© Rudnytskyy V., Melnyk O., Scherbyna V., Myronyuk T. Synthesis of elementary transposition functions controlled by information // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 242-247.

СИНТЕЗ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ПЕРЕСТАНОВОК, КЕРОВАНИХ ІНФОРМАЦІЄЮ

Володимир Рудницький[1], Ольга Мельник[2], Володимир Щербина[3], Тетяна Миронюк[1]

[1]Черкаський державний технологічний університет, Україна
[2]Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Україна
[3]Національний авіаційний університет, Україна

РУДНИЦЬКИЙ Володимир Миколайович, д.т.н.

Рік та місце народження: 1962 рік, м. Золотоноша, Черкаська область, Україна.
Освіта: Харківське вище військове командно-інженерне училище 1984 рік.
Посада: завідувач кафедри системного програмування Черкаського державного технологічного університету з 2006 року.
Наукові інтереси: розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного кодування, створення засобів обчислювальної техніки з необхідними рівнями надійності та захищеності.
Публікації: більше 150 наукових публікацій, серед яких монографії, навчально-методичні розробки, навчальні посібники, наукові статті.
E-mail: RVN_2008@ukr.net

МЕЛЬНИК Ольга Григорівна, к.т.н.

Рік та місце народження: 1987 рік, м. Черкаси, Україна.
Освіта: Академія пожежної безпеки імені Героїв Чорнобиля, 2009 рік; Черкаський національний університет імені Богдана Хмельницького, 2010 рік.
Посада: доцент кафедри будівельних конструкцій Черкаського інституту пожежної безпеки імені Героїв Чорнобиля НУЦЗ України з 2012 року.
Наукові інтереси: методи та засоби побудови комп'ютеризованих систем прогнозування пожеж.
Публікації: більше 40 наукових публікацій, серед яких монографії, навчально-методичні розробки, наукові статті та патенти на винаходи.
E-mail: melnyk_olja_2012@mail.ru

ЩЕРБИНА Володимир Порфирійович

Рік та місце народження: 1950 рік, м. Магдебург, федеральна земля Саксонія-Ангальт, Німеччина.
Освіта: Київський державний університет ім. Т.Г. Шевченка, 1973 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2005 року.
Наукові інтереси: проблеми вищої школи, доуніверситетська освіта та післядипломне навчання, криптографічні перетворення.
Публікації: понад 30 друкованих наукових праць, серед яких навчальні посібники, навчально-методичні комплекси дисциплін, наукові статті та матеріали і тези доповідей на конференціях.
E-mail: smya@nau.edu.ua

МИРОНЮК Тетяна Василівна

Рік та місце народження: 1985 рік, м. Сміла, Черкаська область, Україна.
Освіта: Черкаський державний технологічний університет, 2007 рік.
Посада: асистент кафедри системного програмування Черкаського державного технологічного університету з 2008 року.
Наукові інтереси: розробка математичних методів захисту інформації та їх реалізація на основі операцій криптографічного перетворення.
Публікації: 19 наукових публікацій, серед яких наукові статті, тези доповідей та звіти з науково-дослідних робіт.
E-mail: tanja604@rambler.ru

Анотація. *У даній статті досліджена група однотипних елементарних функцій, що мають однакову складність, для криптографічних перетворень. Для розуміння фізичної сутності цих функцій були побудовані функціональні схеми, аналіз яких показав, що дані функції забезпечують перестановку розрядів у залежності від інформації, що перетворюється. Побудовано модель елементарних функцій перестановок, керованих інформацією, для криптографічних перетворень, коректність якої підтверджено на конкретних прикладах. Визначено суть методу синтезу елементарних функцій перестановок, керованих інформацією, а також показано, що даний метод співпадає з результатами обчислювального експерименту. Доведено можливість використання елементарних функцій перестановок, керованих інформацією, в складі операції криптографічного перетворення для забезпечення перестановки біт, біт між байтами, біт між словами. Наукові результати можуть бути використанні при вдосконаленні існуючих та створенню нових криптопримітивів.*

Ключові слова: *елементарна функція, перестановки, керовані інформацією, модель елементарних функцій, метод синтезу елементарних функцій.*

Постановка проблеми

Інформаційна безпека включає в себе захист інформації, де особливе місце займає криптографія. Розвиток засобів обчислювальної техніки та криптоаналізу завжди вимагав і буде вимагати вдосконалення існуючих та створення нових криптоалгоритмів.

