ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

UDC 004.056.55:004.312.2 DOI: https://doi.org/10.30837/2522-9818.2025.3.126

V. RUDNYTSKYI, S. SEMENOV, N. LADA, V. BABENKO, V. LARIN, T. KOROTKYI

THE MODEL FOR CONSTRUCTING A SET OF SYMMETRIC TWO-OPERAND SET OPERATIONS THAT ALLOW PERVERSION OF OPERANDS BY COMBINING ONE-OPERAND OPERATIONS

The **subject matter** of the article is the scientific and methodological apparatus for constructing and implementing information-driven SET-operations. The **goal** of the work is to construct a model for the synthesis of symmetric two-operand SET-operations that allow permutation of operands and to determine the restrictions on their use in the development of low-resource stream ciphers. The following **tasks** are solved in the article: a model for the synthesis of symmetric two-operand SET-operations that allow permutation of operands is developed; restrictions on the use of this model are determined, which guarantee the construction of symmetric two-operand SET-operations that allow permutation of operands; it is shown that a pseudo-random change in the operating modes of the cryptographic system significantly complicates the processes of cryptanalysis of ciphergrams; modeling of SET-operations based on duplication of single-operand two-bit SET operations is carried out; the technology for constructing two-operand SET-operations based on duplication is applied to obtain a set of two-operand SET-operations. **Methods** of discrete mathematics, Set-theory and situational management have been introduced. Achieved **results**. Synthesized on the basis of this model of SET-operations allow changing the operating mode of stream cryptographic systems from symmetric to asymmetric when permuting operands in the operation. At present, the forefront of modern world experience in cryptographic science is a low-resource cryptographic system. Low-resource cryptography allows ensuring sufficiently stable cryptosystem performance with significant limitations on computational, mass-dimensional, cost and energy resources of the object of interest. One of the most relevant areas of further development of low-resource cryptography is considered to be cryptographic coding. In the process of cryptographic coding, cryptographic coding operations are implemented. The selection of operations is carried out under the control of a pseudo-random sequence, which is implemented by a cryptographic algorithm. **Conclusions**. A model for the synthesis of symmetric two-operand SET-operations that allow permutation of operands has been developed. Restrictions on the use of this model have been determined, which guarantee the construction of symmetric two-operand SET-operations that allow permutation of operands. The achieved results can be useful for the construction of low-resource stream encryption systems. Pseudo-random change of the operating modes of the cryptographic system significantly complicates the processes of cryptanalysis of ciphertexts.

Keywords: two-operand operations; cryptographic protection; low-resource cryptography; SET-encryption; SET-operations; one-operand operations.

Introduction

In the course of researching SET operation architectures, it was found that the results of their implementation depend on the results of the implementation of single-operand SET operations on which they are based [1, 2–5]. Therefore, a detailed analysis of the features of using these operations in the implementation of the simplest stream cipher algorithms, even if they are easily disclosed, is of great importance. This will significantly improve the efficiency of constructing ciphers based on multi-operand SET operations that will implement sets of various single-operand operations and their groups.

A CET operation is an operation in cryptographic encoding theory (CET). A CET operation is a numbered set of elementary functions, each of which forms a corresponding output Ci-quantum (ci-quantum from cryptographic information quantum) of information based on the processing of input Ci-quanta of information. A Ci-quantum is the minimum amount of information that a CET operation operates on [1, 2, 6]. Depending on the application of the CET operation, a ci-quantum can be a bit, byte, word, or double word.

A single-operand CET operation is a substitution table, and its use leads to the implementation of substitutions in the encryption process. In classical cryptography, there are four types of substitution ciphers [1, 4]:

– a simple substitution cipher, in which each character of the plaintext is replaced by another character from the substitution table during encryption;

– a homophonic substitution cipher, which differs from a simple transposition cipher in that each character of the plaintext can be replaced by one of several characters during encryption [5]. Its implementation is

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

associated with an increase in the number of characters used in the ciphertext compared to the plaintext;

– a polygram substitution cipher, in which groups of plaintext characters are replaced by groups of other characters from the substitution table;

– a polyalphabetic substitution cipher, in which several simple substitution ciphers are performed sequentially, the sequence of which is determined by the key [1].

Thus, the construction of a low-resource post-quantum control system in swarms of unmanned complexes and taking into account such features as: limited operating memory, reduced computing power, small physical area for implementation of the assembly, low energy capabilities, real-time response with resistance to external interference when creating a mathematical apparatus for describing linear and nonlinear transformations in permutation fields is a relevant scientific and applied problem.

