Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code

Roman Kochan [1], Serhii Yevseiev[2], Roman Korolyov[3], Stanislav Milevskyi[4], Imad Ireifidzh[5], Tomasz Gancarczyk[6] and Rafal Szklarczyk[7]
[1, 5, 6, 7] University of Bielsko-Biala, 2 Willowa str., Bielsko-Biala, 43-300, Poland; e-mail: rkochan@ad.ath.bielsko.pl, iireifidzh@ath.bielsko.pl, tgancarczyk@ad.ath.bielsko.pl, rszklarczyk@ad.ath.bielsko.pl
[2, 3, 4] Semen Kuznets Kharkiv National University of Economics, 9-A Nauky str., Kharkiv, 61166, Ukraine e-mail: serhii.yevseiev@hneu.net

Abstract— **The development of modern technologies and the emergence of full-scale quantum computers requires a critical revision of the requirements for the level of algorithms cryptographic stability, both post-quantum cryptography, and used in cyberspace and information and communication systems algorithms of traditional and asymmetric cryptography. The analysis of possible approaches to increase the level of cryptographic stability of symmetric cryptography algorithms based on Feistel chains. One of the promising algorithms of symmetric cryptosystems in the conditions of post-quantum cryptography (post-quantum period) according to experts is the algorithm GOST 28147-2009 (DSTU GOST 28147: 2009, GOST R-3412 - 2015) the main advantages of which is the simplicity of implementation and high level crypto stability. However, in a full-scale quantum computer, the effectiveness of cryptographic information security based on symmetric cryptosystems (their level of crypto-stability) can be called into question by the possibility of an attack based on Grover's algorithm, which is easy to use to find the encryption key by brute-force. Methods of increasing the cryptographic stability of block-symmetric algorithm GOST 28147-2009 (DSTU GOST 28147: 2009, GOST R-3412 - 2015) are proposed by increasing the key sequence (by increasing the length of S-blocks), and / or by increasing the number of S- blocks, which increases the level of crypto stability and counteracts a "brute force" attack based on a quantum computer. To confirm the proposed methods of increasing the level of crypto-stability of the symmetric algorithm GOST 28147-2009 (DSTU GOST 28147: 2009), the results of the complexity of operations in the integer ring, expressed in the operations of the processor, which confirms the possibility of implementation of this algorithm without significant increase in energy consumption elementary group operations).**

Keywords— Block-Symmetric Code; Cryptographic Stability; Cryptotransformations

I. INTRODUCTION

The pace of information technology development over the last 15-20 years has contributed to the introduction of computer technology in all areas of human activity. Which in turn was reflected in the reverse of this process. Namely, there has been an increasing interest in the information systems circulating inside information systems, not only from legitimate users and owners, but also from attackers. Therefore, the issue of information security began to attach paramount importance.

The widespread use of cloud computing, remote connectivity from mobile and landline devices through general purpose networks has led to the "disappearance of the perimeter" of critical systems and a significant complication of their protection. Therefore, security of information and telecommunications systems has become one of the priorities in the modern world. In fact, any message, data block or program code requires the provision of basic security services (preventing unauthorized modification, and in many cases, unauthorized review). To provide basic security services in the context of hybrid and synergistic threats, cryptographic mechanisms based on symmetric (block) or asymmetric cryptography are typically used. The former provide fast cryptotransformatios, but are classified as a secret model of temporary stability, the latter (open-key cryptosystems) provide evidential stability, but produce cryptotransformations slower than 3-5 orders of magnitude slower than symmetric cryptosystems. In practice, fast symmetric cryptographic algorithms are used to provide confidentiality and data integrity services, and asymmetric cryptography algorithms are used to distribute and replace key symmetric cryptos in key data systems. One of the practical algorithms of symmetric cryptography, which is used in automated banking systems, systems of power structures in the post-Soviet space is the algorithm GOST 28147-89, which is defined in the standard of Ukraine – GOST 28147: 2009, Russia – GOST R-3412 - 2015 (code Magma (GOST 28147-89), code "Grasshopper") [1,2]. Thus, despite the long-term development of block symmetric cipher (BSC) GOST 28147-89, this algorithm is used and proposed to be used in modern complex information security methods (CISM) [3–6].

According to the analysis of NIST US specialists in 2018–2019, there are significant doubts in the cryptostability of traditional and asymmetric cryptography algorithms, given the emergence of full-scale quantum

computers that will allow attackers (cybercriminals) to attack and harass criminals. To counteract such threats, in 2018 NIST US launched a competition to develop a post-quantum cryptography algorithm. Thus, in order to increase the level of crypto-stability, a topical question arises in the development or modification of modern algorithms for block-symmetric encryption, taking into account the requirements for post-quantum cryptography in the conditions of modern threats, namely the increase of the level of crypto-stability of block symmetric cipher, GOST 28147, used in practice.

