UDC 681.3.06 **doi: 10.20998/2522-9052.2019.4.16**

V. Rudnitsky[1], R. Berdibayev[2], R. Breus[1], N. Lada[1], M. Pustovit[3]

[1] Cherkasy State Tehnological University, Cherkasy, Ukraine
[2] Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
[3] Cherkassy Institute of Fire Safety named after Chernobyl Heroes, Cherkasy, Ukraine

# SYNTHESIS OF REVERSE TWO-BIT DUAL-OPERATED STRICTLY STRAIGHT CRYPTOGRAPHIC CODING ON THE BASIS OF ANOTHER OPERATION

**Abstract.** Based on the analysis of a group of two-bit two-operand operations of strict stable cryptographic coding, the relations between direct and inverse operations are established and formalized and their correctness is proved. Applying the technology of combining single-operand strict rigorous cryptographic coding into two-operand operations and using established interconnections, we propose a method of synthesis of inverse operations for known direct operations. This method provides the construction of the inverse operation by converting the second operand of two-bit two-operand operations of strict stable cryptographic coding. The article examines the entire sequence of mathematical transformations that provides the synthesis of a formalized operation model, suitable for practical application in crypto primitives, by constructing models of the relationships between operations and the synthesis of a reverse operation model. The synthesized operations are implemented both at the software and hardware levels and provide the ease of achieving the effect of strictly stable cryptographic coding.

**Keywords**: cryptographic coding; decoding; inverse operations; cryptocurrencies; permutations; encryption reliability; strict stable cryptographic coding; operation synthesis; second operand.

## Introduction

**Formulation of the problem**. Nowadays, information security has become one of the most important areas for the successful development of any society. Information resources, as cybercrime is on the rise, require the development of new and ongoing improvements to existing remedies [1]. First of all, it concerns cryptographic protection of information. Recent trends in the development of cryptology, among many promising trends, are the synthesis of new cryptocurrency operations [2].

It is worth saying that the ways of building new cryptocurrency operations for streaming and block encryption remain poorly studied.

For example, maximizing the uncertainty of encryption results can be obtained through crypto conversion operations that meet the criteria of strict, stable cryptographic encoding [3].

**Analysis of recent research and publications.** For the first time, the criterion of strict stable coding for evaluating the quality of elementary functions and operations from which the cryptocurrency algorithms are built is proposed in work [4].

Works [5, 6] are devoted to the construction of single-operand strict stable coding operations. However, the main disadvantage of these operations is the limited range of tasks where they can be applied, compared to two-operand operations [7].

Works [8, 9] are devoted to one of the approaches of constructing new two-operand permutation operations. This approach provided the construction of operations suitable for practical application.

In works [10, 11] the construction of two-bit two-operand operations of strict stable cryptographic coding and inverse operations was carried out.

The combination of inverse transformation with direct implementation of the method of increasing the stability and reliability of streaming encryption provides a fairly high uncertainty of the results of cryptocurrencies, regardless of the quality of the sequencing sequences. However, the widespread use of the obtained two-bit two-operand operations of strict stable cryptographic coding is limited by the complexity of constructing the model of inverted transformation and the practical implementation of the cryptosystem as a whole.

The purpose of the work is to establish relationships and to develop a method of synthesis of inverted two-bit two-operand operations of strict stable cryptographic coding on the basis of conversion of the second operand for use in stream and block ciphers.

## Basic material

The group of two-bit two-operand operations of strict stable cryptographic encoding includes 24 operations of cryptocurrency, which are given in table 1 [10].

These operations are grouped in Table 1 so that the operation in the first column corresponds to the operation inverted from the second column and vice versa, the operation from the second column corresponds to the operation inverted from the first column, that is, each row presents two inverse operations.

To achieve this, we will try to find relationships between direct and inverse cryptocurrency operations. Let it be a direct operation $O_1^k$ , and then it will be $O_2^k$ an inverse operation.

