=N/2$, where N is the length of the truth table of the Boolean function. Thus, the Boolean function (6) satisfies the SAC.

Extension of the strict avalanche criterion to the case of 4-functions. However, in the case of attacking the cryptographic algorithm a cryptanalyst is not constrained by the means used and can use the approximation of cipher elements by any available means including methods of many-valued logic as it is shown in research carried out in [12]. Thus, when constructing S-boxes it makes sense to consider not only binary affine functions, but also affine functions of many-valued logic through which the S-box of a given size can be represented.

Definition 5 [13]. The mapping $\{0,1,2,...,q-1\}^n \to \{0,1,2,...,q-1\}$ is called the function of the q-valued logic of n variables.

Definition 5 is the definition of Boolean functions when $q=2$. ***Definition 5*** is the definition of 4-functions as mappings $\{0,1,2,3\}^k \to \{0,1,2,3\}$ when $q=4$. Thus, a 4-function is a rule that uniquely associates the vector of k coordinates that take values 0, 1, 2, 3 with a value of 0, 1, 2 or 3.

For example, the *S*-box (5) can be represented using two component 4-functions

$$S=\left\{\begin{array}{cccccccccccccccc} 4 & 7 & 2 & 14 & 1 & 13 & 8 & 11 & 15 & 12 & 6 & 10 & 5 & 9 & 3 & 0 \\ \hline 0 & 3 & 2 & 2 & 1 & 1 & 0 & 3 & 3 & 0 & 2 & 2 & 1 & 1 & 3 & 0 \\ 1 & 1 & 0 & 3 & 0 & 3 & 2 & 2 & 3 & 3 & 1 & 2 & 1 & 2 & 0 & 0 \end{array}\right\}, \tag{7}$$

the cryptographic properties of which also determine the properties of the S-box itself but at the level of quaternary logic.

We propose a general scheme for which the Boolean function and 4-function will be special cases.

Let us consider the q-function of n variables $f(x)$. Let $u=(u_1,u_2,...,u_n)$.

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

Definition 7. The derivative of the function f with respect to the direction of the vector u is the function

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

where $\underset{q}{\oplus}$ means the modulo q addition.

Definition 8. The function of q-valued logic $f(x)$ satisfies the propagation criterion with respect to the vector $u \in V_n$ – $PC(u)$ if its derivative in the direction u is a balanced function, i. e. values $0,1,...,q-1$ are taken with equal probabilities: $p(D_u f(x)=i(\mathrm{mod}\,q))=\dfrac{1}{q}$ 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 variable values for which the derivative takes the value i.

Definition 9. The function of q-valued logic $f(x)$ satisfies the propagation criterion of degree k – $PC(k)$ if it satisfies the propagation criterion $PC(u)$ with respect to all vectors u of weight $1 \le \varpi(u) \le k$.

Definition 10. The function of q-valued logic $f(x)$ satisfies the strict avalanche criterion (SAC) if it satisfies the propagation criterion of degree 1 – $PC(1)$.

In accordance with the definitions introduced, we consider the example of researching the first

4-function of the S-box (7) for compliance with the strict avalanche criterion.

Data analysis in tab. 2 allows us to say that the first component 4-function of the S-box (7) does not satisfy the strict avalanche criterion. Thus*, being optimal in terms of the strict avalanche criterion in a binary sense, the S-box (7) is not optimal in terms of the strict avalanche criterion in a quaternary sense.*

We illustrate our reasoning with examples of well-known cryptoalgorithms.

Research of *S*-boxes of the “Magma” cryptographic algorithm. The approach in which S-boxes were considered as a long-term key was used in the common GOST 28147–89 cryptoalgorithm. In the new edition of the standard GOST R 34.12–2015 the following set of S-boxes was defined [3]

