UDC 004.056.55
ГРНТИ 81.93.29

Babenko V. G.
PhD, Associate Professor,
Associate Professor of the Department of Information Security
and Computer Engineering
Cherkasy State Technological University
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine
Faure E. V.
Doctor of Technical Sciences, Associate Professor,
Professor of the Department of Information Security
and Computer Engineering
Cherkasy State Technological University
Sysoienko S. V.
PhD, Senior Lecturer
of the Department of Information Security and Computer Engineering
Cherkasy State Technological University
Myronets I. V.
PhD, Associate Professor,
Associate Professor of the Department of Information Security
and Computer Engineering
Cherkasy State Technological University
Sysoienko A. A.
PhD student
Cherkasy State Technological University

THE EFFECTIVENESS OF USE OF MATRIX OPERATIONS FOR CRYPTOGRAPHIC TRANSFORMATION IN SLIDING ENCRYPTION PRIMITIVES

Бабенко Вера Григорьевна
кандидат технических наук,
доцент кафедры информационной безопасности
и компьютерной инженерии
Черкасский государственный технологический университет
б-р Шевченка, 460, г. Черкассы, 18000, Украина,
Фаурэ Эмиль Виталиевич
доктор технических наук,
доцент кафедры информационной безопасности
и компьютерной инженерии
Черкасский государственный технологический университет
Сысоенко Светлана Владимировна
кандидат технических наук,
старший преподаватель кафедры информационной безопасности
и компьютерной инженерии
Черкасский государственный технологический университет
Миронец Ирина Валериевна
кандидат технических наук,
доцент кафедры информационной безопасности
и компьютерной инженерии
Черкасский государственный технологический университет
Сысоенко Антон Андреевич
аспирант
Черкасский государственный технологический университет

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ МАТРИЧНЫХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ В ПРИМИТИВАХ СКОЛЬЗЯЩЕГО ШИФРОВАНИЯ

Summary. The authors prove and substantiate that sliding encryption primitives are a partial case of matrix operations based on recurrent sequences. It is carried out the research of matrix operations of cryptographic transformation synthesized on the basis of sum modulo. It is shown how the properties of cryptographic

transformation results change depending on the module value. Methods and recommendations are offered for applying matrix operations based on sum modulo to encrypt information.

Аннотация. В представленной работе доказано и обосновано, что примитивы скользящего шифрования являются частным случаем матричных операций, построенных на основе рекуррентных последовательностей. Проведено исследование матричных операций криптографического преобразования, которые синтезированы на основе операции суммы по модулю. Показано, как меняются свойства результатов криптографического преобразования в зависимости от выбора значения основы модуля. Согласно полученным результатам, предложены способы и рекомендации по применению матричных операций криптографического преобразования на основе суммы по модулю для шифрования информации.

Keywords: information security, automated systems, cryptographic security methods, group communications, matrix operations, cryptographic primitives, sliding encryption, round key, linear modular equations, logical functions.

Ключевые слова: защита информации, автоматизированные системы, криптографические методы защиты, групповые коммуникации, матричные операции, криптографический примитив, скользящее шифрования, ключ раунда, линейные модульные уравнения, логические функции.

Introduction. The latest information technologies and communications are increasingly being implemented in critical applications. In particular, they are used to ensure the functioning of information processes of government institutions, military and industrial complexes, management structures of energy, transport, financial, banking, business, and other activities. Therefore, the vast majority of world countries, including Ukraine, recognize the protection of information resources from unauthorized use as an important component for realizing national interests. The transition to the digital economy has raised new challenges to ensure the security of financial intermediation [1]. The need to improve the effectiveness of information security measures for financial information is primarily due to the rapid growth of successful cyber-attacks on banking and financial institutions over the past few years, both in Ukraine and in other countries.

The proliferation of information networks and distributed automated systems has contributed to the emergence of a new, multilateral or group, form of communication. In the digital economy, financial intermediation in today's infocommunication space can be attributed to this form of communication. Therefore, the implementation of cryptographic data protection is one of the most important theoretical and practical problems of today.

The development of computer science and computer technology combined with information and telecommunication systems has led to a significant increase of information value. It determines the level of information security. Modern information technologies require high-level security for large amounts of data.

The processes for transmitting, disseminating, storing, processing, and using information must be as fast as possible, least costly, as useful as possible, convenient, automated, and secure at the same time. Thus, increasing the efficiency of cryptographic data protection today is one of the pressing problems of information security.

