УДК 004.056

A. V. SOKOLOV, D. A. ISAKOV

AUTHENTICATED ENCRYPTION MODE WITH BLOCKS SKIPPING

Odessa National Polytechnic University, Odessa, Ukraine

Block symmetric ciphers are one of the most important components of modern information security systems. At the same time, in addition to the structure of the applied block symmetric cipher, the cryptographic strength and performance of the information protection system is largely determined by the applied encryption mode. In addition to high performance and high-quality destruction of block statistics, modern encryption modes should also protect encrypted information from occurred or intentionally introduced errors. In this paper, we have developed an encryption mode with blocks skipping and using a pseudo-random key sequence generator, which allows checking the integrity of encrypted information with accurate detection of the place where an error was introduced. In this case, the error detection accuracy is determined by the adjustable parameter of the macroblock size and can be set depending on the level of importance of the protected information. The developed encryption mode is characterized by the following key advantages: reducing the number of required encryption operations by half, while providing a high level of cryptographic quality; more effective destruction of macroblock statistics due to the use of an additional generator of pseudo-random key sequences, the impossibility of propagation of the occurred (intentionally introduced) error outside the macroblock, as well as higher values of the number of protection levels due to the possibility of classifying the initial states of the applied generators of pseudo-random key sequences. As proposed in this paper, the mode of authenticated encryption with blocks skipping can be recommended for use on mobile platforms that are demanding both in terms of the quality and reliability of the protected information and are limited in terms of computing and power resources.

Keywords: cryptography, *encryption mode, block symmetric cipher, pseudo-random key sequence generator.*

1. Introduction and statement of the problem

One of the most important places in modern complex information protection systems is occupied by the cryptographic subsystem, which ensures the impossibility of obtaining the confidential information without knowing the secret key. At the same time, in practice, asymmetric cryptographic algorithms are usually used at the stage of key exchange, while block symmetric cryptographic algorithms are used to encrypt the large amounts of information, and are characterized by much higher performance and reliability.

The development of cryptanalysis methods, as well as progress in the theory of cryptographic strength leads to the need for further improvement of modern block symmetric ciphers [1], as well as the use of more strong cryptographic primitives [2, 3] to increase their performance while maintaining a high level of cryptographic strength.

However, we note that in addition to the structure of the cryptographic algorithm itself and the cryptographic primitives that are used in it, the mode in which the selected cryptographic algorithm is applied to the data has a significant impact on the quality of the cryptographic transformation and its performance.

Encryption mode is a method of using of a block symmetric cipher that allows you to convert a sequence of blocks of open data into a sequence of blocks of an encrypted data [4].

In this case, data from another block can be used to encrypt current block.

The simplest known encryption mode is the Electronic Codebook (ECB) mode, which simply replaces plaintext blocks with ciphertext blocks. It is known [4] that the use of even the most robust block symmetric ciphers in the ECB encryption mode leads to the preservation of block statistics in the original message, which leads to the possibility of partial recovery of encrypted information from the cryptogram. This circumstance makes it impossible to apply the ECB mode in practice.

Today there are a lot of encryption modes that have been created that provide reliable destruction of statistics in encrypted data. These modes include the following: Cipher Block Chaining (CBC), Propagating Cipher Block Chaining

(PCBC), Cipher Feedback (CFB), Output Feedback (OFB). All these modes are based on the principle of concatenation of blocks to be encrypted with already encrypted ones.

A significant disadvantage of these modes with block coupling is their instability to the occurrence of occurred or intentionally introduced errors. So, if an error occurs during the transfer of one of the blocks, this error is propagated to all blocks following this during decryption.

Note also that recently, encryption modes with authentication have become widely used, allowing simultaneous verification of the integrity of encrypted data in the process of their decryption. At the same time, the use of such modes guarantees protection both from errors arising from natural reasons and from errors that were intentionally introduced into the transmitted information. Most of the authenticated encryption schemes used today are designed for use in Internet protocols such as IPsec and TLS, which encrypts only one block (packet) and are practically equivalent to the use of ECB encryption mode. This encryption mode is known to be invalid at the level of encryption of whole files.