II. FORMULATION OF THE PROBLEM AND ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

An effective method of data protection is encryption. The growing capabilities of crypto-analysts and the power of computing technology are forcing us to seek new ways of encryption or to improve the already known ones [7]. One of the common methods of cryptographic information security is block-symmetric ciphers. Block-symmetric ciphers are one of the most common cryptographic primitives. Symmetric block encryption algorithms are one of the most common cryptographic primitives. In addition to providing confidentiality when transmitting and storing information, block-symmetric ciphers are used as basic elements when constructing message authentication codes or generating pseudorandom sequences. For block ciphers, key size determines the value for stability / cost, the number of encryption rounds for reliability / performance, and hardware features for performance / price. As a rule, any two of the three development goals can be easily achieved, while meeting all three requirements is an extremely difficult task [8]. The main advantages of block ciphers include the similarity of encryption and decryption procedures, which usually differ only in order of action. This simplifies the creation of encryption devices, since it allows to use the same blocks in the encryption and decryption chains. The flexibility of block ciphers allows them to be used to build other cryptographic primitives: a pseudorandom sequence generator, a current cipher, an imitation insert, and cryptographic hash codes. Until 2015, DSTU GOST 28147: 2009 (based on GOST 28147-89) [9] was used as the national encryption standard in Ukraine [9], which still provides practical stability in Lavina-E, Triton-E cryptographic security complexes [3], automated banking systems [1], systems of power structures in the post-Soviet space GOST R 34.12 - 2015 (Magma code) [2]. The advantages of the algorithm allow its use in various fields of technology, so [10] proposes a combination of BASE64 and GOST algorithms, which will protect all types of data that exist and easily return to their original form without damaging the original data. This approach, according to the authors, will improve data security by combining transformations. The results of the combination of Base64 and GOST algorithms will allow them to be used to increase the level of cryptostability for various data objects, both in dynamic (online encryption mode) and static (information storage mode).

The GOST 28147–2009 algorithm (DSTU GOST 28147: 2009) was standardized in 1989 and became the official standard for the protection of confidential information for the first time, but the cipher specification remained closed. In 1994, the standard was declassified, published and translated into English. By analogy with the AES (and unlike DES), GOST 28147-89 (DSTU GOST 28147: 2009) is allowed to protect classified information without restriction, as specified in the Russian standard. GOST 28147-89 (DSTU GOST 28147: 2009) is a very serious code that meets the military criteria, designed with the purpose of the most serious applications. A distinguishing feature of the GOST 28147-89 algorithm (DSTU GOST 28147: 2009) is the use of non-fixed replacement units in its structure. It is assumed that with any S-block filling, thirty-two rounds of encryption will be sufficient to withstand such powerful methods of analysis as linear and differential cryptanalysis. The method of linear cryptanalysis, first proposed for the analysis of the DES algorithm [11], is based on the compilation of linear analogs, which with a certain probability describe the work of the crypto algorithm. After the advent of this work, most of the encryption algorithms existing at that time were subjected to analysis using this method. Studies have shown that the linear cryptanalysis method is universal, that is, it can be applied to the analysis of most known symmetric cryptosystems.

For a long time, it was thought that if you keep the S-blocks secret, they can be considered as an additional key [12,13]. However, in [14], a method is proposed, which makes it possible to simply recover the values of the S-blocks used for data encryption.

For more than a quarter of a century, the cryptographic algorithm described in GOST 28147-89 (DSTU GOST 28147: 2009) has been analyzed in the field of cryptography. One of the most well-known results of cryptographic analysis of GOST 28147-89 (GOST 28147: 2009) algorithm is [15], which states that the stability of GOST 28147-89 (GOST 28147: 2009) algorithm can be reduced in comparison with a complete search of the key set, but only in the presence of a large number of known malefactor pairs of plain and plaintext. The main problems of GOST 28147-89 (DSTU GOST 28147: 2009) are related to the incompleteness of the standard regarding the generation of keys and replacement tables. It is believed that the algorithm has "weak" keys and replacement tables [16,17].

In [12], an analysis of GOST 28147–89 (DSTU GOST 28147: 2009) was performed, which shows that the algorithm can be broken by using differential cryptanalysis, only in the case of weak replacement tables, and also presented an algorithm for finding weak S-blocks. The use of this algorithm allows to determine the blocks of use which can weaken the stability of the encryption algorithm with respect to linear cryptanalysis.

[18] presents a compressed attack on the GOST 28147-89 algorithm (DSTU GOST 28147: 2009), which can recover a key with temporal complexity that requires additional research to refine the algorithm in terms of synergistic and hybrid attacks.

To increase the cryptographic stability of GOST 28147-89 (DSTU GOST 28147: 2009), [19] proposed an approach of introducing the dependence of the round keys on the current value of the converted data and the unknown for the attacker of the sequence of subkey selection on the encryption rounds.

III. MATERIALS RESEARCH

This template, modified in MS Word 2003 and saved as "Word 97-2003 & 6.0/95 – RTF" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

The aim of the study is to develop methods for improving cryptotransformations in the block-symmetric encryption algorithm GOST 28147-89 (DSTU GOST 28147: 2009) by increasing the length of subbands from 32 bits to 64 bits, which allows to process input blocks with a length of 128 bits and increase the key from 256 bits to 512 bits without significant changes in the basic steps of the GOST 28147-89 algorithm (DSTU GOST 28147: 2009).

To achieve this goal, the following tasks were set:

– to analyze the rate of cryptotransformations of practical block encryption algorithms;

− to develop methods of increasing the level of cryptostability of the GOST 28147-89 algorithm (DSTU GOST 28147: 2009) and to increase the length (number) of S-blocks, and to enter the assembly operation modulo 264, which in total makes it possible to increase the input blocks up to 128 bits and / or increase the key sequence to 512 bits;

− to perform the analysis of the proposed algorithm modification solutions for the calculation of the processor operations required for ciphertext formation.