Literature review. "Symmetric Block Cryptographic Data Conversion Algorithm with Dynamically Controlled Encryption Parameters" and "Block Symmetric Cryptographic Data Conversion Algorithm with Dynamically Controlled Cryptographic Primitives Stochastic Replacement Process" were presented at the open competition of symmetric block cryptographic algorithms [1]. They first used variable encryption primitives [2]. The main advantage of the proposed solutions is the increase of algorithm cryptographic strength. It is achieved by providing dynamic change in both encryption parameters and cryptographic primitives. However, providing flexible control of encryption process and increasing the number of parameters, including crypto primitives, cause a slowdown in encryption speed. Although this performance loss is negligible, because it is compensated using high-speed hardware.

It is advisable to use this principle of encryption improving for SEP. This can increase the conversion crypto strength. In addition, the basic ways to increase the crypto primitives speed should be considered to ensure their effectiveness.

The papers [3, 4] describe the use of SEPs for symmetric block cryptographic algorithms. In particular, it was proved in [5] that the process of implementing SEP can be paralleled by the use of matrix operations of cryptographic information transformation. In [6, 7] it is proved that matrix operations of cryptographic transformation based on addition modulo can be used to increase crypto strength. The works [8-10] discuss the construction of a mathematical model for performing group matrix cryptographic transformation. The main advantage of its implementation is to increase the speed of cryptographic algorithms.

Therefore, a promising task is to develop methods and recommendations for implementing sliding encryption for a given number of primitive elements based on the use of recursive dependencies.

Formal problem statement. As we know, information security can be done in two ways: restrict access to information by organizational measures, or convert information by the way known only to legitimate users. In today's globalization and digitalization context, information must be transmitted through unsecured communication channels. Therefore, the second method has a clear advantage.

The main characteristics of cryptographic systems are the strength and speed of conversion. Both characteristics need to be permanently increased. This increase should be not less than the increase in productivity of computer facilities.

Considering the success of implementing cryptographic methods of two-way communication security, today the attention of specialists is focused on applying existing and creating new cryptographic algorithms for group communication security. Both theoretical aspects of mathematical improvement of traditional algorithms and practical aspects of development of such software systems are being investigated. At the same time, there are objective obstacles to the widespread practical implementation of software for protecting group information processes. In particular, the problem of resolving the contradiction between providing algorithm cryptographic strength and its speed remains open. There are also significant difficulties in software implementation of already existing cryptographic algorithms and its related services in a group communication environment.

Therefore, the main task of this work is to improve the efficiency of data cryptographic protection by increasing the speed of information transformation through implementing sliding encryption primitives (SEPs) based on matrix operations of cryptographic transformation.

The use of matrix operations of cryptographic transformation in sliding encryption primitives. The process of implementing the logical SEP can be represented by the structural scheme of information transformation (Fig. 1), where key_1 is a round key element, $input_i$ and $output_i$ is i-th elements of input and output data resp. [5, 11].

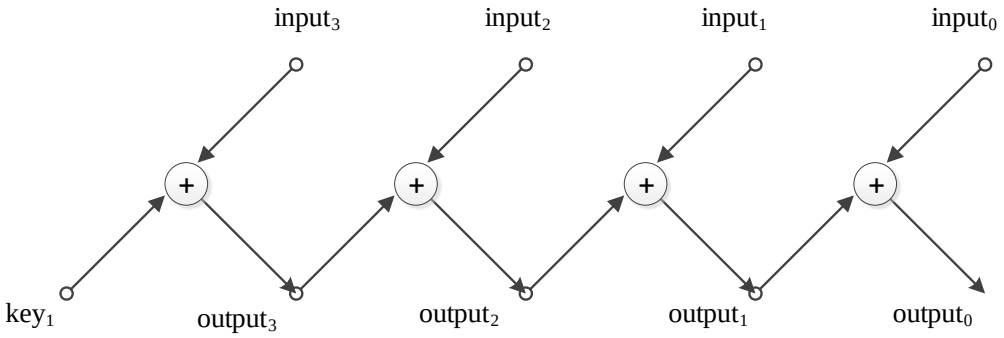

Figure 1. Structural scheme of implementing the direct left-sided SEP

The transformation scheme shown in Figure 1 corresponds to a system of linear modular equations [5, 11]:

$$output_3 = input_3 \oplus key_1;$$
$$output_2 = input_2 \oplus output_3;$$
$$output_1 = input_1 \oplus output_2;$$
$$output_0 = input_0 \oplus output_1.$$

In the shown sequence of information transforming implemented by SEP, operations are performed bit by bit over each pair of adjacent operands.