Another trend in modern cryptography is the creation of new encryption modes that allow a significant acceleration of the operation of block symmetric ciphers. These new encryption modes include the encryption mode proposed in [5] with blocks skipping and using a pseudo-random key sequence generator, which allows to reduce the number of blocks encrypted by a block symmetric cryptographic algorithm by 2 times due to the use of a much faster construction as a pseudo-random key sequence generator (PRKSG). Nevertheless, the encryption mode developed in [5] is not devoid of such a significant drawback as the lack of the ability to check the integrity of messages encrypted in this mode.

It is promising to combine the advantages of the blocks skipping encryption mode and the use of the PRKSG together with encryption modes involving authentication.

The *purpose* of this paper is to develop an encryption mode with blocks skipping and the use of the PRKSG, which allows checking the integrity of encrypted information with accurate detection of the place where the error was introduced.

2. Encryption Mode with blocks skipping and using of PRKSG

Note that in [5], there are two encryption modes proposed, which lead to an increase in the performance of block symmetric ciphers using: with blocks skipping, and also with blocks skipping and use of the PRKSG. These encryption modes are designed for their use on platforms that are sensitive to the consumption of computing resources, primarily on mobile platforms.

It was found that when using a block chaining mechanism (for example, CBC, PCBC, CFB, or OFB encryption modes), it is possible to skip encryption of some blocks while maintaining the correspondence of the output cryptogram to the NIST stochastic quality tests [6]. However, the number of such skipped blocks is insignificant and does not exceed 5% of the total number of encrypted blocks.

For further increase in the performance of the encryption operation in [5] it is proposed to combine the advantages of using block and stream cryptographic algorithms by developing an encryption mode with blocks skipping and using a pseudo-random key sequence generator.

For completeness of the presentation of the material of this paper, we will briefly consider the essence of the encryption mode developed in [5] with blocks skipping, as well as use the PRKSG.

To implement this scheme, such a cryptographic primitive as a pseudo-random key sequence generator (PRKSG) is used. Today there are many effective cryptographically robust pseudo-random key sequence generators [7 … 9]. In [5], it was proposed to use the schemes [10] or [11]. At the same time, the performance of these cryptographic primitives significantly exceeds the performance of block symmetric cryptographic algorithms [11].

Before the start of the encryption operation, the selected PRKSG scheme is initialized using an additional key fragment. In this encryption mode, parameters M and C are entered. At the beginning of the encryption procedure, the variable i is initialized by 0 value. Before applying the block encryption, the condition $i \bmod M \in \{0,1,...,C\}$ is checked and, if the condition is false, instead of encrypting of this block, it is gammed using the next gamma segment obtained using the PRKSG. When the block encryption is finished, the value of the variable i is incremented by 1.