One of the most common approaches when constructing symmetric block ciphers is to use the Feistel network, which allows to obtain the properties of a pseudorandom permutation by repeatedly using a pseudorandom function (round transformation) [20]. Basic cycles are the repeated execution of a basic step using different key elements and differ from each other only by the number of repetitions of the step and the order of use of key elements.

That is, 32-bit fragments are consistently used in encryption rounds K0, K1,…, K7 of the original 256-bit encryption key in the following order: K0, K1, …, K7 – with the exception of the last 8 rounds – the rounds from the 25th to the 31st are used in reverse order K7, K6, …, K0.

It is believed that the stability of the algorithm is determined by the structure of the S-blocks. The input and output of S-blocks are 4-bit numbers, so each S-block can be represented as a string of numbers from 0 to 15, arranged in some order. Then the sequence number will be the input value of the S-blocks, and the number will be the output value of the S-blocks. The scheme of the basic step of cryptotransformation of GOST 28147-89 algorithm (DSTU GOST 28147: 2009) is shown in Fig. 1. The main advantages of GOST 28147-89 (DSTU GOST 28147: 2009) include:

– futility of attack by a complete search;

– ease of implementation and efficient implementation, respectively, high-speed encryption on modern computers.

An increase in BSC crypto-stability is proposed in the algorithm Rijndael (AES, Advanced Encryption Standard) by using dynamic keys based on the multiplication of the converted plaintext block to a polynomial matrix. This mechanism is used in the Kalina BSS (DSTU 7624-2015) and the second GOST R 3412-15 standard.

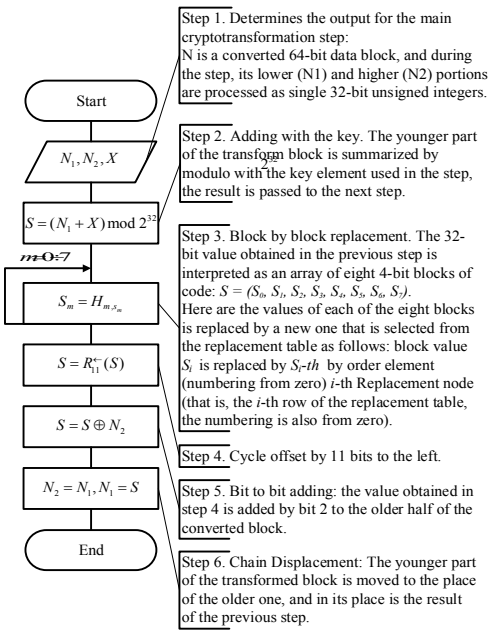

Figure 1. Scheme of the basic step of cryptotransformation algorithm GOST 28147-89 (DSTU GOST 28147: 2009).

In the 1960s, when information technology and computer technology began to flourish, a new science, quantum information theory, emerged. Studying quantum-mechanical states and their ability to participate in the process of information transfer and processing. Quantum theory is a mathematical model of the modern understanding of the physical properties of the surrounding world and physical systems [21].

In the case of appearance a quantum computer that can run the quantum algorithm of Shore cryptanalysis [22] and Grover [23], certain mathematical problems can be solved even with polynomial complexity. Therefore, there may be threats in the information field regarding the provision of cryptographic stability for both asymmetric cryptotransformations and certain symmetric ones. A detailed description of the stability of symmetric systems against quantum cryptanalysis is given in Table I and in [24].

TABLE I. STABILITY OF STANDARD BLOCK SYMMETRIC ENCRYPTION ALGORITHMS AGAINST QUANTUM CRYPTO ANALYSIS

№	Type of crypto system	Block/key size (bit)	The amount of memory needed to attack, qubits	Resistance to attack on	
				message block	key
1	AES–128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
2	AES–256	128/256	128/256	2^{64} ($10^{19,2}$)	2^{128} ($10^{38,4}$)
3	DES	64/56	64/56	2^{32} ($10^{9,6}$)	2^{28} ($10^{8,4}$)
4	GOST–28147	64/256	64/256	2^{32} ($10^{9,6}$)	2^{128} ($10^{38,4}$)
5	Kalina-128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
6	Kalina-512	512/512	512/512	2^{256} ($10^{76,8}$)	2^{256} ($10^{76,8}$)

Table I shows that the stability of symmetric ciphers when attacked using a quantum algorithm is significantly reduced. This means that DES can be completely compromised and cannot be considered stable, its stability will be 228. Even with AES, it is desirable to use a 256 bit key. That is, in general, Grover's algorithm, although it reduces the stability of modern symmetric cryptosystems, still requires a sub-exponential number of quantum gates, unlike the Shore algorithm.

The results presented in Table I require an increase in the length of the key sequence in modern block-symmetric ciphers, including GOST 28147-89 (DSTU GOST 28147: 2009). It is desirable to use symmetric cryptosystems with system-wide parameters of more than 256 bits that can be considered resistant to quantum cryptanalysis based on the Grover algorithm [23].

Tables II-V show the comparative results of studies of the rate of BSC cryptotransformations that are used in practice in modern CSIS. Implementation was carried out for different platforms: Odroid HC2 (lUbuntu 18.04, 32-bit, ARMv7-a Cortex-A17.Cortex-A7), RaspberryPI 4 (lUbuntu 18.04, 64-bit, ARMv8-a Cortex-A53), Asus Tinkerboard (TinkerOS , 32-bit, Cortex-A17 ARMv7-a). For measurement, we used the Cipher + v2.1 library [24], which has expert opinion of the State Secretariat of Communications of Ukraine on the correctness of implementation of cryptographic algorithms and their use [25].