Therefore, the creation of modern technology for building cryptographic systems involves the development of a theory of cryptographic encoding of information resources circulating in the network in near real time. In the course of our dissertation research, we will refer to this as CET encryption.

Analysis of the problem and existing methods

In [1], it is shown that highly efficient stream cipher systems can be built based on the use of SET operations (cryptographic encoding operations). In terms of their architecture, SET operations can be single-operand, two-operand, and multi-operand. Several approaches have been developed for constructing groups of symmetric two-operand SET operations: synthesis of groups of two-operand operations based on simulation results [3]; synthesis of groups of symmetric two-operand operations based on permutable circuits [4]; synthesis of groups of symmetric two-operand operations based on duplication of single-operand two-bit operations of the base group [5]. However, the practical implementation of these approaches to the synthesis of symmetric two-operand SET operations is associated with a number of difficulties. To synthesize groups of symmetric two-operand operations based on simulation results, it is necessary to have simulation results, but as the bit width of SET operations increases, the simulation time (required computing power) increases exponentially. The implementation of other approaches requires the availability of predefined symmetric two-operand SET operations.

Identification of previously unsolved parts of the general problem

Among stream ciphers based on SET operations, symmetric stream ciphers based on symmetric single-operand SET operations [1] are the least complex to implement. However, their disadvantage is the implementation of a single-operand SET operation of only one substitution table. The use of two-operand operations in stream ciphers provides the possibility of pseudo-random use of several substitution tables [2]. It is difficult to find or construct a new unknown symmetric two-operand operation that allows the permutation of operands for the subsequent synthesis of a group of modified SET operations with similar properties. Unfortunately, this problem has not been solved to date.

The purpose of this article is to construct a model for synthesizing symmetric two-operand SET operations that allow operand permutation and to determine the limitations on its use in the development of low-resource stream ciphers.

Main material

Let us consider the implementation of SET operation modeling based on the duplication of single-operand two-bit SET operations [1, 7–9].

When constructing two-operand operations, we will use the group of single-operand SET operations given in Table 1.

To construct a set of two-operand SET operations that allow operand permutation, we will use a two-operand SET operation [1, 9]:

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

Using the technology of constructing two-operand SET operations based on duplication, we obtain a set of two-operand SET operations [5, 10].

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

Table 1. *Discrete models of direct and inverse single-operand SET operations* [1]

$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}=C'_1(x)$	$C_7(x)=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=C'_7(x)$	$C_{13}(x)=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=C'_{13}(x)$	$C_{19}(x)=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=C'_{19}(x)$
$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}=C'_2(x)$	$C_8(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}=C'_{20}(x)$ $C'_8(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}=C_{20}(x)$	$C_{14}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}=C'_{14}(x)$	$C_{20}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}=C'_8(x)$ $C'_{20}(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}=C_8(x)$
$C_3(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=C'_3(x)$	$C_9(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}=C'_9(x)$	$C_{15}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=C'_{21}(x)$ $C'_{15}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=C_{21}(x)$	$C_{21}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=C'_{15}(x)$ $C'_{21}(x)=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}=C_{15}(x)$
$C_4(x)=\begin{bmatrix}x_2\\x_1\end{bmatrix}=C'_4(x)$	$C_{10}(x)=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=C'_{16}(x)$ $C'_{10}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=C_{16}(x)$	$C_{16}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=C'_{10}(x)$ $C'_{16}(x)=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=C_{10}(x)$	$C_{22}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=C'_{22}(x)$
$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}=C'_6(x)$	$C_{11}(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}=C'_{18}(x)$	$C_{17}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}=C'_{24}(x)$	$C_{23}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=C'_{12}(x)$
$C'_5(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}=C_6(x)$	$C'_{11}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}=C_{18}(x)$	$C'_{17}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=C_{24}(x)$	$C'_{23}(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}=C_{12}(x)$
$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}=C'_5(x)$	$C_{12}(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}=C'_{23}(x)$	$C_{18}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}=C'_{11}(x)$	$C_{24}(x)=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=C'_{17}(x)$
$C'_6(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}=C_5(x)$	$C'_{12}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=C_{23}(x)$	$C'_{18}(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}=C_{11}(x)$	$C'_{24}(x)=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}=C_{17}(x)$

