Akademia Techniczno-Humanistyczna w Bielsku-Białej
WYDZIAŁ BUDOWY MASZYN I INFORMATYKI
Inżynier XXI wieku
XI Inter University Conference „Engineer of XXI Century" – 10 December 2021

RESEARCH METHODS FOR AVALANCHE PROPERTIES OF MANY-VALUED LOGIC COMPONENT FUNCTIONS

Artem Sokolov[1], Nadiia Kazakova[2] , Oleksii Fraze-Frazenko[2]

[1] Department of Cybersecurity and Software, Odessa Polytechnic National University, Odessa, Ukraine, radiosquid@gmail.com, https://www.opu.ua
[2] Department of Information Technologies, Odessa State Environmental University, Odessa, Ukraine, kaz2003@ukr.net, https://odeku.edu.ua

Block symmetric ciphers are a very important component of any information security system. To develop and estimate the quality of block symmetric ciphers, today their representation in the form of Boolean functions is used, to which cryptographic quality criteria are applied, the most important of which are the error propagation criterion and the strict avalanche criterion. Recent research shows that the representation of structures of cryptographic algorithms using the mathematical apparatus of Boolean functions is not exhaustive; the possibility of their representation using many-valued logic must be considered, for which the special criteria for cryptographic quality may be applied. In the paper we represent the results of research of the avalanche characteristics of S-boxes of some known cryptographic algorithms.

The core of any cryptographic algorithm is its nonlinear transformation, represented by an S-box or a set of S-boxes (substitution table). As a basis for research and measurement of the cryptographic quality of the S-box, the mathematical apparatus of component Boolean functions.

Nevertheless, the cryptanalyst is not constrained in the ways of representing the structures of cryptographic algorithms and, in addition to the mathematical apparatus of Boolean functions, can apply the mathematical apparatus of functions of many-valued logic. This circumstance makes it necessary to research the cryptographic properties of the many-valued logic component functions of modern cryptographic algorithms in order to perform a comprehensive assessment of their cryptographic quality and develop recommendations for its improvement. One of the main criteria, which largely characterizes the level of diffusion, is the error propagation criterion and its special case, a strict avalanche criterion (SAC).

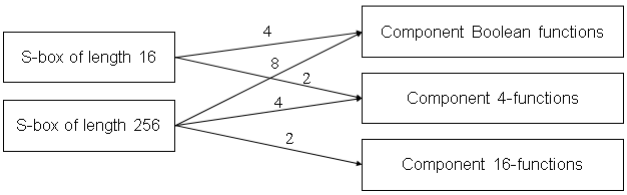
The purpose of this paper is to research and compare the avalanche properties of the component functions of the many-valued logic of cryptographic algorithms AES (USA), Kalyna (Ukraine), Kuznechik (Russia) and BelT (Belarus).

Traditionally, compliance of a cryptographic construction when it is represented by Boolean functions, to a strict avalanche criterion requires an equal probability of changing the output of a its cryptographic construction when changing any of its input bits.

In modern cryptography theory the method for estimation of the compliance of cryptographic constructions to a strict avalanche criterion was generalized to the case of functions of many-valued logic. Of practical interest is the application of this method for assessing the compliance of modern cipher constructions to the requirements of a strict avalanche criterion when they are represented by functions of many-valued logic.

To solve this problem, in this paper, we introduce two new indicators of cryptographic quality: the maximum and integral deviation from the SAC, and also calculate their values for modern ciphers in order to perform the comparative analysis.

5	9	2	4	8	7	3	10	15	1	13	11	6	14	0	12
1	1	0	0	0	1	1	0	1	1	1	1	0	0	0	0
0	0	1	0	0	1	1	1	1	0	0	1	1	1	0	0
1	0	0	1	0	1	0	0	1	0	1	0	1	1	0	1
0	1	0	0	1	0	0	1	1	0	1	1	0	1	0	1
1	1	2	0	0	3	3	2	3	1	1	3	2	2	0	0
1	2	0	1	2	1	0	2	3	0	3	2	1	3	0	3



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

Functions of many-valued logic are a more general mathematical object in comparison with Boolean functions.

For example, Boolean functions are, by definition, mappings $\{0,1\}^k \to \{0,1\}$, that is, a special case of Definition 1 at value q=2.

Definition 2. The weight $\varpi(u)$ of a q-valued vector is the number of its nonzero components.

Definition 3. The derivative of a q-function $f(x)$ in the direction of the vector u is a function $D_u f(x) = f(x \oplus_q u) - f(x) \pmod q$ where $\oplus_q$ means addition modulo q.