TABLE II. RESULTS OF ESTIMATION OF SPEED OF CRYPTOTRANSFORMATIONS IN DIFFERENT MODES OF ENCRYPTION (ODROID HC2 (LUBUNTU 18.04, 32-BIT)

BSC mode	GOST 28147-89 [256 bit]	AES [256 bit]	DES [64 bit]	TDES [192 bit]	DSTU 7624:2014 [256-256]
Encrypt ECB	30.1637 MB/s	63.3521 MB/s	36.3114 MB/s	12.8773 MB/s	27.4637 MB/s
Encrypt CTR	29.6478 MB/s	60.3086 MB/s	35.5076 MB/s	12.6535 MB/s	26.8965 MB/s
Encrypt CFB	30.2113 MB/s	62.7216 MB/s	36.0103 MB/s	12.6727 MB/s	27.1915 MB/s
Encrypt OFB	30.243 MB/s	64.0648 MB/s	41.9519 MB/s	13.6511 MB/s	27.3882 MB/s
Encrypt CBC	29.8577 MB/s	58.1844 MB/s	35.6153 MB/s	13.1662 MB/s	27.1583 MB/s
MAC	MAC [32] 58.7775 MB/s	MAC [16] 62.8684 MB/s	MAC [8] 38.4901 MB/s	MAC [8] 1.38384 MB/s	27.4141 MB/s

TABLE III. RESULTS OF ESTIMATION OF SPEED OF CRYPTOTRANSFORMATIONS IN DIFFERENT MODES OF ENCRYPTION (ODROID HC2 (ARMV7-A CORTEX-A17.CORTEX-A7)

BSC mode	GOST 28147-89 [256 bit]	AES [256 bit]	DES [64 bit]	TDES [192 bit]	DSTU 7624:2014 [256-256]
Encrypt ECB	30.1637 MB/s	61.4251 MB/s	41.7321 MB/s	15.3814 MB/s	51.4927 MB/s
Encrypt CTR	30.0124 MB/s	56.88 MB/s	38.0042 MB/s	14.8546 MB/s	50.0886 MB/s
Encrypt CFB	29.3113 MB/s	59.4122 MB/s	40.7367 MB/s	15.2402 MB/s	50.6435 MB/s
Encrypt OFB	30.0146 MB/s	61.4688 MB/s	44.9945 MB/s	15.7744 MB/s	51.1768 MB/s
Encrypt CBC	29.1913 MB/s	60.6436 MB/s	42.0668 MB/s	15.4144 MB/s	51.302 MB/s
MAC	MAC [32] 58.151 MB/s	MAC [16] 60.1394 MB/s	MAC [8] 44.9826 MB/s	MAC [8] 15.9271 MB/s	54.1123 MB/s

TABLE IV. RESULTS OF ESTIMATION OF SPEED OF CRYPTOTRANSFORMATIONS IN DIFFERENT MODES OF ENCRYPTION (RASPBERRYPI 4 (LUBUNTU 18.04, 64-BIT, ARMV8-A CORTEX-A53)

BSC mode	GOST 28147-89 [256]	AES [256 bit]	DES [64 bit]	TDES [192 bit]	DSTU 7624:2014 [256-256]
Encrypt ECB	25.0504 MB/s	59.2453 MB/s	34.9145 MB/s	12.7049 MB/s	46.0961 MB/s
Encrypt CTR	24.905 MB/s	54.1214 MB/s	33.64 MB/s	12.6163 MB/s	44.8905 MB/s
Encrypt	24.2883	57.5137	34.9716	12.7023	45.8623

CFB	MB/s	MB/s	MB/s	MB/s	MB/s
Encrypt OFB	24.5271 MB/s	59.8068 MB/s	37.2013 MB/s	13.041 MB/s	46.1758 MB/s
Encrypt CBC	24.1828 MB/s	58.2614 MB/s	34.6554 MB/s	12.6704 MB/s	45.8618 MB/s
MAC	MAC [32] 48.514 MB/s	MAC [16] 58.9047 MB/s	MAC [8] 37.0322 MB/s	MAC [8] 13.0943 MB/s	41.1067 MB/s

TABLE V. RESULTS OF ESTIMATION OF SPEED OF CRYPTOTRANSFORMATIONS IN DIFFERENT MODES OF ENCRYPTION (ASUS TINKERBOARD (TINKEROS, 32-BIT, ARMV7-A CORTEX-A17)

BSC mode	GOST 28147-89 [256]	AES [256 bit]	DES [64 bit]	TDES [192 bit]	DSTU 7624:2014 [256-256]
Encrypt ECB	29.6252 MB/s	50.0463 MB/s	31.6846 MB/s	12.7874 MB/s	21.6193 MB/s
Encrypt CTR	28.9882 MB/s	47.7739 MB/s	30.5259 MB/s	12.6454 MB/s	20.8175 MB/s
Encrypt CFB	29.4786 MB/s	49.4106 MB/s	31.0148 MB/s	12.7495 MB/s	21.7054 MB/s
Encrypt OFB	29.4421 MB/s	50.1308 MB/s	35.9993 MB/s	13.3862 MB/s	22.0405 MB/s
Encrypt CBC	29.0924 MB/s	49.4424 MB/s	30.9995 MB/s	12.6811 MB/s	22.0167 MB/s
MAC	MAC [32] 57.2663 MB/s	MAC [16] 49.6144 MB/s	MAC [8] 35.9926 MB/s	MAC [8] 1.34331 MB/s	22.1839 MB/s

