УДК 004.056

В. М. Рудницький[1], *д.т.н, професор*
e-mail: rvn_2008@ukr.net
Л. А. Шувалова[1], *к.т.н, доцент*
e-mail: shuvalova-l2015@yandex.ru
О. Б. Нестеренко[2], *ад'юнкт*
e-mail: nesterenko.apb@gmail.com
[1]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2]Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля
Національного університету цивільного захисту України
вул. Онопрієнка, 8, м. Черкаси, 18034, Україна

ПОБУДОВА ПРИМІТИВІВ СТРОГОГО СТІЙКОГО КОДУВАННЯ МІНІМАЛЬНОЇ СКЛАДНОСТІ

У статті представлено результати побудови повної множини чотирирозрядних математичних моделей строгого стійкого кодування мінімальної складності. Досліджено та побудовано метод синтезу алгоритму мінімальної складності побудови операцій строгого стійкого кодування. Цей метод полягає в тому, що проводиться попарне інвертування деякої кількості розрядів та інвертується половина розрядів вхідної інформації, при цьому враховуються обмеження, що в кожній парі переставлених розрядів може інвертуватися лише один розряд. Для забезпечення мінімальної складності технічної реалізації отримано залежності для розрахунку кількості операцій строгого стійкого кодування.

Ключові слова: *Інтернет речей, конфіденційність доступу, криптографічне перетворення інформації, математична модель.*

Постановка проблеми. Розвиток комп'ютерних систем та мереж привів до значного збільшення потоків обміну інформацією. Останнім часом активно розвивається Інтернет речей.

Інтернет речей (Internet of Things, скорочено – IoT) – це концепція комунікації об'єктів («речей»), які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція припускає виконання пристроями певних дій без втручання людини. Таким чином, всі пристрої в будинках, в автомобілях, на користувачеві виконують обробку інформації, її аналіз та обмін між собою і, залежно від результатів, приймають рішення і виконують певні дії. Сфера IoT – один із головних світових трендів. Звичні пристрої стають частиною Інтернет-мережі і виконують нові функції. Для реалізації IoT необхідна система, яка включала б у себе «розумні речі» – пристрої, оснащені датчиками; мережу доступу і передачі інформації (мобільну або фіксовану); а також платформи для управління мережею, пристроями і додатками.

Але для широкого впровадження IoT необхідна конфіденційність доступу і управління. Адже перехоплення управління IoT може призвести до небажаних результатів і створити передумови загрози матеріальним цінностям і навіть життю людей.

Виходячи з цього, захист конфіденційної інформації управління IoT є актуальним. Вирішення цієї задачі лежить у межах проблеми забезпечення якості захисту каналів передачі конфіденційної управлінської інформації.

Аналіз останніх досліджень і публікацій. В [1] визначено в групі дворозрядних операцій криптографічного кодування операції, які гарантовано забезпечують зміну половини бітів вхідної інформації. Розглянуто можливість досягнення строгого лавинного ефекту операціями, які відповідають критерію строгого стійкого кодування, для чого представлено таку послідовність наборів дворозрядних даних, щоб два сусідні набори, а та-

кож перший і останній набори відрізнялися лише одним розрядом. Повторне виконання операцій криптографічного кодування призводить до невідповідності результатів кодування критерію строгого лавинного ефекту.

В [2] для дворозрядних операцій криптографічного перетворення інформації неможливо на основі перебору провести аналіз на строге стійке кодування. Забезпечено побудову операцій з заданими властивостями без необхідності проведення і дослідження на основі повного перебору, використавши таблицю мінімальних кодових відстаней за Хеммінгом для побудови операцій криптографічних перетворень, які відповідають критерію строгого стійкого кодування,

В [3] представлено результати дослідження та розробки методу синтезу операцій криптографічного перетворення, які відповідають критерію строгого стійкого кодування, на основі мінімальної відстані за Хеммінгом. Представлення цих операцій дискретними моделями забезпечує мінімальний час їх реалізації на апаратному та програмному рівнях. Крім того, ці операції забезпечать заміну таблиць підстановок дискретними моделями, що значно знизить вимоги до обсягу пам'яті спеціалізованих обчислювальних систем, оскільки втрачається необхідність збереження великої кількості таблиць перестановок. Можливість синтезу великої кількості операцій криптографічного перетворення за критерієм строгого стійкого кодування забезпечує можливість вибирати моделі невеликої складності, які забезпечать криптографічне перетворення інформації з меншим часом при тих самих характеристиках результатів перетворення.

