УДК 003.26:004.056.55

В.М. Рудницький[1], В.Г. Бабенко[2], Т.А. Стабецька[1]

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

УЗАГАЛЬНЕНИЙ МЕТОД СИНТЕЗУ ОБЕРНЕНИХ НЕЛІНІЙНИХ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

В роботі представлено узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення, побудованих на основі спеціальних логічних функцій розширеного матричного криптографічного перетворення n-ї розрядності. На конкретних прикладах знаходження математичної моделі оберненої операції криптографічного перетворення підтверджено коректність застосування розробленого методу синтезу нелінійних операцій.

Ключові слова: *метод синтезу, матрична модель, матриця доповнень, елементарна функція, операція оберненого перетворення, нелінійна операція, розширене матричне криптографічне перетворення.*

Вступ

Постановка проблеми. На сьогоднішній день важливою задачею криптографії є створення швидкісних криптографічних методів, які дозволяють здійснювати оперативне перетворення інформації, що зменшує час доступу до конфіденційних інформаційних ресурсів та підвищує конфіденційність збереження інформації. Основною задачею вдосконалення криптографічних методів є пошук нових функцій криптографічного перетворення, які дозволяють зменшити час криптографічної обробки інформації. На сьогоднішній день досліджені лише дворозрядні та трирозрядні операції криптографічного перетворення інформації. В залежності від кількості розрядів, над якими здійснюється криптоперетворення, визначається час криптографічної обробки інформації. Таким чином, важливим напрямком досліджень є розробка методів синтезу операцій криптографічного перетворення великої розрядності, застосування яких дозволяє підвищити швидкодію криптоалгоритмів.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити [1, 2], де було розглянуто методи синтезу операцій розширеного матричного криптографічного перетворення на основі визначеної групи трирозрядних логічних функцій. В [3] був запропонований метод синтезу матричних моделей операцій прямого та оберненого криптографічного перетворення інформації. Проте не досліджено операції розширеного матричного криптографічного перетворення вищих порядків. Суть дослідження в [4] полягає в отриманні формалізованої матричної моделі нелінійної операції криптографічного перетворення n-ої розрядності, а також правил синтезу елементарних функцій розширеного матричного криптографічного перетворення. Але у проаналізованих літературних джерелах відсутні методи синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення для n змінних.

Мета статті полягає у розробці узагальненого методу синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення.

Основний матеріал

У загальному вигляді операції криптографічного прямого перетворення, побудовані на основі елементарних функцій розширеного матричного криптографічного перетворення будуть описані наступною моделлю:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus a_i \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_l \tilde{x}_m \oplus c_i \\ x_j \oplus a_j \tilde{x}_i \tilde{x}_k \ldots \tilde{x}_l \tilde{x}_m \oplus c_j \\ x_k \oplus a_k \tilde{x}_i \tilde{x}_j \ldots \tilde{x}_l \tilde{x}_m \oplus c_k \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_l \oplus a_l \tilde{x}_i \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_m \oplus c_l \\ x_m \oplus a_m \tilde{x}_i \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_l \oplus c_m \end{pmatrix}, \qquad (1)$$

де $i, j, k, l, m \in [1, \ldots, n]$ $\quad n \in N$, $\quad i \neq j \neq k \neq l \neq m$, $a_t, x_t, c_t \in [0,1]$, $\quad t \in \{i, j, k, l, m\}$; x_t – операнди-розряди інформації; $\tilde{x}_t$ – операнди-розряди інформації, які можуть входити у доповнення у прямому та інверсному вигляді; a_t – коефіцієнти доповнень елементарних функцій, які визначають кількість замін елементарних функцій на функції розширеного матричного криптографічного перетворення; c_t – ознака наявності групи операцій інверсії.

Таким чином, рядки операції прямого перетворення являють собою елементарні функції розширеного матричного криптографічного перетворення. Причому для реалізації процесу як прямого так і оберненого перетворення, операція розширеного матричного перетворення повинна бути невиродженою, тобто складатися лише з тих елементарних функцій, у

доповненнях яких менше ніж $(n-2)$ однойменні змінні мають однакове інверсне значення [4, 5].

