Methods of information systems protection

UDC 004.056.55 **doi:** https://doi.org/10.20998/2522-9052.2021.2.19

Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Anastasiya Nimchenko

Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

DEVELOPMENT OF PROCEDURES FOR MODIFYING THE CIPHER GOST 28147

Abstract. The entry of mankind into the era of high technologies, the rapid growth of computer technology contributes to the expansion of the range of electronic services. To ensure the security of confidential information, personal data, cryptographic systems of traditional cryptography (symmetric cryptosystems) and public key cryptography (asymmetric cryptosystems) are used. As a rule, the former provides security services, the latter provide key distribution. However, in the conditions of totalitarian surveillance in society by the special services of developed countries, cryptographic tabs are embedded in cryptographic algorithms, which, on the one hand, provide “quick” access for special services to confidential information, and on the other hand, allow intruders to break into the cryptosystem and obtain user data. The article proposes a modification of the well-known GOST 28147-89 algorithm, which ensures the "elimination" of possible crypto-bookmarks and an increase in crypto-resistance in the post-quantum period (the emergence of a full-scale quantum computer that allows hacking modern symmetric and asymmetric cryptosystems based on Grover and Shor algorithms). It is proposed to use the procedures for modifying the block-symmetric encryption algorithm (BSEA) GOST 28147-89 (2009, 2015) in OFB mode, which will make it possible to form a pseudo-random sequence based on dynamic changes in the S-box, and provide the required level of security.

Keywords: block-symmetric cipher; stream cipher; GOST 28147-89; DSTU 28147-2009.

Problem statement

The entry of mankind into the era of high technologies, 4.0 Industrialization allowed the rapid growth of the computing capabilities of the world community, which made it possible in 2015 to develop and implement not only 1 billion Internet things that replenished cyberspace, but also practically made it possible to realize a full-scale quantum computer. A quantum computer allows computing several billion times faster, expanding the range of services in almost all areas of life. This circumstance is an unconditional positive factor affecting the innovative nature of the development of the real sector of the economy, healthcare, services, leisure and, of course, education. However, along with this, this trend is increasingly revealing the acuteness of the problems, the negative consequences of informatization. To the greatest extent, these problems are associated with the possibilities of unauthorized access to information resources, critical infrastructure facilities belonging to other individuals, business entities, the banking sector, and other states. This is directly related to the need to ensure not only national, but also state security [1].

Analysis of recent research and publications

The widespread use of cloud technologies, means of remote connection from mobile and remote stationary devices through general-purpose networks lead to the “disappearance of the perimeter” of critical systems and a significant complication of their protection. All this leads to the need to implement security at least of the security loop of business processes that ensure the continuity of production and form the profits of companies (organizations, etc.). A prerequisite for this is the use of cryptographic means of protection in modern information, communication and cyber-physical systems. Symmetric block ciphers are one of the most common cryptographic systems that provide the basic security services of modern ISO/OSI model protocols and cyberspace. In addition to providing confidentiality and integrity services transmitted over the network or stored locally, BSEA are used as a constructive element of other primitives (hashing functions, message authentication codes, pseudo-random sequence generators, etc.) But when launching a quantum cryptanalysis algorithm by Shore [2] and Grover [3], one can solve mathematical problems in a multi-fold manner. Such a phenomenon can lead to chaos in cyberspace, the destruction of critical infrastructure facilities, and a decrease in confidence in security services based on symmetric and asymmetric cryptography. The emergence of a full-scale quantum computer practically infinitely expands the range of threats and modification of attacks, the emergence of new targeted attacks with characteristics of synergy and hybridity. A detailed description of the stability of symmetric systems against quantum cryptanalysis is given in Table 1 and in article [4]. From the table 1 shows that the stability of symmetric ciphers in the attack using a quantum algorithm is significantly reduced. This means that GOST 28147 can be completely compromised and it will not be possible to consider it stable, its stability will be equal to 2^{256}. Even with AES, it is desirable to use a key of 256 bits. That is, in general, Grover's algorithm, although it reduces the stability of modern symmetric cryptosystems, but still requires a subexponentially number of quantum gates in contrast to the Shore algorithm.

