INFORMATION TECHNOLOGY

Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування

Н. В. Лада [1]*, Р. В. Бреус [1], С. В. Лада [2]

[1] Черкаський державний технологічний університет, Черкаси, Україна
[2]Управління Державної служби України з надзвичайних ситуацій у Черкаській області, Черкаси, Україна
*Corresponding author. E-mail: Ladanatali256@gmail.com

Paper received 14.08.20; Accepted for publication 28.08.20.

https://doi.org/10.31174/SEND-NT2020-238VIII29-05

Анотація. В статті показано і доведено, що ідентичне перетворення другого операнда операцій криптоперетворення модифікує пряму операцію та синтезує обернену операцію до модифікованої. Випадковий вибір одноопераднних операцій для перетворення другого операнда двохопераднної операції забезпечує випадкову модифікацію операцій криптоперетворення. Таким чином, була отримана можливість одночасної генерації моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого кодування для підвищення стійкості і надійності потокового шифрування.

Ключові слова: *комп'ютерна криптографія, криптографічне кодування; строге стійке криптографічне кодування; синтез операцій; варіативність крипто алгоритмів.*

Вступ. Однією з головних тенденцій розвитку сучасного суспільства є формуванням глобального інформаційного простору. Розвиток глобальних світових інформаційно-телекомунікаційних систем та мереж призвів до значного збільшення інформаційних потоків і відповідно до потреби формування принципово нових технологій і засобів інформаційної комунікації. Зростання кількості та цінності інформації, що передається, прямопропорційно впливає на зростання потреб в інформаційній безпеці. Якісний захист інформації стає надзвичайно важливим.

Особливе значення при захисті важливої для держави та фізичних і юридичних осіб інформації набуває впровадження нових перспективних напрямів розвитку комп'ютерної криптографії [1]. Один з таких напрямів полягає у створенні, на основі логічних операцій криптоперетворення, нових швидкодіючих алгоритмів. Даний підхід забезпечує збільшення криптостійкості за рахунок значного збільшення кількості операцій і відповідно -варіативності алгоритмів криптоперетворення [2].

Велика кількість операцій криптоперетворення дозволила будувати методи синтезу операцій з наперед заданими властивостями [2]. До таких операцій можна віднести операції строгого стійкого криптографічного кодування (ССК). Слід зазначити, що операції строгого стійкого криптографічного кодування є придатними для використання як в потоковому так і в блоковому шифруванні [3]. Крім того, використання криптоопераций, які відповідають критерію строгого стійкого криптографічного кодування забезпечує максимальну невизначеність результатів шифрування [4].

Аналіз останніх досліджень і публікацій.

Одними з найперших робіт, присвячених синтезу та аналізу операцій за критерієм строгого стійкого кодування для побудови алгоритмів криптоперетворення є роботи [5-6]. В роботі [7] зазначено, що за рахунок синтезу значної кількості операцій криптографічного перетворення за критерієм ССК можливо забезпечити такий вибір моделей криптоперетворення інформації, при якому характеристики результатів перетворення не погіршаться, моделі будуть мати невелику складність, а час крипто перетворення зменшиться. Метод синтезу операцій криптографічного перетворення за критерієм ССК, на основі мінімальної відстані за Хеммінгом представлено в роботі [8]. В роботі [9] встановлено, що критерію ССК може відповідати лише невелика частина операцій криптоперетворення. Наприклад, серед дворозряних операцій їх лише чотири.

Подальші роботи присвячені побудові нових, придатних для практичного застосування операцій криптографічного перетворення за критерієм строгого стійкого кодування більшої розрядності [10-12], а також побудові обернених операцій [13-14]. Проте на даний час окремо розглядалися методи синтезу прямих і обернених операцій. Одночасна модифікація прямих і обернених операцій ССК не розглядалася.

Метою даної статті є дослідження можливості одночасної генерації моделей прямих і обернених двохрозрядних двохоперандних операцій ССК на основі перетворення другого операнда.

Результати та їх обговорення.