To find a relationship, we present a direct and inverted crypto conversion operation in the expanded view [11], which shows the relationship between single-operand cryptocurrencies of the first operand, depending on the value of the second operand.

*Table 1* – **Group of two-bit two-operand operations of strict stable cryptographic coding**

| Cryptocurrency Operation | Cryptocurrency Operation | Cryptocurrency Operation |
|---|---|---|
| $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}$ | $O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ | $O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}$ |
| $O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}$ | $O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ | $O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}$ |
| $O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$ | $O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2\\ k_2\end{bmatrix}$ | $O_9^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2\\ k_2\end{bmatrix}$ |
| $O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2\\ k_2\end{bmatrix}$ | $O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1\\ k_1\end{bmatrix}$ | $O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1\\ k_1\end{bmatrix}$ |
| $O_{13}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}$ | $O_{14}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}$ | $O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}$ |
| $O_{16}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}$ | $O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ | $O_{18}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}$ |
| $O_{19}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}$ | $O_{20}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1\\ k_1\end{bmatrix}$ | $O_{21}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$ |
| $O_{22}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2\\ k_2\end{bmatrix}$ | $O_{23}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2\\ k_2\end{bmatrix}$ | $O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$ |

$$\text{So}: \quad O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_2\\ \bar{k}_2\end{bmatrix}=$$

$$=\begin{cases}\begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, & if\ k_1=0;\ k_2=0; \qquad \begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, & if\ k_1=0;\ k_2=1;\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, & if\ k_1=1;\ k_2=0; \qquad \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, & if\ k_1=1;\ k_2=1;\end{cases}$$

$$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}=$$

$$=\begin{cases}\begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, & if\ k_1=0;\ k_2=0; \qquad \begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, & if\ k_1=0;\ k_2=1;\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, & if\ k_1=1;\ k_2=0; \qquad \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, & if\ k_1=1;\ k_2=1,\end{cases}$$

where x – is the value of the first operand, and k – the value of the second operand.

Operations $O_1^k$ and $O_2^k$ differ in order of placement of a single-operand operation of the first operand. The order of placement of a single-operand processing operation of the first operand is determined by the value of the second operand (condition of execution). Therefore, in order to construct a reverse operation, it is sufficient to change the conditions of its execution in a direct operation. You can establish relationships between operations based on the model of converting the value of the second operand of the direct operation into the value of the second operand of the inverse operation.

With this in mind, let's establish a relationship between the values of the second operands based on the construction of a discrete transformation model. To do this, we use the value of the second operand of the direct operation as input, and as the output of the value of the second operand of the inverse operation as a result of the implementation of the model of discrete transformation. To minimize the discrete automaton, we construct a truth table. It is Table 2.

*Table 2* – **The truth table of the discrete automatic transformer $O_1^k$ in $O_2^k$**

| The second operand of the direct operation | | The second operand of the inverse operation | |
|---|---|---|---|
| $k_1$ | $k_2$ | $k_1^*$ | $k_2^*$ |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 |

Minimizing this truth table, we obtain a discrete model of the automaton for constructing the second operand of the inverse operation:

$$k_1^*=k_1,\ \ k_2^*=k_1\oplus k_2.$$

This model makes it possible to construct a reverse operation $O_2^k$ on the basis of a direct operation $O_1^k$ .By analogy, we examine the relationship between operations $O_3^k$ and $O_6^k$ .

Let's take a direct operation $O_3^k$ , then the operation $O_6^k$ will be reversed. In the expanded view, the operations $O_3^k$ and $O_6^k$ will look like this:

$$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_1\\ \bar{k}_1\end{bmatrix}=$$

$$=\begin{cases}\begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, & if\ k_1=0;\ k_2=0; \qquad \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, & if\ k_1=0;\ k_2=1;\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, & if\ k_1=1;\ k_2=0; \qquad \begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, & if\ k_1=1;\ k_2=1;\end{cases}$$

$$O_6^{\kappa}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=$$

$$=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, & if\ k_1=0; \\ & k_2=0; \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, & if\ k_1=1; \\ & k_2=0; \end{cases} \quad \begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, & if\ k_1=0; \\ & k_2=1; \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, & if\ k_1=1; \\ & k_2=1; \end{cases}$$

where $x$ – is the value of the first operand, $k$ – is the value of the second operand.

