Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

UDC 004.056.55:004.312.2
DOI: https://doi.org/10.30837/ITSSI.2022.20.035

N. LADA, Y. RUDNYTSKA

IMPLEMENTATION OF A METHOD FOR SYNTHESIZING GROUPS OF SYMMETRIC DOUBLE-OPERAND OPERATIONS OF CRYPTOGRAPHIC INFORMATION CODING FOR BLOCK ENCRYPTION SYSTEMS

The **object** of the study is the processes of building groups of symmetric double-operand operations of cryptographic coding of information. The **subject** of the study are features of the implementation of a generalized method of synthesis groups of symmetric two-operand operations of cryptographic coding information for "lightweight cryptography". The purpose of this work is to investigate the process of building and implementing a method of synthesis of groups of symmetric multibit double-operand operations of information cryptographic coding to provide automation for finding ways to increase the variability, and stability of lightweight cryptoalgorithms. The following **tasks** are solved in the article: to determine the mathematical group of single-operand operations, on the basis of which the realization of the method of synthesis of groups of symmetric double-operand operations of cryptographic coding will be presented; to offer the search technology of symmetric double-operand operations; to evaluate power of synthesized groups of operations, and their influence on variability and stability of " lightweight cryptography" algorithms. The following **results** were obtained: the technology for determining symmetric double-operand operations, which will be the basis for the synthesis of a group of symmetric double-operand operations, was proposed. A method for synthesizing groups of symmetric double-operand cryptographic information coding operations for block encryption systems was proposed and implemented. On the example of module-two addition with correction and the use of three-digit single-operand operations, the practical implementation of this method was shown. Based on the synthesized operations and the given quantitative characteristics of the set of single-operand operations, the power of synthesized groups of operations and their influence on the variability and stability of "lightweight cryptography" algorithms were evaluated. **Conclusions:** the proposed and implemented method of synthesis of groups of symmetric double-operand operations of cryptographic coding information allows to provide the possibility of increasing the variability of lightweight crypto-algorithms. Synthesis of symmetric cryptographic coding operations belonging to different mathematical groups provides increase of algorithm's crypto stability. Application of synthesized cryptographic coding operations leads to significant increase of variability of cryptoalgorithms and their complexity.

Keywords: cryptographic encoding; lightweight cryptography; synthesis of symmetric operation groups.

Introduction

Statement of the problem. The development of information technology and the digitalization of society have led to the need to process large amounts of data in real time. However, there are a number of applications of information technology related to the need to process sensitive information with limited resources. To solve these problems traditional crypto-algorithms were not effective enough [1 - 3]. Their solution is the use of "lightweight cryptography" using cryptographic coding operations. This approach provides both theoretical and practical solution to the important scientific and technical problem of providing protection of personal information resources and secure functioning of personal information management systems under existing hardware limitations.

Analysis of recent research and publications

The development of lightweight cryptoalgorithms is conducted mainly in the direction of using special restrictions of traditional algorithms on the block size, number of internal states, simplification of rounds algorithms and their number [3, 5 - 7]. However, it should be noted that the development of lightweight cryptoalgorithms focuses on block-based crypto algorithms [8].

The second way of developing "lightweight cryptography" is to build crypto-algorithms based on cryptographic coding operations [9, 10]. Synthesized cryptographic coding operations based on discrete substitution table models implement both linear and nonlinear information transformations [11, 12].

Among cryptographic coding operations, a special place belongs to double-operand operations, which provide a random implementation of substitution tables. [13, 14]. Among a variety of double-operand operations it is reasonable to allocate symmetric double-operand operations [15, 16], which can find wide application both in block and stream encryptions.

However, at present multi-digit double-operand operations of cryptographic conversion remain insufficiently investigated. It should be noted that the digit capacity of double-operand operations means the minimum amount of information to be converted [13]; the units of the minimum amount of information can be bits, bytes, words, etc.

The **aim** of the article. To study the process of construction and implementation of the method of synthesis of groups of symmetric multi-digit double-operand operations of cryptographic coding of information to provide automation of finding ways to increase the variability of lightweight cryptoalgorithms.

Main part

A double-operand cryptographic encoding operation is an operation, which converts the value of the first operand based on one of several single-operand operations, depending on the value of the second operand. In other words, a double-operand operation is a formalized tuple of single-operand operations from which only the single-operand operation whose ordinal number is determined by the second operand will be implemented

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

for information conversion.

If at identical values of the second operand the two-operand operation realizes both direct and reverse cryptographic transformation, this operation will be symmetric.

