УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2018.6.113**

В. М. Рудницький[1], Н. В. Лада [1], І. М. Федотова-Півень [1], М. О. Пустовіт [2], О. Б. Нестеренко[2]

[1] Черкаський державний технологічний університет, Черкаси, Україна
[2] Інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси, Україна

ПОБУДОВА ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ

Метою роботи є розробка моделей двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення придатних для практичного застосування в потокових і блокових шифрах. **Результати.** Основний критерій строгого стійкого кодування полягає в досягненні максимальної невизначеності результатів шифрування при мінімальних затратах. Проте, доноопернадні операції, незважаючи на те, що вони відповідають критерію строгого стійкого кодування, не мають широкого застосування в криптографічних алгоритмах. Це зумовлено тим, що вони є одноопернадними. Для практичного застосування даних результатів доцільно їх адаптувати до обробки двох операндів. У статті побудувана модель операції криптографічного додавання яка забезпечила двохвохрозрядне двохоперандне строге стійке криптографічне кодування: Отримана в статті операція забезпечує реалізацію строгого стійкого криптографічного кодування при її застосуванні в потокових шифрах. Основною перевагою синтезованої операції над моделлю строгого стійкого криптографічного кодування є простота її реалізації як на апаратному так і програмному рівні. Застосовуючи інші поєднання одноопераннних операцій строгого стійкого криптографічного перетворення можна отримувати інші аналогічні двохоперандні операції. **Висновки.** На основі дослідження і поєднання одноопернадних операцій строгого стійкого криптографічного кодування синтезовано двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення, придатну для практичного застосування в потокових і блокових шифрах як на апаратному так і програмному рівні. Запропонований в роботі підхід дозволяє розширити, за рахунок синтезу нових моделей операцій строгого стійкого перетворення, інструментальні засоби побудови крипто примітивів нового покоління.

Ключові слова: криптографічне кодування, криптоперетворення, додавання за модулем два, перестановки, надійність шифрування, строге стійке криптографічне кодування, синтез операцій.

Вступ

Постановка проблеми. На сьогоднішній день криптографічний захист інформації залишається одним із найважливіших при забезпеченні інформаційної безпеки [1]. Однин з перспективних напрямів розвитку криптографії полягає у розширенні спектра операцій криптографічного перетворення інформації з заданими властивостями на основі логічних функцій [2]. Особливе місце при дослідженні даних операцій криптоперетворення є операції що забезпечують максимальну криптостійкість. Саме такими операціями і є операції строгого стійкого криптографічного кодування [2].

Аналіз останніх досліджень і публікацій. В роботах [4–6] представлено синтез двохоперандних операцій крипто перетворення для потокового шифрування на основі додавання за модулем з точністю до перестановки. Дані операції будуються на основі перестановок операндів та перестановок результатів виконання додавання за модулем. Для оцінки ефективності операцій криптоперетворення в [3]. вводяться критерії криптографічного та строгого криптографічного кодування. Сутність даних критеріїв полягає в ймовірності зміни біта інформації при виконанні над нею криптоперетворення. Строге криптографічне кодування забезпечує невизначеність кожного перетвореного біта інформації з ймовірністю одна друга. Побудові одноопернадних операцій строгого стійкого кодування присвячені роботи [4–6]. Проте, застосування операцій строгого стійкого криптографічного кодування в потокових шифрах потребують подальшого дослідження. Це пов'язано з тим що в потокових шифрах необхідно одночасно обробляти інформаційну послідовність і гамуючу двохопернадними операціями.

Метою роботи є розробка моделей двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення придатних для практичного застосування в потокових і блокових шифрах.

Основний матеріал

В [6] наведена повна множина дворозрядних операцій криптографічного перетворення інформації, а також виділено чотири дворозрядні операції, які відповідають критерію строгого стійкого кодування:

$$F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \quad F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \qquad (1)$$

$$F_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \quad F_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}. \qquad (2)$$

Основний критерій строгого стійкого кодування полягає в досягненні максимальної невизначеності результатів шифрування при мінімальних затратах [4]. Саме тому використання операцій (1, 2) дає змогу підвищувати якість криптографічних алгоритмів та швидкості їх реалізації [4]. Проте, дані операції, незважаючи на те, що вони відповідають критерію строгого стійкого кодування, не мають широкого застосування в криптографічних алгоритмах. Це зумовлено тим, що вони є одноопернадними. Для практичного застосування даних результатів доцільно їх адаптувати до обробки двох операндів.

