Prerequisites for Developing a Methodology for Estimating and Increasing Cryptographic Strength based on Many-Valued Logic Functions

Artem Sokolov[a], Nadiia Kazakova[b], Lydia Kuzmenko[c], and Mariia Mahomedova[c]

[a] *Odessa National Polytechnic University, 1 Shevchenko ave., Odessa, 65044, Ukraine*
[b] *Odessa State Environmental University, 15 Lvovskaya str., Odessa, 65016, Ukraine*
[c] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

Symmetric cryptographic algorithms are one of the most important components of information security systems, which determines the relevance of the task of estimation and further increasing of their efficiency. The rapid development of cryptanalysis methods, in particular, using the representation of structures of cryptographic algorithms based on many-valued logic functions, and the development of quantum cryptanalysis methods, as well as the actual absence of a comprehensive theoretical apparatus for the estimation of cryptographic quality of many-valued logic component functions and synthesis methods for cryptographic constructs, which are high quality in terms of many-valued logic functions, create an objective contradiction in modern cryptography. In this paper, we represent the prerequisites for the development of a methodology for estimation of cryptographic strength based on many-valued logic functions, which is in turn based on the criteria and indicators of the cryptographic quality of many-valued logic functions, as well as methods for their calculation. We also present the results of applying the developed methodology to common block symmetric ciphers made it possible to identify a cryptographic quality reserve that can be obtained by improving their structure, considering the representation of their constructs using functions of many-valued logic.

Keywords

Cryptography, cryptographic quality, many-valued logic function.

1. Introduction

One of the most important components of modern information security systems is the cryptographic subsystem, which solves the problem of ensuring the integrity, confidentiality, and authentication of transmitted and stored information. In this case, the main component of the cryptographic subsystem is the block symmetric cipher (BSC) used for cryptographic transformation of large amounts of data. These components are so often used in information processing and transmission systems that the blocks corresponding to them are now implemented in processors in the form of separate hardware modules [1]. We also note the fact that in many countries the described cryptographic constructions are standardized and are used to protect the information in the specialized information systems which are critical for national security. In particular, in Ukraine, the Kalyna crypto algorithm which is described by the DSTU 7624:2014 standard [2], is used to protect the information in military and civilian systems for processing and storing information.

These circumstances make the task of estimation and improving the cryptographic quality of these algorithms especially urgent.

The fundamental principles on which any modern cryptographic algorithm is built are the principles of diffusion and confusion proposed by C. Shannon [3]. However, like Shannon's theorem,

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: sokolov.a.v@opu.ua (A.1); kaz2003@ukr.net (B.2); lido4ok@gmail.com (C.3); m.mahomedova.asp@kubg.edu.ua (C.4)
ORCID: 0000-0003-0283-7229 (A.1); 0000-0003-3968-4094 (B.2); 0000-0001-7392-0324 (C.3); 0000-0001-9395-840X (C.4)

the principles of diffusion and confusion give only the idea of the quality of cryptographic constructions and the cryptographic algorithms built on their basis. Nonetheless, they provide neither specific methods for estimation of the quality of cryptographic primitives and cryptographic algorithms, nor methods for constructing cryptographic primitives and algorithms that would best implement the principles of diffusion and confusion.

Since the formulation of the principles of diffusion and confusion by C. Shannon, many attempts have been made to create a comprehensive theory for estimating the quality of cryptographic algorithms and primitives based on them, which would be focused on the estimation of the ability of cryptographic algorithms components and their superpositions to resist possible attacks using modern cryptanalysis methods.

Nevertheless, the further development of cryptanalysis methods, in particular, the emergence of cryptanalytic attacks based on many-valued logic functions [4], as well as the active development of quantum cryptanalysis methods [5], determines the need for further improvement of methods for estimation of the cryptographic quality of existing structures, and the development of new cryptographic constructions, and cryptographic algorithms that meet the developed cryptographic quality criteria.

The purpose of this paper is to research the prerequisites for creating a methodology for estimation and increasing the cryptographic strength based on the mathematical apparatus of many-valued logic functions.

2. Modern Methods for Cryptographic Quality Estimation

Currently, many approaches have been created to estimate the cryptographic quality, in particular, based on the analysis of stochastic properties of the output sequences of cryptographic algorithms [6], in which, for example, stochastic quality tests can be used [7]. There is also an approach for research of the degree of implementation of the principles of diffusion and confusion in the cryptographic algorithm, based on the research of its reduced copies [8], which was applied to the cryptographic algorithms Kalyna [9], Rijndael [10] and others [11]. There is also a method for estimation of the quality of implementation of the principles of diffusion and confusion by the cryptographic algorithm based on the research of the number of iterations required to reach steady-state inherent to the random substitution [12], as well as other approaches applicable for specific cryptographic algorithms.

