УДК 003.26:004.056.55

Стабецька Т. А.,
Черкаський державний технологічний університет, м. Черкаси, Україна

МАТЕМАТИЧНЕ ОБҐРУНТУВАННЯ УЗАГАЛЬНЕНОГО МЕТОДУ СИНТЕЗУ ОБЕРНЕНИХ ОПЕРАЦІЙ НЕЛІНІЙНОГО РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У статті проведено математичне обґрунтування узагальненого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення, які будуються на основі спеціальних логічних нелінійних функцій та подаються у вигляді матричних моделей. Також на прикладі показано коректність застосування створеного методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення.

Ключові слова: *операція прямого перетворення; операція оберненого перетворення; матриця доповнень; операція розширеного матричного криптографічного перетворення.*

Постановка проблеми

На даному етапі розвитку інформаційних технологій, який відзначається роботою з великими обсягами інформації, виникає ряд проблем, пов'язаних зі збереженням основних характеристик інформації, таких як цілісність, конфіденційність та доступність. Для їх вирішення розроблено ряд методів та засобів, серед яких важливе місце займають криптографічні методи. Одним із таких методів є метод синтезу прямих та обернених операцій розширеного матричного криптографічного перетворення інформації, який ґрунтується на основі використання спеціальних логічних функцій. За допомогою даних операцій здійснюється побудова криптоалгоритмів, швидкість дії яких залежить від розрядності операцій, які використовуються для перетворення інформації. Тому актуальним є питання розробки методів синтезу багаторозрядних операцій розширеного матричного криптографічного перетворення.

Аналіз останніх досліджень і публікацій

Провівши аналіз останніх досліджень і публікацій, варто виділити роботи [1; 2], в яких запропоновано метод синтезу трирозрядних операцій криптографічного перетворення інформації на основі елементарних операцій розширеного матричного представлення. У роботі [3] сформульовано правило побудови прямих багаторозрядних операцій розширеного матричного криптографічного перетворення. Суть дослідження в [4] полягає в побудові методу синтезу обернених багаторозрядних операцій нелінійного розширеного матричного криптографічного перетворення. Проте не було математично обґрунтовано коректність отриманого методу синтезу обернених багаторозрядних операцій розширеного матричного криптоперетворення. Тому для подальшого використання цього методу важливо побудувати математичне доведення його коректності.

Мета статті полягає у проведенні математичного обґрунтування коректності отриманого методу синтезу багаторозрядних обернених операцій розширеного матричного криптографічного перетворення.

Основний матеріал

Для проведення математичного обґрунтування побудованого методу синтезу обернених операцій розширеного матричного криптографічного перетворення введемо такі позначення:

$F_k^{(n)}$ – операція прямого перетворення n-ї розрядності;

$F_d^{(n)}$ – операція оберненого перетворення n-ї розрядності;

Правило синтезу обернених операцій розширеного матричного криптографічного перетворення сформулюємо у вигляді теореми.

Теорема. Для того, щоб побудувати обернену операцію розширеного матричного криптографічного перетворення, потрібно:

1. побудувати лінійну операцію оберненого перетворення в матричному представленні;
2. побудувати нелінійну матрицю доповнень без урахування знаків інверсії;
3. розставити в 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.

Доведення: Доведення проводиться методом математичної індукції. Покажемо спочатку, що теорема справджується для операції оберненого перетворення третьої розрядності. Потім припускаємо, що вона вірна для операції оберненого перетворення n-ї розрядності і доводимо теорему для операції оберненого перетворення (n+1)-ї розрядності.

1. Щоб довести теорему для операції оберненого перетворення 3-ї розрядності, виберемо довільну операцію прямого перетворення 3-ї розрядності $\overline{F}_k^{(3)}$, побудуємо для неї операцію розширеного матричного криптографічного оберненого перетворення $\overline{F}_d^{(3)}$, згідно зі сформульованою теоремою та покажемо, що отримана операція $\overline{F}_d^{(3)}$ задовольняє рівність: $\overline{F}_d^{(3)} \otimes \overline{F}_k^{(3)} = \overline{F}_r^{(3)}$, де $\overline{F}_r^{(3)}$ – еталонна (початкова) матриця або матриця-результат.