Definition 4. The function of q-valued logic $f(x)$ satisfies the error propagation criterion for vector $u \in V_k$ — PC(u) , if its derivative in the direction u is a balanced function, that is, values $0,1,...,q-1$ are taken with equal probabilities: $p(D_u f(x) = i \pmod q) = 1/q$ for all $0,1,...,q-1$.

Definition 5. The function of q-valued logic satisfies the of error propagation criterion of degree m – PC(m), if it satisfies the error propagation criterion for all vectors u of weight $1 \le \varpi(u) \le m$.

Definition 6. A function of q-valued logic satisfies a strict avalanche criterion (SAC) if it satisfies the error propagation criterion of degree 1 – PC(1).

In essence, the strict avalanche criterion is a rigorous requirement that is quite difficult to fulfill, especially while maintaining compliance of the S-box to other criteria of cryptographic quality, primarily the criterion of high nonlinearity.

Therefore, the S-boxes of practically used BSC, in particular, the cryptoalgorithms AES, Kalyna, BelT and Kuznechik researched in this paper do not satisfy the requirements of SAC even in the sense of component Boolean functions. However, it is clear that the S-box of practically used cryptoalgorithms should be as close as possible to satisfy the strict avalanche criterion.

To solve the problem of estimating and comparing avalanche properties of real S-boxes, it is advisable to introduce two indicators of cryptographic quality: maximum and integral deviation from SAC.

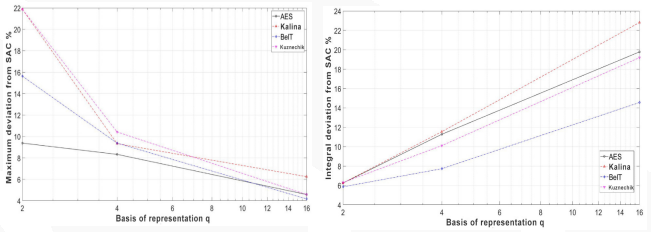
Definition 7. The maximum deviation of the S-box from the SAC when it is represented by component *q*-functions is the maximum among all deviations from the SAC of its component *q*-functions.

Definition 8. The integral deviation of the S-box from the SAC when it is represented by the component q-functions is the total value of the deviations from the SAC of all its component q-functions.

In Table we show the values of maximum and integral deviation from the SAC for cryptographic algorithms AES, Kalyna, BelT and Kuznechik.

Crypto-algorithm	Binary case		Case of 4-functions		Case of 16-functions	
	$\Delta_{\max} K_{Df_1}$ (%)	ΔK_{Df_1} (%)	$\Delta_{\max} K_{Df_4}$ (%)	ΔK_{Df_4} (%)	$\Delta_{\max} K_{Df_{16}}$ (%)	$\Delta K_{Df_{16}}$ (%)
AES	12 (9.38%)	516 (6.25%)	16 (8.33%)	1040 (11.28%)	11 (4.58%)	2848 (19.78%)
Kalyna	28 (21.88%)	512 (6.25%)	18 (9.33%)	1064 (11.55%)	15 (6.25%)	3284 (22.81%)
BelT	20 (15.63%)	480 (5.86%)	18 (9.38%)	712 (7.73%)	10 (4.17%)	2096 (14.56%)
Kuznechik	28 (21.88%)	516 (6.3%)	20 (10.42%)	932 (10.11%)	11 (4.58%)	2764 (19.19%)

We present the charts for the values of maximum and integral deviation from the SAC for cryptographic algorithms AES, Kalyna, BelT and Kuznechik.



The indicators of maximum and integral deviation from the strict avalanche criterion of S-boxes are introduced, which allows to estimate and compare the degree of deviation from SAC for the functions of many-valued logic.

A research and comparison of avalanche properties of component functions of many-valued logic of cryptoalgorithms AES (USA), Kalyna (Ukraine), Kuznechik (Russia) and BelT (Belarus) were performed, which allowed to obtain the following conclusions:

1. for the substitution constructions of the researched BSC the general tendency of decrease of the maximum deviation from SAC while increasing a basis of representation q value is established. In this case, a greater decrease in the maximum deviation from the SAC indicates higher quality of the cryptographic transformation.
2. for the substitution constructions of the researched BSC the general tendency of increase of integral deviation from SAC while increasing a basis of representation q is established. Smaller values of the increase of the integral deviation from the SAC indicate a higher quality of cryptographic transformation.
3. a comparative analysis of the compliance of BSC to SAC of the component functions of many-valued logic showed that among the researched ciphers BSC BelT meets its requirements most of all.

Ministerstwo Edukacji i Nauki
Dofinansowano z programu „Doskonała nauka" Ministra Edukacji i Nauki