To ensure security in the post-quantum period, NIST U.S. specialists in February 2019 announced a competition for post-quantum cryptography algorithms. Definitions of practical durability set by NIST requirements provide five levels of durability [5, 6]:

1) definition of a key of the 128-bit block cipher;
2) search for a collision of a 256-bit hash function;
3) collision search for 384-bit hash function;

4) determination of the key of the 256-bit block cipher;

5) 384-bit block cipher key definition.

Table 1 – **Strength of standard block-symmetric encryption algorithms against quantum cryptoanalysis**

Crypto-system	Block / key size, (bits)	The amount of memory required for the attack, (bits)	Resistance when attacking:	
			message	key
AES-128	128/128	128/128	2^{64}	2^{64}
AES-256	128/256	128/256	2^{64}	2^{128}
DES	64/56	64/56	2^{32}	2^{28}
GOST-28147	64/256	64/256	2^{64}	2^{256}
Kalina-128	128/128	128/128	2^{64}	2^{64}
Kalina-512	512/512	512/512	2^{256}	2^{256}

Thus, the modification of BSEA, which are the standards of symmetric encryption, and are used in information and switching systems of critical infrastructure objects is an urgent task in the post-quantum period.

The purpose of the article is to develop procedures for improving the stream encryption algorithm based on the block-symmetric encryption algorithm GOST 28147-89 through the use of dynamically changing nonlinear transformations (S-boxes).

The main objectives of the study:

- analysis of the basic procedures of the block cipher algorithm GOST 28147-89;

- development of procedures for improving the method of forming a pseudo-random sequence based on GOST 28147-89.

Analysis of the block cipher algorithm GOST 28147-89

GOST 28147-89, adopted in 1990, was a standard establishing a unified cryptographic transformation algorithm for information processing systems in networks of electronic computers, which determined the rules for data encryption and the development of an imitation insert. The cryptographic transformation algorithm was intended for hardware or software implementation, met the cryptographic requirements and, according to its capabilities, did not impose restrictions on the degree of secrecy of the protected information [5].

One of the operating modes of GOST 28147-89 was the gamming mode, the structural diagram of which is shown in Fig. 1.

The data is displayed on 64-bit blocks, encrypted in the modulo 2 mode in the CM_5 summator with the cipher scale, as it is rotated in blocks of 64 bit. The initial filling of drives N_1, N_2 (sync message S) is encrypted in the simple replacement mode in accordance with 256 bits of the key are entered into the RAM. A 64-bit binary sequence $S = (S_1, S_2, ... S_{64})$ is entered into the drives N_1, N_2, which is the initial filling of these drives for the subsequent generation of M blocks of the cipher gamma.

The encryption algorithm for a 64-bit block of open data in the simple replace mode consists of 32 cycles. In the first cycle, the initial filling of the accumulator N_1 is summed modulo 2^{32} in the adder CM_1 with the filling of the accumulator X_0, while the filling of the accumulator N_1 is preserved.

