УДК 004.056.55:004.312.2

В.М. Рудницький,
доктор технічних наук, професор, професор Черкаського державного технологічного університету, м. Черкаси, Україна,
Н.В. Лада,
кандидат технічних наук, асистент кафедри Черкаського державного технологічного університету, м. Черкаси, Україна,
І.М. Федотова-Півень,
кандидат технічних наук, доцент, доцент Черкаського державного технологічного університету, м. Черкаси, Україна,
М.О. Пустовіт,
старший викладач Інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, м. Черкаси, Україна

СИНТЕЗ ОБЕРНЕНИХ ДВОРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ

На основі технології поєднання одноопераднних операцій строгого стійкого криптографічного кодування запропоновано підхід, який дозволяє синтезувати обернені операції для відомих прямих дворозрядних двохоперандних операцій строгого стійкого криптографічного перетворення інформації. У статті на прикладі побудови однієї 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, що забезпечує простоту досягнення ефекту строгого стійкого криптографічного кодування.

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

На основе технологии сочетания одноопераднных операций строгого устойчивого криптографического кодирования предложен подход, который позволяет синтезировать обратные операции для известных прямых двухразрядных двухоперандных операций строгого устойчивого криптографического преобразования информации. В статье на примере построения одной операции рассматривается вся последовательность математических преобразований, которая обеспечивает синтез формализованной модели операции пригодной для практического применения в криптопримитивах. Синтезированные операции реализуются как на программном так и на аппаратном уровнях, что обеспечивает простоту достижения эффекта строгого устойчивого криптографической кодирования.

***Ключевые слова:** криптографическое кодирование, декодирование, обратные операции, криптопреобразования, перестановки, надежность шифрования, строгое устойчивое криптографическое кодирование, синтез операций.*

Постановка проблеми. На сьогодні інформаційна безпека стає одним із найпріорітетніших напрямів успішного розвитку будь-якого суспільства. Зростання рівня кіберзлочинності потребує розробки нових та постійного вдосконалення вже існуючих засобів захисту інформаційних ресурсів. У першу чергу, це стосується криптогафічного захисту інформації. Сучасна криптологія розвивається за багатьма перспективними напрямами, одим з яких є синтез нових операцій криптоперетворення.

Але слід зазначити, що шляхи побудови нових операцій криптоперетворення для потокового та блокового шифрування залишаються недостатньо вивченими. Також недостатньо уваги приділяється і питанням застосування нових синтезованих операцій строгого стійкого криптографічного кодування в сучасних криптоалгоритмах.

Аналіз останніх досліджень і публікацій

Вперше критерій строгого стійкого кодування для оцінки якості елементарних функцій і операцій, з яких будуються алгоритми криптоперетворення, запропоновано в роботі [1]. Побудові одноопераднних операцій строгого стійкого кодування присвячені роботи [2–3]. Проте основним недоліком цих операцій є обмежене коло задач, де вони можуть застосовуватися, порівняно з двохопераднними операціями [4]. Одному із підходів побудови нових двохопераднних операцій на основі перестановок присвячено роботи [5–6]. Цей підхід забезпечив побудову придатних для практичного застосування операцій. Проте отримані операції не задовольняють критерій строгого стійкого кодування, а синтезу обернених операцій увага взагалі не приділялася.

Метою роботи є моделювання обернених дворозрядних двохопераднних операцій строгого стійкого криптографічного перетворення для застосування в потокових і блокових шифрах.

Основний матеріал

Оскільки синтезована операція будувалася для застосування в потокових шифрах, то доцільно синтез оберненої операції проводити з врахуванням можливості використання в прямому та оберненому каналах шифрування однакових гамуючих послідовностей.

Для вирішення цієї задачі необхідно в моделях двохопераднних операцій прямого і оберненого криптоперетворення використовувати однакові коди команд управління для прямих і обернених одноопераднних операцій.

У роботі [5] наведені чотири операції, які відповідають критерію строгого стійкого кодування, а саме:

$$F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \quad (1)$$

$$F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \quad (2)$$

$$F_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \quad (3)$$

$$F_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \tag{4}$$

Для одноопераднних операцій криптоперетворення (1–4), на основі яких забезпечується строге стійке криптографічне кодування, обернені одноопераднді операції наведені в [7].

$$F^k_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \rightarrow F^d_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \tag{5}$$

$$F^k_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \rightarrow F^d_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \tag{6}$$

$$F^k_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \rightarrow F^d_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \tag{7}$$

$$F^k_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \rightarrow F^d_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \tag{8}$$

Побудуємо обернену операцію для дворозрядної операції строгого стійкого криптографічного кодування (9):

$$O_{3\_10,12\_5,5\_12,10\_3} = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \oplus y_2 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \oplus \bar{y}_2 \end{bmatrix}. \tag{9}$$

Оскільки ця операція задана моделлю (10)

$$O^k_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases}, \tag{10}$$

тоді з врахуванням (5–8) отримаємо обернену операцію строгого сійкого криптографічного переворення (11):

$$O^{d}_{3\_10,12\_5,12\_5,3\_10} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1 \end{cases}. \quad (11)$$

Скористаємося технологією синтезу двохоперандних операцій криптоперетворення на основі одноопераднних для побудови оберненої операції.