Криптографічні примітиви, хоча вони й примітиви, мають більш складну структуру, ніж операції для криптоперетворення такі, як додавання за модулем, зсув, перестановка, підстановка та інші. Виявлення нових операцій, здатних для ефективного криптоперетворення, дозволить вдосконалити криптопримітиви. Вирішення даної задачі знаходиться на межі криптографії, теорії алгоритмів та алгебри логіки.

Як знаходити нові операції крипто-переворення? Наприклад, над байтом інформації (8 біт) можна виконати 258! операцій криптографічного перетворення [1]. Іншими словами – існує 258! таблиць підстановки, кожна з яких описується за допомогою 8 елементарних функцій криптографічного перетворення. На сьогоднішній день не існує можливості дослідити всі елементарні функції для перетворення байту інформації навіть без їх композиції в операції криптоперетворення. Проблематично навіть мінімізувати таблицю підстановки для байту інформації. Проте дана задача практично вирішується для 5 – 6 бітних підстановок. Отримавши нові елементарні функції та побудувавши на їх основі операції криптоперетворення, можна знайти нові можливості для вдосконалення криптопримітивів. Зрозумівши фізичний зміст даних елементарних функцій та операцій криптоперетворення, будуть отримані можливості для побудови нових криптопримітивів.

В даній статті обмежимося дослідженням синтезу лише однієї групи трирозрядних елементарних функцій для побудови групи операцій криптографічного перетворення.

Аналіз останніх досліджень і публікацій

Серед останніх досліджень і публікацій варто виділити: [2], де проведено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації; [3], де проведено синтез множин моделей спеціалізованих трирозрядних логічних функцій і здійснено групування моделей трирозрядних логічних функцій для криптографічного перетворення за обраними критеріями; [4, 5], де виведені твердження для елементарних функцій перестановок, керованих інформацією.

Проте в даних дослідженнях не вивчалася можливість практичної реалізації трирозрядних елементарних функцій.

Мета статті полягає у формалізації правил побудови елементарних функцій перестановок, керованих інформацією, для криптографічних перетворень.

Виклад основного матеріалу

На сьогоднішній день визначені набори трирозрядних елементарних функцій, на основі яких будуються операції криптографічного перетворення, є актуальними для засобів захисту інформації і не досліджувалися раніше.

Набори груп трирозрядних елементарних функцій криптографічного перетворення представляють собою функції, які складаються з трьох елементарних функцій, модель даних яких аналогічна по складності сумі по модулю 2. А це означає, що дані набори є простими і не вимагають значних ресурсів для реалізації засобами обчислювальної техніки.

Результати представлені в табл. 1 [6].

Таблиця 1

Визначені елементарні функції мінімальної складності

№ функції	*Результат виконання*	*Дискретна модель*
83	01010011	$x_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3$
163	10100011	$x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_3$
46	00101110	$x_1 \cdot \overline{x}_2 \vee x_2 \cdot \overline{x}_3$
71	01000111	$x_1 \cdot x_2 . \vee \overline{x}_2 \cdot x_3$
139	10001011	$x_1 \cdot x_2 \vee \overline{x}_2 \cdot \overline{x}_3$
53	00110101	$\overline{x}_1 \cdot x_2 . \vee x_1 \cdot x_3$
58	00111010	$\overline{x}_1 \cdot x_2 . \vee x_1 \cdot \overline{x}_3$
184	10111000	$\overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot \overline{x}_3$
116	01110100	$\overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3$
92	01011100	$x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3$
172	10101100	$x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3$
29	00011101	$x_1 \cdot \overline{x}_2 \vee x_2 \cdot x_3$

Закінчення таблиці 1

197	11000101	$\overline{x}_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3$
202	11001010	$\overline{x}_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_3$
209	11010001	$\overline{x}_1 \cdot \overline{x}_2 \vee x_2 \cdot x_3$
226	11100010	$\overline{x}_1 \cdot \overline{x}_2 \vee x_2 \cdot \overline{x}_3$
39	00100111	$x_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3$
141	10001101	$x_1 \cdot x_3 \vee \overline{x}_2 \cdot \overline{x}_3$
114	01110010	$\overline{x}_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3$
27	00011011	$x_1 \cdot \overline{x}_3 \vee x_2 \cdot x_3$
78	01001110	$x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot x_3$
177	10110001	$\overline{x}_1 \cdot \overline{x}_3 \vee x_2 \cdot x_3$
228	11100100	$\overline{x}_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot x_3$
216	11011000	$\overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot \overline{x}_3$

Для отримання елементарних функцій криптографічних перетворень, приведених в таблиці 1, скористаємося методом перестановки розрядів, основна задача якого полягає в зміні одного розряду елементарної функції двома іншими.