The tables above confirm the results of the estimation of the speed of transformations of BSC in the work [6], in which it is noted that the Kalina-256 algorithm is inferior to AES and GOST 28147-89 both in terms of performance and memory requirements. It is especially advisable to use the algorithm GOST 28147-89 (DSTU 28147 - 2009) instead of "Kalina" in the strict requirements for the amount of code [6]. The analysis of the tables II-V confirms that the GOST 28147-2009 (DSTU 28147 - 2009) algorithm has advantages over the cryptotransformation rate over all practical algorithms (including the "Grasshopper" RF GOST P3412 - 2015) except the APS NPP. This allows us to consider the algorithm as a practical algorithm in CSIS.

Development of a method of increasing the level of cryptotransformation of the GOST 28147-89 algorithm (DSTU GOST 28147: 2009) by increasing the length of S-blocks (option 1)

When conducting the AES competition, the algorithm of block encryption DFS (Decorrelated Fast Cipher) was developed [27]. The algorithm was created through the collaboration of two organizations: the telecommunications giant France Telecom and the higher education institution Ecole Normale Superieure (ENS).

DFC is a block cipher with a block length of 128 bit representing 8-round Feistel Network. A 64-bit encryption function with eight different round keys is used Ki, i-1…n, n = 8 each 128 bit, which are obtained from one source encryption key. Each round, the encryption function uses the left half of the source text (block) and the two 64-bit keys, which are half the corresponding round, to obtain 64-bit encrypted text. The resulting encrypted left half of the block is added to the right. Then, according to the idea of the Feistel network, the left and right parts of the block change places. Decryption is the same as encryption using round keys in the reverse order. The length of the encryption output key is not limited to the three fixed sizes specified by the AES contest (128, 192, and 256 bits) and can be variable in size from 0 to 256 bits. During the encryption, the assembly operation is performed on the module 2128. The results of studies of this algorithm make it possible to make changes to the algorithm of the basic step GOST 28147-89 (DSTU GOST 28147: 2009), which is presented in Fig. 2.

The distinctive stages of advanced cryptotransformations of the main step of GOST 28147-89 (DSTU GOST 28147: 2009) are steps 1 – 4. In Fig. 2 the length of each S-block is increased from S0, S1,…, S15 to S0, S1, …, S255.

The changes made in Step 3 make it possible to increase the length of the sub-blocks to 64 bits and prevent the S-block from being overrun completely (from 16! To 256! Possible combinations), but require an increase in memory to store eight S-blocks measuring 256 bytes each. In GOST 28147-89 (DSTU GOST 28147: 2009) the length of the S block is 64 bits.

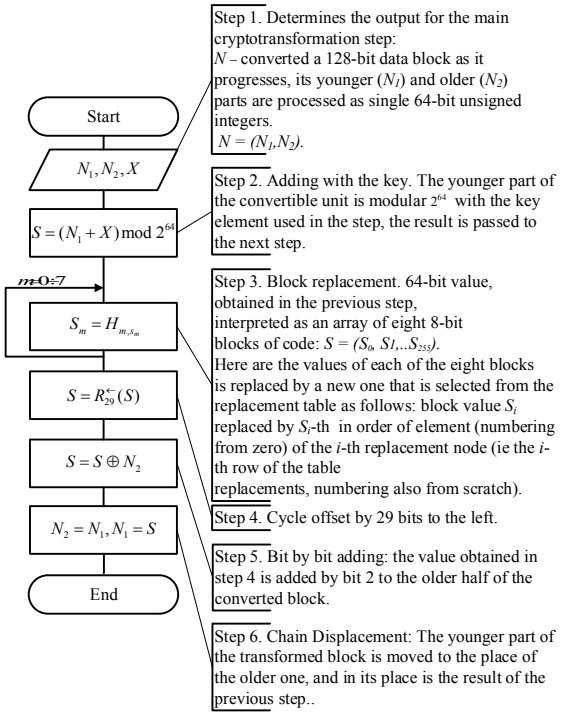

Figure 2. Scheme of the basic step of cryptotransformation GOST 28147-89 (GOST 28147: 2009) with extended S-block length (option 1).

Thus, the proposed method of increasing the level of cryptostability is based on increased lengths of the S-block, which allows to increase the level of cryptostability

in proportion to the increase in the length of the round tables of nonlinearity.

Development of a method of increasing the level of cryptotransformation of the GOST 28147-89 algorithm (DSTU GOST 28147: 2009) by increasing the length of S-blocks (option 2)

The distinctive stages of advanced cryptotransformations of the main step of GOST 28147-89 (DSTU GOST 28147: 2009) are steps 1-4 shown in Fig. 3.