The study of sliding encryption multiple primitive made it possible to state the following. The functions for converting sliding encryption elements are represented by recurrent sequences and are special cases from the whole variety of recurrent sequences that can be applied for synthesizing matrix operations of cryptographic transformation [12].

Thus, the function of converting one element of six-fold simplified sliding encryption can be described in a recurrent sequence $q_n = q_{n-8} \oplus input_{n-2} \oplus input_n$ where q_i is element of sequence of six-fold encryption. The six-fold SEP based on this recurrent sequence can be represented as a matrix model [11, 13]:

$$Output = \begin{pmatrix} input_1 \\ input_2 \\ input_1 \oplus input_3 \\ input_2 \oplus input_4 \\ input_3 \oplus input_5 \\ input_4 \oplus input_6 \\ input_5 \oplus input_7 \\ input_6 \oplus input_8 \\ input_1 \oplus input_7 \oplus input_9 \\ input_2 \oplus input_8 \oplus input_{10} \\ input_1 \oplus input_3 \oplus input_9 \oplus input_{11} \\ input_2 \oplus input_4 \oplus input_{10} \oplus input_{12} \\ input_3 \oplus input_5 \oplus input_{11} \oplus input_{13} \\ input_4 \oplus input_6 \oplus input_{12} \oplus input_{14} \\ . \ . \ . \ . \ . \ . \ . \ . \end{pmatrix} \oplus$$

$$\oplus \begin{pmatrix} key_1 \oplus key_2 \oplus key_3 \oplus key_4 \oplus key_5 \oplus key_6 \\ key_2 \oplus key_3 \oplus key_5 \\ key_1 \oplus key_2 \oplus key_3 \oplus key_6 \\ key_2 \oplus key_3 \\ key_4 \oplus key_5 \oplus key_6 \\ key_5 \\ key_6 \\ 0 \\ key_1 \oplus key_2 \oplus key_3 \oplus key_4 \oplus key_5 \oplus key_6 \\ key_2 \oplus key_3 \oplus key_5 \\ key_1 \oplus key_2 \oplus key_3 \oplus key_6 \\ key_2 \oplus key_3 \\ key_4 \oplus key_5 \oplus key_6 \\ key_5 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \end{pmatrix},$$

where key_i is a round key elements.

The recurrent sequence that describes the round key processing unit is represented as $key_n=key_{n-8}$ since $key_1 \oplus key_2 \oplus \ldots \oplus key_n = key_k$ and round key random elements are formed on the basis of the same algorithm. Consider Shannon's theorem, which proves that reusing the same algorithm does not increase transformation strength. It can then be argued that reusing round key elements does not increase cryptographic strength.

On this basis, it became possible to optimize the operation of cryptographic transformation of round key processing unit without crypto strength reducing by the following model [11]:

$$Output = \begin{pmatrix} input_1 \\ input_1 \oplus input_2 \\ input_1 \oplus input_2 \oplus input_3 \\ input_1 \oplus input_2 \oplus input_3 \oplus input_4 \\ input_1 \oplus input_2 \oplus input_3 \oplus input_4 \oplus input_5 \\ . \ . \ . \ . \ . \ . \ . \ . \\ input_1 \oplus input_2 \oplus input_3 \oplus . \ . \ . \ . \oplus input_n \end{pmatrix} \oplus \begin{pmatrix} key_1 \\ key_2 \\ key_3 \\ key_4 \\ key_5 \\ key_6 \\ key_6 \\ \ldots\ldots\ldots \\ key_L \end{pmatrix},$$

where L is a number of rounds.

Thus, the optimized operation compared to the implementation of matrix operation allows increasing: the round key processing speed for the SEP model up to 5 times; the speed of cryptographic conversion operations up to 2 times.

This optimization allows reducing the hardware complexity of SEP implementing by reducing the number of sum modulo 2 operations.

A generalized expression of the recurrent sequence is obtained to describe the multiple direct SEP [14]: $output_i^k = output_{i-1}^k \oplus output_i^{k-1}$ where

$output_0^k = output_d^{k-1}$, $i \in \{1, \dots, d\}$, k is a number of rounds of sliding transformation, and d is the bitness of transformation, and $output_i^j$ is i-th element of output data for j-th round resp.