$$S=\begin{bmatrix} 12 & 4 & 6 & 2 & 10 & 5 & 11 & 9 & 14 & 8 & 13 & 7 & 0 & 3 & 15 & 1 \\ 6 & 8 & 2 & 3 & 9 & 10 & 5 & 12 & 1 & 14 & 4 & 7 & 11 & 13 & 0 & 15 \\ 11 & 3 & 5 & 8 & 2 & 15 & 10 & 13 & 14 & 1 & 7 & 4 & 12 & 9 & 6 & 0 \\ 12 & 8 & 2 & 1 & 13 & 4 & 15 & 6 & 7 & 0 & 10 & 5 & 3 & 14 & 9 & 11 \\ 7 & 15 & 5 & 10 & 8 & 1 & 6 & 13 & 0 & 9 & 3 & 14 & 11 & 4 & 2 & 12 \\ 5 & 13 & 15 & 6 & 9 & 2 & 12 & 10 & 11 & 7 & 8 & 1 & 4 & 3 & 14 & 0 \\ 8 & 14 & 2 & 5 & 6 & 9 & 1 & 12 & 15 & 4 & 11 & 0 & 13 & 10 & 3 & 7 \\ 1 & 7 & 14 & 13 & 0 & 5 & 8 & 3 & 4 & 15 & 10 & 6 & 9 & 12 & 11 & 2 \end{bmatrix}. \tag{9}$$

Tab. 3 shows the values of the basic criteria for the cryptographic quality of S-boxes (9).

The data analysis in tab. 3 dictates the need for further improvement of the substitution constructions of the cryptoalgorithm “Magma” and similar ones.

Table 2

Example of finding the derivative of 4-function

$f(X)$	$u=01$	$D_{01}f$	$u=02$	$D_{02}f$	$u=03$	$D_{03}f$	$u=10$	$D_{10}f$	$u=20$	$D_{20}f$	$u=30$	$D_{30}f$
$f(00)=0$	3	3	2	2	2	2	1	1	3	3	1	1
$f(01)=3$	2	3	2	3	0	1	1	2	0	1	1	2
$f(02)=2$	2	0	0	2	3	1	0	2	2	0	3	1
$f(03)=2$	0	2	3	1	2	0	3	1	2	0	0	2
$f(10)=1$	1	0	0	3	3	2	3	2	1	0	0	3
$f(11)=1$	0	3	3	2	1	0	0	3	1	0	3	2
$f(12)=0$	3	3	1	1	1	1	2	2	3	3	2	2
$f(13)=3$	1	2	1	2	0	1	2	3	0	1	2	3
$f(20)=3$	0	1	2	3	2	3	1	2	0	1	1	2
$f(21)=0$	2	2	2	2	3	3	1	1	3	3	1	1
$f(22)=2$	2	0	3	1	0	2	3	1	2	0	0	2
$f(23)=2$	3	1	0	2	2	0	0	2	2	0	3	1
$f(30)=1$	1	0	3	2	0	3	0	3	1	0	3	2
$f(31)=1$	3	2	0	3	1	0	3	2	1	0	0	3
$f(32)=3$	0	1	1	2	1	2	2	3	0	1	2	3
$f(33)=0$	1	1	1	1	3	3	2	2	3	3	2	2

Table 3

The values of the main criteria for the cryptographic quality of the “Magma” cryptoalgorithm *S*-boxes

S-box	Algebraic degree of nonlinearity deg(S)	Nonlinearity distance SNl	Maximum absolute values of the matrix of correlation coefficients $\max\limits_{i,j}\{\lvert c_{i,j}\rvert\}$	Compliance with the SAC in a binary sense	Compliance with the SAC in a quaternary sense
S_1	2	4	0.5	–	–
S_2	2	4	0.5	–	–
S_3	3	4	0.5	–	–
S_4	3	4	0.25	–	–
S_5	2	4	0.5	–	–
S_6	3	4	0.5	–	–
S_7	2	4	0.5	–	–
S_8	3	4	0.5	–	–

Experimental search for S-boxes satisfying SAC in a quaternary sense. The problem of finding S-boxes that satisfy the SAC in a quaternary sense is important from a practical point of view. Nevertheless, we note that even the search for 4-functions of length $N = 16$ (that is, the smallest of those having practical sense) satisfying the SAC in a quaternary sense is associated with considerable computational difficulties because the number of 4-functions of this length is 4 294 967 296.

However, it is known that the construction of bijective S-boxes is possible only on the basis of balanced 4-functions [14].

Obviously, the total number of balanced 4-functions of length $N = 16$ is $J = C_{16}^4 \cdot C_{12}^4 \cdot C_8^4 \cdot C_4^4 =$ $1820 \cdot 495 \cdot 70 \cdot 1 =$ $= 63063000$, which is significantly less than the total number of 4-functions of length $N = 16$.

We experimentally (by exhaustive search of all variants) established that in a given volume of balanced 4-functions there are 7680 functions satisfying the SAC in a quaternary sense.

Direct verification established the properties of the functions of this set.