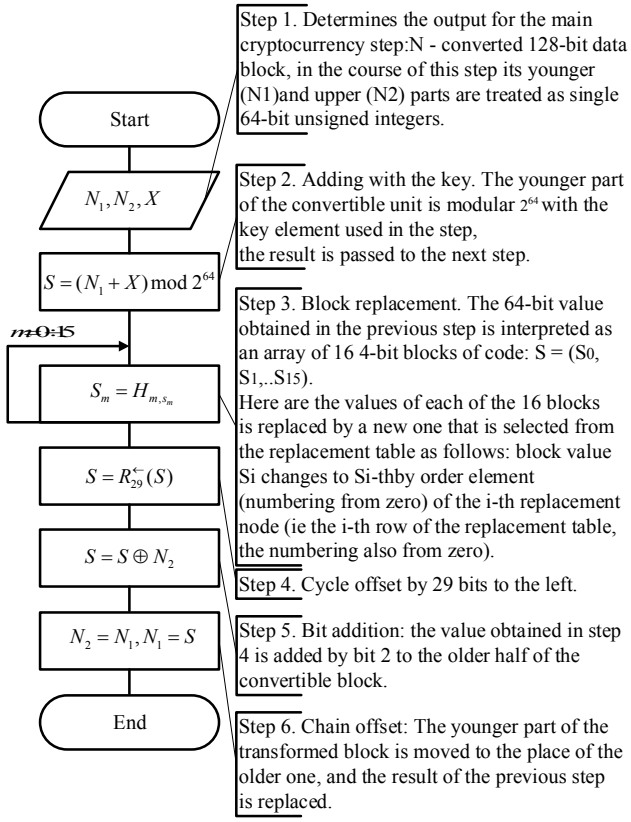

Figure 3. Scheme of the basic step of cryptotransformation with increased number S-blocks (option 2).

The changes made in step 3 increase the number of S-blocks from 8 to 16 and make it possible to increase the length of plain text sub-blocks to 64 bits. In general, the length of the plaintext input block increases to 128 bits. The changes require an increase in memory to store sixteen bits of S-blocks. Thus, the proposed method of increasing the level of crypto-stability is based on increased numbers of S-blocks, which allows to increase the level of crypto-stability by increasing the key space of the round keys.

Discussion of results of modification methods of GOST 28147-89 (DSTU GOST 28147: 2009)

The proposed methods of increasing the level of crypto-stability in changes of the basic step of cryptotransformation GOST 28147-89 (DSTU GOST 28147: 2009) allow to increase the length of the key sequence from 256 bits to 512 bits, without changing the basic steps used in GOST 28147-89, which significantly complicates conducting brute force attacks, and cryptanalysis methods.

In [28] the complexity of operations in an integer ring, expressed in processor operations, are presented, which are presented in Table VI (w – dimension of machine word, m – the length of the binary equivalent number).

TABLE VI. THE COMPLEXITY OF OPERATIONS IN AN INTEGER RING, EXPRESSED IN THE OPERATIONS OF THE PROCESSOR

Mathematical operation	Number of CPU operations
Classic modulo cast	$\frac{m}{w}\left(\frac{m}{w}+2\right)+\frac{m}{w}$
Modulo cast by Barret	$\frac{m}{w}\left(\frac{m}{w}+4\right)$
Modulo cast by Montgomery	$\frac{m}{w}\left(\frac{m}{w}+1\right)$
Adding without modulo cast	$\frac{m}{w}$
Subtraction without modulo cast	$\frac{m}{w}$
Montgomery multiplication without modulo cast	$\left(2\frac{m}{w}^{3}+2V\right)+\left(4\frac{m}{w}^{2}+6\frac{m}{w}+2\right)$

Using the values from Table VI we will calculate the processor operations for the main step of cryptotransformation of algorithms GOST 28147-89 (DSTU GOST 28147: 2009) and GOST 28147-89 (DSTU GOST 28147: 2009) (Option 1, Option 2) (Table VII).

TABLE VII. THE NUMBER OF PROCESSOR OPERATIONS FOR THE MAIN STEP OF CRYPTOTRANSFORMATION GOST 28147-89 (GOST 28147: 2009) AND GOST 28147-89 (GOST 28147: 2009) (OPTION 1, OPTION 2)

Step number	GOST 28147–89 (DSTU GOST 28147:2009) ($m=32$)	Advanced GOST 28147-89 (DSTU GOST 28147:2009) (option 1, $m=64$)	Advanced GOST 28147-89 (DSTU GOST 28147:2009) (option 2, $m=64$)

Step number	GOST 28147–89 (DSTU GOST 28147:2009) ($m = 32$)	Advanced GOST 28147-89 (DSTU GOST 28147:2009) (option 1, $m = 64$)	Advanced GOST 28147-89 (DSTU GOST 28147:2009) (option 2, $m = 64$)
Step 1	$3\frac{m}{w}$ (three input operators)	$3\frac{m}{w}$ (three input operators)	$3\frac{m}{w}$ (three input operators)
Step 2	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method
Step 3	$8\frac{m}{w}$ block by block replacement (8 blocks)	$8\frac{m}{w}$ block by block replacement (8 blocks)	$16\frac{m}{w}$ block by block replacement (8 blocks)
Step 4	$\frac{m}{w}$ cyclic shift	$\frac{m}{w}$ cyclic shift	$\frac{m}{w}$ cyclic shift
Step 5	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method	$\frac{m}{w}+\frac{m}{w}\left(\frac{m}{w}+1\right)$ ading and module cast by the Montgomery method
Step 6	$2\frac{m}{w}$ offset by a chain (2 operators)	$2\frac{m}{w}$ offset by a chain (2 operators)	$2\frac{m}{w}$ offset by a chain (2 operators)
Total	$16\frac{m}{w}+2\frac{m}{w}\left(\frac{m}{w}+1\right)$	$16\frac{m}{w}+2\frac{m}{w}\left(\frac{m}{w}+1\right)$	$24\frac{m}{w}+2\frac{m}{w}\left(\frac{m}{w}+1\right)$
Total for $w = 64$	9,5 oper./32 bits	20 oper./64 bits	28 oper./64 bits
In total for the encryption cycle	304 oper./64 bits	640 oper./128 bits	896 oper./128 bits
Number of operations for forming 1 bit of ciphertext	4,75	5	7