At the same time, there is no doubt that the main cryptographic construction that determines the quality of a cryptographic algorithm is the S-box [13].

Definition 1 [13]. A $k_1 \times k_2$ bit substitution block or S-box is a mapping $\{0,1\}^{k_1} \to \{0,1\}^{k_2}$, that is, a mapping that uniquely maps any input k_1 bit vector to an output k_2 bit vector.

The structure of the S-box and, therefore, its cryptographic properties can be completely determined by the Q-sequence of length $N = q^k$. If a given Q-sequence contains all elements of a monotonically increasing sequence $0,1,...,N-1$, then such an S-box is called a bijective and can be used in practical schemes of modern cryptographic algorithms. It is clear that the total cardinality of the class of bijective S-boxes of length N is $N!$.

The choice of specific S-boxes for practical use is based on their research in accordance with the generally accepted approach, which involves the use of the mathematical apparatus of Boolean functions. For this, the coding Q-sequence is decomposed into a set of component Boolean functions, which can be represented using their truth tables. Further, for each of the component Boolean functions, a set of cryptographic quality criteria is applied.

In summary, we represent in Fig. 1 a classification of the main approaches to the research of the cryptographic quality of cryptographic algorithms.

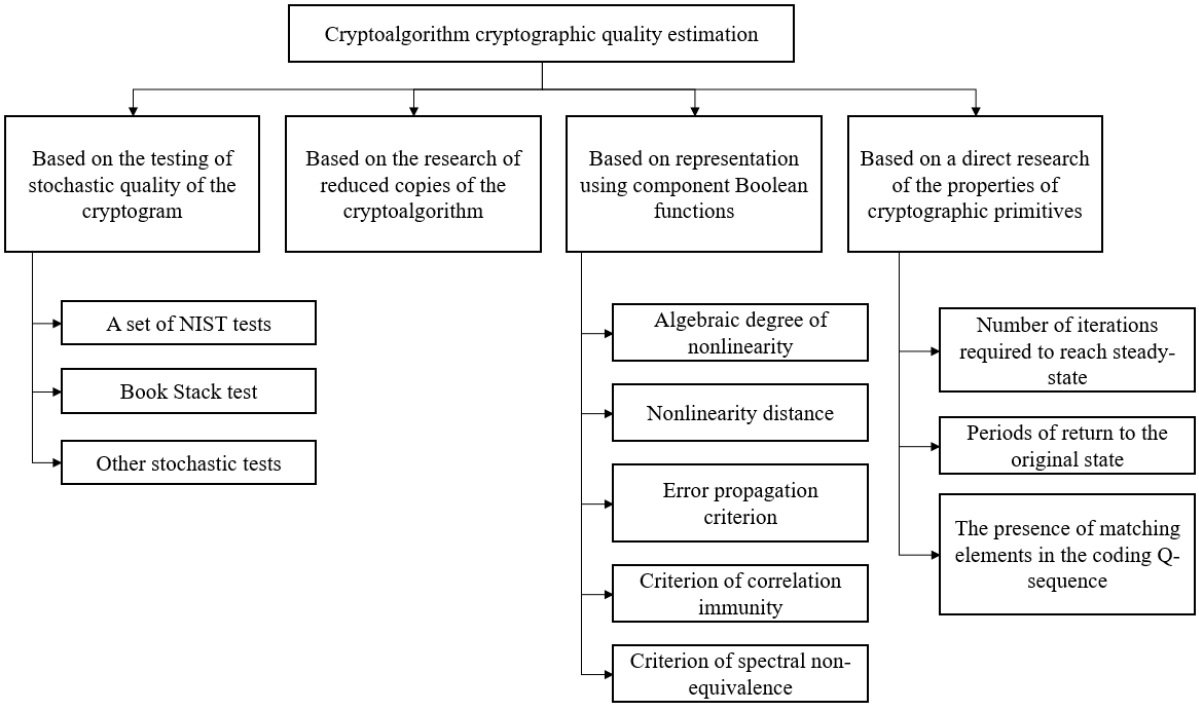

Figure 1: Classification of the main approaches to estimate the cryptographic quality of cryptographic algorithms