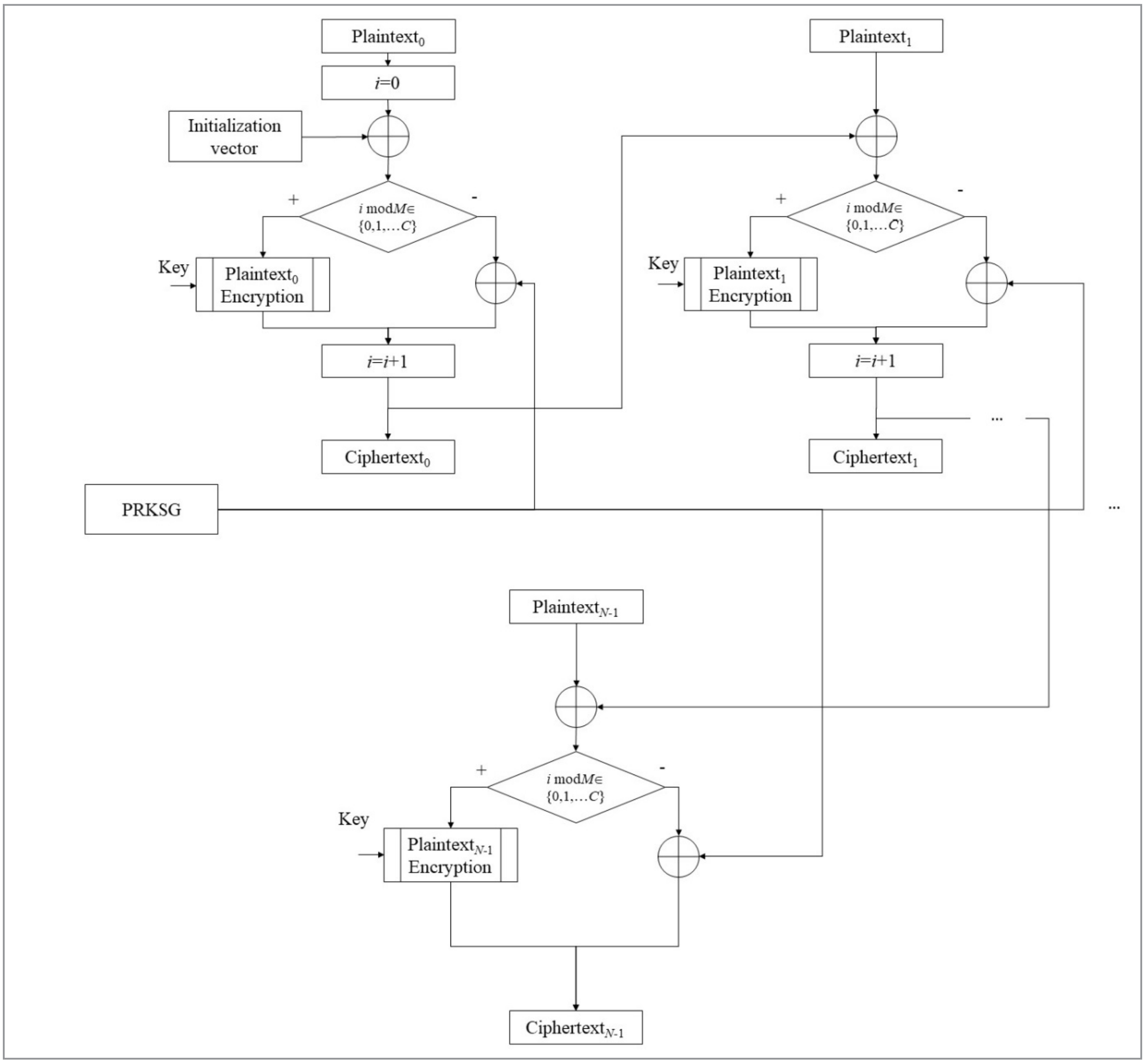

Fig. 1 – CBC encryption mode with block skipping and application of the PRKSG

Empirical research performed in [5] showed that the scheme shown in Fig. 1 provides a high level of cryptographic quality of the resulting cryptograms for the values $M = 2$ and $C = 0$, i.e. when skipping encryption of every second block of encrypted text.

3. Authenticated encryption mode with block skipping and use of the PRKSG

Today, there are three main approaches for constructing modes with block authentication [12]. Let's take a quick look at each of these approaches.

The first Encrypt-then-MAC approach assumes that the original block of data is encrypted first, after which a hash function is applied to it (which, in general, can be a single-key cryptographic algorithm). The resulting message is a combination of the encrypted message and the hash value of the encrypted message, which certifies its integrity. In general, the cryptographic algorithm key and the hash function key do not match.

The second Encrypt-and-MAC approach assumes simultaneous encryption and hashing of the original data. The resulting message is a combination of the encrypted message and the hash value of the original message. In this case, the same key is used for the cryptographic algorithm and hash function.

The third MAC-then-Encrypt approach involves finding the hash value of the original message, which is appended to the original message, after which this sequence is encrypted. Thus, the resulting message is the encrypted original message and the value of its hash function. In this case, the same key is used for the hash function and the cryptographic algorithm.

Note that, in principle, each of the listed approaches can be combined with an encryption mode with blocks skipping and using the PRKSG. However, in the following we describe the new Authenticated Block Skip Encryption Mode with the use of the Encrypt-and-MAC approach.

Let's describe the operation of the proposed encryption mode in the form of specific steps.

Step 1. The original file of length N is divided into N/k blocks, where k is the block length of the applied cryptographic algorithm.