The difference between these operations is the location of a single-operand operation of the first operand, which is determined by the value of the second operand, that is, its condition of execution.

According to the above mentioned, in order to construct a reverse operation, it is sufficient to change the conditions of its execution in a direct operation, that is, the relationships between operations can be established on the basis of the model of converting the value of the second operand of the direct operation into the value of the second operand of the reverse operation.

We establish the relationship between the values of the second operands by constructing a discrete transformation model by using the value of the second operand of the direct operation as input, and the value of the second operand of the inverse operation as the result of the implementation of the model of discrete transformation.

Let's construct the truth table of the discrete model of the automaton for $O_3^k$ and $O_6^k$ (Table 3):

*Table 3* – **The truth table of the discrete automatic transformer $O_3^k$ and $O_6^k$**

| The second operand of the direct operation | | The second operand of the inverse operation | |
|---|---|---|---|
| $k_1$ | $k_2$ | $k_1^*$ | $k_2^*$ |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 |

By minimizing this truth table, we obtain a discrete model of the automaton for constructing the second operand of the inverse operation:

$$k_1^*=k_2,\quad k_2^*=k_1.$$

The machine model for constructing the second operand of the inverse operation makes it possible to construct the inverse operation $O_6^k$ on the basis of a direct operation $O_3^k$.

As stated earlier, let's examine the relationship between operations $O_4^k$ and $O_5^k$.

In this case, $O_4^k$ is a direct operation, and the operation $O_5^k$ will be reversed. In the expanded view the operations $O_4^k$ $O_5^k$ and have the following form:

$$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, & if\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, & if\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, & if\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, & if\ k_1=1;\ k_2=1 \end{cases},$$

$$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, & if\ k_1=0; \\ & k_2=0; \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, & if\ k_1=0; \\ & k_2=1; \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, & if\ k_1=1; \\ & k_2=0; \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, & if\ k_1=1; \\ & k_2=1, \end{cases}$$

where x – is the value of the first operand, k – is the value of the second operand.

Similar to the previous operations, let us examine the relationships between operations $O_4^k$ and $O_5^k$ and construct a truth table for the discrete model of the automaton for $O_4^k$ and $O_5^k$ (Table 4):

*Table 4* – **The truth table of the discrete automatic transformer $O_4^k$ and $O_5^k$**

| The second operand of the direct operation | | The second operand of the inverse operation | |
|---|---|---|---|
| $k_1$ | $k_2$ | $k_1^*$ | $k_2^*$ |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |

By minimizing this truth table, we obtain a discrete model of the automaton for constructing the second operand of the inverse operation:

$$k_1^*=\overline{k_1\oplus k_2},\ k_2^*=k_2.$$

The discrete model makes it possible to construct a reverse operation $O_5^k$ based on a direct operation $O_4^k$.

By analogy, the relationships between all the two-bit two-operand operations of the rigorous robust cryptographic encryption operations investigated were found. Formalized relationships between direct and inverse operations allow us to construct a method of synthesizing inverted two-bit two-operand operations of rigorously stable cryptographic coding on the basis of second operand transformation.

A synthesis of the inverse operation is considered in work [11] taking into account the possibility of using the same gamma sequences in the direct and inverse channels of encryption. The inverse operation of strictly stable cryptographic coding, as well as the direct operation, are simply implemented at both hardware and

software levels. Since the synthesis of direct and inverse operations revealed that there is a recurrence of operations, there is a need to use the second operand transform to improve the quality of cryptographic coding. The obtained interconnections created the theoretical basis for the construction of a method of synthesis of inverted two-bit two-operand operations of strict stable cryptographic coding on the basis of the second operand transformation.