To construct inverse SET operations, we use the relationship between operations:

$$C(x,y)=\begin{cases}C_i, \ if \ y_1=0; y_2=0\\ C_j, \ if \ y_1=0; y_2=1\\ C_n, \ if \ y_1=1; y_2=0\\ C_m, \ if \ y_1=1; y_2=1\end{cases}\leftrightarrows\leftrightarrows\leftrightarrows\leftrightarrows\Rightarrow C'(x,y)=\begin{cases}C'_i, \ if \ y_1=0; y_2=0\\ C'_j, \ if \ y_1=0; y_2=1\\ C'_n, \ if \ y_1=1; y_2=0\\ C'_m, \ if \ y_1=1; y_2=1\end{cases} \quad (2)$$

The results of constructing a set of two-operand SET operations based on operation (1) are shown in Table 2.

In the process of analyzing the results of modeling SET operations based on the duplication of single-operand two-bit operations in Table 2, it was assumed that two-operand SET operations can be synthesized by combining single-operand SET operations. This assumption is based on the fact that when using the method of duplicating basic groups based on asymmetric SET operations, the resulting two-operand SET operations of the operand processing model do not coincide. Therefore, it can be argued that two-operand SET operations can be synthesized not only by duplicating basic groups, but also by combining single-operand cryptotransformation operations [1, 11–13].

In the process of creating two-operand operations, it is possible to combine symmetric single-operand operations, symmetric and asymmetric single-operand operations, as well as asymmetric single-operand operations [1].

When forming sets of two-operand operations, the operation of processing the first operand (x) is sequentially combined with the operations of processing the second operand (y). Since all operations for processing the second operand are used in the synthesis of the set, the construction of a set of symmetric and asymmetric two-operand operations will depend on the first operand. Based on this, it can be assumed that when selecting a symmetric single-operand operation for processing the first operand, a set of symmetric two-operand operations can be obtained [1, 14–16].

Let's build two-operand operations by combining single-operand operations. To form a set of two-operand operations, let's select the first single-operand SET operation $C_1(x)$.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Table 2. *A synthesized set of models of asymmetric two-operand two-bit double-cycle operations based on operation duplication for the first encryption scenario* [1]

	Inversion operations			
	$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$
Basic operations				
$C(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$ $C'_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$ $C'_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$ $C'_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$ $C'_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$
$C(x)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}$	$C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1\oplus y_2 \end{bmatrix}$ $C'_{2,8,20,14}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$ $C'_{20,14,2,8}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$ $C'_{14,20,8,2}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$ $C'_{8,2,14,20}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$
$C(x)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}$	$C^k_6=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}$ $C'_{3,9,21,15}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2\oplus 1 \end{bmatrix}$ $C'_{9,3,15,21}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_2 \end{bmatrix}$ $C'_{21,15,3,9}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_2\oplus 1 \end{bmatrix}$ $C'_{15,21,9,3}(x,y)=\begin{bmatrix} x_1 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$
Inversion operations				
$C(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$C_{4,16,22,10}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2 \\ y_1 \end{bmatrix}$ $C'_{4,10,22,16}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2 \\ y_1\oplus 1 \end{bmatrix}$ $C'_{16,22,10,4}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$ $C'_{10,4,16,22}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_1\oplus 1 \end{bmatrix}$ $C'_{22,16,4,10}(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$
$C(x)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}$	$C_{5,23,17,11}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2 \\ y_2 \end{bmatrix}$ $C'_{6,12,24,18}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2 \\ y_2\oplus 1 \end{bmatrix}$ $C'_{18,24,12,6}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_2 \end{bmatrix}$ $C'_{24,18,6,12}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_2\oplus 1 \end{bmatrix}$ $C'_{12,6,18,24}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$
$C(x)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}$	$C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$ $C'_{5,11,23,17}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1\oplus 1 \end{bmatrix}$ $C'_{23,17,5,11}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_2\oplus 1 \\ y_1 \end{bmatrix}$ $C'_{11,5,17,23}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1\oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus 1 \end{bmatrix}$ $C'_{17,23,11,5}(x,y)=\begin{bmatrix} x_2 \\ x_1\oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

Let's place the first 4 two-operand SET operations based on the 4 single-operand SET operations given in the first row of Table 1.

$$C_{1,1}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix} \qquad (3)$$

Substituting the value of the second operand into the model of operation (3), we obtain a tuple model of a two-operand SET operation [1].

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

the tuple model, the numbering of tuple elements coincides with the numbering of SET operations given in Table 1.