Прикладом множини двохоперандних операцій, які можуть застосовуватись в перспективних потокових шифрах є операції додавання за модулем два з точністю до перестановки. Для подальшого дослідження необхідно побудувати операцію по аналогії з операціями додавання по модулю два з точністю

до перестановки побудованими в [3,4], і наведеними в наведену в табл. 1. Необхідність побудови аналогічних операцій обумовлена тим, що їх застосування в потокових шифрах забезпечує підвищення стійкості і надійності шифрування [4, 7].

Таблиця 1 – **Група операцій додавання за модулем два з точністю до перестановки**

$O_{1.1}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$O_{2.1}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\end{vmatrix}$
$O_{1.2}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$O_{2.2}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix}$
$O_{1.3}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\end{vmatrix}$	$O_{2.3}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\end{vmatrix}$
$O_{1.4}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$O_{2.4}^{\oplus}=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix}$
$O_{3.1}^{\oplus}=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\end{vmatrix}$	$O_{3.3}^{\oplus}=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\end{vmatrix}$
$O_{3.2}^{\oplus}=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix}$	$O_{3.4}^{\oplus}=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix}$

Виходячи з виразів (1, 2) побудуємо модель операції криптографічного додавання яка забезпечить двохвохрозрядне двохоперандне строге стійке криптографічне кодування:

$$O_{3\_10,12\_5,5\_12,10\_3}= \\ =\begin{cases}\begin{bmatrix}x_1 \\ x_2\oplus 1\end{bmatrix},\ k_1=0;\ k_2=0; \begin{bmatrix}x_1\oplus 1 \\ x_2\end{bmatrix},\ k_1=0;\ k_2=1; \\ \begin{bmatrix}x_2 \\ x_1\oplus 1\end{bmatrix},\ k_1=1;\ k_2=0; \begin{bmatrix}x_2\oplus 1 \\ x_1\end{bmatrix},\ k_1=1;\ k_2=1.\end{cases} \quad (3)$$

Скористаємося технологією синтезу двохоперандних операцій криптоперетворення на основі одноопераднних. Для спрощення побудови операції, придатної для практичного застосування, проведемо побудову в три етапи. На першому етапі побудуємо спрощену операцію, без врахування інверсій розрядів. Виходячи з (3) модель даної операція є такою:

$$O_{3\_5,3\_5,5\_3,5\_3}= \\ =\begin{cases}\begin{bmatrix}x_1 \\ x_2\end{bmatrix},\ k_1=0;\ k_2=0; \begin{bmatrix}x_1 \\ x_2\end{bmatrix},\ k_1=0;\ k_2=1; \\ \begin{bmatrix}x_2 \\ x_1\end{bmatrix},\ k_1=1;\ k_2=0; \begin{bmatrix}x_2 \\ x_1\end{bmatrix},\ k_1=1;\ k_2=1.\end{cases}$$

Перетворимо дану операцію з врахуванням значень команд реалізації в якості другого аргументу:

$$O_{3\_5,3\_5,5\_3,5\_3}= \\ =\begin{cases}\begin{bmatrix}x_1 \\ x_2\end{bmatrix}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix},\ \text{якщо } k_1=0;\ k_2=0; \\ \begin{bmatrix}x_1 \\ x_2\end{bmatrix}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix},\ \text{якщо } k_1=0;\ k_2=1; \\ \begin{bmatrix}x_2 \\ x_1\end{bmatrix}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix},\ \text{якщо } k_1=1;\ k_2=0; \\ \begin{bmatrix}x_2 \\ x_1\end{bmatrix}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix},\ \text{якщо } k_1=1;\ k_2=1.\end{cases}$$

Опираючись на отримані взаємоперетворення, операцію $O_{3\_5,3\_5,5\_3,5\_3}$ можна записати як:

$$O_{3\_5,3\_5,5\_3,5\_3}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix} \quad (4)$$

