UDC 004.056.55:004.312.2
DOI: 10.15587/2312-8372.2020.202099

Lada N.,
Dzyuba V.,
Breus R.,
Lada S.

SYNTHESIS OF SETS OF NON-SYMMETRIC TWO-OPERAND TWO-BIT CRYPTO OPERATIONS WITHIN THE PERMUTATION ACCURACY

Об'єктом дослідження є процеси побудови операцій для криптографічного захисту інформації, тому що вимоги до інформаційної безпеки постійно зростають. Підвищення стійкості криптографічних перетворень напряму залежать від складності та варіативності криптоалгоримму. Підвищити варіативність можливо за рахунок збільшення спектру операцій криптоперетворення. Значно збільшити кількість операцій криптоперетворення можливо за рахунок синтезу несиметричних операцій. Дана робота присвячена створенню методологічного забезпечення синтезу та аналізу множин двооперандних дворозрядних криптооперацій з точністю до перестановки. Проведені дослідження базуються на результатах обчислювального експерименту, що полягає в синтезі двохоперандних дворозрядних криптооперацій на основі однооперандних, з подальшим пошуком пар операцій прямого та коректного оберненого криптоперетворення на основі повного перебору. В процесі обчислювального експерименту отримані пари двохоперандних операцій, представлені кортежами з чотирьох однооперандних операцій. Формалізація отриманих результатів забезпечила математичне представлення операцій, придатне для практичної реалізацій. Для спрощення складності практичної реалізації, синтезовані операції поділені на 24 множини по 24 операції. Поділ операцій відбувався за рахунок застосування шаблонів таблиць істинності множин операцій з точністю до перестановки операндів. Встановлено, що на основі використання шаблону будь-якої операції може бути побудована вся множина операцій з точністю до перестановки. Крім того, аналіз синтезованих множин показав, що множини симетричних і несиметричних операцій не перетинаються. Отримано 20 множин несиметричних двооперандних двохрозрядних операцій, а також 4 множини симетричних операцій. Подальше дослідження кожної синтезованої множини несиметричних операцій криптоперетворення забезпечить можливість встановлення взаємозв'язків між операндами операції та між операціями в цілому. Застосування синтезованих несиметричних операцій дасть змогу підвищити надійність криптоалгоритмів потокового шифрування інформації за рахунок значного збільшення варіативності крипографічних перетворень. В свою чергу застосування синтезованих множин операцій спростить практичну реалізацію в комп'ютерній криптографії.

Ключові слова: *комп'ютерна криптографія, несиметричні операції криптоперетворення, множини операцій, варіативність криптоалгоритмів.*

Received date: 06.02.2020
Accepted date: 02.03.2020
Published date: 30.04.2020

1. Introduction

In the modern scientific literature, in recent years, papers devoted to the study of modified symmetric operations in cryptographic algorithms for stream encryption, different from the classical modulo addition have appeared [1–3]. Such studies include, for example, modulo addition operations up to a permutation [4]. However, the operations of crypto conversion of information are not limited to symmetrical. Most of them are asymmetric, that is, the encoding operation will be different from the decoding operation. These operations are an order of magnitude larger [5, 3].

It should be noted that by analogy with symmetric operations used in stream encryption, studies of asymmetric operations will be more effective in terms of grouping into mathematical groups. The allocation of mathematical groups of asymmetric streaming encryption operations will allow to study the properties of such operations and establish the relationship between them. It will also simplify the software and hardware implementation of cryptographic algorithms with their use and improve the quality of encryption through the use of various operations from various mathematical groups [6, 7]. But despite the prospects for their application, the study of these operations in stream encryption was not paid at all. Thus, *the object of research* is the processes of constructing operations for cryptographic protection of information, as the requirements for information security are constantly growing. *The aim of research* is to create methodological support for the synthesis and analysis of sets of two-operand two-bit crypto operations within the permutation accuracy.

2. Methods of research

The study is based on the application of the approaches described in [8, 9]. The starting point of the study is the results of a computational experiment to search for two-operand two-bit crypto conversion operations.

Symmetric crypto conversion operations have the following properties [10]:

AôB = C; BôA = C; AôC = B; CôA = B;

BôC = A; CôB = A, (1)

where A and B – input information; C – result of the operation; ô – operation designation.

Unlike symmetric operations, which perform direct and inverse transformations; asymmetric operations exist only in combination of direct and inverse operations. In this case, the inverse operation may change when the operands are rearranged. Based on this pair of operations for asymmetric cryptographic conversion should have the following properties:

AôB = C; BôA = C; AõC = B; CóA = B;

BõC = A; CóB = A, (2)

where A and B – input information; C – result of the operation; ô – designation of a direct operation; õ, ó – designation of inverse operations.

