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 \( O^k_1 \), and then it will be \( O^k_2 \) 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 |
|--------------------------|--------------------------|--------------------------|
| \( O^1_k \) = \[ x_1 \cdot k_i \oplus x_2 \cdot k_1 \oplus k_2, x_1 \cdot k_i \oplus x_2 \cdot k_1 \oplus k_2 \] | \( O^2_k \) = \[ x_1 \cdot k_i \oplus x_2 \cdot k_1 \oplus k_2, x_1 \cdot k_i \oplus x_2 \cdot k_1 \oplus k_2 \] | \( O^3_k \) = \[ x_1 \cdot (k_i \oplus k_2) \oplus x_2 \cdot (k_i \oplus k_2) \oplus k_1, x_1 \cdot (k_i \oplus k_2) \oplus x_2 \cdot (k_i \oplus k_2) \oplus k_1 \] |
| \( O^4_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^5_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^6_k \) = \[ x_1 \cdot (k_i \oplus k_2) \ominus x_2 \cdot (k_i \oplus k_2) \ominus k_1, x_1 \cdot (k_i \oplus k_2) \ominus x_2 \cdot (k_i \oplus k_2) \ominus k_1 \] |
| \( O^7_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^8_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^9_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] |
| \( O^10_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^11_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] | \( O^12_k \) = \[ x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2, x_1 \cdot k_i \ominus x_2 \cdot k_1 \ominus k_2 \] |

So: \( O^1_k = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \oplus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \oplus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] \)

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

Operations \( O^1_k \) and \( O^1_k \) 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 \( O^k \) in \( O^k \)

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

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

\( k_1^* = k_1, k_2^* = k_2 \).

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 \( O^1_k \) and \( O^1_k \).

Let's take a direct operation \( O^1_k \), then the operation \( O^2_k \) will be reversed. In the expanded view, the operations \( O^1_k \) and \( O^2_k \) will look like this:

\( O^1_k = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \oplus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \oplus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] \)

\( O^2_k = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \ominus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] = \left[ \begin{array}{c} x_1 \\ x_2 \end{array} \right] \ominus \left[ \begin{array}{c} k_1 \\ k_2 \end{array} \right] \)
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-operation 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 using the value of the second operand of the direct operation as input, and the value of the second operand of the reverse 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 \( O_4^k \) (Table 3):

| 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 | 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 \( O_4^k \).

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 \( O_4^k \) and \( O_5^k \) have the following form:

\[
O_4^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \end{bmatrix}, \quad \text{if} \quad k_1 = 0; \quad k_2 = 0
\]

\[
O_5^k = \begin{bmatrix} x_1 \cdot \overline{k_2} \oplus x_2 \cdot \overline{k_2} \\ x_1 \cdot k_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \end{bmatrix} = \begin{bmatrix} x_1 \end{bmatrix}, \quad \text{if} \quad k_1 = 0; \quad k_2 = 1
\]

\[
O_6^k = \begin{bmatrix} x_1 \cdot \overline{k_2} \oplus x_2 \cdot \overline{k_2} \\ x_1 \cdot k_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \end{bmatrix} = \begin{bmatrix} x_1 \end{bmatrix}, \quad \text{if} \quad k_1 = 1; \quad k_2 = 0
\]

\[
O_7^k = \begin{bmatrix} x_1 \cdot \overline{k_2} \oplus x_2 \cdot \overline{k_2} \\ x_1 \cdot k_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \end{bmatrix} = \begin{bmatrix} x_1 \end{bmatrix}, \quad \text{if} \quad k_1 = 1; \quad k_2 = 1
\]

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):

| 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 | 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:

\[
k_1^* = k_1 \oplus k_2, \quad k_2^* = k_2.
\]

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-operation 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-operation 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

$$O^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus k_2$$

is an encoding operation, and

$$O^d = O^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \cdot k_2 \\ k_1 \cdot k_2 \\ k_1 \cdot k_2 \end{bmatrix}$$

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

$$O^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus k_1$$

$$O^d = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus k_1$$

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

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

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 operation** | **Inverted operation** | **Model of the machine of construction of the second operand of the inverse operation** |
| | | **3** |
| | **1** | **2** |  |
| $O^k_1$ | $O^k_2$ | $O^k_3$ |
| $O^d_1$ | $O^d_2$ | $O^d_3$ |
| $O^k_4$ | $O^d_4$ | $O^k_5$ |
| $O^d_5$ | $O^k_6$ | $O^d_6$ |
| $O^k_7$ | $O^d_7$ | $O^k_8$ |
| $O^d_8$ | $O^k_9$ | $O^d_9$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |
| $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ | $k_1^* = k_2$, $k_2^* = k_1$ |