By analogy, we obtain the other three tuple models of SET operations [1].

$$C_{1,7}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_7\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\oplus 1\end{bmatrix}=C_{7,1,19,13}(x,y)$$

$$C_{1,13}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{13}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\end{bmatrix}=C_{13,19,1,7}(x,y)$$

$$C_{1,19}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{19}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix}=C_{19,13,7,1}(x,y)$$

Let us form models of inverse SET operations based on relation (2) and find the relationship between the obtained pairs of operations. [1, 17].

As $C_1(x)\Rightarrow C_1'(x)$, $C_7(x)\Rightarrow C_7'(x)$; $C_{13}(x,y)\Rightarrow C_{13}(y,x)=C_{13}'(x,y)$, $C_{19}(x)\Rightarrow C_{19}'(x)$, then, according to expression (2), we get:

$C_{1,7,13,19}(x,y)\Rightarrow C'_{1,7,13,19}(x,y)$, that means $C_{1,1}(x,y)\Rightarrow C'_{1,1}(x,y)$.

$C_{7,1,19,13}(x,y)\Rightarrow C'_{7,1,19,13}(x,y)$, that means $C_{1,7}(x,y)\Rightarrow C'_{1,7}(x,y)$.

$C_{13,19,1,7}(x,y)\Rightarrow C'_{13,19,1,7}(x,y)$, that means $C_{1,13}(x,y)\Rightarrow C'_{1,13}(x,y)$.

$C_{19,13,7,1}(x,y)\Rightarrow C'_{19,13,7,1}(x,y)$, that means $C_{1,19}(x,y)\Rightarrow C'_{1,19}(x,y)$.

We synthesize the following four operations based on the second row of Table 1.

Let's create a SET operation $C_{1,2}(x,y)$ analogous to the operation $C_{1,1}(x,y)$.

$$C_{1,2}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix}=C_{1,19,13,7}(x,y)$$

Then: $\left(C_{1,19,13,7}(x,y)\Rightarrow C'_{1,19,13,7}(x,y)\right)\Rightarrow\left(C_{1,2}(x,y)\Rightarrow C'_{1,2}(x,y)\right)$.

By analogy, we will construct operations

$$C_{1,8}(x,y),\ C_{1,14}(x,y),\ C_{1,17}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\end{bmatrix}$$

$$C_{1,8}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_8\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\oplus 1\end{bmatrix}=C_{7,13,19,1}(x,y);$$

$$\left(C_{7,13,19,1}(x,y)\Rightarrow C'_{7,13,19,1}(x,y)\right)\Rightarrow\left(C_{1,8}(x,y)\Rightarrow C'_{1,8}(x,y)\right).$$

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

$$C_{1,14}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{14}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_2\end{bmatrix}=C_{13,7,1,19}(x,y);$$

$$\left(C_{13,7,1,19}(x,y)\Rightarrow C'_{13,7,1,19}(x,y)\right)\Rightarrow\left(C_{1,14}(x,y)\Rightarrow C'_{1,14}(x,y)\right).$$

$$C_{1,20}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{20}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_2\oplus 1\end{bmatrix}=C_{20,1,7,13}(x,y);$$

$$\left(C_{20,1,7,13}(x,y)\Rightarrow C'_{20,1,7,13}(x,y)\right)\Rightarrow\left(C_{1,20}(x,y)\Rightarrow C'_{1,20}(x,y)\right).$$

Let's find patterns between operations
based on the fourth row of Table 1:

$$C_{1,4}(x,y),\ C_{1,10}(x,y),\ C_{1,16}(x,y),\ C_{1,22}(x,y)$$

$$C_{1,4}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_4\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\end{bmatrix}=C_{1,13,7,19}(x,y);$$

$$\left(C_{1,13,7,19}(x,y)\Rightarrow C'_{1,13,7,19}(x,y)\right)\Rightarrow\left(C_{1,4}(x,y)\Rightarrow C'_{1,4}(x,y)\right).$$

$$\left(C_{20,14,8,2}(x,y)\Rightarrow C_{20,14,8,2}(y,x)=C'_{8,14,20,2}(x,y)\right)\Rightarrow\left(C_{2,19}(x,y)\ \Rightarrow C_{2,19}(y,x)=C'_{2,8}(x,y)\right);$$

$$\left(C_{7,19,1,13}(x,y)\Rightarrow C'_{7,19,1,13}(x,y)\right)\Rightarrow\left(C_{1,10}(x,y)\Rightarrow C'_{1,10}(x,y)\right).$$

