ISSN 2664-9969

UDC 004.312.2
DOI: 10.15587/2706-5448.2024.306980

Volodymyr Rudnytskyi,
Nataliia Lada,
Maksym Herashchenko,
Tymofii Korotkyi,
Tetiana Stabetska

MODELING RELATIONSHIPS IN NON-COMMUTATIVE TWO-OPERAND TWO-BIT CET-OPERATIONS OF A DOUBLE CYCLE WHEN PERMUTING THE OPERANDS

The object of the research is relationships in non-commutative two-operand two-bit CET-operations of a double cycle when operands are permuted. The article is devoted to studying the results of the computational experiment, which is in building a model of relationships in non-commutative two-operand two-bit CET-operations of a double cycle with the operands permutation in order to ensure the possibility of building cryptographic systems with XOR sequence encryption. The theoretical and practical results of the work are obtained on the basis of the computational experiment data. The results of researching the CET-operations data make it possible to build cryptographic systems with XOR sequence ciphering and to improve the quality of low-resource stream encryption systems. The mathematical description of the computational experiment results made it possible to establish relationships between pairs of non-commutative two-operand two-bit CET-operations of a double cycle when operands are permuted. The possibility of constructing a group of commutative two-operand two-bit CET-operations of a double cycle based on the modification of a known two-operand operation by one-operand operations to within the permutation of the crypto-transformation results has been studied. The correctness of constructing a group of CET-operations, both without operand permutation and such that allow operand permutation, has been verified. The model for building a group of asymmetric two-operand two-bit CET-operations of a double cycle, which allow the operands permutation is proposed. Applying the substitution model made it possible to obtain pairs of interrelated operations in this group. The obtained pairs of interconnected operations provide a description of modification for direct and inverse non-commutative CET operations when permuting the operands. The obtained results provide the possibility of building cryptographic systems that encrypt both the input open information under the control of the XOR sequence and the XOR sequence under the control of the input open information. Further research will be aimed at establishing relationships in non-commutative two-operand two-bit CET operations of the triple cycle when operands are permuted.

Keywords: *cryptographic coding, low-resource cryptography, CET-operations, asymmetric operations, operands permutation, stream ciphering.*

Received date: 29.04.2024
Accepted date: 25.06.2024
Published date: 29.06.2024

How to cite
Rudnytskyi, V., Lada, N., Herashchenko, M., Korotkyi, T., Stabetska, T. (2024). Modeling relationships in non-commutative two-operand two-bit CET-operations of a double cycle when permuting the operands. Technology Audit and Production Reserves, 3 (2 (77)), 30–35. doi: https://doi.org/10.15587/2706-5448.2024.306980

1. Introduction

Modern trends in the field of information technologies are aimed at minimizing devices and simultaneously increasing their functional capabilities [1]. In addition, there is a rapid increase in the amount of information that needs to be transmitted, processed and stored on these devices, especially in real time. It is worth noting that the hardware and software resources involved in the transmission, processing and storage of information may be reduced due to a reduction in size or energy consumption. Also, the issue of protecting information on these low-resource devices is becoming increasingly important [2, 3]. The consumer prefers gadgets, the risk of leaking its personal information from which will be minimal. Thus, due to the reliable protection of information, confidentiality and privacy become one of the leading competitive advantages of modern information technology, starting from the consumer household level, the level of the Internet of Things, smart home systems, SMART technologies, etc. to the protection of confidential information in electronic banking or state systems administration [4–7]. For example, the idea of the «State in a smartphone» is very popular, but in terms of information protection, it should be ensured primarily at the level of low-resource gadgets. And this is not to mention the protection of information and data transmission on unmanned aerial vehicles or robotic land-use complexes.

Currently, cryptographic protection of information remains one of the most effective protections of information [8, 9]. However, the above-mentioned requirements for software and hardware resource limitations make the use of a large number of crypto-algorithms impossible or ineffective. That is why so-called «low resource» [10] or «lightweight» cryptography [11–13] is gaining rapid development today. A large number of studies in this area are devoted to the effectiveness of solutions for physical and cryptographic security of quantum-immune IoT [14], analysis of light cryptography for embedded systems [15], modification of light cryptography schemes [16], comparison of light cryptographic algorithms [17, 18], etc. However, insufficient attention has been paid to improving the quality of low-resource stream encryption systems.