Нехай операція прямого перетворення задана матрицею:

$$\overline{F}_k^{(3)} = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \\ x_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j \end{pmatrix}, \qquad (1)$$

де $i, j, k \in [1,2,3]$, $i \neq j \neq k$;

x_i, , x_j, x_k – операнди-розряди інформації;

$\tilde{x}_i, \tilde{x}_j, \tilde{x}_k$ – операнди-розряди інформації, які можуть входити в доповнення у прямому та інверсному вигляді.

Позначимо рядки операції (1) змінними y_1, y_2, y_3 відповідно:

$$\overline{F}_k^{(3)} = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \\ x_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \end{matrix} \qquad (2)$$

Припустимо, для визначеності, що операція лінійного оберненого перетворення має вигляд:

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

Тоді, за теоремою, операція оберненого перетворення матиме вигляд:

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

Покажемо, що результатом виконання операції оберненого перетворення буде вираз:

$$\overline{F}_r = \begin{pmatrix} x_j & & \\ & x_i & \\ & & x_k \end{pmatrix}.$$

Опишемо процес виконання дій кожного рядка:

1) $y_2 \oplus \tilde{y}_1 \overline{\tilde{y}}_3 = x_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \oplus \left(\tilde{x}_i \oplus \tilde{x}_j \tilde{x}_k\right)\left(\overline{\tilde{x}}_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j\right) = x_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \oplus \tilde{x}_i \overline{\tilde{x}}_k \oplus$
$\oplus \tilde{x}_i \overline{\tilde{x}}_i \overline{\tilde{x}}_j \oplus \tilde{x}_j \tilde{x}_k \overline{\tilde{x}}_k \oplus \tilde{x}_j \tilde{x}_k \overline{\tilde{x}}_i \overline{\tilde{x}}_j = x_j$;

2) $y_1 \oplus \tilde{y}_2 \tilde{y}_3 = x_i \oplus \tilde{x}_j \tilde{x}_k \oplus \left(\tilde{x}_j \oplus \tilde{x}_i \overline{\tilde{x}}_k\right)\left(\tilde{x}_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j\right) = x_i \oplus \tilde{x}_j \tilde{x}_k \oplus \tilde{x}_j \tilde{x}_k \oplus$
$\oplus \tilde{x}_j \overline{\tilde{x}}_i \overline{\tilde{x}}_j \oplus \tilde{x}_i \overline{\tilde{x}}_k \tilde{x}_k \oplus \tilde{x}_i \overline{\tilde{x}}_k \overline{\tilde{x}}_i \overline{\tilde{x}}_j = x_i$;

3) $y_3 \oplus \overline{\tilde{y}}_1 \overline{\tilde{y}}_2 = x_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j \oplus \left(\overline{\tilde{x}}_i \oplus \tilde{x}_j \tilde{x}_k\right)\left(\overline{\tilde{x}}_j \oplus \tilde{x}_i \overline{\tilde{x}}_k\right) = x_k \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j \oplus \overline{\tilde{x}}_i \overline{\tilde{x}}_j \oplus$
$\oplus \overline{\tilde{x}}_i \tilde{x}_i \overline{\tilde{x}}_k \oplus \tilde{x}_j \tilde{x}_k \overline{\tilde{x}}_j \oplus \tilde{x}_j \tilde{x}_k \tilde{x}_i \overline{\tilde{x}}_k = x_k$.

Отже, теорема вірна для операції оберненого перетворення третьої розрядності.

2. Припустимо, що теорема правильна для операції оберненого перетворення n-ї розрядності $\overline{F}_d^{(n)}$. Це означає, що операція оберненого перетворення $\overline{F}_d^{(n)}$, побудована згідно з вимогами теореми, задовольняє рівність:

$$\overline{F}_d^{(n)} \otimes \overline{F}_k^{(n)} = \overline{F}_r^{(n)} \qquad (3)$$

Опишемо детальніше, що мається на увазі. Виберемо для цього деяку операцію прямого перетворення n-ї розрядності $\overline{F}_k^{(n)}$ та покажемо, що побудована для неї операція $\overline{F}_d^{(n)}$ задовольняє рівність (3).