$$C_{1,16}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{16}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\end{bmatrix}=C_{13,1,19,7}(x,y);$$

$$\left(C_{13,1,19,7}(x,y)\Rightarrow C'_{13,1,19,7}(x,y)\right)\Rightarrow\left(C_{1,16}(x,y)\Rightarrow C'_{1,16}(x,y)\right).$$

$$C_{1,22}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{22}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus 1\end{bmatrix}=C_{19,7,13,1}(x,y);$$

$$\left(C_{19,7,13,1}(x,y)\Rightarrow C'_{19,7,13,1}(x,y)\right)\Rightarrow\left(C_{1,22}(x,y)\Rightarrow C'_{1,22}(x,y)\right).$$

Let's form inverse operations $C'_{1,5}(x,y)\ \ C'_{1,11}(x,y),\ C'_{1,17}(x,y),\ C'_{1,23}(x,y).$

$$C_{1,5}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_5\begin{pmatrix}k_1\\k_2\end{pmatrix}=\begin{bmatrix}y_1\\y_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\end{bmatrix}=C_{1,19,7,13}(x,y);$$

$$\left(C_{1,19,7,13}(x,y)\Rightarrow C'_{1,19,7,13}(x,y)\right)\Rightarrow\left(C_{1,5}(x,y)\Rightarrow C'_{1,5}(x,y)\right).$$

$$C_{1,11}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{11}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\oplus 1\end{bmatrix}=C_{7,13,1,19}(x,y);$$

$$\left(C_{7,13,1,19}(x,y)\Rightarrow C'_{7,13,1,19}(x,y)\right)\Rightarrow\left(C_{1,11}(x,y)\Rightarrow C'_{1,11}(x,y)\right).$$

$$C_{1,17}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{17}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\end{bmatrix}=C_{13,7,19,1}(x,y);$$

$$\left(C_{13,7,19,1}(x,y)\Rightarrow C'_{13,7,19,1}(x,y)\right)\Rightarrow\left(C_{1,17}(x,y)\Rightarrow C'_{1,17}(x,y)\right).$$

$$C_{1,23}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{23}\begin{pmatrix}k_1\\k_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}=C_{19,1,13,7}(x,y);$$

$$\left(C_{19,1,13,7}(x,y)\Rightarrow C'_{19,1,13,7}(x,y)\right)\Rightarrow\left(C_{1,23}(x,y)\Rightarrow C'_{1,23}(x,y)\right)$$

By analogy, we will create all other pairs of two-operand SET operations based on the operation $C_1(x)$. The simulation results are shown in Table 3.

The summary results of modeling operations based on the first operation of processing the first operand $C_1(x)$ (Table 3) showed that regardless of the operation of processing the second operand, if the single-operand operation of processing the first operand is symmetric, then all two-operand operations built on its basis will be symmetric [1, 18].

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Table 3. *A synthesized set of models of two-operand two-bit operations obtained by combining single-operand two-bit cryptographic transformation operations with the operation* $C_1(x)$ [1]

$C_1(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$					**Basic operations**		**Inversion operations**		
	$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$C_1(y)=\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$	$C_2(y)=\begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$	$C_3(y)=\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_4(y)=\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$	$C_5(y)=\begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_6(y)=\begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}$
$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$C_{1,1}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$	$C_{1,7}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,13}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}$	$C_{1,19}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,2}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$	$C_{1,3}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,4}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$	$C_{1,5}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,6}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}$
$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$C_{1,2}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$	$C_{1,8}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,14}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}$	$C_{1,20}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,3}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,9}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{1,10}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}$	$C_{1,11}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{1,12}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix}$
$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$C_{1,13}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}$	$C_{1,14}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}$	$C_{1,15}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,16}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \end{bmatrix}$	$C_{1,4}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$	$C_{1,10}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}$	$C_{1,17}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,18}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \end{bmatrix}$	
$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$C_{1,19}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,20}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$	$C_{1,21}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{1,22}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$	$C_{1,5}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,11}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{1,17}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$	$C_{1,23}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	
				$C_{1,24}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$	$C_{1,6}(x,y)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}$				

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

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Let us formalize this conclusion:

$$C(x,y) = C_i(x) \oplus C_j(y) = C'(x,y) \qquad (4)$$

where $C_i(x) = C_i'(x)$.