To improve the quality of low-resource stream encryption systems, it is advisable to use CET-operations. The effectiveness of using CET-operations in cryptographic systems, built on the basis of addition modulo two, has been proven in a number of works [19, 20]. Among CET-operations, a special place is occupied by operations that allow the permutation of operands, because they allow both the encryption of input information and the encryption of the blocking sequence to be implemented in stream encryption systems [21].

The purpose of the work is to build a model of relationships in non-commutative two-operand two-bit CET-operations of a double cycle when operands are permuted based on the results of a computational experiment. This will provide the possibility of building cryptographic systems with the encryption of the inhibitory sequence.

2. Materials and Methods

To search for two-bit two-operand CET-operations, a computational experiment was conducted to find tuples of two-bit two-operand CET-operations that allow operands to be permuted [22]. To conduct the experiment, a group of two-bit single-operand CET-operations was numbered, shown in Table 1 [23].

According to the simulation results, 576 operations were constructed, of which 96 were symmetric operations and 480 were non-symmetric operations [24]. Symmetric operations that allow the permutation of operands are commutative, because $C(x,y)=C(y,x)$. Let's consider asymmetric operations, which allow the permutation of operands, as non-commutative, because $C(x,y)=C(y,x)$.

Table 1

Discrete models of two-bit one-operand CET operations

$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$C_7(x)=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	$C_{13}(x)=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	$C_{19}(x)=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$C_8(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	$C_{14}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	$C_{20}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
$C_3(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$C_9(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$C_{15}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$C_{21}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
$C_4\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$C_{10}(x)=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	$C_{16}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	$C_{22}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$C_{11}(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$C_{17}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$C_{23}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$C_{12}(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	$C_{18}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	$C_{24}(x_1)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

The synthesized CET-operations obtained by the results of the experiment were divided into 24 groups of operations with accuracy up to the permutation of the result [25]. Among the constructed groups of CET-operations, 4 groups of symmetric operations and 20 groups of asymmetric operations were singled out [25]. The results of the study of groups of symmetric two-bit, two-operand CET-operations, which allow the permutation of operands, are given in [26]. Among the asymmetric groups of CET-operations, 6 groups of double-cycle operations and 14 groups of triple-cycle operations were singled out [21]. However, non-symmetric (non-commutative) two-bit two-operand CET-operations, which allow the permutation of operands, were practically not studied. However, it is these operations that make it possible to build stream ciphers that provide cryptographic transformation of both the input information under the control of the inhibiting sequence and the inhibiting sequence under the control of the input information [21].

3. Results and Discussions

To establish relationships between two-bit, two-operand CET-operations of a double cycle, obtained by permuting the operands, let's examine the group of operations with precision up to the permutation of the result, selected on the basis of the CET-operation $C_{1,7,19,13}(x,y)$. This two-operand CET-operation is a tuple of one-operand CET-operations of operand transformation x ($C_1(x)$; $C_7(x)$; $C_{19}(x)$; $C_{13}(x)$), united by the second operand y. According to the results of the CET-operation experiment $C_{1,7,19,13}(x,y)$, the CET-operation corresponds to $C_{3,9,15,21}(x,y)$, since $C_{3,9,15,21}(x,y)=C_{1,7,19,13}(y,x)$. The relationship between the CET-operations of the transformation of input information x, when permuting the operands, is denoted as $C_{1,7,19,13}(x,y)\leftrightarrow C_{3,9,15,21}(x,y)$. The group of CET-operations is a group of double-loop operations. The peculiarity of groups of operations of a double cycle is the presence of interconnected transformations, which is as follows: if $C_{1,7,19,13}(x,y)\leftrightarrow C_{3,9,15,21}(x,y)$, then $C_{3,9,15,21}(x,y)\leftrightarrow C_{1,7,19,13}(x,y)$. In CET-operations of a double cycle, repeated permutations of operands will lead to the return of the initial operation: $C_{1,7,19,13}(x,y)\leftrightarrow C_{3,9,15,21}(x,y)\leftrightarrow C_{1,7,19,13}(x,y)$.