Дослідимо можливість одночасної генерації моделей прямих і обернених двохрозрядних двохоперандних операцій ССК шляхом перетворення другого операнда за допомогою одноопераднних операцій.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного кодування інформації O_1^k [7].

Наприклад $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ де x і k - перший та другий операнди операції відповідно, а нижніми індексами позначені розряди біт операндів. Тоді обернену їй операцію можна представити як [7]:

$$O_1^{k/} = O_1^d = O_2^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} \quad (1)$$

Нехай над другим операндом операції O_1^k буде виконано одноопераднде перетворення F_1. Нехай

$F_1 = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$, де y_1 і y_2 - перший і другий біти операнда.

В результаті виконання одноопераднодної операції над другим операндом буде реалізована підстановка $k_1 = y_1 \oplus y_2$ і $k_2 = y_2$. В результаті виконання даної підстановки отримаємо іншу операцію кодування O_2^k :

$$F_1(O_1^d) = \begin{bmatrix} x_1 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \oplus x_2 \cdot ((y_1 \oplus y_2) \oplus y_2) \\ x_1 \cdot ((y_1 \oplus y_2) \oplus y_2) \oplus x_2 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_2^d \cdot$$

Виходячи з того, що $O_1^d = O_2^k$, $O_2^d = O_1^k$ то можна стверджувати, що $F_1(O_1^k) = F_1(O_2^d)$. Тобто виконання одноопераднодного перетворення другого операнда в операціях кодування і декодування забезпечує побудову другої операції кодування і відповідної їй операції декодування.

Перевіримо дане твердження на прикладі перетворення другого операнда операції O_2^k за допомогою тієї самої одноопераднодної операції F_1.

$$F_1(O_2^d) = \begin{bmatrix} x_1 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \oplus x_2 \cdot ((y_1 \oplus y_2) \oplus y_2) \\ x_1 \cdot ((y_1 \oplus y_2) \oplus y_2) \oplus x_2 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^d$$

Перевіримо отриманий результат при використанні іншої одноопераднодної операції F_2

Нехай $F_2 = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$. Тоді В результаті виконання одноопераднодної операції над другим операндом операції O_1^k буде реалізована підстановка $k_1 = y_2$ і $k_2 = y_1 \oplus y_2$. В результаті виконання даної підстановки отримаємо іншу операцію кодування O_3^k :

$$F_2(O_1^k) = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{y_1 \oplus y_2} \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = O_3^k \cdot$$

$$F_2(O_2^k) = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus (y_1 \oplus y_2))} \oplus x_2 \cdot (y_2 \oplus (y_1 \oplus y_2)) \\ x_1 \cdot (y_2 \oplus (y_1 \oplus y_2)) \oplus x_2 \cdot (y_2 \oplus (y_1 \oplus y_2)) \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{y_1 \oplus y_2} \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = O_4^k = O_3^d$$

Виконаємо аналогічне перетворення над операцією декодування O_2^d :

$$F_2(O_2^d) = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{y_1 \oplus y_2} \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = O_4^d = O_3^k$$

Таким чином отримуємо наступну пару двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, які виконують пряме і обернене перетворення інформації.

$$F_1(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2)} \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot \overline{(y_1 \oplus y_2)} \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_2^k \cdot$$

Виконаємо аналогічне одноопераднодне перетворення над операцією декодування O_1^d . В результаті перетворення отримаємо іншу операцію декодування O_2^d :

$$F_1(O_2^k) = \begin{bmatrix} x_1 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \oplus x_2 \cdot ((y_1 \oplus y_2) \oplus y_2) \\ x_1 \cdot ((y_1 \oplus y_2) \oplus y_2) \oplus x_2 \cdot (\overline{(y_1 \oplus y_2) \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k$$

Як бачимо, перевірка дала позитивний результат. Також необхідно перевірити вищезазначене твердження на прикладі операції декодування O_2^d за допомогою тієї самої одноопераднодної операції F_1.