Condition (4) will be satisfied if, for a symmetric unary operation on which a set of symmetric binary operations is based, there exists a group of symmetric inversion operations [1]. Based on this restriction, the correct implementation of the synthesis model (4) can be represented as follows:

$$C_i(x,y) = C_j\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus C_1\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = C_i'(x,y) \qquad (5)$$

where $C_1\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix}$ operation of halting the results of the operation $C_j\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ performance.

Since modifications of single-operand SET operations by gammification are placed in the rows of Table 1, only SET operations placed in rows where direct and inverse transformations coincide correspond to condition 5 [1].

For two-bit two-operand operations, only 4 sets of symmetric operations can be constructed based on single-operand operations $C_1(x)$, $C_7(x)$, $C_{13}(x)$ and $C_{19}(x)$. These operations are symmetric and represent a group of inversion operations [1]. The number of sets coincided with the results of the computational experiment.

For three-bit two-operand SET operations, 8 sets of symmetric operations can be constructed based on single-operand SET operations, and for four-bit two-operand SET operations, 16 sets of symmetric operations can be constructed.

Research results and discussion

However, it should be noted that rearranging operands in synthesized operations will result in the implementation of another SET operation, which will be asymmetric.

The research revealed that for encoding and decoding operations, the first operand will be information, and the second operand will be a fading sequence. Any two-bit two-operand cryptographic transformation operation can be represented as the execution of one of four single-operand two-bit operations on the first operand, depending on the value of the two bits of the second operand.

The use of these operations in the creation of cryptographic systems will ensure the formation of low-resource stream cipher systems. The permutation of operands in SET operations will allow changing the operating mode of the cryptographic system from symmetric to asymmetric and vice versa.

Conclusions and prospects for further development

A model for synthesizing symmetric two-operand SET operations that allow operand permutation has been developed. The restrictions on the use of this model guarantee the construction of symmetric two-operand SET operations that allow operand permutation. The use of this model provides the possibility of synthesizing SET operations for building low-resource stream cipher systems. SET operations synthesized on the basis of this model allow changing the operating mode of stream cryptographic systems from symmetric to asymmetric when swapping operands in the operation. Pseudorandom changes in the operating modes of a cryptographic system significantly complicate the processes of cryptanalysis of ciphertexts.

A promising direction for further research is the development of a method for constructing discrete-casual models of three-bit SET operations of information-controlled permutations by combining single-operand operations of two-bit SET operations.

References

1. Rudnytskyi, V. M. (2024), "Architecture of CET-operations and stream encryption technologies: monograph" / V. M. Rudnytskyi, N. V. Lada, G. A. Kuchuk, D. A. Pidlasy. Cherkasy: publisher Ponomarenko R.V., 374 p. ISBN 978-966-2554-81-6 URL: https://dndivsovt.com/index.php/monograph/issue/ view/22/22
2. Kosenko, V., Persiyanova, E., Malyeyeva, O. (2017), "Methods of managing traffic distribution in information and communication networks of critical infrastructure systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (2), P. 48–55. DOI: https://doi.org/10.30837/2522-9818.2017.2.048