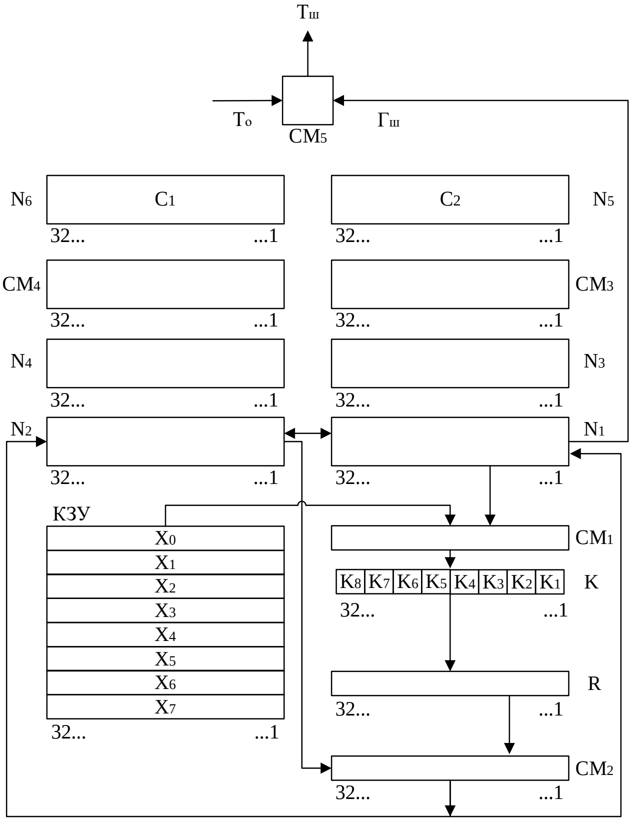

Fig. 1. Gamming mode GOST 28147-89

The result of the summation is converted in the substitution block K and the resulting vector is fed to the input of the register R. where it is cyclically shifted by eleven steps towards the higher bits. The result of the shift is summed bitwise modulo 2 in the CM_2 adder with 32-bit filling of the N_2 drive. The result obtained in CM_2 is written to N_1, while the old filling N_1 is overwritten in N_2. The result of encryption is written to 32-bit drives N_3 and N_4, so. that filling N_1 is overwritten in N_3, and filling N_2 is overwritten in N_4. The filling of the N_4 drive is summed modulo (23^2-1) in the CM_4 adder with a 32-bit constant C_1 from the N_6 drive, the result is written to N_4. The filling of the drive N_3 is summed modulo 232 in the CM_3 adder with a 32-bit constant C_2 from the drive N_5, the result is written to N_3. The filling N_3 is overwritten in N_1, and the filling N_4 is overwritten in N_2, while the filling N_3, N_4 is preserved. The filling of N_1 and N_2 is encrypted in simple replace mode. The filling N_1, N_2 obtained as a result of encryption forms the first 64-bit block of the cipher gamut, which is summed bitwise modulo 2 in the adder CM_5 with the first 64-bit block of open data. This scheme uses the substitution block K, which consists of 8 static substitution blocks [7].

The article proposes to use a schema with dynamically changing substitution blocks. The block diagram is shown in Fig. 2. This diagram consists of the following steps:

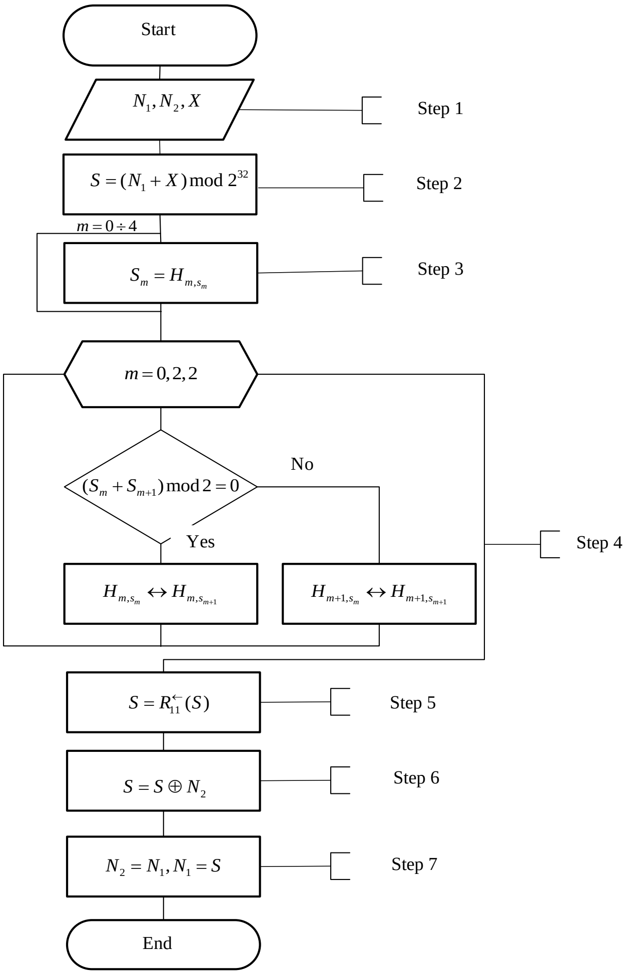
Start
N_1, N_2, X
Step 1
$S = (N_1 + X) \bmod 2^{32}$
Step 2
$m = 0 \div 4$
$S_m = H_{m,s_m}$
Step 3
$m = 0,2,2$
$(S_m + S_{m+1}) \bmod 2 = 0$
No
Yes
Step 4
$H_{m,s_m} \leftrightarrow H_{m,s_{m+1}}$
$H_{m+1,s_m} \leftrightarrow H_{m+1,s_{m+1}}$
$S = R_{11}^{\leftarrow}(S)$
Step 5
$S = S \oplus N_2$
Step 6
$N_2 = N_1, N_1 = S$
Step 7
End

