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

МЕТОД СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КОДУВАННЯ

В статті представлено результати дослідження та побудови 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 рівні. 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.

Ключові слова: *криптографічне перетворення інформації; критерій строгого стійкого кодування, таблиця перестановок, дискретна модель.*

Постановка проблеми. На сьогодні в інформаційному просторі швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Проблема забезпечення необхідного рівня захисту інформації є досить складною, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних та організаційних заходів і застосування специфічних методів і засобів, а створення цілісної системи організаційних заходів і застосування специфічних методів та засобів захисту інформації [1]. Особливо важливим є захист інформації в комп'ютерних системах та мережах.

Захист інформації повинен забезпечувати попередження завдання шкоди внаслідок втрати (розкрадання, знищення, перекручування, підробки) інформації в будь-якому її вигляді. Щоб гарантувати високий ступінь захисту інформації, необхідно постійно вирішувати складні науково-технічні завдання розробки та вдосконалення засобів її захисту [2].

Серед усього спектра методів захисту даних від несанкціонованого доступу особливе місце займають криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання. Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії [3, 4].

Тому актуальною є розробка криптографічних алгоритмів захисту інформації, які забезпечать максимальну криптостійкість.

Побудова алгоритмів комп'ютерної криптографії базується на використанні операцій криптографічного перетворення інформації. Побудова операцій, які забезпечують строге стійке кодування, приведе до підвищення якості криптографічних алгоритмів та швидкості їх реалізації.

Аналіз останніх досліджень і публікацій. В попередніх дослідженнях проведено аналіз повної групи дворозрядних криптографічних операцій [5, 6, 7]. Узагальнено дослідження груп математичних операцій матричного криптографічного перетворення та розширеного матричного криптографічного перетворення.

Встановлено, що критерію строгого стійкого кодування відповідає лише незначна частина операцій. Серед дворозряних операцій їх лише чотири [8].

Виходячи з цього, стає актуальною задача побудови операцій криптографічного перетворення, які відповідають критерію строгого стійкого кодування, з більшою розрядністю.

Мета статті – побудувати метод синтезу операцій криптографічного перетворення, які відповідають критерію строгого стійкого кодування.

Виклад основного матеріалу. Однією з характеристик криптоалгоритмів є лавинний ефект – поняття в криптографії, яке зазвичай застосовується до блочних шифрів та хеш-функцій. Це важлива криптографічна властивість для шифрування, яка означає, що зміна значення малої кількості бітів у вхідному тексті або в ключі веде до «лавинної» зміни значень вихідних бітів шифротексту.

В алгоритмах з декількома проходами лавинний ефект зазвичай досягається завдяки тому, що на кожному проході зміна одного вхідного біта веде до декількох вихідних [9].

В операціях, які відповідають критерію строгого стійкого кодування, зміна одного розряду вхідної інформації приводить до зміни одного розряду результату, тобто до зміни вихідних бітів з ймовірністю ½.

Представивши таку послідовність наборів дворозрядних даних, щоб два сусідні набори, а також перший і останній набори відрізнялися лише одним розрядом, отримаємо можливість досягнення строгого лавинного ефекту операціями, які відповідають критерію строгого стійкого кодування.

Результат виконання операцій криптографічного кодування в другому раунді не відповідає критерію строгого стійкого кодування, отже, такі операції доцільно використовувати в одному раунді шифрування.

Встановлено, що для дворозрядних операцій криптографічного перетворення інформації неможливо на основі перебору провести аналіз на строге стійке кодування. Використавши таблицю мінімальних кодових відстаней за Хеммінгом для побудови операцій криптографічних перетворень, які відповідають критерію строгого стійкого кодування, забезпечено побудову операцій з заданими властивостями без необхідності проведення їх дослідження на основі повного перебору [10].

Узагальнення отриманих результатів створює можливість побудови методу синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування.

Отримати строге стійке кодування можна тоді, коли кількість розрядів парна.