The group of asymmetric two-bit two-operand double-cycle CET-operations is given in Table 2.

Table 2

A group of asymmetric two-bit two-operand double-cycle CET-operations

CET-operation		CET-operation	
$C(x,y)$	$C(y,x)$	$C(x,y)$	$C(y,x)$
$C_{1,7,19,13}(x,y)$	$C_{3,9,15,21}(x,y)$	$C_{3,9,15,21}(x,y)$	$C_{1,7,19,13}(x,y)$
$C_{7,1,13,19}(x,y)$	$C_{9,3,21,15}(x,y)$	$C_{9,3,21,15}(x,y)$	$C_{7,1,13,19}(x,y)$
$C_{13,19,7,1}(x,y)$	$C_{15,21,3,9}(y,x)$	$C_{15,21,3,9}(x,y)$	$C_{13,19,7,1}(x,y)$
$C_{19,13,1,7}(x,y)$	$C_{21,15,9,3}(x,y)$	$C_{21,15,9,3}(x,y)$	$C_{19,13,1,7}(x,y)$
$C_{6,18,12,24}(x,y)$	$C_{4,16,22,10}(y,x)$	$C_{4,16,22,10}(x,y)$	$C_{6,18,12,24}(x,y)$
$C_{12,24,6,18}(x,y)$	$C_{10,22,16,4}(x,y)$	$C_{10,22,16,4}(x,y)$	$C_{12,24,6,18}(x,y)$
$C_{18,6,24,12}(x,y)$	$C_{16,4,10,22}(x,y)$	$C_{16,4,10,22}(x,y)$	$C_{18,6,24,12}(x,y)$
$C_{24,12,18,6}(x,y)$	$C_{22,10,4,16}(x,y)$	$C_{22,10,4,16}(x,y)$	$C_{24,12,18,6}(x,y)$
$C_{5,23,17,11}(x,y)$	$C_{2,20,8,14}(x,y)$	$C_{2,20,8,14}(x,y)$	$C_{5,23,17,11}(x,y)$
$C_{11,17,23,5}(x,y)$	$C_{8,14,2,20}(x,y)$	$C_{8,14,2,20}(x,y)$	$C_{11,17,23,5}(x,y)$
$C_{17,11,5,23}(x,y)$	$C_{14,8,20,2}(x,y)$	$C_{14,8,20,2}(x,y)$	$C_{17,11,5,23}(x,y)$
$C_{23,5,11,17}(x,y)$	$C_{20,2,14,8}(x,y)$	$C_{20,2,14,8}(x,y)$	$C_{23,5,11,17}(x,y)$

ISSN 2664-9969

Applying the technology of synthesis and research of two-operand operations on the basis of one-operand [27], let's investigate a pair of interconnected operations $C_{7,1,13,19}(x,y)\leftrightarrow$ $\leftrightarrow C_{9,3,21,15}(x,y)=C_{7,1,13,19}(y,x)$ represented by the second row of the Table 2.

Let's build a model of the operation $C_{7,1,13,19}(x,y)$:

$$C_{7,1,13,19}(x,y)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=0,\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=1,\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=0,\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=1,\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=0;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus k_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=1.\end{cases}\quad(1)$$

Based on expression (1), let's get an improved operation model:

$$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}.\quad(2)$$

Let's build an improved operation model $C_{9,3,21,15}(x,y)$:

$$C_{9,3,21,15}(x,y)=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=0,\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=1,\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=0,\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=1,\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=0;\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=1.\end{cases}\quad(3)$$

The improved operation model obtained on the basis of expression (3) will be presented as:

$$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}.\quad(4)$$

Based on expressions (2) and (4), it can be stated that the permutation of operands will lead to the implementation of the following relationships between CET-operations:

$$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}\Rightarrow$$

$$\Rightarrow C_{7,1,13,19}(y,x)=C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix};\quad(5)$$

$$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}\Rightarrow$$

$$\Rightarrow C_{9,3,21,15}(y,x)=C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}.\quad(6)$$

Let's examine a pair of interconnected operations $C_{13,19,7,1}(x,y)\leftrightarrow C_{15,21,3,9}(x,y)$ represented by the third row of Table 2.