Let us consider in detail the generally accepted approach involving the research of the cryptographic quality of component Boolean functions. So, after representing a cryptographic construct using Boolean functions, a set of cryptographic quality criteria is applied to them. Today, these criteria for cryptographic quality include the following:

1. Algebraic degree of nonlinearity, which characterizes the degree of algebraic complexity of the output of a Boolean function with respect to its input variables [14]. The algebraic degree of nonlinearity shows how nonlinear are Boolean functions that are part of a cryptographic construction from an algebraic point of view. When designing constructions for cryptographic algorithms, researchers try to increase the algebraic degree of nonlinearity of their component Boolean functions.
2. Nonlinearity distance, which characterizes the degree of distancing of a Boolean function from the set of Boolean functions that are considered linear [15]. As such a set, a set of affine functions (codewords of the first-order Reed-Muller code) is usually used. However, to estimate the level of nonlinearity, other constructions can also be used, which are considered linear. For example, quadratic Boolean functions can be used as such constructions [16]. At the same time, there are two approaches to estimate the nonlinearity of a given Boolean function: in the time domain and the domain of Walsh-Hadamard transform coefficients.
3. Correlation relationship between the output and the input of the S-box, which is determined by the statistical dependence of the output of the S-box on its input. For a quantitative estimation of the level of statistical dependence, the mathematical apparatus of the matrix of correlation coefficients [17] between the vectors of the output and the input is used. The following cryptographic quality indicators can be applied to the correlation coefficients matrix:
   a. The maximum absolute value of the elements of the matrix of correlation coefficients between the output and input vectors.
   b. The number of zero elements in the matrix of correlation coefficients. Good quality of the cipher is the case when each of the elements of the matrix of correlation coefficients is equal to zero, which is possible when each of the component Boolean functions of the S-box is correlation immune [18], at least of the first order.
4. Error propagation criterion, which characterizes the ability of a cryptographic construction to propagate minor changes in the input text or key element to the entire ciphertext [19]. There is an error propagation criterion in the direction of a certain vector, which is fed to the input of a

cryptographic structure as an additional influence, as well as an error propagation criterion of a given order. The numerical determination of the correspondence of the cryptographic construction to the error propagation criterion is carried out on the basis of the mathematical apparatus of the derivatives of Boolean functions [14]. The error propagation criterion of the first-order is called as strict avalanche criterion (SAC). Note, that the strict avalanche criterion is a quite strict requirement for cryptographic constructions, therefore, in practice, the criterion of the maximum avalanche effect is often used, which is satisfied if all weights of all derivatives of component Boolean functions in all directions of weight 1 have a value equal to at least half the length of the cryptographic construction [20]. The error propagation criterion, the strict avalanche criterion, and the criterion for the maximum avalanche effect play a special role not only in the theory of analysis and synthesis of symmetric block ciphers but also in the synthesis of cryptographically strong hash functions [21].

5. Linear redundancy of component Boolean functions. The research of component Boolean functions [22] of some cryptographic primitives, for example, the Nyberg construction [23], shows that they have a certain mathematical relationship with each other. This relationship weakens the level of confusion that the researched cryptographic primitive can provide, and, accordingly, strengthens the cryptanalyst's capabilities to describe the crypto algorithm as a whole. In [24], a new method for determining the equivalence of component Boolean functions was proposed, which greatly simplifies the practical task of determining the affine equivalence of component Boolean functions of cryptographic constructions. This approach is based on a basic elementary structure definition. Thus, to reduce the level of linear redundancy, the design of cryptographic constructions should be performed in such a way that their component Boolean functions have a different elementary structure.

3. Representation of Cryptographic Constructions by the Many-Valued Logic Functions

Nevertheless, the cryptanalyst is not constrained in the chosen mathematical apparatus, with the help of which the representation of the constructions of the cryptographic algorithm is carried out with the subsequent attack. In addition to the mathematical apparatus of Boolean functions used in the construction of cryptographic algorithms, the representation using 4-functions, as well as using 16-functions, can be used for almost all modern ciphers. At the same time, the developers of cryptographic algorithms usually do not consider these possible representations and do not research their cryptographic quality. This circumstance determines the need to build, develop and generalize the criteria of cryptographic quality and the practical aspects of their use for the functions of many-valued logic.