Step 2. Before the start of encryption, the length μ of the macroblock is set, the counter of the number of the encrypted block is initialized $i=0$, the counter of the values of the hash function of the macroblocks is initialized $l=0$, and two cryptographically strong PRKSG are initialized: $PRKSG_1$ and $PRKSG_2$. In this case, the initial states of the PRKSG are part of the secret key.

Step 3. Using the generator $PRKSG_1$, a gamma fragment G_μ of the length k is generated, which is the initialization vector of this macroblock.

Step 4. Assign a value G_μ to the initialization vector IV.

Step 5. Perform addition modulo 2 of the initialization vector IV with the plaintext block, and further the value of the resulting block is assigned to a variable a.

Step 6. If i is even, the block a is encrypted. Otherwise, we generate the next gamma fragment of the length k using $PRKSG_2$ and perform its summation modulo 2 with the block a. The result of the above actions is assigned to a ciphertext variable C_i.

Step 7. Save the next fragment of the ciphertext C_i. We assign a value C_i to the initialization vector IV. We increment the counter of the encrypted block number $i=i+1$.

Step 8. If $i=N/k-1$ (end of file is reached) we calculate the value of the hash function of the block C_i and write it to a memory cell H_l. END. Otherwise, go to *Step 9*.

Step 9. If $i \bmod \mu \equiv 0$ (the last block of the macroblock was processed): calculate the value of the hash function of the block C_i and write it to the memory cell H_l. We increment the counter of macroblock hash function values $l=l+1$. Go to *Step 3*. Otherwise, go to *Step 5*.

In Fig. 2 we show an encryption scheme that implements the developed algorithm.

In this case, the decryption scheme is built similarly to the encryption scheme (Fig. 2).

Further, similar to the encryption procedure, we describe the decryption procedure for the proposed encryption mode in the form of specific steps.

Step 1. The encrypted file of length N is divided into N/k blocks, where k is the block length of the applied cryptographic algorithm.

Step 2. Before decryption begins, the length μ of the macroblock is set (this value must be agreed with the party who performed the encryption), the counter of the encrypted block number is initialized $i=0$, the counter of the hash function values of the macroblocks is initialized $l=0$, and two cryptographically strong PRKSG are initialized: $PRKSG_1$ and $PRKSG_2$. In this case, the initial states of the PRKSG are part of the secret key and must correspond to those used for encryption.

Step 3. Using the $PRKSG_1$ generator, generate a gamma fragment G_μ of the length k, which is the initialization vector for this macroblock.

Step 4. Assign a value G_μ to the initialization vector IV.

Step 5. If i is even, the block C_i is decrypted. Otherwise, we generate the next gamma fragment of the length k using $PRKSG_2$ and perform its summation modulo 2 with the block C_i. The result of the above actions is assigned to a variable a.

Step 6. The addition modulo 2 of the initialization vector IV with the block of decrypted text is performed, as a result of which the value of the resulting block is assigned to a variable a.

Step 7. Save the next fragment of the decrypted text a. We assign a value C_i to the initialization vector IV. We increment the counter of the encrypted block number $i=i+1$.

Step 8. If $i=N/k-1$ (end of file is reached) we calculate the value of the hash function of the block C_i and compare it with the value H_l saved during encryption. END. Otherwise, go to *Step 9*.

Step 9. If $i \bmod \mu \equiv 0$ (the last block of the macroblock was processed): calculate the value of the hash function of the block C_i and compare it with the value H_l saved during encryption. Increment the counter of macroblock hash function values $l=l+1$. Go to *Step 3*. Otherwise, go to *Step 5*.

The proposed scheme (Fig. 2) of the authenticated encryption mode with blocks skipping and using the PRKSG allows us to obtain the