Definition 11. Let us call a new sequence $T_2 = \{t_j\}$, $j = N-1, N-2, ..., 0$ a mirror image of the sequence $T1 = \{t_i\}$, $i = 0, 1, ..., N-1$.

Property 1. The sequence obtained as a result of mirroring a balanced sequence satisfying the SAC in a quaternary sense also satisfies the SAC in a quaternary sense.

For example, let us consider one of the 4-functions satisfying SAC in a quaternary sense

$$f_0 = \{0001023212312133\}. \qquad (10)$$

Performing its mirroring we obtain a new 4-function, which also satisfies the SAC in a quaternary sense

$$f_1 = \{3312132123201000\}. \qquad (11)$$

Property 2. Sequences obtained by applying the following 8 of the 24 possible single-valued mappings of the alphabet of the sequence satisfying the SAC in a quaternary sense also satisfies the SAC in a quaternary sense

$$\left\{\begin{matrix}0&1&2&3\\0&1&2&3\end{matrix}\right\};\quad \left\{\begin{matrix}0&1&2&3\\0&3&2&1\end{matrix}\right\};\quad \left\{\begin{matrix}0&1&2&3\\1&0&3&2\end{matrix}\right\};$$

$$\left\{\begin{matrix}0&1&2&3\\1&2&3&0\end{matrix}\right\};\quad \left\{\begin{matrix}0&1&2&3\\2&1&0&3\end{matrix}\right\};\quad \left\{\begin{matrix}0&1&2&3\\2&3&0&1\end{matrix}\right\}; \qquad (12)$$

$$\left\{\begin{matrix}0&1&2&3\\3&0&1&2\end{matrix}\right\};\quad \left\{\begin{matrix}0&1&2&3\\3&2&1&0\end{matrix}\right\}.$$

Let us consider an increasing sequence of non-negative integers from 0 to $n-1$

$$u = \{0, 1, 2, 3, ..., n-1\}. \qquad (13)$$

Definition 12 [15]. By the dyadic shift operator we shall mean the matrix of the size $n \times n$, each row of which is obtained in accordance with the following rule

$$Dyad_i(n) = u_i \oplus i, \qquad (14)$$

where the sign $\oplus$ means addition modulo 2.

Thus, the 16th order dyadic shift operator has the following form

$$Dyad(16) = \begin{bmatrix} 0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\ 1&0&3&2&5&4&7&6&9&8&11&10&13&12&15&14\\ 2&3&0&1&6&7&4&5&10&11&8&9&14&15&12&13\\ 3&2&1&0&7&6&5&4&11&10&9&8&15&14&13&12\\ 4&5&6&7&0&1&2&3&12&13&14&15&8&9&10&11\\ 5&4&7&6&1&0&3&2&13&12&15&14&9&8&11&10\\ 6&7&4&5&2&3&0&1&14&15&12&13&10&11&8&9\\ 7&6&5&4&3&2&1&0&15&14&13&12&11&10&9&8\\ 8&9&10&11&12&13&14&15&0&1&2&3&4&5&6&7\\ 9&8&11&10&13&12&15&14&1&0&3&2&5&4&7&6\\ 10&11&8&9&14&15&12&13&2&3&0&1&6&7&4&5\\ 11&10&9&8&15&14&13&12&3&2&1&0&7&6&5&4\\ 12&13&14&15&8&9&10&11&4&5&6&7&0&1&2&3\\ 13&12&15&14&9&8&11&10&5&4&7&6&1&0&3&2\\ 14&15&12&13&10&11&8&9&6&7&4&5&2&3&0&1\\ 15&14&13&12&11&10&9&8&7&6&5&4&3&2&1&0 \end{bmatrix}. \qquad (15)$$

Property 3. Sequences obtained by applying the dyadic shift operator to the original sequence satisfying the SAC in a quaternary sense also satisfies the SAC in a quaternary sense.

For example, the following 16 sequences that satisfy the SAC in a quaternary sense can be obtained by applying the dyadic shift operator (15) on the basis of the sequence (11) satisfying the SAC in a quaternary sense

$$\begin{array}{ll}
\{0001023212312133\}; & \{1231213300010232\}; \\
\{0010202321131233\}; & \{2113123300102023\}; \\
\{0100320231123321\}; & \{3112332101003202\}; \\
\{1000232013213312\}; & \{1321331210002320\}; \\
\{0232000121331231\}; & \{2133123102320001\}; \\
\{2023001012332113\}; & \{1233211320230010\}; \\
\{3202010033213112\}; & \{3321311232020100\}; \\
\{2320100033121321\}; & \{3312132123201000\}.
\end{array} \tag{16}$$

Definition 13. By the 4-shift operator we shall mean the matrix of the size $n \times n$ each row of which is obtained in accordance with the following rule

$$4ad(n) = u_i \underset{4}{\oplus} i, \tag{17}$$

where the sign $\underset{4}{\oplus}$ means addition modulo 4.