On the other hand, quantum computers are developing dynamically, which already today allows us to speak about the formation of post-quantum cryptographic methods that will be relevant when quantum computers will develop and quantum attacks will be carried out with their help [5]. Note that the key of the modern symmetric cryptographic algorithm is a pseudo-random sequence. Thus, with a sufficiently large key length, it is required to use a brute force attack or use of any structural vulnerability to attack the cryptographic algorithm, in contrast to the use of algorithmic attacks, for example, using Shor's algorithm [25], which can be used to break asymmetric cryptographic algorithms. This fact makes it especially urgent, in the conditions of post-quantum cryptography, to research in detail and improve the structure of cryptographic algorithms, for any of their representations, especially with the help of functions of many-valued logic.

Let us introduce the definition of a many-valued logic function we need.

Definition 1 [26]. A function of the q-valued logic of k variables is a mapping $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Many-valued logic functions are more general mathematical objects than Boolean functions. So, for value $q=2$, **Definition 1** is the definition of Boolean functions.

Many-valued logic is one of the experiences of expanding the boundaries of awareness and formal description of the logical connections of the real world. With the generally accepted meaning of binary logic, J. Łukasiewicz [27] drew attention to many-valued logic which is the way of displaying

different shades of information in sentences. Thus, a direction of many-valued logic arose, in which many famous mathematicians, economists, philosophers worked, interested in improving the quality of information transfer.

Let us consider (see Table 1) how the S-box of length $N=16$ practically used in modern cryptographic algorithms can be represented not only with the help of component Boolean functions but also with the help of many-valued logic functions.

Table 1.
S-box representation using Boolean and many-valued logic functions

Q	4	7	2	14	1	13	8	11	15	12	6	10	5	9	3	0
f_{20}	0	1	0	0	1	1	0	1	1	0	0	0	1	1	1	0
f_{21}	0	1	1	1	0	0	0	1	1	0	1	1	0	0	1	0
f_{22}	1	1	0	1	0	1	0	0	1	1	1	0	1	0	0	0
f_{23}	0	0	0	1	0	1	1	1	1	1	0	1	0	1	0	0
f_{40}	0	3	2	2	1	1	0	3	3	0	2	2	1	1	3	0
f_{41}	1	1	0	3	0	3	2	2	3	3	1	2	1	2	0	0

At the same time, the constructions of such cryptographic algorithms as AES, Kalyna, Kuznechik, and BelT, etc. which have an S-boxes length $N=256$, can be represented using Boolean functions, 4-functions, and 16-functions, i.e. they have 3 possible representations by many-valued logic functions.

Each of the component q-functions determines the cryptographic quality of the cryptographic construction as a whole and, accordingly, each of them should be carefully tested.

Thus, today there is an objective contradiction between the developed methods of attacks on cryptographic algorithms with the possible representation of their structures by functions of many-valued logic, while simultaneously developing promising methods of attacks using quantum computers and the actual absence of a comprehensive mathematical apparatus designed to estimate the cryptographic quality of component functions of many-valued logic and methods for synthesis of cryptographic structures that are high quality in terms of many-valued logic functions.

The solution to this contradiction can be obtained by developing a methodology for estimation and increasing the cryptographic strength based on functions of many-valued logic.

The presented methodology for estimation of the cryptographic quality is based on the following criteria for the cryptographic quality of many-valued logic functions in conjunction with the corresponding indicators of cryptographic quality:

1. The criterion for the algebraic degree of nonlinearity of many-valued logic functions, which is determined based on the algebraic normal form synthesized using the method [28] over a simple or extended Galois field. At the same time, to compare the algebraic degrees of nonlinearity, the indicator of the relative algebraic degree of nonlinearity was introduced as a percentage of a given degree of nonlinearity of the maximum value, which allows comparing the algebraic degrees of nonlinearity of q-functions of different lengths and for different bases q. Larger values of the relative algebraic degree of nonlinearity indicate a higher quality of the cryptographic construction.

2. The criterion for the nonlinearity of many-valued logic functions, which is determined in accordance with the spectral or time method [29] based on the degree of content of Vilenkin-Chrestenson functions in the researched component function of the many-valued logic. In view of the existence of many-valued logic bent-functions for an arbitrary given number of variables k, to compare the nonlinearity of q-functions of different lengths and for different bases q, an indicator of the relative nonlinearity of the q-function was introduced as a percentage of the nonlinearity of a given q-function of the nonlinearity of bent-functions of a given length. At the same time, larger values of the relative nonlinearity indicate a higher quality of the cryptographic structure.