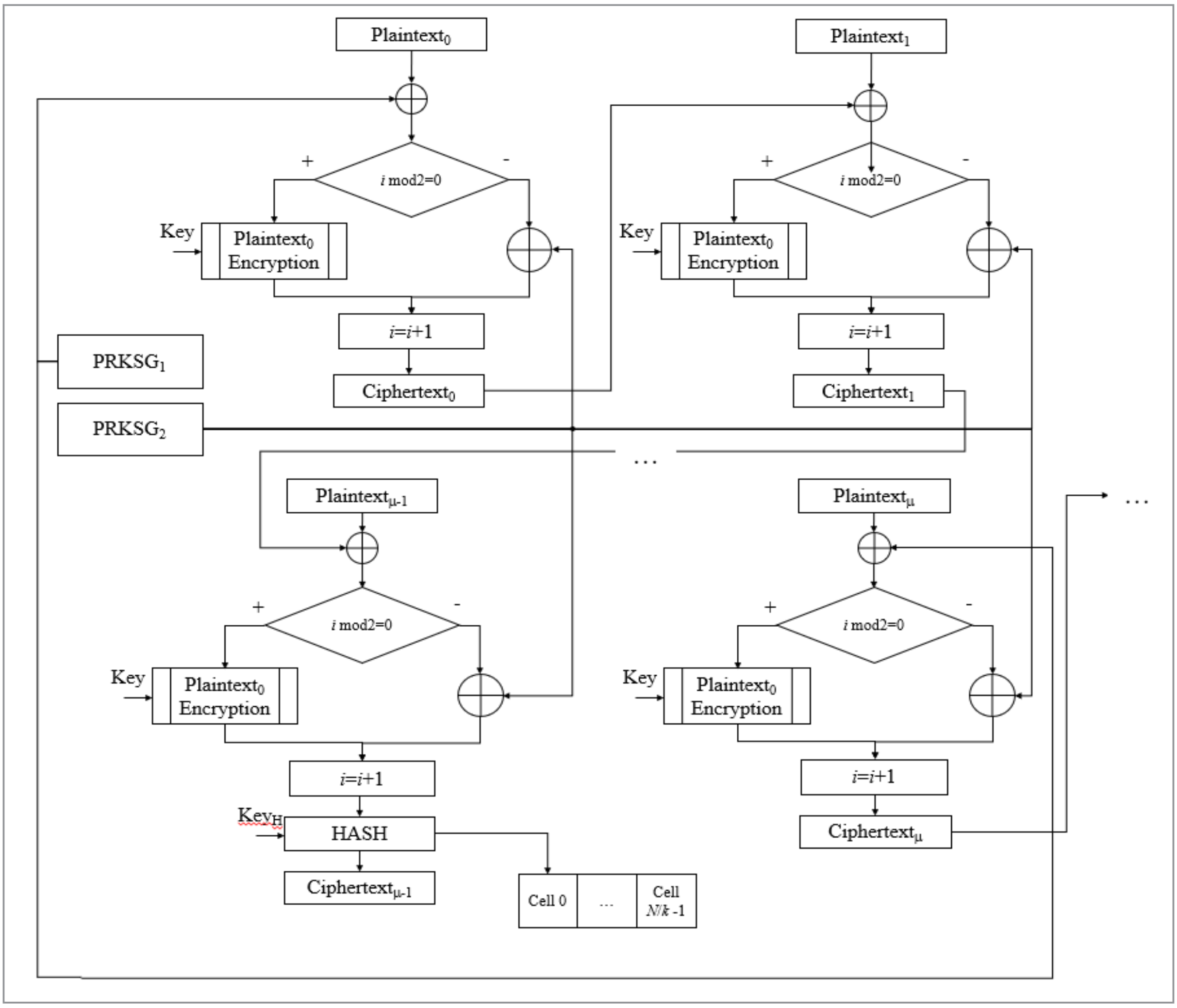

Fig. 2. Authenticated encryption mode with blocks skipping and the use of the PRKSG

following advantages over the scheme with blocks skipping and using the PRKSG, as well as the classical encryption scheme with authentication:

a. the proposed mode allows not only to detect intentional and / or unintentional violation of the integrity of information, but to precisely determine its position with an accuracy up to the size of the macroblock length μ;

b. by varying the value of the macroblock length μ, it is possible to set the accuracy of the location of the integrity violation that occurred, however, smaller values of the macroblock lengths lead to an increase in the size of the vector of values of hash functions of macroblocks, which leads to the need to transfer large amounts of information. Thus, the proposed encryption mode is adaptable due to the change in value of μ depending on the properties of the transmission channel (storage device) of information and the value of the information itself;

c. in contrast to the traditional encryption modes with block chaining, in the event of an error, its propagation will be limited to the limits of the macroblock;

d. the proposed scheme for the dynamic generation of new values of the initialization vectors for each macroblock makes it possible to destroy the statistical relationships between macroblocks much more efficiently.