Thus, the 16th order 4-shift operator has the following form

$$4ad(16) = \begin{bmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
1 & 2 & 3 & 0 & 5 & 6 & 7 & 4 & 9 & 10 & 11 & 8 & 13 & 14 & 15 & 12 \\
2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 14 & 15 & 12 & 13 \\
3 & 0 & 1 & 2 & 7 & 4 & 5 & 6 & 11 & 8 & 9 & 10 & 15 & 12 & 13 & 14 \\
4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 & 1 & 2 & 3 \\
5 & 6 & 7 & 4 & 9 & 10 & 11 & 8 & 13 & 14 & 15 & 12 & 1 & 2 & 3 & 0 \\
6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 14 & 15 & 12 & 13 & 2 & 3 & 0 & 1 \\
7 & 4 & 5 & 6 & 11 & 8 & 9 & 10 & 15 & 12 & 13 & 14 & 3 & 0 & 1 & 2 \\
8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
9 & 10 & 11 & 8 & 13 & 14 & 15 & 12 & 1 & 2 & 3 & 0 & 5 & 6 & 7 & 4 \\
10 & 11 & 8 & 9 & 14 & 15 & 12 & 13 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\
11 & 8 & 9 & 10 & 15 & 12 & 13 & 14 & 3 & 0 & 1 & 2 & 7 & 4 & 5 & 6 \\
12 & 13 & 14 & 15 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
13 & 14 & 15 & 12 & 1 & 2 & 3 & 0 & 5 & 6 & 7 & 4 & 9 & 10 & 11 & 8 \\
14 & 15 & 12 & 13 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 \\
15 & 12 & 13 & 14 & 3 & 0 & 1 & 2 & 7 & 4 & 5 & 6 & 11 & 8 & 9 & 10
\end{bmatrix}. \tag{18}$$

Property 4. Sequences obtained by applying the 4-shift operator of the original sequence satisfying the SAC in a quaternary sense also satisfies the SAC in a quaternary sense.

For example, the following 16 sequences that satisfy the SAC in a quaternary sense can be obtained by applying the 4-shift operator (18) on the basis of the sequence (11) satisfying the SAC in a quaternary sense

$$\begin{array}{ll}
\{0001023212312133\}; & \{1231213300010232\}; \\
\{0010232023111332\}; & \{2311133200102320\}; \\
\{0100320231123321\}; & \{3112332101003202\}; \\
\{1000202311233213\}; & \{1123321310002023\}; \\
\{0232123121330001\}; & \{2133000102321231\}; \\
\{2320231113320010\}; & \{1332001023202311\}; \\
\{3202311233210100\}; & \{3321010032023112\}; \\
\{2023112332131000\}; & \{3213100020231123\}.
\end{array} \tag{19}$$

Table 4

Cryptographic properties of the proposed set of *S*-boxes

S-box	Algebraic degree of nonlinearity $\deg(S)$	Nonlinearity distance *SNl*	Maximum absolute values of the matrix of correlation coefficients $\max\limits_{i,j}\left\{\left\lvert c_{i,j}\right\rvert\right\}$	Compliance with the SAC in a binary sense	Compliance with the SAC in a quaternary sense
$S_1 \ldots S_8$	3	4	0.5	+	+

On the basis of the obtained 7680 balanced 4-functions which satisfy SAC in a quaternary sense it was possible to construct 245760 bijective S-boxes. 8192 of them simultaneously satisfy the SAC in a binary sense. It was established experimentally that in addition to compliance with the SAC in a quaternary and binary sense each of the 8192 built S-boxes of length $N = 16$ has the maximum nonlinearity distance $SNl = 4$, the algebraic degree of nonlinearity $\deg(S) = 3$, and the maximum absolute values of the correlation coefficient matrix $\max\limits_{i,j}\left\{\left\lvert c_{i,j}\right\rvert\right\} = 0.5$.