Виходячи з (5), модель спрощеної операції без врахування інверсій буде задана виразом (12):

$$O^{d}_{3\_5,3\_5,5\_3,5\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1 \end{cases} = O^{k}_{3\_5,3\_5,5\_3,5\_3} = \begin{bmatrix} x_1 \cdot \overline{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \overline{k}_1 \end{bmatrix}. \quad (12)$$

Побудуємо двохоперандну операцію обробки сигналів інверсії. Модель цієї операції відповідно до (5) можна представити:

$$\overline{O}^{d}_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1 \end{cases}.$$

Перетворимо обернену операцію обробки сигналів інверсії з урахуванням значень команд реалізації в якості другого аргументу:

$$\overline{O}^{d}_{3\_10,12\_5,5\_12,10\_3}=\begin{cases}\begin{bmatrix}0\\1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}1\\0\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}1\\0\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}0\\1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}.$$

Операцію $\overline{O}^{d}_{3\_10,12\_5,5\_12,10\_3}$ можна записати як:

$$\overline{O}^{d}_{3\_10,12\_5,5\_12,10\_3}=\begin{cases}\begin{bmatrix}0\\1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}1\\0\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}1\\0\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}0\\1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}. \quad (13)$$

На основі додавання за модулем два моделей (6) і (7) і отримаємо операцію $O^{d}_{3\_10,12\_5,12\_5,3\_10}$ (14):

$$O^{d}_{3\_10,12\_5,12\_5,3\_10}=\begin{bmatrix}x_1\cdot\overline{k}_1\oplus x_2\cdot k_1\\x_1\cdot k_1\oplus x_2\cdot\overline{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\oplus k_2\\k_2\oplus k_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\cdot\overline{k}_1\oplus x_2\cdot k_1\oplus k_2\oplus k_2\\x_1\cdot\overline{k}_1\oplus x_2\cdot k_1\oplus k_2\oplus k_2\oplus 1_2\end{bmatrix}. \quad (14)$$

Представимо обернену операцію (14) як операцію обробки двох аргументів (15):

$$O^{d}_{3\_10,12\_5,12\_5,3\_10}=\begin{bmatrix}x_1\cdot\overline{y}_1\oplus x_2\cdot y_1\oplus y_1\oplus y_2\\x_1\cdot y_1\oplus x_2\cdot\overline{y}_1\oplus y_1\oplus y_2\oplus 1\end{bmatrix}. \quad (15)$$

Обернена операція строгого стійкого криптографічного кодування (15), як і пряма операція (9), просто реалізуються як на апаратному, так і програмному рівнях.

Застосування прямої і оберненої дворозрядної двохоперандної операції строгого стійкого криптографічного кодування в методі підвищення стійкості і надійності потокового шифрування [5] забезпечить створення нових якісних можливостей для розробників потокових шифрів.

Висновки

Таким чином, проведене дослідження дало змогу розробити модель оберненого дворозрядного двохоперандного строгого стійкого криптографічного перетворення. Поєднання отриманого оберненого перетворення разом із прямим при реалізації методу підвищення стійкості і надійності потокового шифрування забезпечить максимальну невизначеність результатів криптоперетворення незалежно від якості гамуючих послідовностей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Рудницький В.М., Шувалова Л.А., Нестеренко О.Б.* Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. Наукові праці: науково-методичний журнал. Миколаїв: Чорноморський державний університет імені Петра Могили, 2017. С. 74–77.

2. *Нестеренко О.Б., Рудницький В.М., Шувалова Л.А.* Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. Вісник інженерної академії України: часопис. Київ, 2016. Вип. 3. С. 105–108.

3. *Рудницький В.М., Шувалова Л.А., Нестеренко О.Б.* Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. Вісник ЧДТУ. Черкаси, 2017. Вип. 1. С. 5–10.

4. *Лада Н.В., Козловська С.Г.* Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2018. Т. 1(47). С. 127–130.

5. *Рудницький В.М., Лада Н.В., Бабенко В.Г.* Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ТОВ "ДІСА ПЛЮС", 2018. – 184 с.

6. *Бабенко В.Г., Лада Н.В.* Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2(118). С. 116–118.

7. *Рудницький В.М.* Криптографічне кодування: обробка та захист інформації: колективна монографія. Харків: ТОВ "ДІСА ПЛЮС", 2018. 139 с.

REFERENCES

1. *Rudnitskyi V.M., Shuvalova L.A. and Nesterenko O.B.* (2017). Analiz dvorozriadnykh operatsii kryptohrafichnoho koduvannia za kryteriiem strohoho lavynnoho efektu. "Analysis dorasdaddy operations of cryptographic encoding according to the criterion of the strict avalanche effect, Scientific works: scientific and methodological journal". Mykolaiv: Petro Mohyla Black Sea State University. P. 74–77 [in Ukrainian].