Let us formalize and prove the correctness of the application of detected interconnections for the construction of inverted two-bit two-operand operations of strict stable cryptographic coding by transformation of the second operand. If

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$$

is an encoding operation, and

$$O_1^d = O_2^\kappa = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$$

is a decoding operation, then $O_1^k$ can be applied as $O_1^d$, provided $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$. Because these operations are specified by models:

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ if\ k_1 = 0;\ k_2 = 0; & \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, if\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ if\ k_1 = 1;\ k_2 = 0; & \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, if\ k_1 = 1;\ k_2 = 1. \end{cases}$$

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ if\ k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, if\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ if\ k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, if\ k_1 = 1;\ k_2 = 1. \end{cases}$$

Thus, using the transformation of the second operand, we obtain:

$$O_1^{k*} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, if\ k_1^* = 0;\ k_2^* = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, if\ k_1^* = 0;\ k_2^* = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ if\ k_1^* = 1;\ k_2^* = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, if\ k_1^* = 1;\ k_2^* = 1; \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, if\ k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, if\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ if\ k_1 = 1;\ k_2 = 1; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, if\ k_1 = 1;\ k_2 = 0; \end{cases} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ if\ k_1 = 0; \\ \ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \ if\ k_1 = 1 \\ \ k_2 = 0; \end{cases} \quad \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \ if\ k_1 = 0; \\ \ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ if\ k_1 = 1; \\ \ k_2 = 1; \end{cases} = O_1^d,$$

which was to prove.

By analogy, inverse operations were built for the whole group of two-bit two-operand operations of strict stable cryptographic coding.

The results of this study are shown in Table 5.

*Table 5* – **Results of synthesis of operations based on established relationships**

| **Direct cryptocurrency operation** | **Inverted cryptocurrency operation** | **Model of the machine of construction of the second operand of the inverse operation** |
|---|---|---|
| **1** | **2** | **3** |
| $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ | $O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ | $k_1^* = k_2,\ k_2^* = k_1$ |
| $O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ | $O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ | |
| $O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ | $O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ | $k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$ |
| $O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ | $O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ | |
| $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ | $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ | $k_1^* = k_1$ $k_2^* = k_1 \oplus k_2$ |
| $O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ | $O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$ | |

*End of table 5*

| 1 | 2 | 3 |
|---|---|---|
| $O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ | $O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$ | $k_1^* = k_1$<br>$k_2^* = \overline{k_1 \oplus k_2}$ |
| $O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ | $O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ | |
| $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ | $O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ | $k_1^* = \overline{k_1 \oplus k_2}$<br>$k_2^* = k_2$ |
| $O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ | $O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$ | |
| $O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ | $O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ | $k_1^* = k_1 \oplus k_2$<br>$k_2^* = k_2$ |
| $O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ | $O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ | |

This table identifies defined subgroups of transactions that have the same interconnections, which simplifies cryptographic information security algorithms.

The above sequence of establishing relationships and mathematical transformations can be considered as a developed method of synthesis of inverted two-bit two-operand operations of strict stable cryptographic coding on the basis of transformation of the second operand. The use of inverted two-bit two-operand operation of strict stable cryptographic coding on the basis of transformation of the second operand in the method of increase of stability and reliability of stream encryption will provide creation of new qualitative opportunities for developers of stream ciphers.

## Conclusions

Thus, in the course of the study, the relationships between all two-bit two-operand operations of the group of operations of strict stable cryptographic coding were established. The relationship between direct and reverse operations was applied to the construction of reverse operations. The method of synthesis of inverted two-bit two-operand operations of strict stable cryptographic coding on the basis of transformation of the second operand is developed.