Якщо операція розширеного матричного криптографічного прямого перетворення без врахування групи операцій інверсії задана виразом:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus a_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_l \tilde{x}_m \\ x_j \oplus a_j \tilde{x}_i \tilde{x}_k ... \tilde{x}_l \tilde{x}_m \\ x_k \oplus a_k \tilde{x}_i \tilde{x}_j ... \tilde{x}_l \tilde{x}_m \\ ..... \\ x_l \oplus a_l \tilde{x}_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_m \\ x_m \oplus a_m \tilde{x}_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_l \end{pmatrix}, \qquad (2)$$

тоді операція розширеного матричного криптографічного оберненого перетворення буде задана виразом:

$$\overline{F}_d = \begin{pmatrix} y_p \oplus b_p \tilde{y}_q \tilde{y}_r ... \tilde{y}_s \tilde{y}_t \\ y_q \oplus b_q \tilde{y}_p \tilde{y}_r ... \tilde{y}_s \tilde{y}_t \\ y_r \oplus b_r \tilde{y}_p \tilde{y}_q ... \tilde{y}_s \tilde{y}_t \\ ..... \\ y_s \oplus b_s \tilde{y}_p \tilde{y}_q \tilde{y}_r ... \tilde{y}_t \\ y_t \oplus b_t \tilde{y}_p \tilde{y}_q \tilde{y}_r ... \tilde{y}_s \end{pmatrix}, \qquad (3)$$

де $p,q,r,s,t \in [1,...,n]$, $n \in N$, $p \neq q \neq r \neq s \neq t$, $b_j, y_j \in [0,1]$, $j \in \{p,q,r,s,t\}$; y_j – операнди-розряди інформації, які отримані в результаті застосування операції прямого перетворення відповідно. b_j – коефіцієнти доповнень елементарних функцій операції оберненого перетворення;

Матричні моделі (2), (3) можливо представити у вигляді суми двох матриць: матриці аргументів, яка є лінійною та нелінійної матриці доповнень.

$$\overline{F}k = \overline{F}_k^{lin} \oplus \overline{F}_k^{nonlin}, \qquad (4)$$

де $\overline{F}_k^{lin} = \begin{pmatrix} x_i \\ x_j \\ x_k \\ ... \\ x_l \\ x_m \end{pmatrix}$, $\overline{F}_k^{nonlin} = \begin{pmatrix} a_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_l \tilde{x}_m \\ a_j \tilde{x}_i \tilde{x}_k ... \tilde{x}_l \tilde{x}_m \\ a_k \tilde{x}_i \tilde{x}_j ... \tilde{x}_l \tilde{x}_m \\ ..... \\ a_l \tilde{x}_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_m \\ a_m \tilde{x}_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_l \end{pmatrix}$.

Тоді результатом виконання операції оберненого перетворення повинен бути вираз, що має такий запис:

$$\overline{F}_r = \begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & ... & \\ & & & x_n \end{pmatrix}, \qquad (5)$$

де $\overline{F}_r$ – еталонна матриця або матриця-результат; $x_1, x_2, ..., x_n$ – початкові операнди-розряди інформації.

Розглянемо докладніше процес знаходження операції оберненого перетворення.

Введемо поняття індексу рядка. Індекс рядка – це індекс першого доданка елементарної функції або, що те ж саме, індекс аргументу, на основі якого синтезована елементарна функція розширеного матричного криптографічного перетворення.