В результаті дослідження групи дворозрядних операцій криптографічного перетворення було встановлено, що строге стійке кодування можливе лише тоді, коли мінімальна кодова відстань за Хеммінгом між результатами перетворення буде дорівнювати одиниці. Спираючись на це, можна допустити, що для забезпечення строгого стійкого кодування чотирирозрядних кодів мінімальна кодова відстань за Хеммінгом повинна дорівнювати 2, для шестирозрядних кодів – 3 і т. д., тобто ½ довжини розряду.

Знайти в явному вигляді результати перетворення, які відповідають критерію строгого стійкого кодування можна на основі використання таблиць мінімальних кодових відстаней за Хеммінгом.

Розглянемо приклади знаходження результатів перетворення на основі таблиць мінімальних кодових відстаней за Хеммінгом. Мінімальні кодові відстані для чотирьох розрядів представлені в табл. 1.

Таблиця 1

Таблиця мінімальних кодових відстаней за Хемінгом для чотирьох розрядів

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	1	1	2	1	2	2	3	1	2	2	3	2	3	3	4
1	1	0	2	1	2	1	3	2	2	1	3	2	3	2	4	3
2	1	2	0	1	2	3	1	2	2	3	1	2	3	4	2	3
3	2	1	1	0	3	2	2	1	3	2	2	1	4	3	3	2
4	1	2	2	3	0	1	1	2	2	3	3	4	1	2	2	3
5	2	1	3	2	1	0	2	1	3	2	4	3	2	1	3	2
6	2	3	1	2	1	2	0	1	3	4	2	3	2	3	1	2
7	3	2	2	1	2	1	1	0	4	3	3	2	3	2	2	1
8	1	2	2	3	2	3	3	4	0	1	1	2	1	2	2	3
9	2	1	3	2	3	2	4	3	1	0	2	1	2	1	3	2
10	2	3	1	2	3	4	2	3	1	2	0	1	2	3	1	2
11	3	2	2	1	4	3	3	2	2	1	1	0	3	2	2	1
12	2	3	3	4	1	2	2	3	1	2	2	3	0	1	1	2
13	3	2	4	3	2	1	3	2	2	1	3	2	1	0	2	1
14	3	4	2	3	2	3	1	2	2	3	1	2	1	2	0	1
15	4	3	3	2	3	2	2	1	3	2	2	1	2	1	1	0

Оскільки у варіантах побудови можуть брати участь тільки перетворення, які мають мінімальну кодову відстань 2, видаливши непотрібні фрагменти таблиці, отримаємо таблицю вибору варіантів побудови (табл. 2).

Таблиця 2

Вибір варіантів побудови

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

При виборі варіантів побудови потрібно визначити таку операцію перетворення, щоб отримати гарантовано мінімальну кодову відстань за Хеммінгом, отже, досягти строгого лавинного ефекту.

Таблиця 3

Вибір варіантів побудови (варіант 1)

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Таблиця 4

Вибір варіантів побудови (варіант 2)

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Таблиця 5

Вибір варіантів побудови (варіант 3)

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Розглянемо більш детально варіанти побудови, представлені в таблиці 6.

Таблиця 6

Варіант 1					Варіант 2					Варіант 3				
3	0	0	1	1	12	1	1	0	0	5	0	1	0	1
2	0	0	1	0	13	1	1	0	1	7	0	1	1	1
1	0	0	0	1	14	1	1	1	0	4	0	1	0	0
0	0	0	0	0	15	1	1	1	1	6	0	1	1	0
7	0	1	1	1	7	0	1	1	1	2	0	0	1	0
6	0	1	1	0	6	0	1	1	0	9	1	0	0	1
5	0	1	0	1	5	0	1	0	1	3	0	0	1	1
4	0	1	0	0	4	0	1	0	0	11	1	0	1	1
11	1	0	1	1	11	1	0	1	1	1	0	0	0	1
10	1	0	1	0	10	1	0	1	0	0	0	0	0	0
9	1	0	0	1	9	1	0	0	1	15	1	1	1	1
8	1	0	0	0	8	1	0	0	0	8	1	0	0	0
15	1	1	1	1	0	0	0	0	0	10	1	0	1	0
14	1	1	1	0	1	0	0	0	1	14	1	1	1	0
13	1	1	0	1	2	0	0	1	0	13	1	1	0	1
12	1	1	0	0	3	0	0	1	1	12	1	1	0	0
$F_1 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$					$F_2 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_3 \\ x_4 \end{bmatrix}$					F_3				