Мета статті – розробити метод синтезу груп операцій строгого стійкого кодування найменшої складності та оцінити його потужність.

Аналіз публікацій [1–3] показав, що моделі криптографічного строгого стійкого кодування мають найменшу складність тоді, коли вони базуються лише на перестановках та інверсіях. Група дворозрядних операцій строгого стійкого кодування включає в себе чотири операції:

$$F_1 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}; \quad F_2 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix};$$

$$F_3 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}; \quad F_4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix};$$

Аналогічні операції строгого стійкого кодування, побудовані на перестановках, відомі для чотирьох розрядів:

$$F_1 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}; \quad F_2 = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \end{bmatrix};$$

$$F_3 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}; \quad F_4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix};$$

Виходячи з наведених моделей, можна зробити попередній висновок, що для отримання алгоритму строгого стійкого кодування можна використати операції інверсії та перестановки. При цьому половина розрядів вхідної інформації повинна бути інвертована.

Для підтвердження і уточнення цієї ідеї проведемо обчислювальний експеримент, суть якого полягає у використанні повної групи перестановок для чотирьох розрядів та інвертуванні половини розрядів вхідної інформації (50 перестановок).

Виходячи з цього, можна зробити прогноз, що максимальна кількість n-розрядних операцій строгого стійкого кодування мінімальної складності буде обраховуватись за виразом

$$K_{n,сск} = n! \cdot C_n^{n/2}$$

де $C_n^{n/2}$ – кількість сполучень з n по $n/2$.

Тоді кількість дворозрядних операцій строгого стійкого кодування буде визначатися як $K_{2,сск} = 2! \cdot C_2^1 = 4$, а чотирирозрядних – виразом $K_{4,сск} = 4! \cdot C_4^2 = 144$.

Перевіримо і уточнимо кількісні та якісні характеристики за результатами обчислювального експерименту.

Формалізовані результати обчислювального експерименту наведені в табл. 1.

Таблиця 1

Формалізовані результати обчислювального експерименту

№ п/п	Операція	№ п/п	Операція	№ п/п	Операція
1	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \end{bmatrix}$	2	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	3	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$
4	$F=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	5	$F=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$	6	$F=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$
7	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \\ x_2 \end{bmatrix}$	8	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_4 \\ x_3 \\ x_2 \oplus 1 \end{bmatrix}$	9	$F=\begin{bmatrix} x_1 \\ x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \end{bmatrix}$
10	$F=\begin{bmatrix} x_1 \\ x_4 \\ x_3 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	11	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	12	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$
13	$F=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	14	$F=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$	15	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \end{bmatrix}$
16	$F=\begin{bmatrix} x_1 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \end{bmatrix}$	17	$F=\begin{bmatrix} x_1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \end{bmatrix}$	18	$F=\begin{bmatrix} x_1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$
19	$F=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	20	$F=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$	21	$F=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$
22	$F=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$	23	$F=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	24	$F=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$
25	$F=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	26	$F=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$	27	$F=\begin{bmatrix} x_3 \oplus 1 \\ x_4 \oplus 1 \\ x_1 \\ x_2 \end{bmatrix}$
28	$F=\begin{bmatrix} x_3 \oplus 1 \\ x_4 \\ x_1 \\ x_2 \oplus 1 \end{bmatrix}$	29	$F=\begin{bmatrix} x_3 \\ x_4 \oplus 1 \\ x_1 \oplus 1 \\ x_2 \end{bmatrix}$	30	$F=\begin{bmatrix} x_3 \\ x_4 \\ x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$

Продовження табл. 1

31	$F=\begin{bmatrix} x_3 \oplus 1 \\ x_2 \oplus 1 \\ x_1 \\ x_4 \end{bmatrix}$	32	$F=\begin{bmatrix} x_3 \oplus 1 \\ x_2 \\ x_1 \\ x_4 \oplus 1 \end{bmatrix}$	33	$F=\begin{bmatrix} x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_4 \end{bmatrix}$
34	$F=\begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$	35	$F=\begin{bmatrix} x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \end{bmatrix}$	36	$F=\begin{bmatrix} x_4 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \end{bmatrix}$
37	$F=\begin{bmatrix} x_4 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \oplus 1 \end{bmatrix}$	38	$F=\begin{bmatrix} x_4 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	39	$F=\begin{bmatrix} x_4 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \end{bmatrix}$
40	$F=\begin{bmatrix} x_4 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \end{bmatrix}$	41	$F=\begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \end{bmatrix}$	42	$F=\begin{bmatrix} x_4 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Отже, якщо не відбуваються перестановки, то інвертуватися можуть два будь-які біти. Інвертуватися може розряд, який не переставлявся. Якщо два біти переставити місцями, то інвертуватися може лише один із них. Якщо переставити місцями три біти, то операцію строгого стійкого кодування отримати не можна при будь-якому інвертуванні.