Let us consider synthesis of symmetric three-digit two-operand cryptographic coding operations.

The number of single-operand cryptographic encoding operations is defined [10].

$$K_o^1(n) = 2^n!, \quad (1)$$

$$K_o^1(n) = K_{об}(n) \cdot K_{оп}(n) \cdot K_{оu}(n) = K_{об}(n) \cdot n! \cdot 2^n \quad (2),$$

where n – operation digit, $K_{об}(n)$, $K_{об}(n) \cdot n!$, $K_{оu}(n) = 2^n$ the number of basic operations, transposition operations, and inversion operations, respectively.

Based on expressions (1) and (2) the number of two-digit single-operand cryptographic coding operations is defined [9]:

$$K_o^1(2) = 4! = 24.$$

$$K_o^1(2) = K_{об}(2) \cdot 2! \cdot 2^2 = 3 \cdot 6 \cdot 4 = 24.$$

Since, according to the results of the experiment, there are 96 symmetric two-digit double-operand operations, and they make up 4 groups of 24 operations, we can assume that: $K_o^2(2) = 96 = 4 \cdot 2^2!$. So,

$$K_o^2(n) = k \cdot 2^n! \quad (3)$$

where k – number of groups of symmetric n-digit double-operand cryptographic coding operations.

The number of operations in each group of symmetric three-digit two-order operations according to (3) is defined: $K_o^2(3) = k \cdot 2^3! = k \cdot 8!$ and is 40 320 operations [17].

In practice, it is currently impossible to synthesize a group of such a number of operations. This is due to the lack of a single mathematical apparatus allowing to simulate the whole set of three-digit single-operand operations [10]. Therefore, in the process of synthesis of symmetric three-digit two-operand operations we will limit ourselves only to synthesis of basic double-operand operations based on matrix single-operand operations.

According to [17], the number of basic three-digit single-operand matrix operations is 28 operations. These operations are presented in table 1.

Table 1. *Basic group of three-digit single-operand matrix cryptographic coding operations*

$F_1^k = F_1^d = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$	$F_8^k = F_8^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$	$F_{15}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ $F_{15}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{22}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$ $F_{22}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$F_2^k = F_2^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix}$	$F_9^k = F_9^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{16}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_3 \end{pmatrix}$ $F_{16}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ $F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
$F_3^k = F_3^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$F_{10}^k = F_{10}^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{17}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ $F_{17}^d = \begin{pmatrix} x_1; \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{24}^k = F_{24}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
$F_4^k = F_4^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$	$F_{11}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ $F_{11}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{18}^k = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$ $F_{18}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{25}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$ $F_{25}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

The end **Table 1**

$F_5^k = F_5^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{12}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{19}^k = F_{19}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{26}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{12}^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}$		$F_{26}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix}$
$F_6^k = F_6^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{13}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_2 \end{pmatrix}$	$F_{20}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{27}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{13}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{20}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{27}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$F_7^k = F_7^d = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{14}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{21}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{28}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{14}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{21}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{28}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$

Therefore, in the process of synthesis of symmetric three-digit double-operand matrix operations of cryptographic coding we will use numbering of single-operand operations according to table 1.

To develop and implement the method of synthesis of groups of symmetric double-operand operations of cryptographic coding information for block encryption systems it is necessary to establish a symmetric double-operand operation based on which we will conduct the synthesis.

Let us consider in more detail the operation $O_1^{4\oplus}$, on the basis of which the synthesis of the fourth group of symmetric two-operand operations of cryptographic coding was performed [15]:

$$O_1^{4\oplus} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix} \quad (4)$$

Based on expression (4), the operation $O_1^{4\oplus}$ can be called a bitwise addition operation module-two with correction.

When developing the method of synthesis of groups of symmetric double-operand operations of cryptographic coding synthesis was performed on the basis of operations:

1) module-two additon:
- digit addition by module-two;
- digit addition module-two with correction;

2) module four additon:
- left-handed module four addition;
- right handed module four addition.