It should be noted that for ô = õ = ó the asymmetric operation will coincide with the symmetric.

For experimental synthesis of two-operand operations, let's use many single-operand crypto conversion operations, given in Table 1 [11].

Table 1

Single-operand two-bit cryptographic information conversion operations

$F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_7 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{13} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{19} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	$F_8 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{14} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{20} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_3 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_9 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{15} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{21} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$F_4 = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{16} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{22} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_5 = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{11} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{17} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{23} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$F_6 = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	$F_{12} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{18} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{24} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Single-operand and two-operand operations of cryptographic information conversion are used. During the experiment, let's use a table representation of single-operand and two-operand operations. Based on this two-operand operation, the crypto conversion operation can be represented by the matrix $A[i,j]$, where i – the results of the j single-operand operation [12].

In order for the operation to correspond to expression (2), the following conditions must be met:

1. In each column of the transformation matrix there should be no repetition of the command (value of the operand).

2. In each row of the transformation matrix, the value of the operand (instruction) should not be repeated.

3. The matrix should be symmetric with respect to the main diagonal for constructing symmetric operations ($A[i,j] = A[j,i]$), and asymmetric – for constructing asymmetric operations ($A[i,j] \neq A[j,i]$).

During the experiment, let's synthesize double-operand operations by combining four single-operand operations by exhaustive search. To find pairs of asymmetric operations, a programmatic search was performed for the inverse crypto conversion for all possible synthesized two-operand two-bit operations. The essence of the search is as follows: on the set of input data, a crypto conversion operation was performed, which was taken directly. If the reverse operation exists for the direct operation, then the result of the reverse operation must coincide with the set of input data. As a direct operation, all synthesized crypto-digest operations were selected. For each direct operation, the reverse was searched by enumerating the entire set of input operations. The pairs of operations found will be asymmetric and symmetric crypto conversion operations.

During the experiment, 576 operations were obtained, of which 96 were symmetric operations, and 480 were asymmetric. Symmetric operations were investigated in a number of works [13–15]. Asymmetric operations received and published for the first time, and require further research.

To significantly reduce the amount of work in the study of symmetric operations, they were divided into 4 groups of operations. Further research of each group separately provided the opportunity to establish relationships between operands of an operation and between operations as a whole.

Let's consider the possibility of dividing asymmetric operations into sets of operations by analogy with symmetric operations. The results will provide an opportunity for further research aimed at the automatic synthesis of these operations and their practical application in computer cryptography.

In the process of a computational experiment, pairs of two-operand operations are obtained, represented by sets of single-operand operations. For example:

«1, 13, 19, 7» «6, 12, 18, 24».

Let's formalize these sets in the operation of direct and reverse asymmetric crypto conversion.

Since $O^k \to O^d$, then

$$O^d_{1,13,19,7} \to O^d_{1,13,19,7} = O^k_{6,12,18,24}$$

or

$$O^d_{1,13,19,7} \to O^d_{6,12,18,24},$$

where is the reflection of the relationship between direct and reverse operations (coding and decoding transactions). Indices in two-operand operations denote tuples of single-operand operations in the numbering of the Table 1.

Substituting one-operand operations in the designation of two-operands, let's obtain.

Let's formalize these tuples in the operation of direct and reverse asymmetric crypto conversion.

Since, then, or, where is the reflection of the relationship between direct and reverse operations (coding and decoding transactions). Indices in two-operand operations denote sets of single-operand operations in the numbering of the Table 1.

Substituting single-operand operations in the designation of two-operand, let's obtain:

$$O^k_{1,13,19,7} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ if } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ if } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ if } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ if } k_1 = 1;\ k_2 = 1 \end{cases} \rightarrow$$

$$\rightarrow O^d_{6,12,18,24} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{ if } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ if } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ if } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ if } k_1 = 1;\ k_2 = 1, \end{cases}$$

where x_i, k_i – value of the i-th bits of the first and second operands, respectively.

To separate experimentally obtained operations into sets, it is proposed to use templates of truth tables of operations up to permutation. 24 templates of sets of operations were constructed up to an operand permutation, some of which are given in Table 2.