112
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 Kozlovskaia, S.G. (2018), “Application of operations of cryptographic addition module two with precision to permutation in stream ciphers”, Control, navigation and communication systems, PNTU, Poltava, Vol. 1 (47), pp. 127–130, DOI: https://doi.org/10.26906/SUNZ2018.1.127.
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
В. М. Рудницкий — доктор технических наук, профессор, заведующий кафедрой информационной безопасности и компьютерной инженерии, Чerkasy State Technological University, Cherkasy, Ukraine; Volodymir Rudnitsky — Doctor of Technical Sciences, Professor, Head of the Department of Information Security and Computer Engineering, Cherkasy State Technical University, Cherkasy, Ukraine; e-mail: rrn_2008@ukr.net; ORCID ID: http://orcid.org/0000-0003-3473-7433

Рат Бердибайев — кандидат политических наук, доцент, заведующий кафедрой систем информационной безопасности, Almaty Institute of Power Engineering and Telecommunications, Almaty, Kazakhstan; e-mail: r.berdybaev@auses.kz; ORCID ID: http://orcid.org/0000-0002-8341-9645

Бреус Роксолана Василиевна — ассистент кафедры информационной безопасности и компьютерной инженерии, Черкасский державный технологический университет, Черкаси, Украина; Roksolana Breus — Assistant of the Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine; e-mail: rskay1986@ukr.net; ORCID ID: http://orcid.org/0000-0001-6281-2017

Лада Наталия Володимирна — кандидат технических наук, ассистент кафедры информационной безопасности и компьютерной инженерии, Чerkasy State Technological University, Cherkasy, Ukraine; Nataliia Lada — Candidate of Technical Sciences, Assistant of the Department of Information Security and Computer Engineering, Cherkasy State Technical University, Cherkasy, Ukraine; e-mail: ladanatali256@ukr.net; ORCID ID: http://orcid.org/0000-0002-7682-2970

Пустовит Михаил Александрович — старший преподаватель кафедры техники и засобов гражданской защиты, Чerkasy State Technological University, Cherkasy, Ukraine; 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 оберненных двохразрядных двохоперандных операций строго стойкого криптографического кодирования на основе перетворення другого операції

В. М. Рудницкий, Р. Ш. Бердибайев, Р. В. Бреус, Н. В. Лада, М. О. Пустовит

Анотація. На основі аналізу групи двохразрядних двохоперандних операций строго стойкого криптографического кодирования встановлено і формалізовано взаємозв'язки між прямими і оберненими операціями та доведено їх коректність. Застосовувши технологію поєднання однооперандних операцій строго стойкого криптографического кодування в двохразрядні операції і використаний встановлені взаємозв'язки, запропоновано метод синтезу обернень операцій для відомих прямих операцій. Даний метод забезпечує побудову оберненої операції шляхом перетворення другого операції двохразрядної двохоперандної операції строго стойкого криптографического кодування. У статті на прикладах побудовано 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 криптопримітках. Синтезовані операції реалізуються як на програмному, так і на апаратному рівнях. У статті представлена простота досягнення ефекту строго стойкого криптографического кодування.

Ключові слова: криптографичне кодування; декодування; обернені операції; криптоперетворення; перестановки; надійність шифрування; строго стойке криптографичне кодування; синтез операцій; другий операнд.

Синтез обратных двухуразрядных двухоперандных операций строго устойчивого криптографического кодирования на основе преобразования второго операнда

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

Аннотация. На основе анализа группы двухуразрядных двухоперандных операций строго устойчивого криптографического кодирования установлены и формализованы взаимосвязи между прямыми и обратными операциями и доказана их корректность. Применив технологию объединения однооперандных операций строго устойчивого криптографического кодирования в двухуразрядные операции и используя установленные взаимосвязи, предложено метод синтеза обратных операций для известных прямых операций. Данный метод обеспечивает построение обратной операции путем преобразования второго операції двухуразрядной двухоперандной операції строго устойчивого криптографического кодирования. В статье на примерах построены модели взаимосвязей между операциями и синтез моделей обратной операции рассматривается вся последовательность математических преобразований, которая обеспечивает синтез формализованной модели операций, пригодной для практического применения в криптопримитивах. Синтезированные операции реализуются как на программном, так и на аппаратном уровнях, и обеспечивают простоту достижения эффекта строго устойчивого криптографического кодирования.

Ключевые слова: криптографическое кодирование; декодирование; обратные операции; криптоперобразование; перестановка; надежность шифрования; строго устойчивое криптографическое кодирование; синтез операций; второй operand.