The transposition of elementary functions in operations does not affect the number of modified groups of operations with a transposition accuracy. The only operation that implements the encoding of a bit of information regardless of the serial number of the bit is the digit addition by module two. Based on this we can define the following list of operations:

1) module-two additon:
- digit addition by module-two:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} \quad (5)$$

- digit addition module-two with correction;

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix} \quad (6)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \oplus x_3)\cdot(k_1 \oplus k_3) \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \oplus (x_2 \oplus x_3)\cdot(k_2 \oplus k_3) \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \oplus (x_2 \oplus x_3)\cdot(k_2 \oplus k_3) \end{bmatrix}$$

2) module four additon:
- left-handed module four addition:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \cdot k_2 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \cdot k_3 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix};$$

- right handed module four addition:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_1 \cdot k_1 \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix};$$

3) module eight additon:
- left-handed module eight addition;

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_3 \cdot k_3 \vee k_2 \cdot x_3 \cdot k_3) \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_3 \cdot k_3 \vee x_3 \cdot x_2 \cdot k_2 \vee k_3 \cdot x_2 \cdot k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix}$$

- right handed module eight addition.

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_1 \cdot k_1 \vee k_2 \cdot x_1 \cdot k_1) \end{bmatrix} \quad O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_1 \cdot k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \cdot k_1 \vee x_1 \cdot x_2 \cdot k_2 \vee k_1 \cdot x_2 \cdot k_2) \end{bmatrix}.$$

The given operations differ in mathematical representation and truth tables of transactions. Generalized tables of transactions with permutation accuracy also differ. Based on this, at least 14 groups of symmetric double-operand operations of cryptographic information coding for block encryption systems will be constructed based on the proposed synthesis method.

Let's synthesize basic group of symmetric three-digit double-operand matrix operations of cryptographic coding based on operation (6). For this purpose, we introduce a substitution in the operation

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

$$y_1 = x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2);$$

$$y_2 = x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2);\ y_3 = x_3 \oplus k_3$$

Using the basic three-digit single-operand matrix operations shown in table 1, we obtain 28 basic three-digit single-operand matrix operations:

$$O_1 = F_1(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_2 = F_2(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_3 = F_3(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_4 = F_4(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

$$O_5 = F_5(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_6 = F_6(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_7 = F_7(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_8 = F_8(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_9 = F_9(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{10} = F_{10}(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{11} = F_{11}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{12} = F_{12}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{13} = F_{13}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \end{bmatrix};$$

$$O_{14} = F_{14}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{15} = F_{15}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{16} = F_{16}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_1 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{17} = F_{17}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$O_{18} = F_{18}(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{19} = F_{19}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{20} = F_{20}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{21} = F_{21}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{22} = F_{22}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{23} = F_{23}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{24} = F_{24}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{25} = F_{25}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{26} = F_{26}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{27} = F_{27}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{28} = F_{28}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix}.$$

To verify the correctness of the results of the synthesis of the obtained symmetric matrix operations, the requirements to the symmetry of the transactions given by the truth tables were applied. Additionally, each operation was verified by taking into account the complete enumeration of all input data.

Similarly, groups of symmetric double-operand operations based on an operation by using both a complete group of three-digit single-operand matrix operations and groups of three-digit single-operand nonlinear operations were synthesized. When constructing symmetric double-operand operations based on nonlinear three-digit single-operand nonlinear operations, it was found that the complexity of the models increased. This complication is related to the necessity of transition from representation of discrete models based on addition by module two to representation of discrete models in the basis of "AND-OR-NET"

During the process of implementation the method of synthesis the groups of symmetric double-operand

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

operations of cryptographic coding of information was found the following:

- based on each selected three-digit double-operand operation according to (3) 6 permutation operations will be constructed [17]. By applying the inversion of elementary functions, 8 inversion operations will be constructed of each obtained operation [17]. This will make it possible to extract 48 modifications of this operation from one symmetric three-digit double-operand operation, each of which is suitable for constructing a group of operations based on it.;

- the application of the proposed method of synthesis of groups of symmetric double-operand operations of cryptographic coding information for block coding systems based on one symmetric double-operand operation by using 28 three-digit basic matrix operations [17] will provide the construction of a group of 28 symmetric double-operand operations. The use of 48 modifications of the symmetric double-operand operation will provide the construction of 48 groups of operations, including 1344 symmetric three-digit double-operand matrix operations.;

- since the total number of three-digit single-operand matrix operations includes 1344 operations [17], then based on one symmetric three-digit double-operand operation will be built 64512 symmetric three-digit double-operand matrix operations.

- the maximum number of synthesized symmetric three-digit double-operand operations based on one given operation will be 1935360 operations since the full group of three-digit single-operand operations is 40320 (but their formalization is complicated by the absence of a single mathematical apparatus describing the whole set of linear and nonlinear single-operand operations). the maximum number of synthesized symmetric three-digit double-operand operations based on one given operation will be 1935360 operations since the full group of three-digit single-operand operations is 40320 (but their formalization is complicated by the absence of a single mathematical apparatus describing the whole set of linear and nonlinear single-operand operations)..