Table 2

Templates of truth tables of sets of operations within the operand permutation

Operand value	Template 1				Template 2				…	Template 24			
	0	1	2	3	0	1	2	3	…	0	1	2	3
0	*a*	*b*	*d*	*c*	*a*	*d*	*c*	*b*	…	*a*	*d*	*c*	*b*
1	*b*	*c*	*a*	*d*	*b*	*a*	*d*	*c*		*b*	*c*	*a*	*d*
2	*c*	*d*	*b*	*a*	*c*	*b*	*a*	*d*		*c*	*b*	*d*	*a*
3	*d*	*a*	*c*	*b*	*d*	*c*	*b*	*a*		*d*	*a*	*b*	*c*

Note: $a, b, c, d \in \{0,1,2,3\}$, $a \neq b \neq c \neq d$

Operation templates are necessary for constructing sets of operations by sorting the truth tables of experimentally synthesized operations.

3. Research results and discussion

According to the results of sorting the synthesized operations on the basis of the proposed templates, 24 sets of operations were obtained, 24 operations in each plural. Examples of constructed sets of operations are given in Table 3.

Table 3

Set of double-operand two-bit operations

No.	Set 1	Set 2	…	Set 24
1	$O^k_{1,8,20,13} \rightarrow O^d_{3,11,15,23}$	$O^k_{1,20,13,8} \rightarrow O^d_{2,7,14,19}$	…	$O^k_{1,19,16,10} \rightarrow O^d_{2,11,17,20}$
2	$O^k_{13,20,8,1} \rightarrow O^d_{15,23,3,11}$	$O^k_{4,23,10,17} \rightarrow O^d_{5,16,11,22}$	…	$O^k_{5,17,9,21} \rightarrow O^d_{4,24,12,16}$
3	$O^k_{2,19,7,14} \rightarrow O^d_{5,21,17,9}$	$O^k_{5,16,11,22} \rightarrow O^d_{4,23,10,17}$	…	$O^k_{2,8,18,24} \rightarrow O^d_{1,21,15,7}$
4	$O^k_{24,9,15,6} \rightarrow O^d_{22,7,4,13}$	$O^k_{8,1,20,13} \rightarrow O^d_{7,14,19,2}$	…	$O^k_{10,16,1,19} \rightarrow O^d_{11,20,2,17}$
5	$O^k_{6,15,9,24} \rightarrow O^d_{4,13,22,7}$	$O^k_{10,17,4,23} \rightarrow O^d_{11,21,5,16}$	…	$O^k_{9,21,17,5} \rightarrow O^d_{12,4,16,24}$
…	…	…	…	
20	$O^k_{5,22,16,11} \rightarrow O^d_{2,24,8,18}$	$O^k_{14,19,2,7} \rightarrow O^d_{13,8,1,20}$	…	$O^k_{14,20,6,12} \rightarrow O^d_{13,9,3,19}$
21	$O^k_{16,5,11,22} \rightarrow O^d_{18,2,24,8}$	$O^k_{15,6,9,24} \rightarrow O^d_{18,21,12,3}$	…	$O^k_{15,3,11,23} \rightarrow O^d_{18,22,10,6}$
22	$O^k_{10,23,17,4} \rightarrow O^d_{12,20,6,14}$	$O^k_{21,12,3,18} \rightarrow O^d_{24,15,6,9}$	…	$O^k_{22,4,13,7} \rightarrow O^d_{23,8,14,5}$
23	$O^k_{3,12,18,21} \rightarrow O^d_{1,10,19,16}$	$O^k_{19,2,7,14} \rightarrow O^d_{20,13,8,1}$	…	$O^k_{20,14,12,6} \rightarrow O^d_{19,3,9,13}$
24	$O^k_{21,18,12,3} \rightarrow O^d_{19,16,1,10}$	$O^k_{24,15,6,9} \rightarrow O^d_{21,12,3,18}$	…	$O^k_{23,11,15,3} \rightarrow O^d_{22,6,18,10}$

The analysis of synthesized sets shows that 20 sets consist solely of asymmetric double-operand operations. The obtained results allow to state that the sets of symmetric and asymmetric operations do not intersect. In addition, using a template corresponding to each set allows to create the whole set of asymmetric operations with any operation of this set.

The uniqueness of each of the 576 truth tables indicates that all synthesized operations are different, and the presence of the corresponding decoding operations obtained as a result of a practical experiment allows to be practically implemented. The use of synthesized sets of operations will provide an increase in the variability of cryptographic transformations of stream encryption.

4. Conclusions

Based on the results of a computational experiment, 576 two-bit two-operand cryptographic coding operations were constructed, of which 96 were symmetric operations, and 480 were asymmetric.

The synthesized operations are divided into 24 sets of 24 operations, of which 20 are sets of asymmetric operations and 4 are sets of symmetric operations. Operations were separated using 24 truth table templates.