Fig. 2. Gamming mode of the improved GOST 28147-89

Step 1. Input of initial data for the main step of crypto-transformation N - 64-bit block of input data is converted into two 32-bit integers (low (N_1) and high (N_2) parts);

Step 2. Addition with a key. The lower part of the transformed block is added modulo with the key element used in the step.

Step 3. Block replacement. The 32-bit value obtained in the previous step is interpreted as an array of four 8-bit code blocks: $S_m = (S_0, S_1, S_2, ... S_{255})$.

Further, the value of each of the four blocks is replaced with a new one, which is selected according to the substitution table as follows: the value of the S_i block is changed to the S_i-th element in order (numbering from zero) of the i-th substitution node (i.e., the i-th row of the substitution table, numbering also from zero). In other words, an element from the substitution table with a row number equal to the number of the replaced block and a column number equal to the value of the replaced block as an 8-bit non-negative integer is selected as a replacement for the block value.

Step 4. Dynamically change the table of substitutions as follows: if the sum $S_0 + S_1$ is an even number, then the values of $S_0 \leftrightarrow S_1$ of table H_0 are swapped, otherwise $S_0 \leftrightarrow S_1$ of table H_1. If the sum $S_2 + S_3$ is an even number, then the values of $S_2 \leftrightarrow S_3$ of table H_2 are interchanged, otherwise $S_2 \leftrightarrow S_3$ of table H_3.

Step 5. Cyclic shift 11 bits to the left.

Step 6. Bitwise addition: the value obtained in step 3 is added bitwise modulo 2 with the upper half of the converted block.

Step 7. Shift along the chain: the lower part of the converted block is shifted to the place of the older one, and the result of the previous step is placed in its place.

The use of such a transformation makes it possible to dynamically (based on a simple pseudo-random sequence generator) form the OFB mode and provide the required level of cryptographic strength.

The structural diagram of a well-developed algorithm ca-n be described by a multi-round diagram, as shown in Fig. 3.

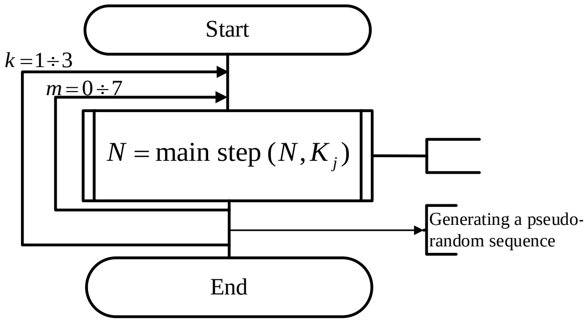
Start
$k = 1 \div 3$
$m = 0 \div 7$
$N = \text{main step}\,(N, K_j)$
Generating a pseudo-random sequence
End

Fig. 3. Scheme of pseudo-random sequence formation

The article proposes three procedures for modifying BSEA GOST 28147. The proposed modes for the formation of pseudo-droplet sequencing at K=1, K=2, K=3, allow to increase the length of the key sequence and provide the required level of creep resistance in the post-quantum period.