Проаналізувавши описаний аналітично процес знаходження операції оберненого перетворення (2-5) та використавши наступні властивості логічних операцій: $X \oplus 1 = \overline{X}$, $X \oplus X = 0$, $X \cdot \overline{X} = 0$, отримано правило синтезу операцій розширеного матричного криптографічного оберненого перетворення. Воно формулюється так: для того, щоб побудувати операцію розширеного матричного криптографічного оберненого перетворення, потрібно:

1) побудувати лінійну операцію оберненого перетворення у матричному представленні;

2) побудувати нелінійну матрицю доповнень без врахування знаків інверсії;

3) розставити у доповненнях знаки інверсій, враховуючи, що індекси інвертованих змінних x_i $(i = 1,...,n)$ операції прямого перетворення визначають індекси інвертованих змінних y_j $(j = 1,...,n)$ операції оберненого перетворення, враховуючи наступну відповідність: кожній інвертованій змінній x_i $(i = 1,...,n)$ доповнення елементарної функції операції прямого перетворення ставиться у відповідність рядок з $i-$м індексом, а номер цього рядка є індексом інвертованої змінної y_j $(j = 1,...,n)$ доповнення елементарної функції операції оберненого перетворення.

Приклад 1.

Нехай операція розширеного матричного криптографічного прямого перетворення задана матрицею:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1 \overline{x}_3 \overline{x}_4 \\ x_4 \oplus \overline{x}_1 \overline{x}_2 \overline{x}_3 \\ x_1 \oplus \overline{x}_2 x_3 x_4 \\ x_3 \oplus x_1 x_2 x_4 \end{pmatrix}. \qquad (6)$$

Побудуємо для неї операцію розширеного матричного криптографічного оберненого перетворення.

Позначимо рядки матриці (6) змінними y_1, y_2, y_3, y_4 відповідно:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1 \overline{x}_3 \overline{x}_4 \\ x_4 \oplus \overline{x}_1 \overline{x}_2 \overline{x}_3 \\ x_1 \oplus \overline{x}_2 x_3 x_4 \\ x_3 \oplus x_1 x_2 x_4 \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \\ \to y_4 \end{matrix}. \qquad (7)$$

1. Побудуємо лінійну матрицю оберненого перетворення для матриці

$$\overline{F}_k^{lin} = \begin{pmatrix} x_2 \\ x_4 \\ x_1 \\ x_3 \end{pmatrix}.$$

Вона є оберненою матрицею до $\overline{F}_k^{lin}$ і утворюється в процесі транспонування даної. Таким чином лінійна матриця оберненого перетворення матиме вигляд:

$$\overline{F}_d^{lin} = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_2 \end{pmatrix}.$$

2. Побудувавши відповідні доповнення, операція оберненого перетворення без врахування знаків інверсії матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \widetilde{y}_1\widetilde{y}_2\widetilde{y}_4 \\ \widetilde{y}_2\widetilde{y}_3\widetilde{y}_4 \\ \widetilde{y}_1\widetilde{y}_2\widetilde{y}_3 \\ \widetilde{y}_1\widetilde{y}_3\widetilde{y}_4 \end{pmatrix}.$$

3. Розстановку знаків інверсії у нелінійній матриці доповнень операції оберненого перетворення проводимо наступним чином:

Розстановка знаків інверсії доповнення 1-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_1. Її доповнення $\overline{x}_2x_3x_4$ містить одну інвертовану змінну – x_2. Їй відповідає перший рядок операції прямого перетворення, тому змінна y_1 буде інвертованою у доповненні елементарної функції першого рядка нелінійної матриці доповнень операції оберненого перетворення.

Розстановка знаків інверсії доповнення 2-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_2. Її доповнення $x_1\overline{x}_3\overline{x}_4$ містить дві інвертовані змінні – x_3 та x_4. Змінній x_3 відповідає четвертий рядок, а змінній x_4 відповідає другий рядок операції прямого перетворення, тому змінні y_2 та y_4 будуть інвертованими у доповненні елементарної функції другого рядка нелінійної матриці доповнень операції оберненого перетворення.

Розстановка знаків інверсії доповнення 3-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_3. Її доповнення $x_1x_2x_4$ не містить інвертованих змінних. Тому доповнення елементарної функції третього рядка нелінійної матриці доповнень операції оберненого перетворення не містить інвертованих змінних.