$$F_3 = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_4 \\ \overline{x}_1 \cdot \overline{x}_2 \vee x_1 \cdot x_2 \cdot x_4 \vee x_1 \cdot x_3 \cdot \overline{x}_4 \\ \overline{x}_1 \cdot \overline{x}_2 \cdot x_4 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_4 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \cdot \overline{x}_4 \\ \overline{x}_1 \cdot \overline{x}_3 \cdot x_4 \vee \overline{x}_2 \cdot \overline{x}_3 \cdot \overline{x}_4 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot x_3 \cdot \overline{x}_4 \end{bmatrix}$$

Для побудови операцій строгого стійкого кодування необхідно визначити парну кількість розрядів ($k = 2n$). Оскільки в результаті перетворення мінімальна кодова відстань за Хеммінгом має бути $\frac{1}{2}k$, то $\frac{1}{2}k = n$. Будуємо таблицю мінімальних кодових відстаней за Хемміногом для k -розрядного коду.

Далі потрібно побудувати таблицю вибору варіантів побудови для мінімальної відстані n ; вибрати варіанти побудови 2^k цифр, при цьому коди цифр не повинні повторюватись; мінімізувати таблицю істинності для варіантів побудови; результати мінімізації представляють математичні моделі операцій, які забезпечують строге стійке кодування.

Висновки. Розроблено метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. Представлення цих операцій дискретними моделями забезпечує мінімальний час їх реалізації як на апаратному, так і на програмному рівні. Крім того, слід відзначити, що 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.

Список літератури

1. Венбо Мао. Современная криптография : теория и практика / Мао Венбо ; пер. с англ. – М. : Издательский дом «Вильямс», 2005. –768 с.
2. Малець І. О. Роль та проблеми функціонування телекомунікаційних систем при надзвичайних ситуаціях / І. О. Малець // Електронний науковий архів Науково-технічної бібліотеки Національного університету «Львівська політехніка». – 2011. – Режим доступу до статті : http://ena.lp.edu.ua
3. Криптографическая защита информации / А. В. Яковлев, А. А. Безбогов, В. В. Родин, В. Н. Шамкин. – Тамбов : Изд-во ТГТУ, 2006. – 140 с.
4. Соколов В. Ю. Інформаційні системи і технології: навч. посіб. / В. Ю. Соколов. – К. : Вид-во ДУІКТ, 2010. – 138 с.
5. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 130–139.
6. Рудницький В. М. Алгебраїчна структура множини логічних операцій кодування / В. М. Рудницький, В. Г. Бабенко, Д. А. Жиляєв // Наука і техніка Повітряних Сил Збройних Сил України : науко-техн. журнал – Харків : ХУПС ім. І. Кожедуба. – 2011. – Вип. 2(6). – С. 112–114.
7. Рудницький В. М. Систематизація повної множини логічних функцій для криптографічного перетворення інформації / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко // Системи обробки інформації : зб. наук. праць. – Вип. 8 (98). –Х. : ХУПС ім. І. Кожедуба, 2011. – С. 184–188.
8. Рудницький В. М. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування / В. М. Рудницький, Л. А. Шувалова, О. Б. Нестеренко // Вісник інженерної академії України : часопис. – Київ, 2016. – Вип. 3. – С. 105–108.
9. Richard A. Mollin. Codes: the guide to secrecy from ancient to modern times. – Chapman & Hall/CRC, 2005. – С. 142.
10. Квасников В. П. Синтез таблиц минимальных кодовых расстояний по Хеммингу / В. П. Квасников, В. Н. Рудницкий, В. Г. Бабенко // Електроніка та системи управління. – 2006. – № 3 (9). – С. 47–52.