Results that shown in Table VII confirm the possibility of applying the proposed methods of increasing the level of stability of the block symmetric cipher GOST 28147-89 (DSTU GOST 28147: 2009) by increasing the length of the S-block and / or increasing the number of S-blocks without significant energy costs for the formation of cryptograms. Thus, the conducted analysis of energy costs allows to provide practical implementation of the proposed methods of increasing the stability of the algorithm in the post-quantum period.

The performed analysis of works [29–34] showed that the current state of the computer technology theoretically allows to consider the possibility of breaking modern practical algorithms of symmetric encryption, such as AES, Kalina (DSTU 7624: 2014), GOST 28147 - 2009 (DSTU GOST 28147: 2009). , GOST R-3412 - 2015 ("Magma" (GOST 28147 - 2009), "Grasshopper"), but their sustainability satisfies them to ensure the confidentiality and integrity of information resources.

IV. Conclusion

1. An analysis of the formation of block symmetric ciphers on the basis of the Feistel network (chain) showed that the main element that provides nonlinearity of cryptotransformations is the S-box. That is why its stability provides cryptographic stability of keys (master key, round keys) and allows to resist modern attacks based on cryptanalysis methods. Thus, in order to provide the required level of cryptostability of the algorithm as a whole, methods (approaches) are needed that will allow to increase the key data in the S-box (S-box).

2. The proposed methods of increasing the level of stability provide an improvement of the basic step of

cryptotransformation, which is used in the algorithm of block-symmetric encryption GOST 28147-89 (DSTU GOST 28147: 2009). The proposed solutions allow to change the key sequence from 256 bits to 512 bits without changing the basic steps of GOST 28147–2009 (DSTU GOST 28147: 2009) algorithm. Increasing the number of S-blocks will increase the space of key data, provide the required level of encryption stability of ciphertext and process 128 bit data streams, which can increase the speed of cryptotransformations. The proposed solutions require an increase in the size (length) of S-blocks, which leads to an increase in memory for storing S-blocks, but in the opinion of the authors in the conditions of rapid development of computing this is not fundamental.

3. The analysis of the proposed results in the calculation of processor operations for the formation of ciphertext confirms their practical implementation, which is slightly different from the energy costs (number of operations) of the processor for the formation of ciphertext. Thus, there is a practical opportunity to provide the required level of cryptographic stability of the algorithm GOST 28147 - 2009 (DSTU GOST 28147: 2009) in the conditions of requirements for post-quantum cryptography algorithms.

ACKNOWLEDGMENT

Research is supported by University of Bielsko-Biala, Poland.

REFERENCES

[1] On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine https://zakon.rada.gov.ua/laws/show/v0095500-17.

[2] National Standard of the Russian Federation GOST P 34.12 – 2015 https://meganorm.ru/Data2/1/4293762/4293762704.pdf

[3] Devices for information protection http://www.tritel.ua/index.php/ru/produktsiya/sposobi-kzi/lavina-e2013-04-29-12-25-54/lavina-e2013-05-31-15-34-12/kompleks-kriptograficheskoj-zashchity-detail.

[4] Speed cipher "Kalina" and AES https://cyberleninka.ru/article/n/bystrodeystvie-shifrov-kalina-i-aes/viewer

[5] An integrated approach to assessing the reliability of a standard GOST P 34.12 https://cyberleninka.ru/article/n/kompleksnyy-podhod-k-otsenke-nadezhnosti-standarta-gost-r-34-12-2015/viewer.

[6] Effective implementation of the GOST 7624: 2014 block symmetric encryption algorithm («Kalina») for 8/16/32-bit embedded systems http://journals.dut.edu.ua/index.php/dataprotect/article/view/1575.

[7] Avdonin I.A., Budko M.B., Grozov V.A. Organization of protection of data transmitted between unmanned aerial vehicle and ground control station, based on Vernam cipher//Scientific and technical journal of information technologies, mechanics and optics. 2016. T. 16. No. 5. P. 850-855.

[8] Agafin C.C. LW-Modification of encryption algorithm GOST 28147-89/S.S. Agafin S.S.//Security of information technologies. - 2011. - Volume 18 № 4. - P. 109-112

[9] GOST 28147–89 System of information processing. The cryptographic protection. Cryptographic transformation algorithm – M.: Gosstandart of the USSR, 1989.

[10] Combination Base64 and GOST algorithm for security process https://iopscience.iop.org/article/10.1088/1742-6596/1402/6/066054/pdf

[11] Matsui M., Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998. – 386 p.

[12] Babenko L.K., Ishhukova E.A. (2014) Analiz algoritma GOST 28147-89: poisk slabyh blokov // [Algorithm analysis GOST 28147-89: search for weak blocks] Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki. № 2 (151). p. 129 – 138.