Розстановка знаків інверсії доповнення 4-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_4. Її доповнення $\overline{x}_1\overline{x}_2\overline{x}_3$ складається з усіх інвертованих змінних. Тому в доповненні елементарної функції четвертого рядка нелінійної матриці доповнень операції оберненого перетворення усі змінні будуть інвертованими.

Таким чином, отримана операція розширеного матричного криптографічного оберненого перетворення матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \overline{y}_1y_2y_4 \\ \overline{y}_2y_3\overline{y}_4 \\ y_1y_2y_3 \\ \overline{y}_1\overline{y}_3\overline{y}_4 \end{pmatrix} = \begin{pmatrix} y_3 \oplus \overline{y}_1y_2y_4 \\ y_1 \oplus \overline{y}_2y_3\overline{y}_4 \\ y_4 \oplus y_1y_2y_3 \\ y_2 \oplus \overline{y}_1\overline{y}_3\overline{y}_4 \end{pmatrix}.$$

Приклад 2.

Нехай операція розширеного матричного криптографічного прямого перетворення задана матрицею:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3x_4\overline{x}_5 \\ x_5 \\ x_1 \oplus \overline{x}_2\overline{x}_3\overline{x}_4x_5 \\ x_3 \\ x_4 \oplus \overline{x}_1\overline{x}_2x_3x_5 \end{pmatrix} \quad (8)$$

Побудуємо для неї операцію розширеного матричного криптографічного оберненого перетворення.

Позначимо рядки матриці (8) змінними y_1, y_2, y_3, y_4, y_5 відповідно:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3x_4\overline{x}_5 \\ x_5 \\ x_1 \oplus \overline{x}_2\overline{x}_3\overline{x}_4x_5 \\ x_3 \\ x_4 \oplus \overline{x}_1\overline{x}_2x_3x_5 \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \\ \to y_4 \\ \to y_5 \end{matrix} \quad (9)$$

1. Побудуємо лінійну матрицю оберненого перетворення для матриці

$$\overline{F}_k^{lin} = \begin{pmatrix} x_2 \\ x_5 \\ x_1 \\ x_3 \\ x_4 \end{pmatrix}.$$

Вона матиме вигляд:

$$\overline{F}_d^{lin} = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix}.$$

2. При побудові нелінійної матриці доповнень, потрібно врахувати, що елементарні функції y_2 та y_4 не матимуть доповнень, оскільки відповідні їм елементарні функції x_5 та x_3 не є функціями розширеного матричного криптографічного перетворення. Побудувавши відповідні доповнення, операція оберненого перетворення без врахування знаків інверсії матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \widetilde{y}_1\widetilde{y}_2\widetilde{y}_4\widetilde{y}_5 \\ \widetilde{y}_2\widetilde{y}_3\widetilde{y}_4\widetilde{y}_5 \\ \\ \widetilde{y}_1\widetilde{y}_2\widetilde{y}_3\widetilde{y}_4 \\ \\ \end{pmatrix}.$$

3. Розстановку знаків інверсії у нелінійній матриці доповнень операції оберненого перетворення проводимо наступним чином:

Розстановка знаків інверсії доповнення 1-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_1. Її доповнення $\overline{x}_2\overline{x}_3\overline{x}_4x_5$ містить три інвертовані змінні, яким відповідають перший, четвертий і п'ятий рядки операції прямого перетворення, тому змінні y_1, y_4, y_5 будуть інвертованими у доповненні елементарної функції першого рядка нелінійної матриці доповнень операції оберненого перетворення.

Розстановка знаків інверсії доповнення 2-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_2. Її доповнення $x_1\bar{x}_3x_4\bar{x}_5$ містить дві інвертовані змінні – x_3 та x_5, яким відповідають четвертий та другий рядки операції прямого перетворення, тому змінні y_2 та y_4 будуть інвертованими у доповненні елементарної функції другого рядка нелінійної матриці доповнень операції оберненого перетворення.