Застосувавши даний метод до кожної елементарної функції, було отримано набори елементарних функцій для операцій криптографічного перетворення.

Щоб більш детально розглянути визначені набори, можна класифікувати елементарні функції за трьома ознаками:

- елементарної функції x_1, яка виконується над першим розрядом логічної функції:

$$Y = x_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \qquad Y = \overline{x}_1 \cdot x_2 \vee x_1 \cdot x_3$$
$$Y = x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_3 \qquad Y = \overline{x}_1 \cdot x_2 \vee x_1 \cdot \overline{x}_3;$$
$$Y = x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3$$
$$Y = x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_3$$

- елементарної функції x_2, яка виконується над другим розрядом логічної функції:

$$Y = x_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3 \qquad Y = x_1 \cdot \overline{x}_2 \vee x_2 \cdot x_3$$
$$Y = x_1 \cdot x_2 \vee \overline{x}_2 \cdot \overline{x}_3 \qquad Y = x_1 \cdot \overline{x}_2 \vee x_2 \cdot \overline{x}_3;$$
$$Y = \overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_2 \vee x_2 \cdot x_3$$
$$Y = \overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot \overline{x}_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_2 \vee x_2 \cdot \overline{x}_3$$

- елементарної функції x_3, яка виконується над третім розрядом логічної функції:

$$Y = x_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3 \qquad Y = x_1 \cdot \overline{x}_3 \vee x_2 \cdot x_3$$
$$Y = x_1 \cdot x_3 \vee \overline{x}_2 \cdot \overline{x}_3 \qquad Y = x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot x_3.$$
$$Y = \overline{x}_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_3 \vee x_2 \cdot x_3$$
$$Y = \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot \overline{x}_3 \qquad Y = \overline{x}_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot x_3$$

Необхідно провести дослідження отриманих елементарних функцій для криптографічних перетворень. Найпростіше це зробити на схемотехнічному представленні елементарних функцій у вигляді комбінаційних схем.

У загальному вигляді елементарна функція криптографічного перетворення відповідно до визначених наборів буде мати вигляд:

$$Y = x_i \cdot x_j \vee \overline{x}_i \cdot x_k, \qquad (1)$$

де Y – значення вихідного сигналу результату елементарних функцій; x_i, x_j, x_k – значення відповідних розрядів вхідного сигналу, причому x_i приймає пряме й інверсне значення в елементарній функції.

Деякі функціональні схеми пристроїв реалізації визначених елементарних функцій приведено на рис. 1-4.

$Y_1 = x_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3$

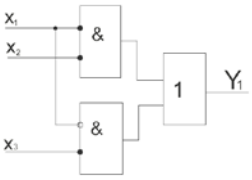

Рис. 1. Функціональна схема функції № 83

$Y_1 = x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_3$

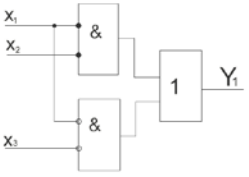

Рис. 2. Функціональна схема функції № 163

$Y_1 = x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3$

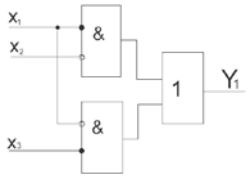

Рис. 3. Функціональна схема функції № 92

$Y_1 = x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3$

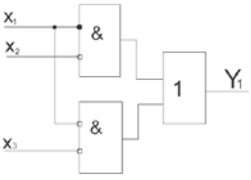

Рис. 4. Функціональна схема функції № 172

Для схемотехнічної реалізації дискретної моделі операцій криптографічного перетворення було використано два логічних елементи І та один логічний елемент АБО при двох вхідних інформаційних сигналах та одному вихідному.

Пристрої, наведені на рис. 1–4, працюють наступним способом: при подачі на інформаційні входи значення змінних x_1, x_2, x_3 в двійковій системі числення виконання елементарної функції криптографічного перетворення посередністю елементів І та АБО згідно виразу (1) на виході Y_1 видається результат виконання відповідної елементарної функції криптографічного перетворення відповідно до керуючої функції x_1.