Метод синтезу алгоритму мінімальної складності побудови операцій строгого стійкого кодування полягає в наступному: проводиться попарне інвертування деякої кількості розрядів та інвертується половина розрядів вхідної інформації, враховуючи при цьому обмеження, що в кожній парі переставлених розрядів може інвертуватися лише один розряд.

Уточнимо кількість операцій, які відповідають критерію строгого стійкого кодування. При застосовуванні лише операції інверсії без застосування операцій перестановки можна отримати операції критерію строгого стійкого кодування, кількість яких визначається наступним чином: для дворозрядного коду кількість операцій визначається за виразом C_2^1, для чотирирозрядного коду – C_4^2, для шестирозрядного коду – C_6^3, для n-розрядного коду за умови, що n – парне число, – $C_n^{\frac{1}{2}n}$.

Для чотирирозрядного коду при виконанні однієї перестановки кількість варіантів перестановок буде дорівнювати C_4^2, при цьому, відповідно до розробленого методу синтезу один із переставлених розрядів повинен бути інвертованим, тому кількість операцій з однією і тією ж перестановкою буде збільшена вдвічі, тому що кожна з операцій відрізняється вибором розряду, який інвертується. Кількість інверсій розрядів, які не переставлялися, для кожної перестановки при одній перестановці менша від загальної кількості інверсій і дорівнюватиме C_2^1. Загальна кількість чотирирозрядних операцій з однією перестановкою визначається як $2 \cdot C_4^2 \cdot C_2^1$. Тоді для шестирозрядного коду кількість операцій з однією перестановкою визначається як $2 \cdot C_6^2 \cdot C_4^2$.

В загальному вигляді кількість n-розрядних операцій строгого стійкого кодування, в яких наявна одна перестановка, буде визначатись як добуток подвоєної кількості перестановкою двох розрядів $\left(2C_n^2\right)$, і кількість інверсій для кожної перестановки розраховується як $C_{n-2}^{\frac{1}{2}(n-2)}$. Виходячи з цього, кількість операцій строгого стійкого кодування, в яких наявна одна перестановка, визначається як $2 \cdot C_n^2 \cdot C_{n-2}^{\frac{1}{2}(n-2)}$.

За аналогією, кількість n-розрядних операцій строгого стійкого кодування, в яких

наявні дві перестановки, буде визначатись як $4 \cdot C_n^2 \cdot C_{n-2}^2 \cdot C_{n-4}^{\frac{1}{2}(n-4)}$

Виходячи з цього, в загальному вигляді кількість операцій *n*-розрядного коду може бути розрахована за таким виразом:

$$C = C_n^{\frac{1}{2}n} + 2^1 \cdot C_{n-2}^2 \cdot C_{n-2}^{\frac{1}{2}(n-2)} + 2^2 \cdot C_n^4 \cdot C_{n-2}^{\frac{1}{2}(n-2)} \cdot C_{n-4}^{\frac{1}{2}(n-4)} + \ldots + 2^k \cdot C_n^{2k} \cdot C_{n-2k}^{\frac{1}{2}(n-2k)},$$

при $0 < k \le \frac{1}{2}n$.

Отриманий вираз дає можливість зробити приблизне оцінювання кількості операцій, що забезпечують строге стійке кодування, які отримані на основі запропонованого методу.

Висновки. Побудовано повну множину чотирирозрядних математичних моделей строгого стійкого кодування мінімальної складності. Запропоновано метод синтезу операцій строгого стійкого кодування мінімальної складності. Отримано залежності для розрахунку кількості операцій строгого стійкого кодування, які забезпечать мінімальну складність технічної реалізації.