Let's build an improved operation model $C_{13,19,7,1}(x,y)$:

$$C_{13,19,7,1}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=0,\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=1,\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=0,\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=1,\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=1;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=0;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=1.\end{cases}\quad(7)$$

The improved operation model, based on expression (7), will be represented by the expression:

$$C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}.\quad(8)$$

Let's build an improved operation model $C_{15,21,3,9}(x,y)$:

$$C_{15,21,3,9}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=0,\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & \text{if } y_1=0;\ y_2=1,\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=0,\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & \text{if } y_1=1;\ y_2=1,\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}, & \text{if } y_1=0;\ y_2=1;\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=0;\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}, & \text{if } y_1=1;\ y_2=1.\end{cases}\quad(9)$$

Based on expression (9), let's obtain:

$$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}. \quad (10)$$

Based on expressions (8) and (10), the following relationships are obtained:

$$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix} \Rightarrow$$

$$\Rightarrow O^d_{13,19,7,1}=C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}; \quad (11)$$

$$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix} \Rightarrow$$

$$\Rightarrow O^d_{15,21,3,9}=C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}. \quad (12)$$

By analogy, all other pairs of related CET-operations listed in Table 2 were studied. The obtained set of improved models of asymmetric two-operand two-bit CET-operations of the double cycle and the established relationships between the models are shown in Table 3.

Analysis of models of asymmetric two-bit two-operand CET-operations of a double cycle, built on the basis of a combination of one-operand operations (1), (3), (7) and (9), do not allow establishing relationships between non-commutative operations when permuting operands.

However, when analyzing the improved models of CET-operations (Table 3), it was found that when the operands are permuted, the model of the CET-operation will be implemented, which is obtained by substitution:

$$\begin{cases} x \to y; \\ y \to x. \end{cases} \quad (13)$$

The implementation of substitution (13) will provide a change in the model of the non-commutative two-operand CET-operation of information encryption when the operands are permuted.

However, the results of the analysis of Table 3 do not allow establishing relationships between CET-operations, and do not allow synthesizing groups of non-commutative double-cycle operations that allow permutation of operands.

The group of double cycle non-commutative CET-operations was selected from the results of the computational experiment (Table 1). The selection was based on the modification of the model implementation with accuracy up to permutation. Modification of the results of the operation is possible based on the application of one-operand CET-operations on them.

Table 3

Synthesized set of models of asymmetric two-operand two-bit double-cycle CET-operations and relationships between models

$C(x)$	Crypto conversion operations			
$C(x,y)$	$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{3,9,15,21}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{4,16,22,10}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{3,9,15,21}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{4,16,22,10}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{5,23,17,11}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{5,23,17,11}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

ISSN 2664-9969

According to [3], it is possible to build a group of operations with accuracy up to permutation of results based on the model:

$$C^*(x, C) = C_i\left(C(x, C)\right), \quad (14)$$

where $i \in \{1; 2; ...; h\}$; h – the number of single-operand CET-operations for converting the result; $h \in \{1; 2; ...; 2^n!\}$.

Let's check the correctness of this model for building a group of CET-operations without permuting the operands listed in Table 3.

Let

$$C_{1,7,19,13}(x,y) = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}.$$

If

$$C(x) = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix},$$

then

$$C(C(x,y)) = \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix} = C_{2,20,8,14}(x,y).$$

If

$$C(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix},$$

than

$$C(C(x,y)) = \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix} = C_{4,16,22,10}(x,y).$$

If

$$C(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix},$$

then

$$C(C(x,y)) = \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix} = C_{17,11,5,23}(x,y).$$

Using the entire group of one-operand two-bit CET-operations given in Table 1, a group of asymmetric two-operand two-bit CET-operations of the double cycle will be obtained, given in Table 3. These results confirm the correctness of the application of model (14) for constructing a group of asymmetric two-operand two-bit CET-operations of a double cycle, which allow the permutation of operands. Applying the substitution model (13), pairs of interrelated operations in this group will be obtained. These interconnected models provide a description of the modification of the non-commutative CET-operation when permuting the operands.