Виходячи з результатів дослідження функціональних схем, отримані елементарні функції в подальшому будемо називати елементарними функціями перестановок, керованих інформацією.

На основі визначених елементарних функцій перестановок, керованих інформацією, можемо вивести наступні твердження.

Твердження 1. Елементарна функція перестановки, керована інформацією, може бути використана для криптографічного перетворення, якщо її елементарна функція використовується в

прямому значенні в першій імпліканті та інверсному значенні в другій імпліканті та навпаки.

Враховуючи твердження 1, можна побудувати модель елементарних функцій для криптографічного перетворення, яка має наступний вигляд:

$$Y = \tilde{\tilde{x}}_i \tilde{\tilde{x}}_j \vee \bar{\tilde{\tilde{x}}}_i \tilde{\tilde{x}}_k , \qquad (2)$$

де Y – значення відповідного розряду вихідного сигналу результату елементарних функцій криптографічного перетворення; $\tilde{\tilde{x}}_i, \tilde{\tilde{x}}_j, \tilde{\tilde{x}}_k$ – значення відповідних розрядів вхідного сигналу.

Властивостями визначеної моделі є:

- i, j, k приймають значення 1, 2, 3, причому $i \neq j \neq k$;
- x_i може приймати пряме або інверсне значення;
- x_j, x_k можуть бути і в прямому, і в інверсному значенні, причому $j \neq k$.

На основі отриманої моделі (2) наведемо декілька прикладів побудови елементарних функцій, керованих інформацією, для криптографічних перетворень.

Приклад

Якщо $i = 1,\ j = 2,\ k = 3,$ то модель елементарних функцій відповідно до виразу (2) для криптографічного перетворення матиме вигляд:

$$Y = \tilde{\tilde{x}}_1 \tilde{\tilde{x}}_2 \vee \bar{\tilde{\tilde{x}}}_1 \tilde{\tilde{x}}_3 .$$

Нехай x_1 – пряме значення, то $Y = x_1 \tilde{\tilde{x}}_2 \vee \bar{x}_1 \tilde{\tilde{x}}_3$, і якщо x_2 і x_3 мають також прямі значення, то в цьому випадку $Y = x_1 x_2 \vee \bar{x}_1 x_3$.

Якщо x_2 – пряме значення, x_3 має інверсне значення, то $Y = x_1 x_2 \vee \bar{x}_1 \bar{x}_3$.

Нехай x_2 – інверсне значення, x_3 має пряме значення, тоді $Y = x_1 \bar{x}_2 \vee \bar{x}_1 x_3$.

Отримані елементарні функції є визначеними елементарними функціями мінімальної складності, що представлені в табл. 1.

Отримані результати дозволяють управляти методом синтезу елементарних функцій, керованих інформацією, на основі виразу 2.

Для цього введемо наступні означення:

1. Основним елементом елементарної функції, керованою інформацією, є елемент, який повторюється в правій і лівій частині елементарної функції, керованої перестановками, в прямому та інверсному значеннях.

2. Додатковим елементом елементарної функції, керованої перестановками, є елемент, який зустрічається один раз або в лівій, або правій частині елементарної функції.

Метод синтезу елементарних функцій перестановок, керованих інформацією, полягає в наступному:

1) визначити індекси основних та додаткових елементів елементарних функцій, керованих перестановками;

2) визначити прямі та інверсні значення елементів елементарних функцій, керованих перестановками;

3) підставити визначені значення у вираз 2 для отримання елементарних функцій перестановок, керованих інформацією;

4) застосувавши пункти 1-3 на цій множині елементарних індексів і прямих та інверсних значень елементарних функцій, керованих перестановками, отримаємо повну множину елементарних функцій перестановок, керованих інформацією.

Даний метод дозволяє отримати елементарні функції перестановок, керованих інформацією, що співпадає з результатами обчислювального експерименту.

Синтезована множина елементарних функцій перестановок, керованих інформацією, необхідна для побудови математичної групи операцій перестановок, керованих інформацією, для їх прямого та оберненого перетворення.