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

3. Zheng, Z.,Tian, K. & Liu, F. (2023), "Modern Cryptography Volume 2. A Classical Introduction to Informational and Mathematical Principle". *Springer: Singapore.* DOI: https://doi.org/10.1007/978-981-19-7644-5
4. Kumar, C., Prajapati, S. & Verma, R. (2022), "A Survey of Various Lightweight Cryptography Block ciphers for IoT devices". *IEEE International Conference on Current Development in Engineering and Technology (CCET)*, Bhopal, India, 2022, P. 1–6. DOI: https://doi.org/10.1109/CCET56606.2022.10080556
5. 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)*, Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022, P. 182–194. ISSN 1613-0073.
6. Thomas, Xuan Meng, W. (2020), "Buchanan. Lightweight Cryptographic Algorithms on Resource-Constrained Devices". Preprints. DOI: https://doi.org/10.20944/PREPRINTS202009.0302.V1
7. Semenov, S., Davydov, V., Kuchuk, N. & Petrovskaya, I. (2021), "Software security threat research", *31st International Scientific Symposium Metrology and Metrology Assurance, MMA 2021*. DOI: https://doi.org/10.1109/MMA52675.2021.9610877
8. Khaled, Salah Mohamed (2020), "New Frontiers in Cryptography. Quantum, Blockchain, Lightweight, Chaotic and DNA". *Springer International Publishing*. Springer, Cham, 104. DOI: https://doi.org/10.1007/978-3-030-58996-7
9. Yalamuri, G., Honnavalli, P. & Eswaran, S. (2022), "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats". *Procedia Comput. Sci*. 215, P. 834–845. DOI: https://doi.org/10.1016/j.procs.2022.12.086
10. Lada, N., Kozlovska, S., Rudnytskyi, S. (2019), "Pobudova matematychnoyi hrupy symetrychnykh operatsiy na osnovi dodavannya za modulem dva". ["The symmetric operations' mathematical group constructing based on modulo-2 addition"]. *Modern special equipment: scientific and practical journal.* Kyiv, 2019. № 4 (59). P. 33–41. DOI: https://elar.naiau.kiev.ua/items/33ebc0b3-4177-4d6f-87a8-95719bb7fabe
11. Rudnytska, Yu., Rudnytsky, S. (2022), "Modelyuvannya symetrychnykh operatsiy kryptohrafichnoho koduvannya". ["Modeling symmetric cryptographic coding operations"]. P*roblems of informatization: Tenth International Scientific and Technical Conference: Abstracts of the Supplementary*. Cherkasy – Baku – Bielsko-Biala – Kharkiv, 24 – 25 November 2022. P. 10. available at: https://nure.ua/wp-content/uploads/2022/tom-1.pdf
12. Larin, V., Trystan, A., Hmyria, V., Strikha, S., Kostashchuk, M., Piontkivskyi, P. (2024), "Forsayt yak innovatsiynyy instrument planuvannya ta realizatsiyi naukovykh tekhnolohiy v oboronno-promyslovomu kompleksi". ["Foresight as an innovative tool for planning and implementing scientific technologies in the defence industry"]. Problems of construction, testing, application and operation of complex information systems, 26 (1), P. 93–106. DOI: https://doi.org/10.46972/2076-1546.2024.26.08
13. Jancarczyk, D., Rudnytskyi, V., Breus, R., Pustovit, M., Veselska, O, & Ziubina, R. (2020), "Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits". (2020) *IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS).* IEEE; 2020 Sep 17; P. 247–254. DOI: https://doi.org/10.1109/IDAACS-SWS50031.2020.9297067.
14. Zakaria, A., Azni, A., Ridzuan, F., Zakaria, N. & Maslina, H. (2023), "Daud Systematic literature review: Trend analysis on the design of lightweight block cipher". *IEEE Journal of King Saud University Computer and Information Sciences*. 35, Issue 5, May, 101550 p. DOI: https://doi.org/10.1016/j.jksuci.2023.04.003
15. Gasser, L. (2023), "Post-quantum Cryptography. In: Mulder", V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) *Trends in Data Protection and Encryption Technologies. Springer*, Cham. DOI: https://doi.org/10.1007/978-3-031-33386-6_10
16. Zakaria, A., et al. (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 p. DOI: https://doi.org/10.1016/j.jksuci.2023.04.003
17. Yasmin, N. & Gupta, R. (2023), "Modified lightweight cryptography scheme and its applications in IoT environment". *Int. j. inf. tecnol*. 15, P. 4403–4414. DOI: https://link.springer.com/article/10.1007/s41870-023-01486-2
18. Sabani, M., et al. (2023), "Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era". *Electronics*, 12(12), 2643 p. DOI: https://doi.org/10.3390/electronics12122643

Надійшла (Received) 25.05.2025

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Відомості про авторів / About the Authors

Rudnytskyi Volodymyr – Doctor of Engineering Science, Professor Principal Researcher of State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine; e-mail: rvn_2008@ukr.net; ORCID ID: https://orcid.org/0000-0003-3473-7433

Semenov Serhii – Doctor of Engineering Science, Professor, Professor at University of the National Education Commission, Krakow, Poland; e-mail: serhii.semenov@uken.krakow.pl; ORCID ID: https://orcid.org/0000-0003-4472-9234

Lada Nataliia – Candidate of Technical Sciences, Leading Researcher State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine; e-mail: Ladanatali256@gmail.com; ORCID ID: https://orcid.org/0000-0002-7682-2970

Babenko Vira – Doctor of Engineering Science, Professor, the chef of the department of Cherkasy State Technological University, Cherkasy, Ukraine; e-mail; verababenko84@gmail.com; ORCID ID: https://orcid.org/0000-0003-2039-2841

Larin Volodymyr – Doctoral Candidate, Candidate of Technical Sciences, Associate Professor, State Scientific Research Institute of Armament and Military Equipment Testing and Certification; e-mail: l_vv83@ukr.net; ORCID ID: https://orcid.org/0000-0003-0771-2660

Korotkyi Tymofii – Post-Graduate of Cherkasy State Technological University, Cherkasy, Ukraine; e-mail: rvn_2008@ukr.net; ORCID ID: https://orcid.org/0009-0003-5159-5892

Рудницький Володимир Миколайович – доктор технічних наук, професор, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, головний науковий співробітник, Черкаси, Україна.