Список літератури

1. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. *Наукові праці:* наук.-метод. журн. Чорноморськ. держ. ун-ту імені Петра Могили. Миколаїв, 2017.
2. Рудницький В. М., Шувалова Л.А., Нестеренко О. Б. 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 Черкаського державного технологічного університету*. *Серія: Технічні науки.* 2017. Вип. 1. С. 5–10.
4. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації:* тези доп. IV міжнар. наук.-техн. конф., 3-4 листопада 2016 р. Черкаси: ЧДТУ; Баку: ВА ЗСАР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. С. 14.
5. Яковлев А. В., Безбогов А. А., Родин В. В., Шамкин В. Н. Криптографическая защита информации. Тамбов: Изд-во ТГТУ, 2006. 140 с.
6. Бабаш А. В., Шанкин Г. П. Криптография. Аспекты защиты. Москва: Солон-Р, 2002. 512 с.
7. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України:* наук.-техн. журн. Харків: ХУПС ім. І. Кожедуба. 2011. Вип. 2 (6). С. 112–114.
8. Mollin Richard A. Codes: the guide to secrecy from ancient to modern times. Chapman & Hall/CRC, 2005. P. 142.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва: Триумф, 2002. 816 с.

References

1. Rudnytskyi, V. M., Shuvalova, L. A. and Nesterenko, O. B. (2017) Analysis of two-digit operations of cryptographic coding according to the criterion of strict avalanche effect. *Naukovi pratsi:* sci.-method. journal of Chornomorsk State University named by Petro Mohyla [in Ukrainian].
2. 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*, (3), pp. 105–108 [in Ukrainian].
3. Rudnytskyi, V. M., Shuvalova, L. A. and Nesterenko, O. B. (2017) Method of synthesis of operations of cryptographic transformation according to the criterion of strict sustainable coding. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, (1), pp. 5–10 [in Ukrainian].
4. Shuvalova, L. A. and Nesterenko, O. B. (2016) Synthesis and analysis of cryptographic operations according to the criterion of strict sustainable coding. In: *the 4th Interdisciplinary Sci.-Tech. Conf.*

«Problems of informatization». Cherkasy, Baku, Belsko-Biala, Poltava, p. 14 [in Ukrainian].
5. Iakovlev, A. V., Bezbogov, A. A., Rodin, V. V. and Shamkin, V. N. (2006) Cryptographic protection of information. Tambov: Izd-vo TGTU, 140 p. [in Russian].
6. Babash, A. V. and Shankyn, H. P. (2002) Cryptography. Aspects of protection. Moscow: Solon-R. 512 p. [in Russian].
7. Rudnytskyi, V. M., Babenko, V. G. and Zhyliaiev, D. A. (2011) Algebraic structure of the set of logical operations coding. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy:* sci.-tech. journal, (2), pp. 112–114 [in Ukrainian].
8. Mollin, R. A. (2005) Codes: the guide to secrecy from ancient to modern times. Chapman & Hall/CRC, p. 142.
9. Shnaier, B. (2002) Applied cryptography. Protocols, algorithms, source texts in C language. Moscow: Tryumf, 816 p. [in Russian].

V. M. Rudnitskyi[1], *Dr.Tech.Sc., professor*
e-mail: rvn_2008@ukr.net
L. A. Shuvalova[1], *Ph.D., associate professor*
e-mail: shuvalova-l2015@yandex.ru
O. B. Nesterenko[2], *advanced student in military academy*
e-mail: nesterenko.apb@gmail.com
[1]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
[2]Cherkasy Institute of Fire Safety named after Chornobyl Heroes of National University of Civil Defense of Ukraine
Onopriienko str, 8, Cherkasy, 18034, Ukraine

CREATION OF PRIMITIVES OF STRICT SUSTAINABLE CODING OF MINIMAL COMPLEXITY

The article presents the results of constructing a complete set of four-digit mathematical models of strict sustainable coding of minimal complexity. The method of synthesis of the algorithm of minimal complexity for construction of operations of strict sustainable coding is investigated and constructed.

This method consists in the fact that pair-wise inverting of a certain number of digits is performed and a half of digits of the input information is inverted, while taking into account the limitations that only one digit can be inverted in each pair of transposed digits. To ensure the minimum complexity of technical implementation, dependencies have been obtained for calculating the number of operations of strict sustainable coding.

Key words: *Internet of Things, confidentiality of access, cryptographic information transformation, mathematical model.*

Стаття надійшла 20.02.2018.

Статтю представляє В. М. Рудницький, д.т.н., професор.