3. The propagation criterion of the many-valued logic functions and the strict avalanche criterion of the many-valued logic functions, which are determined by the research the derivatives of many-valued logic functions in accordance with the method [30]. To assess the degree of correspondence and comparison of q-functions of different lengths and for different bases q,

indicators of integral and maximum deviations from the many-valued logic functions SAC requirements were introduced. Smaller values of the maximum and integral deviations from the SAC requirements indicate a higher quality of the cryptographic construction.

4. The criterion for the correlation independence of the output and input vectors of cryptographic structures [31], as well as the criterion for the independence of the output values of many-valued logic functions from their input variables [32]. On the basis of the proposed criterion for the independence of the output of many-valued logic functions from their input variables, indicators of the maximum and integral deviation from the criterion for the independence of the output of many-valued logic functions from their input are introduced, which are convenient for numerical estimation and comparison of *q*-functions of different lengths and for different bases *q*. Smaller values of the maximum and integral deviations from the criterion of independence of the output of many-valued logic functions from their input indicate a higher quality of the cipher.

The described criteria and the indicators of the cryptographic quality of the many-valued logic functions based on them provide an opportunity to estimate and compare the cryptographic structures of various cryptographic algorithms.

At the same time, there are many practical examples when a cryptographic construction is secure in the terms of Boolean functions and has low quality in the terms of functions of many-valued logic. For example, the S-box $S = \{12,7,14,9,1,4,8,3,2,6,5,11,15,10,13,0\}$ has a nonlinearity distance value of 4 (66.7%, which is the maximum value for S-boxes of this length) of component Boolean functions, while the nonlinearity of 4-functions is only 3.35 (27.92%). Or the S-box $S = \{4,7,2,14,1,13,8,11,15,12,6,10,5,9,3,0\}$ [30], which, being optimal from the point of view of the strict avalanche criterion in the terms of Boolean functions, is not optimal from the point of view of the strict avalanche criterion for component 4-functions.

Thus, the task of design of new cryptographic constructions that are cryptographically qualitative not only from the point of view of their representation with help of Boolean functions but also from the point of view of their representation by functions of many-valued logic seems to be urgent.

4. Evaluation of the Component Many-Valued Logic Functions Cryptographic Quality for the Known Cryptographic Algorithms

The developed methodology for estimation and increasing cryptographic strength can be applied both to estimate and compare the cryptographic quality of existing cryptographic algorithms and to develop new cryptographic primitives and cryptographic algorithms. Next, we use the criteria and indicators of cryptographic quality to estimate and compare the cryptographic properties of such well-known cryptographic algorithms as AES [33], Kalyna [2], BelT [34], and Kuznechik [35] when represented with help of component functions of many-valued logic. In view of the fact that the length of the researched substitution structures of the considered cryptographic algorithms is $N = 256$, they can be represented in the form of component Boolean functions, 4-functions, as well as 16-functions.

We also note that, as in the case of applying the generally accepted approach to the estimation of the cryptographic quality based on Boolean functions, the overall cryptographic quality of a structure is determined by its worst component *q*-function as the weakest component [36].

In Fig. 2 we show the results of calculating the indicators of the cryptographic quality of the many-valued logic functions of the considered cryptographic algorithms.

The general trend is the growth of the algebraic degree of nonlinearity of existing cryptographic algorithms when they are represented by component *q*-functions with larger bases *q*. The largest growth is shown by BelT and Kuznechik (from 87.5% for Boolean functions to 96.67% for 16-functions), the least growth is shown by BSC AES and Kalyna (from 87.5% for Boolean functions to 93.33% for 16-functions).