Note also that the number of protection levels of the presented scheme exceeds the number of protection levels of the AES block symmetric cipher used in it due to the additional use of two PRKSG. For example, when using PRKSG based on dual couples of bent-sequences, the number of protection levels of which is equal to 2^{165}, the number of protection levels of the entire encryption scheme is determined as $\Psi \simeq 2^{256} \cdot 2^{165} \cdot 2^{165} = 2^{586}$.

Conclusion

We note the main results of the research performed:

1. we proposed a new authenticated encryption mode based on a blocks skipping encryption mode using a pseudo-random key sequence generator. In addition to the possibility of skipping of the encryption operation of every second encrypted block while maintaining full compliance of the cryptogram with the NIST stochastic quality tests, the developed mode provides information authentication during decryption. When decrypting the file, it is possible to localize the occurred (intentionally introduced) error with a predetermined accuracy, which depends on the selected macroblock length. At the same time, in the developed encryption mode with authentication, in contrast to traditional encryption modes with block chaining, an error that occurs during decryption is propagated only within one macroblock;
2. the developed encryption mode provides a more efficient destruction of macroblock statistics due to the use of an additional PRKSG to generate individual initialization vectors for each macroblock, as well as a higher number of protection levels due to the possibility of using the initial states of the PRKSG as an additional key;
3. the developed encryption mode with authentication and blocks skipping can be recommended for practical use on mobile platforms, which, on the one hand, are sensitive to occurred (intentionally introduced) errors in the encrypted data, and on the other hand, are demanding on computational and energy resources.

REFERENCES

1. **Zhdanov O.N.** Methodology for selecting key information for a block cipher algorithm. M .: INFRA-M, 2013. 90 p.
2. **Sokolov A.V.** New methods of synthesis of nonlinear transformations for modern ciphers. Lap Lambert Academic Publishing, Germany, 2015. 100 p.
3. **Sokolov A.V., Zhdanov O.N.** Cryptographic constructions based on many-valued logic functions. Monograph. M: Scientific Thought, 2020. 192 p.
4. **Schneier B.** Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015. 784 p.
5. **Sokolov A.V., Korzh A.O.** Study of block skip encryption modes. Informatics and mathematical methods in modeling. 2020, Vol. 10, No. 1/2. P. 100–108.
6. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. National Institute of Standards and Technology Special Publication, 2010. 131 p.
7. **Ishai Y. et al.** Robust pseudorandom generators. International Colloquium on Automata, Languages, and Programming. Springer, Berlin, Heidelberg, 2013. P. 576–588.
8. **Aljohani M. et al.** Performance analysis of cryptographic pseudorandom number generators. IEEE Access. 2019. Vol. 7. P. 39794–39805.
9. **Datcu O., Macovei C., Hobincu R.** Chaos based cryptographic pseudo-random number generator template with dynamic state change. Applied Sciences. 2020. Vol. 10, No. 2. P. 451.
10. **Mazurkov M.I., Sokolov A.V., Barabanov N.A.** The key sequences generator based on bent functions dual couples. Proceedings of Odessa Polytechnic University, 2013. No. 3. P. 150–156.
11. **Sokolov, A.V.** The cellular automata key sequences generator. Proceedings of Odessa Polytechnic University, 2014. No. 1 (43). P. 180–186.
12. **Bellare M., Namprempre C.** Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Journal of Cryptology. 2008. T. 21. No. 4. P. 469–491.