На другому етапі синтезу побудуємо двохоперандну операцію обробки сигналів інверсії. Модель даної операції відповідно до (3) можна представити:

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

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

$$\bar{O}_{3\_10,12\_5,5\_12,10\_3}= \\ \begin{cases}\begin{bmatrix}0 \\ 1\end{bmatrix}=\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix},\ k_1=0;\ k_2=0; \begin{bmatrix}1 \\ 0\end{bmatrix}=\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix},\ k_1=0;\ k_2=1; \\ \begin{bmatrix}0 \\ 1\end{bmatrix}=\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix},\ k_1=1;\ k_2=0; \begin{bmatrix}1 \\ 0\end{bmatrix}=\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix},\ k_1=1;\ k_2=1.\end{cases}$$

Операцію $\bar{O}_{3\_5,3\_5,5\_3,5\_3}$ можна записати як:

$$\bar{O}_{3\_10,12\_5,5\_12,10\_3}= \\ =\left\{\begin{bmatrix}0 \\ 1\end{bmatrix},\ k_1=0;\ k_2=0; \begin{bmatrix}1 \\ 0\end{bmatrix},\ k_1=0;\ k_2=1; \begin{bmatrix}0 \\ 1\end{bmatrix},\ k_1=1;\ k_2=0; \begin{bmatrix}1 \\ 0\end{bmatrix},\ k_1=1;\ k_2=1\right\}=\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix} \quad (5)$$

На основі додавання за модулем 2 поєднаємо (4) і (5) і отримаємо операцію $O_{3\_10,12\_5,5\_12,10\_3}$:

$$O_{3\_10,12\_5,5\_12,10\_3}= \\ =O_{3\_5,3\_5,5\_3,5\_3}\oplus\bar{O}_{3\_10,12\_5,5\_12,10\_3}.$$

Таким чином,

$$O_{3\_10,12\_5,5\_12,10\_3}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2 \\ \bar{k}_2\end{bmatrix},$$

відповідно:

$$O_{3\_10,12\_5,5\_12,10\_3}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\oplus k_2 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\oplus\bar{k}_2\end{bmatrix}. \quad (6)$$

Представимо операцію (6), як операцію обробки двох аргументів.

$$O_{3\_10,12\_5,5\_12,10\_3}=\begin{bmatrix}x_1\cdot\bar{y}_1\oplus x_2\cdot y_1\oplus y_2 \\ x_1\cdot y_1\oplus x_2\cdot\bar{y}_1\oplus\bar{y}_2\end{bmatrix} \quad (7)$$

Отримана операція (7) забезпечує реалізацію строгого стійкого криптографічного кодування при її застосуванні в потокових шифрах. Основною перевагою синтезованої операції над моделлю криптографічного кодування (3) є простота її реалізації як на апаратному так і програмному рівні. Застосовуючи інші поєднання одноопераднних операцій строгого стійкого криптографічного перетворення можна отримувати аналогічні двохоперандні операції.

Висновки

В процесі дослідження синтезовано двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення, придатну для практичного застосування в потокових і блокових шифрах як на апаратному так і програмному рівні. Запропонований в роботі підхід дозволяє розширити, за рахунок синтезу нових моделей операцій строгого стійкого перетворення, інструментальні засоби побудови крипто примітивів нового покоління.

СПИСОК ЛІТЕРАТУРИ

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптология: Теорія. Практика. Застосування: Монографія. Вид.2-ге, перероб. і доп. – Харків: Видавництво «Форт», 2012. – 880 с.
2. Криптографічне кодування: обробка та захист інформації: колективна монографія / під ред. В.М.Рудницького. — Харків: ТОВ «ДІСА ПЛЮС», 2018. – 139 с.
3. Lada N.V. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах / N.V. Lada, S.H. Kozlovska // Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2018. – Вип. 1 (47). – С. 127-130.
4. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія / В.М.Рудницький, Н.В. Лада, В.Г. Бабенко. - Харків: ТОВ «ДІСА ПЛЮС», 2018. – 184 с.
5. 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.
6. Рудницький В.М. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування / В.М. Рудницький, Л.А. Шувалова, О.Б. Нестеренко // "Вісник ЧДТУ". - Черкаси, 2017. – Вип. 1. – С.5-10.
7. Бабенко В. Г. Застосування операцій криптографічного перетворення для синтезу криптоалгоритмів. Сучасна спеціальна техніка. 2014. № 3 (38). С. 49–55.