To assess the cryptographic strength, it is proposed to use the NIST-STS822 package, which allows implementing 189 tests based on 19 methods for checking the information sequence for randomness. During the test, a 108-bit sequence is tested, taking into account the errors of the first and second kind. Carrying out an experimental improvement of the statistical safety of the proprietary well-developed algorithm according to the NIST STS methodology. The test results are presented in the statistical portraits in Fig. 4 – 6. The analysis of the data will show that the statistical portraits of the well-developed algorithm do not compromise their powers to the most beautiful generators.

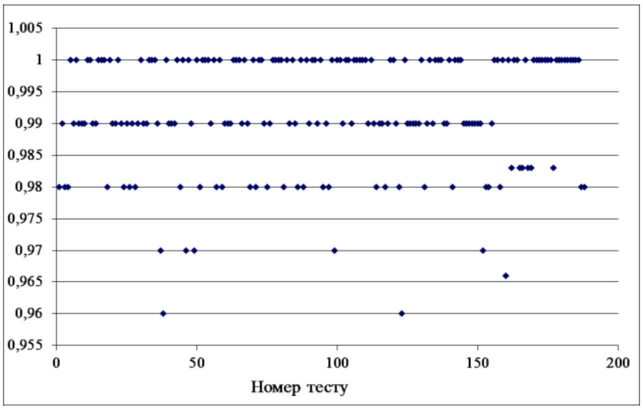

Fig. 4. Statistical portrait of the advanced algorithm at K = 1

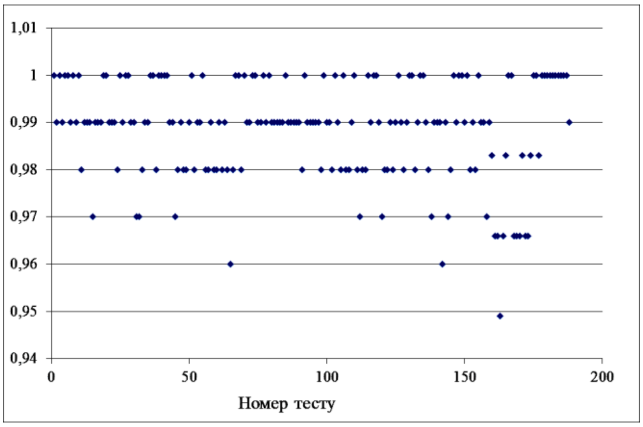

Fig. 5. Statistical portrait of the advanced algorithm at K = 2

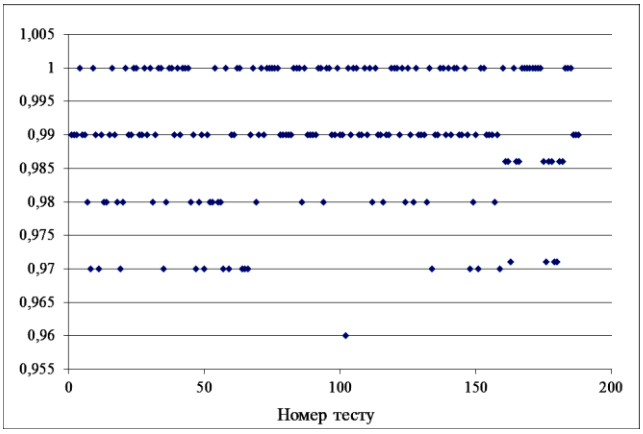

Fig. 6. Statistical portrait of the advanced algorithm at K = 3

The main part of the tests was passed at a very high level, close to 1.

Analysis of the data presented shows that the statistical portraits of the modified block-symmetric encryption algorithm GOST 28147 in OFB mode are not inferior in their properties to the best-known generators. Most of the tests passed with a very high probability, close to 1.