Operations subgroups and their interconnections are identified, which simplifies the construction of cryptographic security algorithms by reducing both software and hardware complexity.

REFERENCES


1. Babenko, V.G., Melnyk, R.P. and Gonchar, S.V. (2014), "Evaluation of the efficiency of using cryptographic transformation operations", *Bulletin of the Academy of Engineering of Ukraine*, Vol. 2, pp. 39–41.
2. Golub, S.V., Babenko, V.G., Rudnitsky, S.V. and Melnyk R.P. (2012), "Improvement of the method of synthesis of operations of cryptographic transformation on the basis of discrete-algebraic representation of operations", *Control, navigation and communication systems*, PNTU, Poltava, No. 2 (22), pp. 163–168.
3. Babenko, V.G., Mironets, I.V. and Rudnitsky, S.V. (2011), "Decoding of information in a group of two-bit operations of cryptographic transformation", *Control, navigation and communication systems*, PNTU, Poltava, Vol. 4 (20), pp. 208–212.
4. Rudnitsky, V.M., Shuvalova, L.A. and Nesterenko, O.B. (2017), "Analysis of two-bit operations of a cryptographic coding on the criterion of a strict avalanche effect", *Scientific works: Scientific and Methodological Journal*, pp. 74–77.
5. Nesterenko, O.B., Rudnitsky, V.M. and Shuvalova, L.A. (2017), "Synthesis of cryptographic transformation operations according to the criterion of strict stable coding", *Bulletin of the Academy of Engineering of Ukraine*, Vol. 3, pp. 105–108.
6. Rudnitsky, V.M., Shuvalova, L.A. and Nesterenko, O.B. (2017), "Method of synthesis of operations of cryptographic transformation by criterion of strict stable coding", *Cherkasy State Technological University Bulletin*, Vol. 1, pp. 5–10.
7. Lada, N.V. and Kozlovskaya, S.G. (2018), "Application of operations of cryptographic addition module two with precision to permutation in streaming ciphers", *Control, navigation and communication systems*, PNTU, Poltava, Vol. 1 (47), pp. 127–130, DOI: https://doi.org/10.26906/SUNZ.2018.1.127
8. Babenko, V.G. and Lada, N.V. (2018), "Synthesis and analysis of cryptographic addition operations module two", *Information processing systems*, KhNUPS, Kharkiv, Vol. 2 (118), pp. 116–118.
9. Rudnitsky, V.M., Lada, N.V., Fedotova-Piven, I.M. and Pustovit, M.O. (2018), "Synthesis of inverted two-bit two-operand operations of strict stable cryptographic coding", *Information processing systems and methods*, State Scientific Research Institute of the Ministry of Internal Affairs of Ukraine, Kyiv, Vol.4 (55), pp. 76–81.
10. Rudnitsky, V.M., Opirsky, I.M., Melnyk, O.G. and Pustovit M.A. (2018), "Synthesis of a group of strict stable cryptographic coding operations for constructing streaming ciphers", *Information security*, Vol. 24, No. 3.
11. Rudnitsky, V.M., Lada, N.V., Fedotova-Piven, I.M., Pustovit, M.O. and Nesterenko, O.B. (2018), "Construction of two-bit two-operand operations of strict stable cryptographic coding", *Control, navigation and communication systems*, PNTU, Poltava, Vol. 6 (52), pp. 113–115, DOI: https://doi.org/10.26906/SUNZ.2018.6.113

Надійшла (received) 22.09.2019
Прийнята до друку (accepted for publication) 13.11.2019

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

**Рудницький Володимир Миколайович** – доктор технічних наук, професор, завідувач кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, Україна;
**Volodymir Rudnitsky** – Doctor of Technical Sciences, Professor, Head of the Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine;
e-mail: rvn_2008@ukr.net; ORCID ID: http://orcid.org/0000-0003-3473-7433