The construction of a group of non-commutative two-operand two-bit CET-operations of a double cycle will allow to expand the range of crypto-transformation operations suitable for use in both block and stream encryption.

To date, no limitations for the practical use of the results of this study have been identified.

The conditions of martial law in Ukraine led to an increase in interest in low-resource cryptography.

Further research will be aimed at establishing relationships in non-commutative two-operand two-bit CET-operations of the triple cycle when operands are permuted.

4. Conclusions

The mathematical description of the results of the computational experiment made it possible to establish relationships between pairs of non-commutative two-operand two-bit CET-operations of a double cycle when operands are permuted. The possibility of constructing a group of commutative two-operand two-bit CET-operations of a double cycle based on the modification of a known two-operand operation with one-operand operations with precision up to the permutation of the results of the crypto-transformation has been studied. The obtained results provide the possibility of building cryptographic systems that encrypt both the input open information under the control of the suppressing sequence and the suppressing sequence under the control of the input open information. Further research will be aimed at establishing relationships in non-commutative two-operand two-bit CET-operations of the triple cycle when operands are permuted.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this study, including financial, personal, authorship, or any other, that could affect the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

Data will be provided upon reasonable request.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Avoine, G., Hernandez-Castro, J. (Ed.) (2021). *Security of Ubiquitous Computing Systems, Selected Topics*. Springer, 265. doi: https://doi.org/10.1007/978-3-030-10591-4
2. Zheng, Z., Tian, K., Liu, F. (2023). Modern Cryptography. Vol. 2. *A Classical Introduction to Informational and Mathematical* Principle. Springer: Singapore. doi: https://doi.org/10.1007/978-981-19-7644-5
3. Sabani, M. E., Savvas, I. K., Poulakis, D., Garani, G., Makris, G. C. (2023). Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era. *Electronics, 12 (12)*, 2643. doi: https://doi.org/10.3390/electronics12122643
4. Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A., Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, Challenges and Solutions. *Blockchain: Research and Applications*, 100178. doi: https://doi.org/10.1016/j.bcra.2023.100178
5. Meng, Y., Zhu, H., Shen, X. (2023). *Security in Smart Home Networks. Wireless Networks*. Cham: Springer, 167. doi: https://doi.org/10.1007/978-3-031-24185-7
6. Amraoui, N., Zouari, B. (2021). Securing the operation of Smart Home Systems: a literature review. *Journal of Reliable Intelligent Environments, 8 (1)*, 67–74. doi: https://doi.org/10.1007/s40860-021-00160-3
7. Alghayadh, F., Debnath, D. (2020). A Hybrid Intrusion Detection System for Smart Home Security. *2020 IEEE International*