Thus, the high cryptographic quality of S-boxes simultaneously satisfying the SAC in a quaternary and in a binary sense is proven. It seems to us reasonable to recommend them for practical use in cryptoalgorithms, for example, in “Magma”. We present one of the possible replacement tables composed of the S-boxes constructed by us and satisfying the SAC in a quaternary and binary sense

$$S = \begin{bmatrix} 0 & 1 & 3 & 7 & 14 & 2 & 10 & 9 & 6 & 12 & 11 & 4 & 13 & 8 & 15 & 5 \\ 1 & 0 & 2 & 6 & 15 & 3 & 11 & 8 & 7 & 13 & 10 & 5 & 12 & 9 & 14 & 4 \\ 3 & 2 & 0 & 4 & 13 & 1 & 9 & 10 & 5 & 15 & 8 & 7 & 14 & 11 & 12 & 6 \\ 2 & 3 & 1 & 5 & 12 & 0 & 8 & 11 & 4 & 14 & 9 & 6 & 15 & 10 & 13 & 7 \\ 8 & 9 & 12 & 0 & 3 & 7 & 2 & 1 & 15 & 5 & 13 & 10 & 11 & 6 & 4 & 14 \\ 9 & 8 & 13 & 1 & 2 & 6 & 3 & 0 & 14 & 4 & 12 & 11 & 10 & 7 & 5 & 15 \\ 11 & 10 & 15 & 3 & 0 & 4 & 1 & 2 & 12 & 6 & 14 & 9 & 8 & 5 & 7 & 13 \\ 10 & 11 & 14 & 2 & 1 & 5 & 0 & 3 & 13 & 7 & 15 & 8 & 9 & 4 & 6 & 12 \end{bmatrix}. \quad (20)$$

Tab. 4 shows the cryptographic properties of the set of S-boxes proposed for practical use, which are the same for the entire set.

Conclusions. We note the main results obtained in the paper:

1. The strict avalanche criterion is extended to the case of functions of q-valued logic for an arbitrary value of *q*.

2. The S-boxes of the “Magma” cryptographic algorithm were researched. The research showed that they do no satisfy the strict avalanche criterion both in terms of Boolean functions and in terms of 4-logic functions.

3. All balanced 4-functions that satisfies the strict avalanche criterion were found experimentally. The class of S-boxes which satisfies the strict avalanche criterion both in terms of Boolean functions and in terms of 4-logic functions is constructed on the basis of the found set of 4-functions. These *S*-boxes also have the maximum possible distance of non-linearity and the algebraic degree of nonlinearity, as well as an acceptable level of correlation of the output and input vectors. Thus, the constructed *S*-boxes can be recommended for practical use including the use in the “Magma” cryptoalgorithm.

References

1. Zhdanov O. N. *Metodica vibora kluchevoi informacii dla algoritmov blochnoigo shifrovania* [The method of selecting key information for the block cipher algorithm]. Moscow, INFRA-M Publ, 2013, 97 p.

2. Sokolov A. V. New methods for synthesizing nonlinear transformations of modern ciphers. Germany, Lap Lambert Academic Publishing, 2015, 100 p.

3. GOST R 34.12–2015. *Kriptograficheskaya zashhita informacii blochnye shifry* [State Standard R 34.12–2015. Cryptographic information protection block ciphers]. Moscow, Standartinform Publ., 2015, P. 21.

4. Nyberg K. Differentially uniform mappings for cryptography. Advances in cryptology, Berlin, Heidelberg, New York, *Proc. of EUROCRYPT’93*, Lecture Notes in Compuer Springer Verlag, 1994, P. 55–65.

5. Mazurkov M. I., Sokolov A. V. [Cryptographic properties of the nonlinear transformation of the cipher Rijndael on the basis of complete classes of irreducible polynomials*]. Trudy Odesskogo politekhnicheskogo universiteta.* 2012, No. 2 (39), P. 183–189 (In Russ.).

6. FIPS 197. Advanced encryption standard. Available at: http://csrc.nist.gov/publications (accessed 07.06.2019).

7. Sokolov A. V., Krasota N. I. [Very nonlinear permutations: synthesis method for S-boxes with maximal 4-nonlinearity]. *Naukovi praczi ONAZ im. O. S. Popova.* 2017, No. 1, P. 145–154.

8. Kim K. Matsumoto T., Imai H. A recursive construction method of S-boxes satisfying strict avalanche criterion. *Proc. of CRYPTO’90*, Springer, Verlag, 1990, P. 565–574.