Since the entire multiplication of operations is described by one template, then with any one operation of any set, it is possible to build the whole set of operations on the basis of the given.

It is established that the truth tables of synthesized operations are not repeated, therefore they are all different. The use of synthesized operations will increase the variability of cryptographic conversion algorithms, and the use of multiple operations will simplify their practical implementation.

References

1. Rudnytskyi, V. M., Opirskyi, I. R., Melnyk, O. H., Pustovit, M. O. (2018). Syntez hrupy operatsii strohoho stiikoho kryptohrafichnoho koduvannia dlia pobudovy potokovykh shyfriv. *Bezpeka informatsii, 24 (3),* 195–200.
2. Pustovit, M. O., Melnyk, O. H., Sysoienko, S. H. (2017). Syntez operatsii obernenoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia informatsii. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky, 4,* 118–124.
3. Bernstein, D., Buchmann, J., Dahmen, E. (2009). *Post-quantum cryptography*. Berlin: Springer, 246. doi: http://doi.org/10.1007/978-3-540-88702-7
4. Lada, N. V., Kozlovska, S. H. (2018). Applying cryptographic addition operations by module twowith accuracy of permutation in stream ciphers. *Control, Navigation and Communication Systems. Academic Journal, 1 (47),* 127–130. doi: http://doi.org/10.26906/sunz.2018.1.127
5. Adki, V., Hatkar, S. (2016). A Survey on Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 6 (6),* 469–475.
6. Rudnytskyi, V., Opirskyy, I., Melnyk, O., Pustovit, M. (2019). The implementation of strict stable cryptographic coding operations. *Advanced Information Systems, 3 (3),* 109–112. doi: http://doi.org/10.20998/2522-9052.2019.3.15
7. Ferguson, N., Schneier, B. (2003). *Practical Cryptography: Designing and Implementing Secure Cryptographic Systems*. Wiley, 432.
8. Kozlovska, S. H. (2018). Syntez hrup dvokhoperandnykh operatsii kryptoperetvorennia na osnovi perestanovochnykh skhem. *Suchasna spetsialna tekhnika, 4 (55),* 44–50.
9. Rudnitsky, V., Berdibayev, R., Breus, R., Lada, N., Pustovit, M. (2019). Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Advanced Information Systems, 3 (4),* 109–114. doi: http://doi.org/10.20998/2522-9052.2019.4.16
10. Rudnytskyi, V. M., Lada, N. V., Babenko, V. H. (2018). *Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky*. Kharkiv: TOV «DISA PLIuS», 184.
11. Lada, N., Kozlovska, S., Rudnitskaya, Y. (2019). Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations. *Central Ukrainian Scientific Bulletin. Technical Sciences, 2 (33),* 181–189. doi: http://doi.org/10.32515/2664-262x.2019.2(33).181-189
12. Hoffstein, J., Pipher, J., Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*. Springer, 523. doi: http://doi.org/10.1007/978-1-4939-1711-2
13. Mao, W. (2003). *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 648.
14. Melnyk, R. P. (2012). Zastosuvannia operatsii rozshyrenoho matrychnoho kryptohrafichnoho peretvorennia dlia zakhystu informatsii. *Systemy obrobky informatsii, 9 (107),* 145–147.
15. Rudnytskyi, V. M. (Ed.) (2018). *Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii.* Kharkiv: TOV «DISA PLIuS», 139.

Lada Nataliia, *PhD, Department of Information Security and Computer Engineering, Cherkasy State Technological University, Ukraine, ORCID: http://orcid.org/0000-0002-7682-2970, e-mail: Ladanatali256@gmail.com*

Dzyuba Viktoriya, *Senior Lecturer, Postgraduate Student, Department of Economics, Finance, Accounting, Mathematical and Information Sciences, Cherkasy branch of the private higher educational institution «European University», Ukraine, ORCID: http://orcid.org/0000-0003-1655-0333, e-mail: viktoriya.dzyuba15@gmail.com*

Breus Roksolana, *Assistant, Department of Information Security and Computer Engineering, Cherkasy State Technological University, Ukraine, ORCID: http://orcid.org/0000-0001-5281-2017, e-mail: skay1986@ukr.net*

Lada Serhii, *Specialist of first category, Department of Information Technology of the Operations Center, Telecommunication Systems and Information Technologies, Department of the State Emergency Service of Ukraine in Cherkassy region, Cherkasy, Ukraine, ORCID: http://orcid.org/0000-0002-2306-9081, e-mail: Raphaello1986@gmail.com*