Семенов Сергій Геннадійович – доктор технічних наук, професор, Університету Національної комісії з питань освіти, професор, Краків, Польща.

Лада Наталія Володимирівна – кандидат технічних наук, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, провідний науковий співробітник, Черкаси, Україна.

Бабенко Віра Григорівна – доктор технічних наук, професор, Черкаський державний технологічний університет, завідувач кафедри, Черкаси, Україна.

Ларін Володимир Валерійович – кандидат технічних наук, доцент, докторант штатний, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна.

Короткий Тимофій Костянтинович – аспірант, Черкаський державний технологічний університет, Черкаси, Україна.

МОДЕЛЬ ПОБУДОВИ МНОЖИНИ СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ СЕТ-ОПЕРАЦІЙ, ЯКІ ДОПУСКАЮТЬ ПЕРЕСТАНОВКУ ОПЕРАНДІВ

Предметом дослідження в статті є науково-методологічний апарат побудови та реалізації СЕТ-операцій керованих інформацією. **Мета роботи** – побудова моделі синтезу симетричних двохоперандних СЕТ-операцій, які допускають перестановку операдів і визначення обмежень на їх використання при розробці малоресурсних потокових шифрів. У статті розв'язано такі **завдання**: розроблено модель синтезу симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів; визначено обмеження на використання даної моделі, які гарантують побудову симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів; показано, що псевдовипадкова зміна режимів роботи криптографічної системи суттєво ускладнює процеси криптоаналізу шифрограм; проведено моделювання СЕТ-операцій на снові дублювання одноопераднних двохрозрядних СЕТ-операцій; застосовано технологію побудови двохоперандних СЕТ-операцій на основі дублювання для отримання множини двохоперандних СЕТ-операцій. Упроваджено **методи** дискретної математики, теорії множин і ситуаційного управління. Досягнуті наступні **результати**: синтезовані на основі даної моделі СЕТ-операцій дозволяють змінювати режим роботи потокових криптографічних систем з симетричного на несиметричний при перестановці місцями операндів в операції. На теперешній час в авангарді сучасного світового досвіду криптографічної науки є малоресурсна криптографічна система. Малоресурсна криптографія дозволяє забезпечити достатньо стійкі показникі криптосистеми при значному обмеженні обчислювальних, масогабаритних, вартісних та енергетичних ресурсів об'єкта інтересу. Одним із найбільш

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

атуальним напрямком подальшого розвитку малоресурсної криптографії вважається криптографічне кодування. В процесі криптографічного кодування реалізуються операції криптографічного кодування. Вибір операцій проводиться під управлінням псевдовипадкової послідовності, яка реалізується криптографічним алгоритмом. **Висновки**. Розроблена модель синтезу симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів. Визначені обмеження на використання даної моделі, які гарантують побудову симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів. Досягнуті результати можуть бути корисними для побудови малоресурсних систем потокового шифрування. Псевдовипадкова зміна режимів роботи криптографічної системи суттєво ускладнює процеси криптоаналізу шифрограм.

Ключові слова: двохоперандні операції; криптографічний захист; малоресурсна криптографія; СЕТ-шифрування; СЕТ-операції; одноперандні операції.

Бібліографічні описи / Bibliographic descriptions

Рудницький В.М., Семенов С. Г., Лада Н.В., Бабенко В.Г., Ларін В.В., Короткий Т.К. Модель побудови множини симетричних двохоперандних сет-операцій, які допускають перестановку операндів. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 3 (33). С. 126–136. DOI: https://doi.org/10.30837/2522-9818.2025.3.126

Rudnytskyi, V., Semenov, S., Lada, N., Babenko, V., Larin, V., Korotkyi, T. (2025), "The model for constructing a set of symmetric two-operand set operations that allow perversion of operands by combining one-operand operations", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (33), P. 126–136. DOI: https://doi.org/10.30837/2522-9818.2025.3.126