**Бердибаєв Рат Шиндалійович** – кандидат політичних наук, доцент, завідувач кафедри систем інформаційної безпеки, Алматинський університет енергетики та зв'язку, Алмати, Казахстан;
**Rat Berdibayev** – Candidate of Political Sciences, Associate Professor, Head of the Department of Information Security Systems, Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan;
e-mail: r.berdybaev@aues.kz; ORCID ID: http://orcid.org/0000-0002-8341-9645

**Бреус Роксолана Василівна** – асистент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, Україна;
**Roksolana Breus** – Assistant of the Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine;
e-mail: skay1986@ukr.net; ORCID ID: http://orcid.org/0000-0001-6281-2017

**Лада Наталія Володимирівна** – кандидат технічних наук, асистент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, Україна;
**Nataliia Lada** – Candidate of Technical Sciences, Assistant of the Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine;
e-mail: ladanatali256@ukr.net; ORCID ID: http://orcid.org/0000-0002-7682-2970

**Пустовіт Михайло Олександрович** – старший викладач кафедри техніки та засобів цивільного захисту, Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Черкаси, Україна;
**Mykhailo Pustovit** – Senior Instructor of Department, Cherkasy Institute of Fire Safety named after Chornobyl Heroes, Cherkasy, Ukraine;
e-mail: m.pustovit@gmail.com; ORCID ID: http://orcid.org/0000-0001-5313-1459

## Синтез обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

В. М. Рудницький, Р. Ш. Бердибаєв, Р. В. Бреус, Н. В. Лада, М. О. Пустовіт

**Анотація**. На основі аналізу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування встановлено і формалізовано взаємозв'язки між прямими і оберненими операціями та доведено їх коректність. Застосувавши технологію поєднання одноопераднних операцій строгого стійкого криптографічного кодування в двохоперандні операції і використавши встановлені взаємозв'язки, запропоновано метод синтезу обернених операцій для відомих прямих операцій. Даний метод забезпечує побудову оберненої операції шляхом перетворення другого операнда двохрозрядної двохоперандної операцій строгого стійкого криптографічного кодування. У статті на прикладах побудови моделей взаємозв'язків між операціями та синтезом моделі оберненої операції розглядається вся послідовність математичних перетворень, яка забезпечує синтез формалізованої моделі операції, придатної для практичного застосування в криптопримітивах. Синтезовані операції реалізуються як на програмному, так і на апаратному рівнях, та забезпечують простоту досягнення ефекту строгого стійкого криптографічного кодування.

**Ключові слова:** криптографічне кодування; декодування; обернені операції; криптоперетворення; перестановки; надійність шифрування; строге стійке криптографічне кодування; синтез операцій; другий операнд.

## Синтез обратных двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования на основе преобразования второго операнда

В. Н. Рудницкий, Р. Ш. Бердыбаев, Р. В. Бреус, Н. В. Лада, М. А. Пустовит

**Аннотация**. На основе анализа группы двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования установлено и формализованы взаимосвязи между прямыми и обратными операциями и доказана их корректность. Применив технологию объединения одноопераднных операций строгого устойчивого криптографического кодирования в двухоперандные операции и использовав установленные взаимосвязи, предложено метод синтеза обратных операций для известных прямых операций. Данный метод обеспечивает построение обратной операции путем преобразования второго операнда двухразрядной двухоперандной операции строгого устойчивого криптографического кодирования. В статье на примерах построения моделей взаимосвязей между операциями и синтезом модели обратной операции рассматривается вся последовательность математических преобразований, которая обеспечивает синтез формализованной модели операции, пригодной для практического применения в криптопримитивах. Синтезаторные операции реализуются как на программном, так и на аппаратном уровнях, и обеспечивают простоту достижения эффекта строгого устойчивого криптографического кодирования.

**Ключевые слова:** криптографическое кодирование; декодирование; обратные операции; криптопреобразование; перестановки; надежность шифрования; строгое устойчивое криптографическое кодирование; синтез операций; второй операнд.