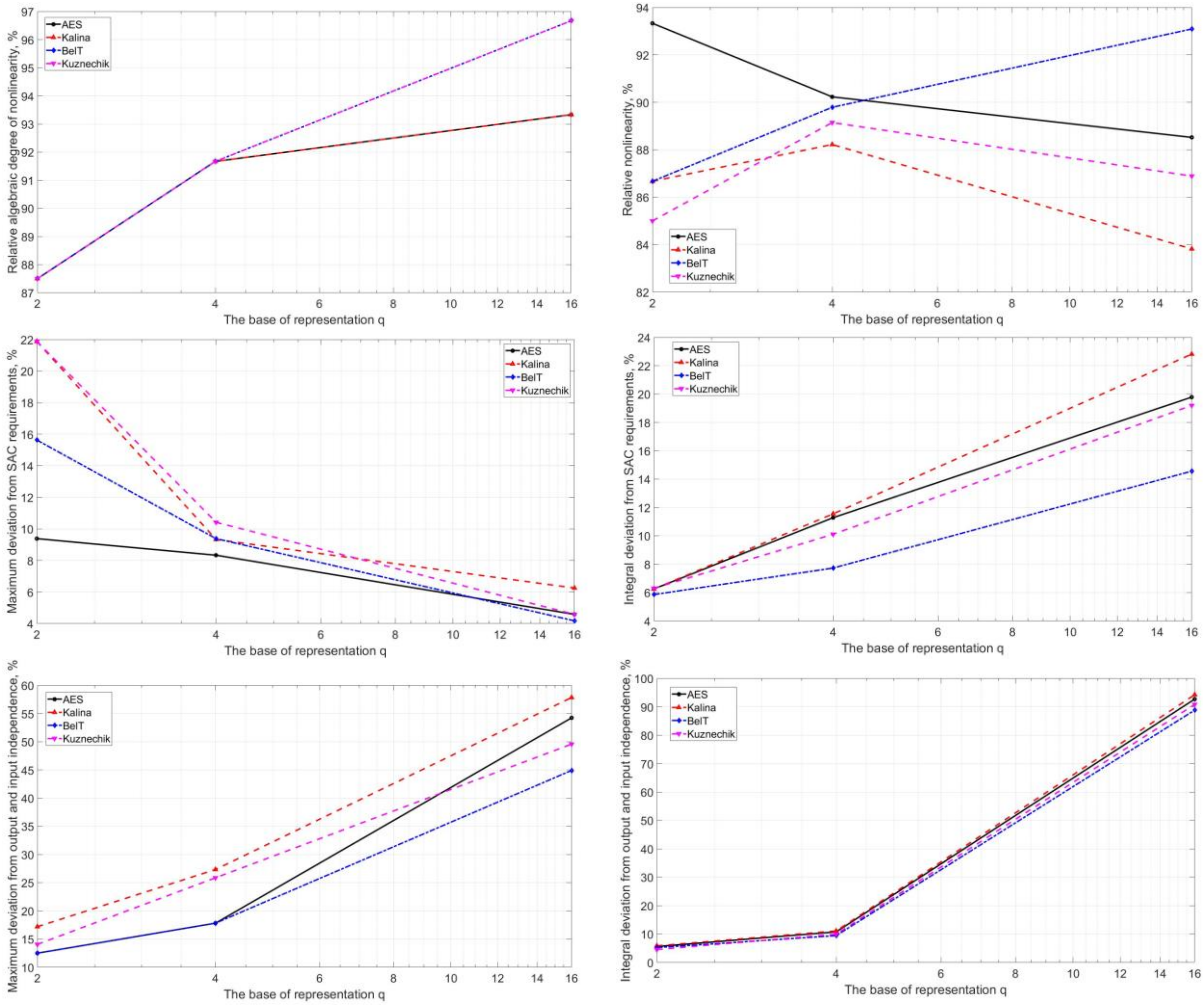

Figure 2: The results of calculation of the cryptographic quality indicators of the considered cryptographic algorithms many-valued logic component functions

The behavior of the nonlinearity of component functions for different bases q depends on the quality of the S-box used in cryptographic algorithms. At the same time, the Belarusian BSC BelT and the Russian Kuznechik demonstrate an increase in nonlinearity when represented by many-valued logic functions (BelT: from 86.67% for Boolean functions to 93.09% for 16-functions, Kuznechik: from 85% for Boolean functions to 86.89% for 16-functions), while the Ukrainian BSC Kalyna demonstrates the greatest decrease in nonlinearity when represented by many-valued logic functions (from 86.67% for Boolean functions to 83.82% for 16-functions), which indicates less confusion that this BSC provides in terms of many-valued logic functions.

For AES-like cryptographic algorithms, there is a general tendency towards a decrease in the maximum deviation from the SAC with an increase in the base q of the representation of component functions. In this case, the largest decrease in the maximum deviation from the SAC is demonstrated by the BSC BelT (from 15.63% for Boolean functions to 4.17% for 16-functions), and the smallest decrease is demonstrated by the BSC Kalyna (from 21.88% for Boolean functions to 6.25% for 16-functions). There is also a general tendency for the integral deviation from the SAC to increase with an increase in the base of the representation q. In this case, the smallest increase in the deviation from the SAC is demonstrated by the BSC BelT (from 5.86% for Boolean functions to 14.56% for 16-functions), and the largest increase is demonstrated by the BSC Kalyna (from 6.25% for Boolean functions to 22.81% for 16-functions).