References

1. Venbo, Mao (2005). Modern cryptography: theory and practice. Moscow: Izdatelskyi dom "Williams", 768 p. [in Russian].
2. Malets, I. O. (2011). The role and problems of functioning of telecommunication systems in emergency situations. Electronic research archive for Scientific-technical library of National University «Lvivska politekhnika» (Lviv). [in Ukrainian], available at: http://ena.lp.edu.ua

3. Yakovlev, A. V., Bezbohov, A. A., Rodyn, V. V. and Shamkyn, V. N. (2006). Cryptographic protection of information. *TSTU*. (Tambov), 140 p. [in Russian].
4. Sokolov, V. Y. (2010). Information systems and technology. *DUIKT*. (Kyiv), 138 p. [in Ukrainian].
5. Babenko, V. G. and Rudnytskyi, S. V. (2012). Implementation of the method of information security based on matrix operations for cryptographic transformation. *Systemy obrobky informatsii* (Kharkiv), No. 9 (107),pp. 130–139 [in Ukrainian].
6. Rudnytskyi, V. M., Babenko, V. G. and Zhyliaiev, D. A. (2011). The algebraic structure of the set of logical operations coding. *Nauko-tekhnichnyi zhurnal «Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy»* (Kharkiv), No. 2(6). pp. 112–114 [in Ukrainian].
7. Rudnytskyi, V. M., Babenko, V. G. and Myronets, I. V. (2011). Systematization of the complete set of Boolean functions for cryptographic transformation of information. *Systemy obrobky informatsii* (Kharkiv), No. 8 (98), pp. 184–188 [in Ukrainian].
8. Rudnytskyi, V. M., Shuvalova, L. A. and Nesterenko, O. B. (2016). The synthesis operations of cryptographic conversion according to the criterion of strict sustainable coding. *Visnyk inzhenernoi akademii Ukrainy* (Kyiv), No. 3, pp.105–108 [in Ukrainian].
9. Mollin, Richard A. (2005). Codes: the guide to secrecy from ancient to modern times. Chapman & Hall/CRC, p. 142.
10. Kvasnykov, V. P., Rudnytskyi, V. N. and Babenko, V. H. (2006). Synthesis tables minimum code distance of the Hamming. *Electronics and control systems*, No. 3, pp. 47–52 [in Russian].

V. M. Rudnitsky[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]
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

THE METHOD OF SYNTHESIS OF CRYPTOGRAPHIC CONVERSION OPERATIONS ACCORDING TO THE CRITERION OF STRICT SUSTAINABLE CODING

The development of cryptographic algorithms for information security that will provide the maximum encryption strength is currently topical.

This article aims at creating the method of synthesis of cryptographic transformation operations that meet strict criterion of sustainable coding, based on the minimum distance by Hemming.

Using the table of the minimum code distances by Hemming for building of the operations of cryptographic transformations that meet the criterion of strict sustainable coding, the building of operations with desired properties without the need for their study, based on complete enumeration, is secured.

Developed method of synthesis operations of cryptographic conversion according to the criterion of strict sustainable coding. The performance of these operations discrete model provides the minimum time for their implementation as hardware and software level. In addition, it should be noted that these operations will provide the replacement of the lookup tables discrete models, which will significantly reduce the amount of memory of specialized computing systems because it defeats the need to maintain a large number of tables of permutations. The possibility of the synthesis of a large number of operations of cryptographic conversion according to the criterion of strict sustainable coding provides the possibility to choose the model of small complexity, which will provide a cryptographic transformation of information with less time with the same characteristics of the conversion results.

Keywords: *cryptographic transformation of information, criterion of strict sustainable coding, table of permutations, discrete model.*

Статтю представляє В. М. Рудницький, д.т.н, професор, Черкаський державний технологічний університет.