Рецензент: д-р техн. наук, проф. І. В. Шостак,
Національний аерокосмічний університет "ХАІ", Київ
Received (Надійшла) 16.10.2018
Accepted for publication (Прийнята до друку) 28.11.2018

Построение двохрозрядних двухоперандных операций строгого устойчивого криптографического кодирования

В. Н. Рудницкий, Н. В. Лада, И. Н. Федотова-Пивень, М. А. Пустовит, О. Б. Нестеренко

Целью работы является разработка моделей двохрозрядних двухоперандных операций строгого устойчивого криптографически преобразования пригодных для практического применения в поточных и блочных шифрах. **Результаты.** Основной критерий строгого устойчивого кодирования заключается в достижении максимальной неопределенности результатов шифрования при минимальных затратах. Однако, одноопернадны операции, несмотря на то, что они соответствуют критерию стро гого устойчивого кодирования, не имеют широкого применения в криптографически алгоритмах. Это обусловлено тем, что они одноопераннимы. Для практического применения данных результатов целесообразно их адаптировать к обработке двух операндов. Авторами выстроенная модель операции криптографической добавления которая обеспечивает двохвохрозря-дне двухоперандных строгое устойчивое криптографическое кодирование. Полученная операция обеспечивает реализацию строгого устойчивого криптографической кодирования при ее применении в потоковых шифрах. Основным преимуществом синтезированной операции над моделью строгого устойчивого криптографической кодирования является простота ее реализации как на аппаратном так и программном уровне. Применяя другие сочетания однооперанних операций строгого устойчивого криптографически преобразования можно получать другие аналогичные двухоперандных операции. **Выводы.** На основе исследования и сочетания одноопернадных операций строгого устойчивого криптографического кодирования синтезированы двохрозрядную двухоперандную операцию строгого устойчивого криптографического преобразования, пригодную для практического применения в поточных и блочных шифрах как на аппаратном так и программном уровне. Предложенный в работе подход позволяет расширить за счет синтеза новых моделей операций строгого устойчивого преобразования, инструментальные средства построения криптопримитивов нового поколения.

Ключевые слова: криптографическое кодирование, криптопреобразования, сложение по модулю два, перестановки, надежность шифрования, строгое устойчивое криптографическое кодирование, синтез операций.

Construction of two-digit two-operand operations of strict and stable cryptographic coding

V. Rudnitsky, N. Lada, I. Fedotova-Piven, M. Pustovit, O. Nesterenko

The purpose of the work is to develop models of two-bit two-operand operations of strictly stable cryptographic transformation suitable for practical application in current and block ciphers. **Results.** The main criterion for strictly stable encryption is to achieve maximum uncertainty of encryption results at minimal cost. However, single-operand operations, despite the fact that they meet the criterion of strictly stable coding, do not have wide application in cryptographic algorithms. This is due to the fact that they are single-operand. For practical application of these results, it is advisable to adapt them to the processing of two operands. The authors constructed a cryptographic add-on operation model that provides a two-part two-operand-day two-operand strictly stable cryptographic encoding. The resulting operation provides the implementation of strict, stable cryptographic encoding when used in stream ciphers. The main advantage of the synthesized operation over the model of strictly stable cryptographic coding is the simplicity of its implementation, both at the hardware and software level. By using other combinations of single-operand operations of a strictly stable cryptographic transformation, other similar two-operand operations can be obtained. **Conclusions**. On the basis of research and a combination of one-operand operations of strict and stable cryptographic coding, a two-digit two-operand operation of a strict, stable cryptographic transformation, suitable for practical application in stream and block cipher both on the hardware and software level, is synthesized. The proposed approach allows expanding, due to the synthesis of new models of operations of strict and stable transformation, instrumental means of constructing new generation crypto primitives.

Keywords: cryptographic coding, cryptographic transformation, adding by module of two, permutations, encryption reliability, strict cryptographic encryption, synthesis of operations.