For AES-like cryptographic algorithms, there is also a general tendency for the maximum deviation from the criterion of the independence of the output of component functions from the input variables to grow with the growth of the base q of the representation of component functions. At the same time, the lowest increase in deviation is demonstrated by the BSC BelT (from 12.5% for

Boolean functions to 44.9% for 16-functions), and the highest increase is demonstrated by the BSC Kalyna (from 17.19% for Boolean functions to 57.82% for 16-functions). The integral deviation from the criterion of independence of the output of component functions from input variables also grows. The smallest increase in deviation is demonstrated by the BSC BelT (from 5.27% for Boolean functions to 88.8% for 16-functions), the highest increase is demonstrated by the BSC Kalyna (from 5.88% for Boolean functions to 94.21% for 16-functions).

5. Conclusion

The research performed in this paper made it possible to draw the following conclusions:

1. At the moment, there is an objective contradiction between the developed methods of attacks on cryptographic algorithms with the possible representation of their structures by functions of many-valued logic, while simultaneously developing promising methods of attacks using quantum computers and the actual absence of a comprehensive mathematical apparatus designed to research the cryptographic quality of component functions of many-valued logic and methods for synthesizing cryptographic structures that are high quality in terms of many-valued logic functions. The solution of this contradiction is a prerequisite for creating a methodology for estimation and increasing cryptographic strength based on the functions of many-valued logic.
2. A methodology for estimation and increasing cryptographic strength based on many-valued logic functions is presented, consisting of the cryptographic quality criteria, indicators, and methods for their calculation. The developed methodology makes it possible to estimate and compare the cryptographic quality of existing cryptographic algorithms, as well as to develop new ones that would be of high quality both in terms of Boolean functions and in terms of functions of many-valued logic.
3. The performed research of the common block symmetric cryptographic algorithms showed that the representation of structures of cryptographic algorithms by functions of many-valued logic leads to the possibility of using the proposed criteria for the cryptographic quality of functions of many-valued logic and, accordingly, a comprehensive estimation of the cryptographic quality of these structures. This fact leads to the need to consider the properties of many-valued logic functions when designing cryptographic algorithms. The results of calculations of cryptographic quality indicators for existing BSC presented in this paper confirm the possibility of further improvement of the cryptographic algorithms considering the properties of many-valued logic functions.

6. References

[1] R. Manley, D. Gregg, A program generator for intel AES-NI instructions, in: International Conference on Cryptology in India, Springer, Berlin, Heidelberg, 2010, pp. 311–327. doi:10.1007/978-3-642-17401-8_22

[2] Sovereign standard of Ukraine DSTU 7624:2014, Information technologies, Cryptographic information protection, Algorithm for symmetric block symmetric transformation, Ministry of Economic Development of Ukraine, 2016.

[3] C. E. Shannon, A Mathematical Theory of Cryptography, Bell System Technical Memo, 1945, MM 45-110-02.

[4] T. Baigneres, J. Stern, S. Vaudenay, Linear Cryptanalysis of Non Binary Ciphers, in: Lecture Notes in Computer Science, 2007, pp. 184–211. Heidelberg. doi:10.1007/978-3-540-77360-3_13

[5] M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover's algorithm to AES: quantum resource estimates, Post-Quantum Cryptography, Springer, Cham, 2 (2016) 29–43.

[6] W. Schindler, W. Killmann, Evaluation criteria for true (physical) random number generators used in cryptographic applications, International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg (2002) 431–449. doi:10.1007/3-540-36400-5_31

[7] A. Rukhin, J. Soto, J. Nechvatal, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standards and Technology Special Publication, 2010, doi:10.6028/nist.sp.800-22