- when implementing the method of synthesis of groups of symmetric double-operand operations of cryptographic coding information in automated intelligent design systems, it is reasonable to represent crypto-transformation operations as mathematical models and truth tables to build in knowledge and data bases.

The application of the technology of building groups of symmetric matrix operations is not limited to the synthesis of groups of two- and three-digit operations. The obtained results allow to considerably expand both possibilities of developers of "lightweight cryptography" and variability of synthesized crypto-algorithms. Simplicity of realization of the offered method of symmetric matrix operations allows to use it for construction and filling of knowledge and data bases of intellectual systems of cryptoalgorithms designing. To ensure the speed of implementation of multi-digit double-operand nonlinear symmetric crypto-transformation operations it is reasonable to use substitution tables, the implementation of which compensates the lack of mathematical apparatus of formalized description of operation models.

Conclusions

The proposed method of synthesis of groups of symmetric double-operand operations of information cryptographic coding provides an opportunity to increase the variability of lightweight cryptoalgorithms by increasing significantly the total number of used operations. Additionally, the synthesis of symmetric cryptographic coding operations belonging to different mathematical groups provides increased crypto stability of the algorithm. Application of the double-operand cryptographic coding operations, to which the synthesized operations belong, leads to an insignificant increase in the complexity associated with implementation of synthesis of operations both at the hardware and software levels.

In the process of implementation of the method of synthesis of groups of symmetric double-operand operations of cryptographic coding of information it was found that on the basis of the known symmetric three-bit double-operand cryptographic conversion operation it is possible to build up to 1935360 its modifications with similar possibilities of use in crypto algorithms. This result allows to increase by an order of magnitude the variability of information protection algorithms.

Further research of the presented topic was expedient to conduct on three-operand, and later on multi-operand operations. However, the received results are suitable for practical use in developing new block encryption systems with increased speed and reliability of cryptographic transformation of information or, for example, in improving generation of pseudorandom sequences.

References

1. Horbenko, I. D., Horbenko, Yu. I. (2012), *Applied cryptology: monograph* [*Prykladna kryptolohiia: monohrafiia*], Kharkiv: Kharkiv National University of Radio Electronics, LLC "Fort", 868 p.
2. Bevz, O. M., Kvetnii, R. N. (2010), *Data Encryption Based on Highly Nonlinear Boolean Functions and Maximum Distance Codes:* monograph [*Shyfruvannia danykh na osnovi vysoko neliniinykh bulevykh funktsii ta kodiv z maksymalnoiu vidstanniu*: monohrafiia], Vinnytsia: Vinnytsia National University of Technology, 96 p.
3. Manifavas, C., Hatzivasilis, G., Fysarakis, K., Rantos, K. (2012), "Lightweight cryptography for embedded systems a comparative analysis", *In: 6th International Workshop on Autonomous and Spontaneous Security SETOP 2012, Springer, LNCS, 8247,* P. 333–349. DOI: https://doi.org/10.1007/978-3-642-54568-9_21
4. Gildas Avoine, Julio Hernandez-Castro (2021), "Security of Ubiquitous Computing Systems", *Selected Topics. Springer,* P. 265 DOI: https://doi.org/10.1007/978-3-030-10591-4
5. Biryukov Alex and Perrin Leo (2017), "State of the art in lightweight symmetric cryptography", *Cryptology ePrint Archive, Report 2017/511,* available at: http://eprint.iacr.org/2017/511, https://eprint.iacr.org/2017/511.pdf