Виконаємо аналогічне перетворення над операцією декодування O_1^d :

$$F_2(O_1^d) = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus (y_1 \oplus y_2) \\ \overline{y_2 \oplus (y_1 \oplus y_2)} \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_3^d$$

Для чистоти експерименту також перевіримо дане твердження на прикладі прямого та оберненого перетворення другого операнда операції O_2^k за допомогою одноопераднодної операції F_2.

Висновки. В процесі проведення досліджень було отримано можливість одночасної побудови пар операцій, які забезпечують пряме і обернене криптографічного перетворення інформації. Таким чином, була отримана можливість одночасної генерації моделей прямих і обернених двохрозрядних двохоперандних операцій ССК на основі перетворення другого операнда для підвищення стійкості і надійності потокового шифрування.

ЛІТЕРАТУРА

1. В.М. Рудницький, Н.В. Лада, І.М. Федотова-Півень, М.О. Пустовіт, О.Б. Нестеренко. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування// Системи управління, навігації та зв'язку. Збірник наукових праць, 2018. IV, Is. 52. С. 113-115.

2. Р.В. Бреус. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда //Системи управління, навігації та зв'язку. Збірник наукових праць, 2019. V. С. 29-32.

3. В.Н. Рудницький. Криптографічне кодування: обробка та захист інформації: колективна монографія. //Харків: ТОВ «ДІСА ПЛЮС», 2018, 139 с.
4. В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О. Г. Мельник. Криптографическое кодирование: методы и средства реализации (часть 2): монография //Х.: Изд-во «Щедрая усадьба плюс», 2014, 224 с.
5. Рудницкий В.Н., Пивнева С.В., Бабенко В.Г., Миронец И.В. и др. Криптографическое кодирование: методы и средства реализации: монография // Тольят. гос. ун-т, 2013, 196 с.
6. В. М. Рудницький, Л. А. Шувалова, О. Б. Нестеренко. Аналіз дворозрядних операцій криптографічного кодування по критерію строгого лавинного ефекту // Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія". Серія : Комп'ютерні технології, 2016, 283, Is. 271. С. 74-77.
7. В. М. Рудницький, Л.А. Шувалова, О. Б. Нестеренко. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування // Вісник інженерної академії України: часопис (Київ), 2016, Is. 3. С. 105–108.
8. В. М. Рудницький, Л. А.Шувалова, О. Б.Нестеренко. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування // Вісник Черкаського державного технологічного університету. Серія: Технічні науки, 2017, I, С. 5–10.
9. В. М. Рудницький, Л. А. Шувалова, О. Б. Нестеренко. Побудова примітивів строгого стійкого кодування мінімальної складності. // Вісник Черкаського державного технологічного університету. Серія: Технічні науки, 2018. I, С. 21–26.
10. В.М. Рудницький, Н.В. Лада, І.М.Федотова-Півень, М.О.Пустовіт, О.Б. Нестеренко. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування // Системи управління, навігації та зв'язку. Збірник наукових праць, 2018. IV, Is. 52, С. 113–115.
11. І.М. Федотова-Півень, Н.В. Лада, Г.В. Канашевич, М.О.Пустовіт. Технологія побудови двохоперандної чотирьохрозрядної операції мінімальної складності для строгого стійкого криптографічного кодування // Системи управління, навігації та зв'язку. Збірник наукових праць, 2019. IV, Is. 56. С. 95-99.
12. V. Rudnytskyi, I. Opirskyy, O. Melnyk, M. Pustovit The implementation of strict stable cryptographic coding operations // Сучасні інформаційні системи, 2019. III(3). С. 109-112.
13. В.М. Рудницький, Н.В. Лада, І.М. Федотова-Півень, М.О. Пустовіт. Синтез обернених дворозрядних двохоперандних операцій строгого стійкого криптографічного кодування //Системи та методи обробки інформації. Збірник наукових праць. Київ: ДНДІ МВС України, 2018. IV, Is.55. С. 76–81.
14. Rudnitsky V., Berdybaev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation //Сучасні інформаційні системи, 2019, III (4), С. 109-114.