The final test results according to the NIST STS method are summarized in Table 2, which shows the number (share) of tests in which testing was passed with a probability of ≥0,99; ≥0,96 and < 0,96.

Analysis of the test results, summarized in table 2. shows that the proposed modification procedures BSEA GOST-28147-89 (2009, 2015) have improved statistical safety indicators (at K = 1).

This approach provides the level of cryptographic strength required in the post-quantum period. They have one of the largest number (proportion) of tests that passed the most stringent criterion with a probability ≥ 0,99 and are not inferior to such well-known generators as the BBS counter mode.

Table 2 – **Results of comparative studies of the statistical safety of the modified and some well-known pseudo-random number generators**

№	Generator	Number of tests in which the test passed the criterion		
		M ≥ 99%	M ≥ 96%	M< 96%
1	G using SHA-1	122(65%)	188 (99,5%)	1 (0,5%)
2	Linear Congruential	139 (74%)	189 (100%)	–
3	Micali-Schnorr	130 (69%)	189 (100%)	–
4	Quadratic Congruential	124 (66%)	181 (96%)	8 (4%)
5	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
6	ANSI X9.17 (3-DES)	121 (64%)	187 (98%)	4 (2%)
7	Blum-Blum-Shub	134 (71%)	189 (100%)	–
8	FIPS 197	126 (67%)	189 (100%)	–
9	**GOST 28147 at K=1**	145(77%)	189 (100%)	–
10	**ГОСТ 28147 at K=2**	129(68%)	188 (99,5%)	1 (0,5%)
11	**ГОСТ 28147 at K=3**	136(72%)	189 (100%)	–

Conclusions

The analysis of the requirements for post-quantum cryptography algorithms puts forward a significant increase in the length of the key sequence (2-3 times), which affects the energy consumption and speed of cryptocurrencies while reducing the safe time to use the key sequence by 30%.

Analysis of the proposed modification procedures algorithm BSEA GOST 28147-89 (2009, 2015) in the mode of quenching has improved statistical safety. It has one of the largest share of tests that passed the most stringent criteria with a probability of 0.99 and is not inferior to known generators as the BBS generator, Micali-Schnorr in counter mode. This provides the required level of stability, the rate of transformation in the post-quantum period.

References

1. Rybalsky, O.V., Khakhanovsky, V.G. and Kudinov, V.A. (2012), *Fundamentals of information security and technical protection of information*, National Academy of Internal Affairs, Kyiv, 104 p.
2. Shor, P.W. (1997), “Polynomial–Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, *S IAM J. Comput*., 26 (5), pp. 1484–1509.
3. Grover, L.K. (1996), “A fast quantum mechanics algorithm for database search”, *Proceeding of the 28th ACM Symposium on Theory of Computation*, ACM Press, New York, pp. 212–219
4. Gorbenko, Y.I. and Ganzya, R.S. (20140, “Analysis of the stability of popular cryptosystems against quantum cryptanalysis based on Grover's algorithm”, *Information protection*, Vol. 16, No. 2, pp. 106–112.

5. Evseev, S.P., Rzaev, H.N. and Cыganenko, A.S. (2016), “Analyz programnoj realyzacyy prjamogo y obratnogo preobrazovanyja po metodu nedvoychnogo ravnovesnogo kodyrovanyja”, *Bezpeka informacii*, 22#2, pp. 196 - 203.
6. (2020), *NIST announced start of post-quantum cryptography standardization*, URL: https://habr.com/ru/post/512410/.
7. (1989), GOST 28147-89, URL: https://files.stroyinf.ru/Data2/1/4294826/4294826698931.pdf

Надійшла (received) 12.02.2021
Прийнята до друку (accepted for publication) 21.04.2021

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Євсєєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: Serhii.Yevseiev@hneu.net; ORCID ID: http://orcid.org/0000-0003-1647-6444.