Наведемо приклади прямих та відповідних їм обернених операцій перестановок, керованих інформацією:

$$F^k_{71,53,27} = \begin{pmatrix} x_1 \cdot x_2 . \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 . \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{pmatrix} \qquad F^d_{71,53,27} = \begin{pmatrix} x_1 \cdot x_2 . \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 . \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{pmatrix}$$

$$F^k_{29,78,58} = \begin{pmatrix} x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 . \vee x_1 \cdot \bar{x}_3 \end{pmatrix} \qquad F^d_{27,92,46} = \begin{pmatrix} x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \end{pmatrix}$$

$$F^k_{27,46,163} = \begin{pmatrix} x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \end{pmatrix} \qquad F^d_{39,29,172} = \begin{pmatrix} x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \end{pmatrix}.$$

У табл. 2 наведені результати прямого криптографічного перетворення на основі наведених прикладів.

Таблиця 2

Результати використання елементарних функцій перестановок, керованих інформацією

			$F^k_{71,53,27} = \begin{pmatrix} x_1 \cdot x_2 . \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 . \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{pmatrix}$				$F^k_{29,78,58} = \begin{pmatrix} x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 . \vee x_1 \cdot \bar{x}_3 \end{pmatrix}$				$F^k_{27,46,163} = \begin{pmatrix} x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \end{pmatrix}$			
x_1	x_2	x_3	71	53	27	$\sum\oplus$	29	78	58	$\sum\oplus$	27	46	163	$\sum\oplus$
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
0	0	1	1	0	0	2	0	1	0	2	0	0	0	1
0	1	0	0	1	0	0	0	0	1	2	0	1	1	1
0	1	1	0	1	1	0	1	0	1	2	1	0	0	3

Закінчення таблиці 2

1	0	0	0	0	1	2	1	1	1	2	1	1	0	1
1	0	1	1	1	0	2	1	1	0	2	0	1	0	3
1	1	0	1	0	1	2	0	1	1	2	1	1	1	1
1	1	1	1	1	1	0	1	0	0	2	1	0	1	1
$\sum\oplus$			2	2	4	8	2	6	6	14	2	4	6	12

У рядках таблиці наведені результати перетворення трьох біт на повній множині вхідних даних. Стовпчики таблиці можна трактувати як результат перетворення одного значення трьох байт інформації. В таблиці також наведено кількісні значення зміни вхідної інформації (стовпчики позначені $\sum\oplus$) при перетворенні біт, та кількісні значення зміни вхідної інформації (рядок позначений $\sum\oplus$) при перетворенні байт.

Виходячи з цього можна стверджувати, що елементарні функції перестановок, керованих інформацією, отримані на основі запропонованої моделі (2), в складі операції криптографічного перетворення забезпечать перестановку біт, біт між байтами, біт між словами і т.д. Крім цього дані елементарні функції органічно поєднують перестановки та можливі інверсії біт, що переставляються.

Просте механічне розширення запропонованої моделі (2) на більшу кількість біт, які будуть переставлятися, наприклад: $Y = \tilde{\tilde{x}}_i\tilde{\tilde{x}}_j\tilde{\tilde{x}}_k \vee \tilde{\tilde{\tilde{x}}}_i\tilde{\tilde{\tilde{x}}}_j\tilde{\tilde{x}}_n$, $Y = \tilde{\tilde{x}}_i\tilde{\tilde{\tilde{x}}}_j\tilde{\tilde{x}}_k \vee \tilde{\tilde{\tilde{x}}}_i\tilde{\tilde{x}}_j\tilde{\tilde{x}}_n$, $Y = \tilde{\tilde{\tilde{x}}}_i\tilde{\tilde{x}}_j\tilde{\tilde{x}}_k \vee \tilde{\tilde{x}}_i\tilde{\tilde{\tilde{x}}}_j\tilde{\tilde{x}}_n$, $Y = \tilde{\tilde{\tilde{x}}}_i\tilde{\tilde{\tilde{x}}}_j\tilde{\tilde{x}}_k \vee \tilde{\tilde{x}}_i\tilde{\tilde{x}}_j\tilde{\tilde{x}}_n$ приведе до втрати інформативності і, як наслідок, задача оберненого криптоперетворення не матиме рішення.

Подальші дослідження будуть направлені на формалізацію методу синтезу операцій криптографічного перетворення на основі моделі елементарних функцій перестановок, керованих інформацією, а також формалізацію методу синтезу операції оберненого криптографічного перетворення при відомій операції прямого криптографічного перетворення на основі перестановок, керованих інформацією.