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)*

6. Mitsuru Matsui (1997), "New block encryption algorithm MISTYC", *In Eli Biham, editor, Fast Software Encryption – FSE'97, pringer, volume 1267 of Lecture Notes in Computer Science, Haifa, Israel, January 20–22,* P. 54–68, available at: https://link.springer.com/chapter/10.1007/BFb0052334
7. Hatzivasilis George, Fysarakis Konstantinos, Ioannis (2018), "Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers", *Cryptographic Engineering*, No. 8 (2), P. 141–184. DOI: https://doi.org/10.1007/s13389-017-0160-y
8. Kerry A. McKay, Larry Bassham, Meltem Sonmez Turan, and Nicky Mouha (2016), "Nistir 8114 - report on lightweight cryptography". DOI: https://doi.org/10.6028/NIST.IR.8114
9. Rudnytsky, V. M., Lada, N. V., Babenko, V. G. (2018), *Cryptographic coding: synthesis of stream encryption operations with accuracy to permutation: monograph* [*Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky: monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 184 p.
10. Rudnitsky, V. M., Milchevich, V. Ya., Babenko, V. G., Melnyk, R. P., Rudnitsky, S. V., Melnyk O. G. (2014), *Cryptographic coding: methods and means of implementation (part 2):* monograph [*Kriptograficheskoe kodirovanie: metody i sredstva realizacii (chast' 2):* monografiya], Monograph, Kharkov: Publishing house "Shchedra sadyba plius", 223p.
11. Rudnytsky, V. M., ed. (2018), *Cryptographic coding: information processing and protection: collective monograph* [*Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kolektyvna monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 139p.
12. Sysoienko, S., Myronets, I., Babenko, V. (2019), "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), CEUR Workshop Proceedings 2353, CEUR-WS.org,* P. 402–412. (Scopus) available at: http://ceur-ws.org/Vol-2353/, http://ceur-ws.org/Vol-2353/paper32.pdf
13. Rudnitsky, V., Berdibayev, R., Breus, R., Lada, N. and Pustovit, M. (2019), "Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation", *Advanced Information Systems, Kharkiv: NTU "KhPI"*, No. 3 (4), P. 109–114. DOI: http://doi.org/10.20998/2522-9052.2019.4.16
14. Lada, N. V., Kozlovska, S. G., Rudnitsky, S. V. (2019), " The symmetric operations' mathematical group constructing based on module-2 addition " ["Pobudova matematy`chnoyi grupy` sy`metry`chny`x operacij na osnovi dodavannya za modulem dva"]. *Modern special technics: scientific and practical journal. Kyiv*, No 4 (59), P.33–41.
15. Lada, N. V., Kozlovska, S. G. and Rudnitskaya, Y. V. (2019), "Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii dodavannia za modulem chotyry "], *Central Ukrainian Scientific Bulletin. Technical Sciences*, No. 2 (33), P. 181–189. DOI: http://doi.org/10.32515/2664-262x. 2019.2(33)
16. Lada, N. V., Rudnitsky, S. V., Zazhoma, V. M. and Rudnytska, Y. V. (2020), " Research and synthesis of a group of symmetric modified operations of right-handed addition by module four" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii pravostoronnoho dodavannia za modulem chotyry"], *Control, Navigation and Communication Systems. Academic Journal. Poltava: PNTU*, No. 1 (59), P. 93–96. DOI: https://doi.org/10.26906/SUNZ.2020.1.093
17. Rudnitsky, V. M., Babenko, V. G., Rudnitsky, S. V. (2012), " Method of synthesis of matrix models of operations of cryptographic recoding of information" ["Metod syntezu matrychnykh modelei operatsii kryptohrafichnoho perekoduvannia informatsii"], *Ukrainian Information Security Research Journal*, Vol 14, No. 3 (56), P. 50–56. DOI: https://doi.org/10.18372/2410-7840.14.3360

Received 18.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Лада Наталія Володимирівна – кандидат технічних наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, м. Черкаси, Україна; e-mail:Ladanatali256@gmail.com; ORCID: https://orcid.org/0000-0002-7682-2970

Lada Nataliia – Candidate of Technical Sciences, Associate Professor of Department of Information Security and Computer Engineering Cherkasy State Technological University, Cherkasy, Ukraine.

Лада Наталия Владимировна – кандидат технических наук, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, г. Черкассы, Украина.

Рудницька Юлія Володимирівна – аспірант кафедри інформаційних технологій проектування Черкаського державного технологічного університету, м. Черкаси, Україна; e-mail: U.V.Rudnitskaya@gmail.com; ORCID: https://orcid.org/0000-0001-6384-0523

Рудницкая Юлия Владимировна – аспирант кафедры информационных технологий проектирования Черкасского государственного технологического университета, г. Черкассы, Украина.

Rudnytska Yuliia – graduate student of Department of Information Technology Design Cherkasy State Technological University, Cherkasy, Ukraine.