[13] Babenko L.K., Ishukova E.A. (2014). Ispol'zovanie slabyh blokov zameny dlja linejnogo kriptoanaliza blochnyh shifrov // [Using weak replacement blocks for linear cryptanalysis of block ciphers] News SFU. Technical science. Thematic issue on "Information security". – Taganrog: Izd-vo TTI JuFU. – № 2(151). – S. 136–147.

[14] Saarien M.-J. A Chosen Key Attack Against the Secret S–boxes of GOST (1998) (unpublished manuscript)

[15] T. Isobe. A Single-Key Attack on the Full GOST Block Cipher, LNCS v. 6733, p. 290–305. Springer, 2011.

[16] A.V. Levkov, A.N. Molchanov (2016). K voprosu o perehode na novyj standart shifrovanija GOST 34.12–2015 // [On the issue of transition to the new encryption standard GOST 34.12–2015] Jelektronnyj zhurnal: nauka, tehnika i obrazovanie. – №4(9). – s. 68–74.

[17] Rostovcev A.G., Mahovenko E.B., Filippov A.S., Chechulin A.A. (2003). O stojkosti GOST 28147–89 // [About resistance GOST 28147–89] Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. – S. 75–83.

[18] Linzhen Lu. A compress slide attack on the full GOST block cipher / Lu Linzhen, Chen Shaozhen // Information Processing Letters . – 2013. – № 113 – p. 634 – 639

[19] Lysenko I. V. Approach to formation of the schedule of keys for a block symmetric cryptoalgorithm of GOST 28147 89 / I.V. Lysenko, G.A. Gvozdinsky / / weapon systems and military equipment. - 2018. - No 1 (53). – p. 163 – 167
Feistel H. Cryptography and Computer Privacy / H. Feistel // Scientific American. – 1973. – V. 228, N. 5. – p. 15–23.

[20] Ryabyy M. Review of current methods of quantum and post-quantum cryptography // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 236–241

[21] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P. W. Shor //S IAM J. Comput. – 1997. – 26 (5). – P. 1484–1509.

[22] Grover L. K. A fast quantum mechanics algorithm for database search [Text] / L. K. Grover // Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. – 1996. – P. 212–219

[23] Biblioteki «ShIFR+» V 2.1. URL: https://cipher.com.ua/uk/products/cipher-plus-version-2-1

[24] V. I. Yesin, M. Karpinski, M. V. Yesina, V. V. Vilihura, O. Veselska and L. Wieclaw, "Approach to Managing Data From Diverse Sources," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 1-6.

[25] Gorbenko Ju. I. (2014). Analiz stijkosti populjarnih kriptosistem proti kvantovogo kriptoanalizu na osnovi algoritmu Grovera / Ju. I. Gorbenko, R. S. Ganzja // [The stability analysis of popular cryptosystems against quantum cryptanalysis based on Grover's algorithm] Zahist informacii: naukovo-praktichnij zhurnal. – K. – Tom 16, № 2. – S. 106–112.

[26] On The Decorrelated Fast Cipher (DFC) and Its Theory? Lars R. Knudsen and Vincent Rijmen https://www.esat.kuleuven.be/cosic/publications/article-367.pdf

[27] Avanzi R., Batina L., Chevallier–Mames B. etc. D.VAM.1 Performance Benchmarks. Revision 1.1 / In: M. Joye ed. // ECRYPT Research report IST–2002–507932. European Network of Excellence in Cryptology. August 3, 2005. –87 p.

[28] Voronkov B.N. (2016) K analizu novyh rossijskih kroptostandartov / B.N. Voronkov [To the analysis of new Russian crop standards] // Vesnik fakul'teta Prikladnoj matematiki,

informatiki i mehaniki,Voronezh, Izd. dom VGU, vyp. 12, 2016, s. 57–60.

[29] Churkin R.V. Ocenka kriptostojkosti algoritma shifrovanija GOST 28147-89 [Evaluation of the cryptographic strength of the encryption algorithm GOST 28147-89] / R.V. Churkin, E.L. Krotova // Nauchnye issledovanija: ot teorii k praktike : materialy VIII Mezhdunar. nauch.-prakt. konf. (Cheboksary, 7 ijunja 2016 g.). V 2 t. T. 1 / redkol.: O.N. Shirokov [i dr.] – Cheboksary: CNS «Interaktiv pljus», 2016. – S. 294-297.

[30] Ocenka kriptostojkosti tablic zamen algoritma gost 28147-89, [Evaluation of the cryptographic stability of the substitution tables of the GOST 28147-89 algorithm] URL: https://cyberleninka.ru/article/n/otsenka-kriptostoykosti-tablits-zamen-algoritma-gost-28147-89.

[31] Analiz verojatnostej differencialov blochnogo shifra «Kalina» (DSTU 7624:2014) [The analysis of the probabilities of differentials of the block cipher Kalina (DSTU 7624: 2014)] URL: http://journals.uran.ua/eejet/article/viewFile/139682/144404

[32] Merinov A., Nesterov K., Zhdanov O. Improvement of the construction technique of substitution blocks for symmetric encryption algorithms / A. S. Merinov, K. A. Nesterov, O. N. Zhdanov //, Sibirskij zhurnal nauki i tehnologij. Tom 20, № 1, s. 20–27.

[33] Obzor atak na AES-128: k pjatnadcatiletiju standarta AES. URL: https://cyberleninka.ru/article/n/obzor-atak-na-aes-128-k-pyatnadtsatiletiyu-standarta-aes

[34] Cryptanalysis of ForkAES. URL: https://eprint.iacr.org/2019/289.pdf