2. *Rudnitskyi V.M., Shuvalova L.A. and Nesterenko O.B.* (2016). Syntez operatsii kryptohrafichnoho peretvorennia za kryteriiem strohoho stiikoho koduvannia. "Synthesis of operations of cryptographic transformation by the criterion of strict sustainable coding", Bulletin of engineering academy of Ukraine, No. (3). P. 105–108 [in Ukrainian].

3. *Rudnitskyi V.M., Shuvalova L.A. and Nesterenko O.B.* (2017). Metod syntezu operatsii kryptohrafichnoho peretvorennia za kryteriiem strohoho stiikoho koduvannia. "The method of synthesis of cryptographic conversion operations according to the criterion of strict sustainable coding", Bulletin of the ChTTU. Cherkasy. Issue 1. P. 5–10 [in Ukrainian].

4. *Lada N.V. and Kozlovska S.H.* (2018). Zastosuvannia operatsii kryptohrafichnoho dodavannia za modulem dva z tochnistiu do perestanovki v potokovykh shyfrakh. "Cryptographic encoding: Synthesis for streaming encryption operations within the accuracy of permutation: monograph", TOV "DISA PLIUS", Poltava: PNTU. vol. 1(47). 127–130 pp. [in Ukrainian].

5. Rudnitskyi V.M., Lada N.V., Babenko V.H. Kryptografichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky. "Cryptographic encoding: synthesis of streaming decoding": monograph. Kharkiv: Disa Plus. 2018. 184 p. [in Ukrainian].

6. *Babenko V.H. and Lada N.V.* (2014). Syntez i analiz operatsii kryptohrafichnoho dodavannia za modulem dva. "Synthesis and analysis of operations of cryptographic addition modulo two", Systems of information processing: Sb. sciences Kharkiv Avenue: HUPPS them. I. Kozheduba. 2(118). 116–118 pp. [in Ukrainian].

7. *Rudnitskyi V.M.* (2018). Kryptohrafichne koduvannia:obrobka ta zakhyst informatsii: kolektyvna monohrafiia. "Cryptographic encoding: processing and protection of information: a collective monograph", TOV "DISA PLIUS", Kharkiv. 139 p. [in Ukrainian].

UDC 004.056.55:004.312.2

V.M. Rudnytskyi,
Doctor of Technical Sciences, Full Professor, Professor,
Cherkasy State Technological University, Cherkasy,Ukraine,
N.V. Lada,
Candidate of Technical Sciences, Assistant Lecturer, Cherkasy State Technological University, Cherkasy,Ukraine,
I.M. Fedotova-Piven,
Candidate of Technical Sciences, Docent, Associate Professor,
Cherkasy State Technological University, Cherkasy,Ukraine,
M.O. Pustovit,
Senior Lecturer, Cherkasy Institute of Fire Safety Named after Heroes of Chernobyl, Cherkasy, Ukraine

SYNTHESIS OF THE INVERSE TWO-BIT TWO-OPERAND OPERATIONS OF STRONG CRYPTOGRAPHIC ENCODING

Construction the new algorithms of stream and block cipher is inextricably linked with the synthesis of new cryptographic transformation operations. Particular attention deserve the operations that in the process of information transformation on the basis of the subdued sequence provide the achievement of strong cryptographic encoding, which means the maximum uncertainty of the cryptographic transformation results. However, it was paid not enough attention to the synthesis of these operations nowadays, and the processes of constructing the inverse operations of strong cryptographic coding were not studied at all.

The purpose of the work is to simulate the inverse two-bit two-operand operations of strong cryptographic transformation for usage in stream and block ciphers. For reaching the purpose, the necessity of using one subdued sequence for direct and inverse transformation was taken into account.

An approach that allows synthesizing reverse operations for known direct two-bit two-operand operations of strong cryptographic information transformation, based on the technology of combining single-operand operations of strong cryptographic encoding, is proposed. The entire sequence of mathematical transformations, which provides the synthesis of a formalized operation model suitable for practical application in cryptographic primitives, is considered in the article on the example of one operation's construction. Synthesized operations are implemented on the software level as well as on the hardware level, which provides an ease of reaching the effect of strong cryptographic encoding.

Thus, the research made it possible to develop a model of an inverse two-bit two-operand strong cryptographic transformation. The combination of the obtained inverse transformation with the direct at implementation the method of increasing the stability and reliability of stream encryption will provide maximum uncertainty for the results of cryptographic transformation, regardless of the subdued sequences' quality.

Keywords: cryptographic encryption, decryption, inverse operations, cryptographic transformations, permutations, reliability of encryption, strong cryptographic encoding, synthesis of operations.

Отримано 30.11.2018
Рецензент Єрохін В.Ф., д.т.н., проф.