REFERENCES

1. V.M. Rudnytsky, N.V. Lada, I.M. Fedotova-Piven, M.O. Pustovit, O.B. Nesterenko. Construction of two-digit two-operand operations of strict stable cryptographic coding // Control, navigation and communication systems. Collection of scientific works, 2018. IV, Is. 52. pp. 113-115.
2. R.V. Breus. Synthesis of two-bit two-operand operations of a strict stable cryptographic coding by the second operand's conversion // Control, Navigation and Comunication Systems. Collection of scientific works, 2019. V,pp. 29-32.
3. V.N. Rudnitsky. Cryptographic coding: information processing and protection: a collective monograph. // Kharkiv: "DISA PLUS", LLC, 2018, 139 p.
4. V.N. Rudnitsky, V.Y. Milchevich, B.Г. Babenko, R.P. Мельник, S.V. Rudnitsky, O.G. Melnik. Cryptographic coding: methods and means of implementation (part 2): monograph // Kh .: Publishing house "Generous estate plus", 2014, 224 p.
5. Rudnytsky V.N., Pivneva S.V., Babenko V.G., Myronets I.V., etc. Cryptographic coding: methods and means of implementation: monograph // Togliatti State University, 2013, 196 p.
6. V. M. Rudnitsky, L. A. Shuvalova, O. B. Nesterenko. Analysis dorasdaddy operations of cryptographic encoding according to the criterion of the strict avalanche effect// Scientific works of the Petro Mohyla Black Sea State University of the Kyiv-Mohyla Academy complex. Series: Computer Technology, 2016, 283, Is. 271. pp. 74-77.
7. V. M. Rudnitsky, L. A. Shuvalova, O. B. Nesterenko. Rudnytskyi, V. M., Shuvalova, L. A. and Nesterenko, O. B. (2016) The synthesis of cryptographic conversion operations according to the criterion of strict sustainable coding // Visnyk inzhenernoi akademii Ukrainy, 2016, Is. 3, pp. 105–108.
8. V. M. Rudnitsky, L. A. Shuvalova, O. B. Nesterenko. The method of synthesis of cryptographic conversion operations according to the criterion of strict sustainable coding // Bulletin of Cherkasy State Technological University. Series: Technical Sciences, 2017, I, pp. 5–10.
9. V. M. Rudnitsky, L. A. Shuvalova, O. B. Nesterenko. Creation of primitives of strict sustainable coding of minimal complexity // Bulletin of Cherkasy State Technological University. Series: Technical Sciences, 2018. I, pp. 21–26.
10. V. M. Rudnitsky, N.V. Lada, I.M. Fedotova-Piven, M.O. Pustovit, O.B. Nesterenko. Construction of two-digit two-operand operations of strict and stable cryptographic coding // Control, Navigation and Comunication Systems. Collection of scientific works, 2018. IV, Is. 52, pp. 113–115.
11. I.M. Fedotova-Piven, N.V. Lada, G.V. Kanashevych, M.O. Pustovit. The technology of building a two-operand four-bit operation of minimal complexityfor strictly sustainable cryptographic coding// Control, Navigation and Comunication Systems. Collection of scientific works, 2019. IV, Is. 56, pp. 95-99.
13. V.M. Rudnitsky, N.V. Lada, I.M. Fedotova-Piven, and M.O. Pustovit. 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,IV, Is.55, pp. 76–81.

Generation of models of direct and inverse two-bit two-operand operations of strict stable cryptographic coding

N. V. Lada, R. V. Breus, S. V. Lada

Abstract. The article shows and proves that the identical transformation of the second operand of cryptocurrency operations modifies the direct operation and synthesizes the inverse operation to the modified one. Random selection of single-operand operations to convert the second operand of a two-operand operation provides a random modification of crypto-conversion operations. Thus, it was possible to simultaneously generate models of direct and inverse two-bit two-operand operations of strict stable coding to increase the stability and reliability of streaming encryption.

Keywords: *computer cryptography, cryptographic coding; strict stable cryptographic coding; synthesis of operations; variability of cryptoalgorithms.*