Розстановка знаків інверсії доповнення 4-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_4. Її доповнення $\bar{x}_1\bar{x}_2x_3x_5$ містить дві інвертовані змінні, яким відповідають третій та перший рядки операції прямого перетворення, тому змінні y_1 та y_3 будуть інвертованими у доповненні елементарної функції четвертого рядка нелінійної матриці доповнень операції оберненого перетворення.

Таким чином, отримана операція розширеного матричного криптографічного оберненого перетворення матиме вигляд:

$$\bar{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \bar{y}_1y_2\bar{y}_4\bar{y}_5 \\ \bar{y}_2y_3\bar{y}_4y_5 \\ \\ \bar{y}_1y_2\bar{y}_3y_4 \\ \\ \end{pmatrix} = \begin{pmatrix} y_3 \oplus \bar{y}_1y_2\bar{y}_4\bar{y}_5 \\ y_1 \oplus \bar{y}_2y_3\bar{y}_4y_5 \\ y_4 \\ y_5 \oplus \bar{y}_1y_2\bar{y}_3y_4 \\ y_2 \end{pmatrix}.$$

Наведені приклади знаходження математичної моделі оберненої операції криптографічного перетворення підтверджують коректність застосування розробленого методу синтезу нелінійних операцій розширеного матричного криптографічного перетворення.

Висновки

У даній статті запропоновано узагальнений метод синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення, створений на основі використання спеціальних логічних функцій розширеного матричного криптографічного перетворення n -ої розрядності.

Застосування отриманих результатів дозволяє підвищити швидкодію та стійкість криптографічних алгоритмів, що є важливими характеристиками криптографічних методів, які дозволяють здійснювати оперативне перетворення інформації, що зменшує час доступу до конфіденційних інформаційних ресурсів та підвищує конфіденційність збереження інформації.

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. *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. статей 1 межд. заочной НПК. – Тольятти: ПВГУС, 2012. – С. 67–77.*
3. *Рудницький В.М.. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2012. – Вип. 4(33). – С.198-200.*
4. *Криптографическое кодирование : коллективная моногр. / Под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Х.: ООО «Щедрая усадьба плюс», 2014. – 239 с.*
5. *Бабенко В.Г. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення / В.Г. Бабенко, Т.А. Стабецька // Системи управління, навігації та зв'язку: зб. наук. пр. – Полтава : ПНТУ, 2013. – Вип. 3(27). – С. 117-119.*

Надійшла до редколегії 18.04.2014

Рецензент: д-р техн. наук, доц. І.В. Шостак, Харківський Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ОБОБЩЁННЫЙ МЕТОД СИНТЕЗА ОБРАТНЫХ НЕЛИНЕЙНЫХ ОПЕРАЦИЙ РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Н. Рудницкий, В.Г. Бабенко, Т.А. Стабецкая

В работе представлен обобщённый метод синтеза обратных нелинейных операций расширенного матричного криптографического преобразования, построенный на основе специальных логических функций расширенного матричного криптографического преобразования n-й разрядности. На конкретных примерах нахождения математической модели обратной операции криптографического преобразования подтверждено корректность применения разработанного метода синтеза нелинейных операций.

Ключевые слова: *метод синтеза, матричная модель, матрица дополнений, элементарная функция, операция обратного преобразования, нелинейная операция, расширенное матричное криптографическое преобразование.*

GENERALIZED METHOD OF SYNTHESIS OF FEEDBACK NONLINEAR OPERATIONS OF EXPANDED MATRIX CRYPTOGRAPHIC TRANSFORMATIONS

V.N. Rudnitskiy, V.G. Babenko, T.A. Stabetskaya

This paper presents a generic method for the synthesis of nonlinear inverse operations expanded matrix cryptographic transformation, built on the basis of specific logical functions extended cryptographic transformation n- digit matrix. With specific examples of finding a mathematical model the inverse operation of cryptographic transformation confirmed the correctness of the developed method for the synthesis of non-linear operations.

Keywords: *synthesis method, matrix model, matrix additions, elementary function, operation of reverse conversion, nonlinear operation, expanded matrix cryptographic transformation.*