An effective way to increase the crypto algorithm security is to use multioperational matrix cryptographic primitives. A computational experiment was conducted to simulate two-operand matrix operations suitable for cryptographic transformation. The essence of the experiment was to search operands combinations for synthesizing the matrix operation, which will provide an avalanche effect in information cryptographic transformation. The result is a set of cryptographic transformation operation models.

The analysis of the experimental results made it possible to generalize them with grouping by the type of transformation (Table 1) [15]. The symbol z denotes the presence of permutation, x_i are the input operands.

Analysis of the results of operation simulations showed that these operation sets are mathematical groups up to permutation. These operations can be used, for example, in multiple SEP implementing. Thus, the synthesis of direct SEP may use other synthesized operations instead of sum modulo 2.

Then a generalized recurrent sequence model can be written as $output_i^k = output_{i-1}^k(\nabla) output_i^{k-1}$ where $output_0^k = output_d^{k-1}$, $i \in \{1, \dots, d\}$, , and $(\nabla)$is a two-operand cryptographic operation.

A multiple SEP operation can be changed for any encryption round. Moreover, it can be changed several times in the encryption round.

The number of SEP elements determines the maximum number of round variable operations. Therefore, a generalized recurrent sequence model of multiple SEP with round variable operations can be represented as $output_i^k = output_{i-1}^k(\nabla k_i) output_i^{k-1}$ where $output_0^{k_i} = output_d^{k_i-1}$, $i \in \{1, \dots, d\}$, , and (∇k_i) is a two-operand cryptographic operation to convert the i-th element for the k-th round.

The use of matrix operations of cryptographic transformation makes it possible to parallel the process of implementing SEP.

The use of matrix operations for multiple simplified sliding encryption reduces the number of operations compared to one-time simplified sliding encryption. This gives benefits both in time and in the complexity of implementing primitives.

Table 1

Generalized models of operation groups

Group number		0	1	2	3	Operation model
1	0	a	b	d	c	$O_{1,7,13,19} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{if} z_1 = 0, z_2 = 0; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 0, z_2 = 1; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \text{if} z_1 = 1, z_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 1, z_2 = 1. \end{cases}$
	1	b	a	c	d	
	2	d	c	a	b	
	3	c	d	b	a	
2	0	a	c	d	b	$O_{2,19,14,7} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \text{if} z_1 = 0, z_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 0, z_2 = 1; \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix} \text{if} z_1 = 1, z_2 = 0; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 1, z_2 = 1. \end{cases}$
	1	c	d	b	a	
	2	d	b	a	c	
	3	b	a	c	d	
3	0	a	b	c	d	$O_{3,9,19,13} = \begin{cases} \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \text{if} z_1 = 0, z_2 = 0; \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 0, z_2 = 1; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 1, z_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \text{if} z_1 = 1, z_2 = 1. \end{cases}$
	1	b	a	d	c	
	2	c	d	b	a	
	3	d	c	a	b	
4	0	a	d	b	c	

	1	d	c	a	b	$O_{4,13,7,22} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \text{if} z_1 = 0, z_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \text{if} z_1 = 0, z_2 = 1; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \text{if} z_1 = 1, z_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \text{if} z_1 = 1, z_2 = 1. \end{cases}$
	2	b	a	c	d	
	3	c	b	d	a	

Conclusion. On the example of SEP, methods for constructing cryptographic primitives have been improved by applying cryptographic transformation matrix operations. This made it possible to build generalized operation models that implement multiple sliding encryption. Generalized recurrent sequences describing the information conversion functions during multiple sliding encryption are obtained. This made it possible to build algorithms for parallel implementing crypto primitives of multiple sliding encryption of a given number of iterations. These results provided an increase in encryption speed of up to 2 times and strength to linear cryptanalysis when implementing multi-round SEP.

The technology of operations synthesis for multioperational matrix cryptographic primitives is proposed. It uses the table model of crypto conversion operation. The technology is based on the new groups of operations up to permutation of both the input operands and the results of the operation.

The application of the results ensured the operation variability in improving multioperational crypto primitives and increased the strength of crypto algorithms built on their basis.

Thus, in this work a method for protecting information from unauthorized use is proposed. It consists in implementing cryptographic primitives of sliding encryption with optimized structure. These primitives were synthesized using cryptographic transformation matrix operations. Multiple SEP or multioperational matrix cryptographic primitives should be used to increase information security.