Conference on Electro Information Technology (EIT), 319–323. doi: https://doi.org/10.1109/eit48999.2020.9208296
8. Zeadally, S., Das, A. K., Sklavos, N. (2021). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things, 14,* 100075. doi: https://doi.org/10.1016/j.iot.2019.100075
9. Yalamuri, G., Honnavalli, P., Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. *Procedia Computer Science, 215*, 834–845. doi: https://doi.org/10.1016/j.procs.2022.12.086
10. Aboshosha, B. W., Dessouky, M. M., Elsayed, A. (2019). Energy Efficient Encryption Algorithm for Low Resources Devices. *The Academic Research Community Publication, 3 (3),* 26–37. doi: https://doi.org/10.21625/archive.v3i3.520
11. Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., Daud, M. (2023). Systematic literature review: Trend analysis on the design of lightweight block cipher. *Journal of King Saud University – Computer and Information Sciences, 35 (5),* 101550. doi: https://doi.org/10.1016/j.jksuci.2023.04.003
12. Thakor, V. A., Razzaque, M. A., Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access, 9,* 28177–28193. doi: https://doi.org/10.1109/access.2021.3052867
13. Kumar, C., Prajapati, S. S., Verma, R. K. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices. *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*. doi: https://doi.org/10.1109/ccet56606.2022.10080556
14. Suomalainen, J., Kotelba, A., Kreku, J., Lehtonen, S. (2018). Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT. *Cryptography, 2 (1),* 5. doi: https://doi.org/10.3390/cryptography2010005
15. Manifavas, C., Hatzivasilis, G., Fysarakis, K., Rantos, K. (2014). Lightweight Cryptography for Embedded Systems – A Comparative Analysis. *Lecture Notes in Computer Science*. Springer, 333–349. doi: https://doi.org/10.1007/978-3-642-54568-9_21
16. Yasmin, N., Gupta, R. (2023). Modified lightweight cryptography scheme and its applications in IoT environment. *International Journal of Information Technology, 15 (8),* 4403–4414. doi: https://doi.org/10.1007/s41870-023-01486-2
17. Khudoykulov, Z. (2024). A Comparison of Lightweight Cryptographic Algorithms. *Lecture Notes in Networks and Systems*. Cham: Springer, 295–304. doi: https://doi.org/10.1007/978-3-031-53488-1_36
18. Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., Alkhzaimi, H. A. (2023). Cryptography Algorithms for Enhancing IoT Security. *Internet of Things, 22,* 100759. doi: https://doi.org/10.1016/j.iot.2023.100759
19. Holub, S., Babenko, V., Rudnytskyi, S. (2012). The method of synthesis of the operations of cryptographic transformations on the basis of addition modulo two. *Systemy obrobky informatsii, 3 (1),* 119–122.
20. Babenko, V., Lada, N. (2016). Analiz rezultativ vykonannia modyfikovanykh operatsii dodavannia za modulem dva z tochnistiu do perestanovky. *The scientific potential of the present*. Vinnytsia: PE Rogalska I.O., 108–111.
21. Rudnytskyi, V., Lada, N., Kuchuk, H., Pidlasyi, D. (2024). *Architecture of CET-operations and stream encryption technologies*. Cherkasy: vydavets Ponomarenko R. V., 374. Available at: https://dndivsovt.com/index.php/monograph/issue/view/22/22
22. Rudnytskyi, V., Lada, N., Kozlovska, S. (2018). Technology of two operand operations construction of information cryptographic transformation by modeling results. *Advanced Information Systems, 2 (4),* 26–30. doi: https://doi.org/10.20998/2522-9052.2018.4.04
23. Rudnytskyi, V., Babenko, V., Zhyliaiev, D. (2011). Alhebraichna struktura mnozhyny lohichnykh operatsii koduvannia. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy, 2 (6),* 112–114.
24. Babenko, V., Lada, N., Lada, S. (2016). Analiz mnozhyny operatsii syntezovanykh na osnovi dodavannia za modulem dva. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky*, 1, 5–11.
25. Lada, N., Dzyuba, V., Breus, R., Lada, S. (2020). Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. *Technology Audit and Production Reserves, 2 (2 (52)),* 28–31. doi: https://doi.org/10.15587/2706-5448.2020.202099
26. Rudnytskyi, V., Babenko, V., Lada, N., Tarasenko, Ya., Rudnytska, Yu. (2022). Constructing symmetric operations of cryptographic information encoding. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021)*. Kyiv: CEUR Workshop Proceedings, 182–194.
27. Rudnytskyi, V. M., Opirskyi, I. R., Melnyk, O. H., Pustovit, M. O. (2018). Synthesis of group operations strong stable cryptographic encode for construction stream cipher. *Ukrainian Scientific Journal of Information Security, 24 (3),* 195–200. doi: https://doi.org/10.18372/2225-5036.24.13430

✉ ***Volodymyr Rudnytskyi,*** *Doctor of Technical Sciences, Professor, Chief Researcher, State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine, e-mail: rvn_2008@ukr.net, ORCID: https://orcid.org/0000-0003-3473-7433*

Nataliia Lada, *PhD, Leading Researcher, State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0002-7682-2970*

Maksym Herashchenko, *Head of Research and Development Department, State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0001-6587-0355*

Tymofii Korotkyi, *Postgraduate Student, Department of Design Information Technologies, Cherkasy State Technological University, Cherkasy, Ukraine, ORCID: https://orcid.org/0009-0003-5159-5892*

Tetiana Stabetska, *PhD, Senior Lecturer, Department of Information Technologies, The Bohdan Khmelnytsky National University of Cherkasy, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0001-9192-5313*

✉ *Corresponding author*