ЛИТЕРАТУРА

1. **Жданов, О.Н.** Методика выбора ключевой информации для алгоритма блочного шифрования.– М.: ИНФРА-М, 2013.– 90 с.
2. **Соколов, А.В.** Новые методы синтеза нелинейных преобразований современных шифров.– Lap Lambert Academic Publishing, Germany, 2015.– 100 с.
3. **Соколов А.В.** Криптографические конструкции на основе функций многозначной логики. Монография / А.В. Соколов, О.Н. Жданов.– М: Научная мысль, 2020.– 192 с.
4. **Schneier B.** Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015. 784 p.
5. **Соколов А.В., Корж А.О.** Исследование режимов шифрования с пропуском блоков. Информатика и математические методы в моделировании. 2020, Т. 10, № 1/2, С. 100–108.
6. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. National Institute of Standards and Technology Special Publication, 2010. 131 p.
7. **Ishai Y. et al.** Robust pseudorandom generators //International Colloquium on Automata, Languages, and Programming.– Springer, Berlin, Heidelberg, 2013.– С. 576–588.
8. **Aljohani M. et al.** Performance analysis of cryptographic pseudorandom number generators //IEEE Access.– 2019.– Т. 7.– С. 39794–39805.

9. **Datcu O., Macovei C., Hobincu R.** Chaos based cryptographic pseudo-random number generator template with dynamic state change //Applied Sciences. 2020. Vol. 10, No. 2.– С. 451.
10. **Мазурков М. И., Соколов А. В., Барабанов Н. А.** Генератор ключевых последовательностей на основе дуальных пар бент-функций. Праці Одеського політехнічного університету, 2013. № 3. С. 150–156.
11. **Соколов, А. В.** Быстродействующий генератор ключевых последовательностей на сонове клеточных автоматов. Праці Одеського політехнічного університету, 2014. № 1(43). С. 180–186.
12. **Bellare M., Namprempre C.** Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Journal of Cryptology. 2008. Т. 21. No. 4. С. 469–491.

Поступила	*После доработки*	*Принята к печати*
30.04.2021	*30.08.2021*	*01.09.2021*

SOKOLOV A., ISAKOV D.

РЕЖИМ ШИФРОВАНИЯ С АУТЕНТИФИКАЦИЕЙ И ПРОПУСКОМ БЛОКОВ

Блочные симметричные шифры являются одной из важнейших составляющих современных систем защиты информации. При этом, помимо структуры примененного блочного симметричного шифра, криптографическая стойкость и быстродействие системы защиты информации во многом определяется примененным режимом шифрования. Помимо высокого быстродействия и качественного разрушения статистики блоков, современные режимы шифрования должны также обеспечивать защиту шифруемой информации от случайных или намеренно вносимых ошибок. В настоящей статье разработан режим шифрования с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей, который допускает проверку целостности зашифрованной информации с точным детектированием места внесения ошибки. При этом точность детектирования ошибки определяется регулируемым параметром размера макроблока и может быть задана в зависимости от уровня важности защищаемой информации. Разработанный режим шифрования характеризуется следующими ключевыми преимуществами: снижение количества необходимых операций шифрования в два раза при сохранении высокого уровня криптографического качества; более эффективное разрушение статистики макроблоков за счет применения дополнительного генератора псевдослучайных ключевых последовательностей, невозможность распространения возникшей (внесенной) ошибки за пределы макроблока, а также более высокие значения числа уровней защиты за счет возможности засекречивания исходных состояний применяемых генераторов псевдослучайных ключевых последовательностей. Предложенный в статье режим аутентифицированного шифрования с пропуском блоков может быть рекомендован к использованию на мобильных платформах, которые являются требовательными как к качеству и достоверности защищаемой информации, так и ограниченными с точки зрения вычислительных и энергетических ресурсов.

***Ключевые** слова: криптография, режим шифрования, блочный симметричный шифр, генератор псевдослучайных ключевых последовательностей.*

Artem Sokolov. Associate Professor of the Department of Cybersecurity and Software, Odessa National Polytechnic University. He is the author of over 100 scientific and methodological publications, including 2 monographs. His research interests include data protection methods based on perfect algebraic constructions.

Артем Соколов. Доцент кафедры Кибербезопасности и программного обеспечения Одесского национального политехнического университета. Является автором более 100 научных и научно-методических публикаций, среди которых 2 монографии. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций.

E-mail: radiosquid@gmail.com

Dmitry Isakov. He is a fourth-year student, specializing in Cybersecurity. Research interests include general issues of information security.

Дмитрий Исаков. Студент четвертого курса по специальности «Кибербезопасность». Научные интересы включают в себя общие вопросы защитой информации.