УДК 004.056.55:004.312.2

В.Г. Бабенко[1], Т.А. Стабецька[2]

[1] *Одеська національна академія зв'язку ім. О.С. Попова, Одеса*
[2] *Черкаський державний технологічний університет, Черкаси*

ПОБУДОВА МОДЕЛІ ОБЕРНЕНОЇ НЕЛІНІЙНОЇ ОПЕРАЦІЇ МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У даній статті отримано модель синтезу нелінійної операції розширеного матричного криптографічного перетворення на основі двох замін, а також сформульовано і доведено теорему про побудову оберненої матриці розширеного матричного криптографічного перетворення при наявності двох замін.

Ключові слова: *трирозрядні логічні функції, операція криптографічного перетворення, матрична модель, обернена операція, операція розширеного матричного перетворення.*

Вступ

Постановка проблеми. Сучасний розвиток інформаційних технологій вимагає удосконалення та покращення показників швидкодії та захищеності інформації, яка закривається за допомогою криптографічних алгоритмів.

Одним із способів удосконалення крипто алгоритмів можна виокремити розширення спектра базових операцій, на основі яких будуються основні перетворення. Головною задачею, що постає в даному випадку, є знаходження таких операцій, які можуть використовуватися для побудови криптоалгоритмів.

Аналіз останніх досліджень та публікацій. В [1-3] запропоновано синтез операцій криптографічного перетворення на основі визначеної групи трирозрядних логічних функцій. Методи синтезу вказаних операцій криптоперетворення на основі заміни й виключення розглянуто в [3,4].

Але на сьогодні недостатньо досліджено методи знаходження обернених нелінійних операцій криптографічного перетворення, що зумовлює ряд задач, що підлягають вирішенню.

Мета статті – для операції розширеного матричного криптографічного перетворення, синтезованої на основі двох замін, розробити правила побудови оберненої операції.

Основний матеріал

Розглянемо операції криптографічного перетворення, синтезовані на основі заміни двох елементарних функцій в операції на функції розширеного матричного перетворення, які були отримані в результаті обчислювального експерименту за допомогою спеціального програмного забезпечення.

Операції, утворені в результаті синтезу на основі i-ої елементарної функції (у випадку коли базова елементарна функція без доповнення) мають вигляд :

$$\vec{F}_k = \begin{pmatrix} x_i \\ x_j \oplus x_i \tilde{x}_k \\ x_k \oplus \overline{x}_i \tilde{x}_j \end{pmatrix} \qquad \vec{F}_k = \begin{pmatrix} x_i \\ x_j \oplus \overline{x}_i \tilde{x}_k \\ x_k \oplus x_i \tilde{x}_j \end{pmatrix},$$

де $\tilde{x}_i, \tilde{x}_j, \tilde{x}_k$ – аргументи з будь-яким значенням інверсії, $\overline{\tilde{x}}_i$ – обернене значення аргументу, $i, j, k \in [1,2,3]$, та $j < k$.

Таким чином, можна записати загальний вигляд матричної моделі операції розширеного криптографічного перетворення на основі i-ї елементарної функції без доповнення:

$$\vec{F}_k = \begin{pmatrix} x_i \\ x_j \oplus \tilde{x}_i \tilde{x}_k \\ x_k \oplus \overline{\tilde{x}}_i \tilde{x}_j \end{pmatrix}.$$

Враховуючи вище зазначене, операції розширеного матричного перетворення, утворені в результаті синтезу на основі i-ої елементарної функції з доповненням, мають вигляд:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \\ x_k \end{pmatrix}; \qquad \overline{F}_k = \begin{pmatrix} x_i \oplus \tilde{x}_j \overline{\tilde{x}}_k \\ x_j \oplus \tilde{x}_i \tilde{x}_k \\ x_k \end{pmatrix};$$

$$\overline{F}_k = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \\ x_k \oplus \tilde{x}_i \overline{\tilde{x}}_j \end{pmatrix}; \qquad \overline{F}_k = \begin{pmatrix} x_i \oplus \overline{\tilde{x}}_j \tilde{x}_k \\ x_j \\ x_k \oplus \tilde{x}_i \tilde{x}_j \end{pmatrix}.$$

Таким чином, можна записати загальний вигляд моделі операції розширеного матричного криптографічного перетворення:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \oplus a_1 \tilde{x}_i \overline{\tilde{x}}_k \\ x_k \oplus a_2 \tilde{x}_i \overline{\tilde{x}}_j \end{pmatrix}, \qquad (1)$$

де a_1, a_2 – коефіцієнти, які визначають наявність доповнення в елементарній функції, при чому лише один з них може дорівнювати 1. $\tilde{x}_i, \tilde{x}_j, \tilde{x}_k$ – аргументи з будь-яким значенням інверсії, $\bar{\tilde{x}}_j$, $\bar{\tilde{x}}_k$ – обернені значення аргументу.