9. Gao S., Ma W., Shen D. Design of bijective S-boxes satisfying the strict avalanche criterion. *USA: Journal of computer information systems*. 2011, No. 6, P. 1967–1973.

10. Sokolov A. V. [Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion]. *Izvestiya vysshikh uchebnykh zavedeniy. Radioelektronika.* 2013, Vol. 56, No. 8, P. 43–52 (In Russ.).

11. Logachev O. A., Salnikov A. A., Yashhenko V. V. *Bulevy funkcii v teorii kodirovaniya i kriptologii* [Boolean functions in coding theory and cryptology]. Moscow, MCzNMO Publ., 2004, 472 p.

12. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptog-

raphy. *International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, Springer, Cham*. 2018, P. 331–339.

13. Zhdanov O. N., Sokolov A. V. [Extending Nyberg construction on Galois fields of odd characteristic]. *Izvestiya vysshikh uchebnykh zavedeniy. Radioelektronika.* 2017, Vol. 60, No. 12, P. 696–703 (In Russ.).

14. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. *Proc. of Asiacrypt'91*. Springer Verlag, 1991, P. 59–72.

15. Mazurkov M. I., Sokolov A. V. [Fast orthogonal transforms based on bent-sequences]. *Informatika ta matematichni metodi v modelyuvanni*. 2014, No. 1, P. 5–13.

Библиографические ссылки

1. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М. : ИНФРА-М, 2013. 97 с.

2. Sokolov A. V. New methods for synthesizing nonlinear transformations of modern ciphers. Germany, Lap Lambert Academic Publishing, 2015, 100 p.

3. ГОСТ Р 34.12–2015 Криптографическая защита информации. Блочные шифры. М. : Стандартинформ, 2015. 21 с.

4. Nyberg K. Differentially uniform mappings for cryptography. Advances in cryptology // Proc. of EUROCRYPT'93. Berlin, Heidelberg, New York. Lecture Notes in Compuer Springer-Verlag. 1994. Vol. 765. P. 55–65.

5. Мазурков М. И., Соколов А. В. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов // Тр. Одесского политехн. ун-та. 2012. № 2(39). С. 183–189.

6. FIPS 197. Advanced encryption standard [Электронный ресурс]. URL: http://csrc.nist.gov/publications (дата обращения: 07.06.2019).

7. Соколов А. В., Красота Н. И. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью // Наукові праці ОНАЗ ім. О. С. Попова. 2017. № 1. С. 145–154.

8. Kim K. Matsumoto T., Imai H. A recursive construction method of S-boxes satisfying strict avalanche criterion // Proc. of CRYPTO'90, Springer, Verlag. 1990. P. 565–574.

9. Gao S., Ma W., Shen D. Design of bijective S-boxes satisfying the strict avalanche criterion // USA: Journal of computer information systems. 2011, № 6. P. 1967–1973.

10. Соколов А. В. Конструктивный метод синтеза нелинейных S-блоков подстановки, соответствующих строгому лавинному критерию // Известия высших учебных заведений. Радиоэлектроника. 2013. Т. 56, № 8. С. 43–52.

11. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М. : МЦНМО, 2004. 472 с.

12. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, Springer, Cham. 2018. P. 331–339.

13. Жданов О. Н., Соколов А. В. О распространении конструкции Ниберг на поля Галуа нечетной характеристики // Известия высших учебных заведений. Радиоэлектроника. 2017. Т. 60, № 12. С. 696–703.

14. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC // Proc. of Asiacrypt'91, Springer Verlag. 1991. P. 59–72.

15. Мазурков М. И., Соколов А. В. Быстрые ортогональные преобразования на основе бент-последовательностей // Інформатика та математичні методи в моделюванні. 2014. № 1. P. 5–13.

Sokolov Artem Viktorovich – Cand. Sc., Senior Lecturer of the Department of Informatics and Information Security Management; Odessa National Polytechnic University. E-mail: radiosquid@gmail.com.

Zhdanov Oleg Nikolaevich – Cand. Sc., Associate Professor at the Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: onzhdanov@mail.ru.

Соколов Артем Викторович – кандидат технических наук, старший преподаватель кафедры информатики и управления защитой информационных систем; Одесский национальный политехнический университет. E-mail: radiosquid@gmail.com.

Жданов Олег Николаевич – кандидат физико-математических наук, доцент кафедры безопасности информационных технологий; Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва. E-mail: onzhdanov@mail.ru.