References:

1. Announcement of the Organizing Committee for the open competition of crypto algorithms on the termination of the application for participation in the competition. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=49027&

2. Navrotsky D.O. Methods of constructing symmetric cryptographic ciphers using three-dimensional transformations: dis. Cand. those. Sciences: 05.13.21 - information security systems. Kyiv, 2017. 243 p. URL: https://er.nau.edu.ua/bitstream/NAU/25391/4/Dissertation_Navrotskyi.pdf

3. Beletsky A.Y., Beletsky A.A., Navrotsky D.A., et al. Primitive polynomials in cryptographic applications. Modern Information Protection. 2011. No. 4. Pp. 5–18. (in Ukrainian).

4. Beletsky A.Y., Beletsky A.A. Cryptographic primitives based on the sliding coding method. SSU Bulletin. 2006. No. 10. Pp. 33–42. (in Ukrainian).

5. V.G. Babenko. Parallel implementation of sliding encryption. Information processing systems: coll. of sciences. Ave. - Kharkiv: HUP I. Kozheduba. 2013. Iss. 9 (116). Pp. 131-134. URL: http://www.hups.mil.gov.ua/periodic-app/article/11317. (in Ukrainian).

6. Rudnitsky V.M., Faure E.V., Sysoienko S.V. Evaluation of the quality of pseudorandom sequences based on module addition. Bulletin of the Academy of Engineering of Ukraine, Kiev. 2016. Iss. 3. Pp. 219-221. (in Ukrainian).

7. Faure E.V., Sysoienko S.V. Method for increasing the stability of pseudorandom sequences to linear cryptanalysis. The scientific potential of the present : proceedings of the International Scientific Conference (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform», Vinnytsia. 2016. Pp. 119–122. (in Ukrainian).

8. S.V. Sysoienko, V.G. Babenko, I.V. Myronets. Construction of a generalized mathematical model of group matrix cryptographic transformation. Modern Special Technique: Scientific and Practical Journal, Kyiv: State Research Institute of the Ministry of Internal Affairs of Ukraine; NAU; Nat. academy intern. Affairs. 2018. Vip. 4 (55). Pp. 96-103. URL: http://suchasnaspetstehnika.com/journal/ukr/2018_3.pdf. (in Ukrainian).

9. S.V. Sysoienko. Estimation of implementation speed of group matrix cryptographic transformation. Management, navigation and communication systems: coll. of sciences. works, Poltava: Poltava. tech. them. Yuriy Kondratyuk. 2018. Iss. 1 (47). Pp. 141–145. (in Ukrainian).

10. Svitlana Sysoienko, Iryna Myronets, Vira Babenko. Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation. Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019. CEUR Workshop Proceedings 2353, CEUR-WS.org 2019. Pp. 402 – 412. (Scopus) URL: http://ceur-ws.org/Vol-2353/paper32.pdf. (in Ukrainian).

11. V.G. Babenko. Optimization of matrix operations of sliding encryption. Weapons systems and military equipment: Sciences. Journal, Kharkiv: HUPS I. Kozheduba. 2013. No. 4 (36). Pp. 132-135 URL: http://www.hups.mil.gov.ua/periodic-app/article/2293. (in Ukrainian).

12. V.G. Babenko. Use of matrix operations of cryptographic transformation for sliding encryption.

Problems of informatization: Mater. the first international. scientific-technical Conf. abstracts, December 19-20, 2013 Cherkasy: ChSTU; Kiev: DUT; Togliatti: TDU; Poltava: PNTU. 2013. P. 22. (in Ukrainian).

13. V.M. Rudnitsky, E.V. Kozlov, V.G. Babenko. Method for parallel implementation of matrix cryptographic transformation operations. Vector of science of Togliatti State University. 2014. №2 (28). Pp. 11-15. (in Russian).

14. V.G. Babenko, O.G. Melnyk, O.B. Nesterenko. Simulation of sliding encryption primitives based on recurrent sequences. Science and Technology of the Air Forces of the Armed Forces of Ukraine, Kharkov: I. Kozheduba. 2015. Iss. 3 (20). Pp. 129-133. URL: http://www.hups.mil.gov.ua/periodic-app/article/13244. (in Ukrainian).

15. Rudnitsky V.N. Milchevich V.Y. Cryptographic coding. Collective monograph. “Generous Manor Plus” Publishing House, Kharkiv. 2014. 240 p. (in Ukrainian).