Як бачимо, матричну модель (1) можливо представити у вигляді суми двох матриць, матриці аргументів, яка є лінійною та нелінійної матриці доповнень.

Введемо поняття індекса рядка. Індекс рядка – це індекс доданка лінійної матриці перетворення. Вважається, що послідовність індексів розширення утворює зростаючу послідовність.

Правило синтезу розширення наступне: для того, щоб утворити розширення одного з рядків матриці, яка позначає операцію розширеного матричного перетворення за допомогою двох інших, потрібно виконати логічне множення цих рядків, інвертуючи при цьому ті рядки, індекси яких співпадають з індексами інвертованих змінних. Тоді побудова моделі оберненої нелінійної операції криптографічного перетворення полягає в наступному.

Теорема. Для того, щоб побудувати для операції розширеного матричного криптографічного перетворення з двома доповненнями операцію оберненого перетворення, потрібно:

1. Побудувати лінійну операцію оберненого перетворення у матричному представленні;

2. Побудувати відповідні два доповнення, враховуючи, що прямі доповнення переходять у прямі, інверсні у інверсні, а у змішаних доповненнях порядок інвертування зберігається, якщо послідовність індексів доповнення співпадає з послідовністю індексів відповідних рядків матричної моделі для операції перетворення, і змінюється в протилежному випадку.

Доведення. Розглянемо одну з можливих операцій перетворення. Для інших доведення аналогічне.Нехай дано матрицю, яка описує операцію розширеного перетворення

$$\bar{F}_k = \begin{pmatrix} x_i \oplus x_j \bar{x}_k \\ x_j \oplus x_i x_k \\ x_k \end{pmatrix}.$$

Кожен рядок матриці $\bar{F}_k$ являє собою операнд-розряд інформації, який отриманий в результаті застосування основної елементарної функції перетворення, тобто $y_i = F_k(x_i)$.

Позначимо рядки матриці $\bar{F}_k$ змінними y_1, y_2, y_3 відповідно.

$$\bar{F}_k = \begin{pmatrix} x_i \oplus x_j \bar{x}_k \\ x_j \oplus x_i x_k \\ x_k \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \end{matrix}.$$

Перш за все будується матриця для лінійної операції оберненого перетворення. Вона визначає порядок розташування змінних y_i, $i \in [1,2,3]$ у шуканій операції оберненого перетворення. Потім будуються відповідні доповнення таким чином, щоб при перетворенні рядків матриці $\bar{F}_k$ згідно з вказаними перетвореннями у матриці $\bar{F}_d$, утворилася діагональна матриця, в якій елементами головної діагоналі є змінні x_i, x_j, x_k відповідно.

Для того, щоб отримати змінну x_i, потрібно за допомогою рядків з j-м та k – м індексами утворити вираз доповнення $x_i \bar{x}_k$ та виконати логічне додавання за модулем 2 з рядком i-го індекса.

Тоді отримаємо: $x_i \oplus x_j \bar{x}_k \oplus (x_j \oplus x_i x_k)\bar{x}_k =$

$= x_i \oplus x_j \bar{x}_k \oplus x_j \bar{x}_k \oplus x_i x_k \bar{x}_k = x_i$.

Використовуючи змінні y_1, y_2, y_3 синтез змінної x_i матиме вигляд: $y_1 + y_2 \bar{y}_3$.

Для того, щоб отримати змінну x_j, потрібно виконати аналогічні дії.

Тоді отримаємо: $x_j \oplus x_i x_k \oplus (x_i \oplus x_j \bar{x}_k) x_k =$

$= x_j \oplus x_i x_k \oplus x_i x_k \oplus x_j \bar{x}_k x_k = x_j$

Використовуючи змінні y_1, y_2, y_3 синтез змінної x_j матиме вигляд: $y_2 + y_1 y_3$.