[8] S. P. Evseev, S. E. Ostapov, R. V. Korolev, The use of mini-versions for evaluating the stability of block-symmetric ciphers, Ukrainian Scientific Journal of Information Security 23 (2017) 100–108. doi:10.18372/2225-5036.23.11796
[9] V. I. Ruzhentsev, S. V. Chichmar, D. I. Savin, Combinatorial properties of the reduced version of the Kalyna cipher, Applied Radioelectronics 9 (2010) 346–348.
[10] V. I. Dolgov, I. V. Lisitskaya, D. E. Khryapin, Attack on the full differential of the reduced version of theblock symmetric cipher Rijndael, Applied radioelectronics: scientific and technical journal 9 (2010) 355–360.
[11] V. I. Dolgov, Research of the cryptographic properties of nonlinear replacing nodes of reduced versions of some ciphers, Applied radioelectronics: scientific and technical journal 8 (2009) 268–277.
[12] I. V. Lisitskaya, K. E. Lisitskiy, On the arrival of iterative ciphers to a stationary state inherent to random substitution, Applied Radioelectronics 12 (2013) 230–235.
[13] O. N. Zhdanov, Methodology for selecting key information for a block cipher algorithm, Moscow, INFRA-M, 2013.
[14] O. A. Logachev, A. A. Sal'nikov, V. V. Jashhenko, Boolean functions in coding theory and cryptology, MCNMO, Moscow, 2004.
[15] W. Maier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, in: Quisquater, J.-J. and Vandewalle, J. (Eds.) Advances in Cryptology — EUROCRYPT ’89, 1990, pp. 549–562. doi:10.1007/3-540-46885-4_53
[16] H. Yan, D. Tang, Improving lower bounds on the second-order nonlinearity of three classes of Boolean functions, Discrete Mathematics 343 (2020) 111698. doi:10.1016/j.disc.2019.111698
[17] M. I. Mazurkov, Synthesis method of optimal substitution constructions based on the criterion of zero correlation between the output and input data vectors, Radioelectronics and Communications Systems 55 (2012) 533–543. doi:10.3103/s0735272712120023
[18] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.), IEEE Transactions on Information theory 30 (1984) 776–780. doi:10.1109/tit.1984.1056949
[19] R. Forrié, The strict avalanche criterion: spectral properties of Boolean functions and an extended definition, in: Advances in Cryptology — CRYPTO’ 88, 1990, pp. 450–468. doi: 10.1007/0-387-34799-2_31
[20] T. G. S, Chandrasekharappa, K. V. Prema, Kumara Shama, S-boxes generated using Affine Transformation giving Maximum Avalanche Effect, International Journal of Computer Science and Engineering, Manipal Institute of Technology, India 3 (2011) 3185–3193.
[21] Y. M. Motara, B. Irwin, Sha-1 and the strict avalanche criterion, in: Information Security for South Africa (ISSA), 2016, pp. 35–40. doi:10.1109/ISSA.2016.7802926.
[22] J. Fuller, W. Millan, Linear Redundancy in S-Boxes, Fast Software Encryption, 10th International Workshop, Sweden, Lund 2887 (2003) 74–86. doi:10.1007/978-3-540-39887-5_7
[23] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology — EUROCRYPT ’93, 1994, pp. 55–64. doi:10.1007/3-540-48285-7_6
[24] A. V. Sokolov, N. A. Barabanov, Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes, Radioelectronics and Communications Systems 58 (2015) 220–227. doi:10.3103/s0735272715050040
[25] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134. doi:10.1109/SFCS.1994.365700.
[26] R. S. Stanković, J. T. Astola, C. Moraga, Representation of Multiple-Valued Logic Functions, Synthesis lectures on digital circuits and systems 7 (2012) 168.
[27] J. Łukasiewicz, Aristotelian syllogistics from the point of view of modern formal logic, Moscow, Foreign literature, 1959.
[28] A. V. Sokolov, O. N. Zhdanov, A. O. Ayvazyan, Synthesis methods of algebraic normal form of many-valued logic functions, System analysis and applied information science 1 (2016) 69–76.
[29] A. V. Sokolov, O. N. Zhdanov, Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties, Journal of Telecommunication, Electronic and Computer Engineering 8 (2016) 39–43.

[30] A. V. Sokolov, O. N. Zhdanov, Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength, Siberian Journal of Science and Technology 20 (2019) 183—190. doi:10.31772/2587-6066-2019-20-2-183-190
[31] O. N. Zhdanov, A. V. Sokolov, Algorithm of construction of optimal according to criterion of zero correlation nonbinary S-boxes, Problems of physics, mathematics and technics 3 (2015) 94–97.
[32] A. V. Sokolov, O. N. Zhdanov, Correlation immunity of three-valued logic functions, Journal of Discrete Mathematical Sciences and Cryptography (2020) 1–17. doi:10.1080/09720529.2020.1781882
[33] FIPS 197. [Electronic resource] Advanced encryption standard, 2001. http://csrc.nist.gov/publications/
[34] STB P 34.101.31-2007. Information technologies, Information protection, Cryptographic algorithms for encryption and integrity control, Minsk, Gosstandart, 2007.
[35] GOST 34.12-2018. Information technology, Cryptographic protection of information, Block cipher, Moscow, Standartinform, 2018.
[36] A. Bessalov, et al., Analysis of 2-isogeny properties of generalized form Edwards curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1–13.