Висновки

У статті за результатами обчислювального експерименту для подальшого дослідження визначена група елементарних функцій мінімальної складності.

Результати моделювання функціональних пристроїв реалізації досліджуваної групи елементарних функцій показали, що вони забезпечують перестановку біт інформації в залежності від інформації, що підлягає перетворенню.

У статті формалізовано правила побудови елементарних функцій перестановок, керованих інформацією, які можуть бути використані для побудови операцій криптографічного перетворення.

На основі наведених прикладів показана можливість використання отриманих елементарних функцій для криптографічного перетворення інформації, представленої бітами, байтами, словами.

Отримані елементарні функції перестановок, керованих інформацією, можуть знайти практичне застосування при вдосконаленні існуючих та створенню нових криптопримітивів.

Література

[1] Криптографическое кодирование: методы и средства реализации. Часть 2: монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О.Г. Мельник. — Х. : Изд-во ООО «Щедрая усадьба плюс», 2014. — 224 с.

[2] Віра Бабенко, Ольга Мельник, Руслан Мельник. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації // Безпека інформації. — 2013. — Т. 19. — №1. — С. 56–59.

[3] Рудницкий С.В. Криптографическое преобразование информации на основе трехразрядных логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. — № 4 (22). — С. 119–122.

[4] Дахно Т.В. Методика синтезу трьохрозрядних логічних функцій мінімальної складності для криптосистем / Дахно Т.В., Миронюк О.М. // Друга міжнародна науково-практична конференція «ІІРТК-2009», 25-28 травня: зб. тез. доп. — К. : НАУ, 2009. — С. 367.

[5] Миронюк Т.В. Синтез елементарних функцій перестановок, керованих інформацією / Т.В. Миронюк, О.Г. Мельник // ІІ Міжнародна науково-практична конференція «Інформаційні технології в освіті, науці й техніці» (ІТОНТ-2014), 24-26 квітня: зб. тез. доп. — Черкаси : ЧДТУ, 2014. — С. 147-148.

[6] Бабенко В.Г. Результати моделювання логічних функцій для криптографії / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Сучасні інформаційні системи. Проблеми та тенденції розвитку : зб. матеріалів 2-ї Міжнар. наук. конф. — Х. : ХНУРЕ, 2007. — С. 421-422.

УДК 003.26:004.056.55 (045)

Рудницкий В.Н., Мельник О.Г., Щербина В.П., Миронюк Т.В. Синтез элементарных функций перестановок, управляемых информацией

Аннотация. *В данной статье исследована группа однотипных элементарных функций, имеющих одинаковую сложность, для криптографических преобразований. Для понимания физической сущности этих функций были построены*

функциональные схемы, анализ которых показал, что данные функции обеспечивают перестановку разрядов в зависимости от информации, что преобразуется. Построена модель элементарных функций, управляемых информацией, для криптографических преобразований, корректность которой подтверждена на конкретных примерах. Определена суть метода синтеза элементарных функций перестановок, управляемых информацией, а также показано, что данный метод совпадает с результатами вычислительного эксперимента. Доказана возможность использования элементарных функций перестановок, управляемых информацией, в составе операции криптографического преобразования для обеспечения перестановки бит, бит между байтами, бит между словами. Научные результаты могут быть использованы при совершенствовании существующих и созданию новых криптопримитивов.
Ключевые слова: *элементарная функция, перестановки, управляемые информацией, модель элементарных функций, метод синтеза элементарных функций.*

Rudnytskyy V., Melnyk O., Scherbyna V., Myronyuk T. Synthesis of elementary transposition functions controlled by information

Abstract. *This article studied a group of the same type of elementary functions with the same complexity for cryptographic transformations. To understand the physical nature of these functions have been built functional circuit, whose analysis showed that these features provide a permutation of digits depending on the information that is converted. A model of elementary functions, control information for cryptographic transformations, correctness of which is confirmed by specific examples is built. Defined the essence of the method of synthesis of elementary functions permutations, control information, and it is shown that this method is consistent with the results of computational experiment. The possibility of using permutations of elementary functions, the control information, comprising operations for cryptographic conversion permutation bits, bits between bytes, bits between words was proved. Research results can be used to improve existing and create new cryptoprimitives.*
Key words: *elementary function, transpositions controlled by information, model of elementary functions, method of synthesis of elementary functions.*

Отримано *8 вересня 2014 року*, затверджено редколегією *26 вересня 2014 року*