Якщо ж у матриці, яка описує операцію криптографічного перетворення, послідовність індексів доповнення не співпадатиме з послідовністю індексів відповідних рядків, тобто послідовність індексів відповідних рядків утворює спадну послідовність, то порядок інвертування зміниться, що зумовлено встановленим порядком розташування змінних у доповненні.

Теорему доведено.

Приклад 1. Побудувати матрицю оберненого перетворення для матриці

$$\bar{F}_k = \begin{pmatrix} x_2 \oplus x_1 \bar{x}_3 \\ x_3 \oplus \bar{x}_1 \bar{x}_2 \\ x_1 \end{pmatrix}$$

Позначимо рядки матриці змінними y_1, y_2, y_3 відповідно:

$$\bar{F}_k = \begin{pmatrix} x_2 \oplus x_1 \bar{x}_3 \\ x_3 \oplus \bar{x}_1 \bar{x}_2 \\ x_1 \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \end{matrix}.$$

Побудуємо лінійну матрицю оберненого

перетворення для матриці $\overline{F}_l = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}$. Вона є оберненою матрицею до $\overline{F}_l$ і утворюється в процесі транспонування даної. Таким чином лінійна матриця оберненого перетворення матиме вигляд: $\overline{F}_l^{-1} = \begin{pmatrix} y_3 \\ y_1 \\ y_2 \end{pmatrix}$.

Доповнення для x_2 отримуємо в результаті логічного множення другого і третього рядків, інвертуючи при цьому другий рядок і розташовуючи множники таким чином, щоб послідовність індексів рядків утворила зростаючу послідовність: $\overline{y}_2 y_3$. Доповнення для x_3 будуємо аналогічно, воно матиме вигляд: $\overline{y}_1 \overline{y}_3$. Таким чином матриця оберненого перетворення матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \oplus \overline{y}_2 y_3 \\ y_2 \oplus \overline{y}_1 \overline{y}_3 \end{pmatrix}.$$

Застосування даної теореми забезпечує синтез обернених операцій розширеного матричного криптографічного перетворення і може знайти своє практичне застосування при розробці програмно-апаратних засобів для систем захисту інформації.

Висновки

У статті сформульовано й доведено правило побудови оберненої операції розширеного матричного криптографічного перетворення на основі двох замін. Використання запропонованих нелінійних операцій розширеного матричного криптографічного перетворення дозволяє розширити множину операцій для побудови систем криптографічного захисту інформації й підвищити їх криптостійкість шляхом додаткового використання даних операцій.

Список літератури

1. Бабенко В. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В. Бабенко, О. Мельник, Р. Мельник // Безпека інформації. – К.: НАУ, 2013. – Т. 19, № 1. – С. 56–59.

2. Рудницкий С.В. Криптографическое преобразование информации на основе трехразрядных логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Веретельник // Вектор науки (ТГУ). – 2012. – № 4 (22). – С. 119-122.

3. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник // Системи обробки інформації. – 2012. – № 9 (107). – С. 145–147.

4. Бабенко В.Г. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления / В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий // Информационные системы и технологии: управление и безопасность : сб. ст. 1-ой МНПК. – Тольятти: ПВГУС, 2012. – С. 67–77.

Надійшла д редколегії 3.09.2013

Рецензент: д-р техн. наук, проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

ПОСТРОЕНИЕ МОДЕЛИ ОБРАТНОЙ НЕЛИНЕЙНОЙ ОПЕРАЦИИ МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Г. Бабенко, Т.А. Стабецкая

В данной статье получена модель синтеза нелинейной операции расширенного матричного криптографического преобразования на основе двух замен, а также сформулировано и доказано теорему о построении обратной операции расширенного матричного криптографического преобразования при наличии двух замен.

Ключевые слова: *трехразрядные логические функции, операция криптографического преобразования, матричная модель, обратная операция, операция расширенного матричного преобразования.*

CONSTRUCTION OF A MODEL OF REVERSE NONLINEAR OPERATION OF EXPANDED MATRIX CRYPTOGRAPHIC TRANSFORMATIONS

V.G. Babenko, T.A. Stabetskaya

In this paper we obtain an model of the synthesis of nonlinear operations of expanded matrix cryptographic transformation on the basis of two substitution, and formulated and proved a theorem on the construction of the reverse operation of expanded matrix cryptographic transformation in the presence of two substitution.

Keywords: *three-digit elementary functions, operation of cryptographic transformations, matrix model, the reverse operation, the operation of expanded matrix transformation.*