Корольов Роман Володимирович – кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Roman Korolyov – Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: korolevrv01@ukr.net; ORCID ID: http://orcid.org/0000-0002-7948-5914.

Ткачов Андрій Михайлович – кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Andrii Tkachov – Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: andrew.tkachov@hneu.net; ORCID ID: http://orcid.org/0000-0003-1428-0173.

Німченко Анастасія Євгеніївна – студентка кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Anastasia Nimchenko – student of the Department of Cybersecurity and Information Technology, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: anastasiya.nimchenko@gmail.com; ORCID ID: http://orcid.org/0000-0002-8098-9597.

Розробка процедур модифікації шифру ГОСТ 28147

С. П. Євсєєв, Р. В. Корольов, А. М. Ткачов, А. Є. Німченко

Анотація. Вступ людства в еру високих технологій, бурхливе зростання обчислювальної техніки сприяє розширенню спектра електронних послуг. Для забезпечення безпеки конфіденційної інформації, персональних даних використовуються криптографічні системи традиційної криптографії (симетричні криптосистеми) і криптографії з відкритим ключем (несиметричні криптосистеми). Як правило, перші забезпечують послуги безпеки, другі - розподіл ключів. Однак в умовах тоталітарної стеження в суспільстві з боку спец служб розвинених держав в криптографічних алгоритмах "вбудовуються" криптографічні закладки, які з одного боку забезпечують "швидкий" доступ спецслужб до конфіденційної інформації, з іншого боку дозволяють зловмисникам зламувати криптосистему і отримувати дані користувачів. У статті пропонується модифікація відомого алгоритму ГОСТ 28147-89, яка забезпечує "усунення" можливих криптозакладок і підвищення криптостійкості в умовах постквантового періоду (поява повномасштабного квантового комп'ютера, який дозволяє зламати на основі алгоритмів Гровера і Шора сучасні симетричні і несиметричні криптосистеми). Пропонується використовувати процедури модифікації блочно-симетричного алгоритму шифрування (БСШ) ГОСТ 28147-89 (2009, 2015) в режимі OFB, що дозволить формувати псевдовипадкову послідовність на основі динамічного зміни S-box, і забезпечити необхідний рівень стійкості.

Ключові слова: блочно-симетричний шифр; потоковий шифр; ГОСТ 28147-89; ДСТУ 28147-2009.

Разработка процедур модификации шифра ГОСТ 28147

С. П. Евсеев, Р. В. Королев, А. М. Ткачев, А. Е. Нимченко

Аннотация. Вступление человечества в эру высоких технологий, бурный рост вычислительной техники способствует расширению спектра электронных услуг. Для обеспечения безопасности конфиденциальной информации, персональных данных используются криптографические системы традиционной криптографии (симметричные криптосистемы) и криптографии с открытым ключом (несимметричные криптосистемы). Как правило, первые обеспечивают услуги безопасности, вторые – распределение ключей. Однако в условиях тоталитарной слежки в обществе со стороны спец служб развитых государств в криптографических алгоритмах “встраиваются” криптографические закладки, которые с одной стороны обеспечивают “быстрый” доступ спецслужб к конфиденциальной информации, с другой стороны позволяют злоумышленникам взламывать криптосистему и получать данные пользователей. В статье предлагается модификация известного алгоритма ГОСТ 28147-89, которая обеспечивает “устранение” возможных криптозакладок и повышение криптостойкости в условиях постквантового периода (появление полномасштабного квантового компьютера, который позволяет взломать на основе алгоритмов Гровера и Шора современные симметричные и несимметричные криптосистемы). Предлагается использовать процедуры модификации блочно-симметричного алгоритма шифрования (БСШ) ГОСТ 28147-89 (2009, 2015) в режиме OFB, что позволит формировать псевдослучайную последовательность на основе динамического изменения S-box, и обеспечить требуемый уровень стойкости.

Ключевые слова: блочно-симметричный шифр; поточный шифр; ГОСТ 28147-89; ДСТУ 28147-2009.