РЕАЛІЗАЦІЯ МЕТОДУ СИНТЕЗУ ГРУП СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ІНФОРМАЦІЇ ДЛЯ СИСТЕМ БЛОКОВОГО ШИФРУВАННЯ

Об'єктом дослідження є процеси побудови груп симетричних двохоперандних операцій криптографічного кодування інформації. **Предметом** дослідження є особливості реалізації узагальненого методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для «полегшеної криптографії». **Мета** роботи – дослідити процес побудови і реалізації методу синтезу груп симетричних багаторозрядних двоопераднних операцій криптографічного

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2524-2296 (online)*

кодування інформації для забезпечення автоматизації пошуку шляхів збільшення варіативності і стійкості полегшених криптоалгоритмів. В статті вирішуються наступні **завдання:** визначити математичну групу одноопераднних операцій на основі якої буде представлено реалізацію методу синтезу груп симетричних двохоперандних операцій криптографічного кодування; запропонувати технологію пошуку симетричних двохоперандних операцій; оцінити потужність синтезованих груп операцій та їх вплив на варіативність та стійкість алгоритмів «полегшеної криптографії». Отримано наступні **результати:** запропоновано технологію визначення симетричних двохоперандних операцій які будуть основою для синтезу групи симетричних двохоперандних операцій; запропоновано та реалізовано метод синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування; на прикладі порозрядного додавання за модулем два з корекцією та використання трьохрозрядних одноопераднних операцій показано практичну реалізацію даного методу; на основі синтезованих операцій та наведених кількісних характеристики множини одноопераднних операцій проведено оцінку потужностість синтезованих груп операцій та їх вплив на варіативність та стійкість алгоритмів «полегшеної криптографії». **Висновки:** запропонований то реалізований метод синтезу груп симетричних двоопераднних операцій криптографічного кодування інформації дозволяє забезпечити можливість збільшення варіативності полегшених криптоалгоритмів. Синтез симетричних операцій криптографічного кодування, що належать різним математичним групам, забезпечує підвищення криптостійкість алгоритму. Застосування синтезованих операцій криптографічного кодування, приводить до значного збільшення варіативності криптоалгоритмів та їх складності.

Ключові слова: криптографічне кодування; полегшена криптографія; синтез груп симетричних операцій.

РЕАЛИЗАЦИЯ МЕТОДА СИНТЕЗА ГРУПП СИМЕТРИЧЕСКИХ ДВУХОПЕРАНДНЫХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ ИНФОРМАЦИИ ДЛЯ СИСТЕМ БЛОЧНОГО ШИФРОВАНИЯ

Объектом исследования есть процессы построения групп симметричных двухоперандных операций криптографического кодирования информации. **Предметом** исследования есть особенности реализации обобщенного метода синтеза групп симметричных двухоперандных операций криптографического кодирования информации для «облегченной криптографии». **Цель** работы – исследовать процесс построения и реализации метода синтеза групп симметричных многоразрядных двухоперандных операций криптографического кодирования информации для обеспечения автоматизации поиска путей увеличения вариативности, и устойчивости облегченных криптоалгоритмов. В статье решаются следующие **задачи:** определить математическую группу одноопераднных операций, на основе которой будет представлена реализация метода синтеза групп симметричных двухоперандных операций криптографического кодирования; предложить технологию поиска симметричных двухоперандных операций; оценить мощность синтезированных групп операций, и их влияние на вариативность и устойчивость алгоритмов "облегченной криптографии". Получены следующие **результаты:** предложена технология определения симметричных двухоперандных операций, которые будут основой для синтеза группы симметричных двухоперандных операций; предложен и реализован метод синтеза групп симметричных двухоперандных операций криптографического кодирования информации для систем блочного шифрования; на примере поразрядного сложения по модулю два с коррекцией, и использования трехразрядных одноопераднных операций показана практическая реализация данного метода; на основе синтезированных операций и приведенных количественных характеристик множества одноопераднных операций проведена оценка мощности синтезированных групп операций и их влияние на вариативность и стойкость алгоритмов «облегченной криптографии». **Выводы:** предложенный и реализованный метод синтеза групп симметричных двухоперандных операций криптографического кодирования информации позволяет обеспечить возможность увеличения вариативности облегченных криптоалгоритмов. Синтез симметричных операций криптографического кодирования, принадлежащих разным математическим группам, обеспечивает повышение криптостойкости алгоритма. Применение синтезированных операций криптографического кодирования приводит к значительному увеличению вариативности криптоалгоритмов и их сложности.

Ключевые слова: криптографическая кодировка; облегченная криптография; синтез групп симметричных операций.

Бібліографічні описи / Bibliographic descriptions

Лада Н. В., Рудницька Ю. В. Реалізація методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 35–43. DOI: https://doi.org/10.30837/ITSSI.2022.20.035

Lada, N., Rudnytska, Y. (2022), "Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 35–43. DOI: https://doi.org/10.30837/ITSSI.2022.20.035