Нехай операція прямого перетворення задається матрицею:

$$\overline{F}_k^{(n)} = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_l \tilde{x}_m \\ x_j \oplus \tilde{x}_i \tilde{x}_k \ldots \tilde{x}_l \tilde{x}_m \\ x_k \oplus \tilde{x}_i \tilde{x}_j \ldots \tilde{x}_l \tilde{x}_m \\ \ldots\ldots\ldots\ldots \\ x_l \oplus \tilde{x}_i \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_m \\ x_m \oplus \tilde{x}_i \tilde{x}_j \tilde{x}_k \ldots \tilde{x}_l \end{pmatrix}, \qquad (4)$$

де $i, j, k, l, m \in [1, \ldots, n]$ $n \in N$, $i \neq j \neq k \neq l \neq m$, $x_t \in [0,1]$, $t \in \{i, j, k, l, m\}$;

x_t – операнди-розряди інформації;

$\tilde{x}_t$ – операнди-розряди інформації, які можуть входити у доповнення в прямому та інверсному вигляді, а побудована для неї операція оберненого перетворення має вигляд:

$$\overline{F}_d^{(n)} = \begin{pmatrix} y_p \oplus \widetilde{y}_q \widetilde{y}_r \ldots \widetilde{y}_s \widetilde{y}_t \\ y_q \oplus \widetilde{y}_p \widetilde{y}_r \ldots \widetilde{y}_s \widetilde{y}_t \\ y_r \oplus \widetilde{y}_p \widetilde{y}_q \ldots \widetilde{y}_s \widetilde{y}_t \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ y_s \oplus \widetilde{y}_p \widetilde{y}_q \widetilde{y}_r \ldots \widetilde{y}_t \\ y_t \oplus \widetilde{y}_p \widetilde{y}_q \widetilde{y}_r \ldots \widetilde{y}_s \end{pmatrix}, \qquad (5)$$

де $p,q,r,s,t \in [1,\ldots,n]$, $n \in N$, $p \neq q \neq r \neq s \neq t$, $y_j \in [0,1]$, $j \in \{p,q,r,s,t\}$;

y_j – операнди-розряди інформації, які отримані в результаті застосування операції прямого перетворення відповідно;

$\widetilde{y}_j$ – операнди-розряди інформації, які можуть входити в доповнення у прямому та інверсному вигляді.

Результатом виконання кожного рядка операції оберненого перетворення повинен бути один із початкових операндів-розрядів інформації. Це означає, що для кожного рядка цієї операції повинна виконуватись рівність:

$$\begin{gathered} y_p + \widetilde{y}_q \widetilde{y}_r \ldots \widetilde{y}_s \widetilde{y}_t = x_i \oplus \widetilde{x}_j \widetilde{x}_k \otimes \ldots \otimes \widetilde{x}_l \widetilde{x}_m \oplus \\ \oplus \left(\widetilde{x}_j \oplus \widetilde{x}_i \widetilde{x}_k \otimes \ldots \otimes \widetilde{x}_l \widetilde{x}_m\right)\left(\widetilde{x}_k \oplus \widetilde{x}_i \widetilde{x}_j \otimes \ldots \otimes \widetilde{x}_l \widetilde{x}_m\right) \otimes \ldots \otimes, \\ \otimes \left(\widetilde{x}_l \oplus \widetilde{x}_i \widetilde{x}_j \widetilde{x}_k \otimes \ldots \otimes \widetilde{x}_m\right)\left(\widetilde{x}_m \oplus \widetilde{x}_i \widetilde{x}_j \widetilde{x}_k \otimes \ldots \otimes \widetilde{x}_l\right) = x_i \end{gathered} \qquad (6)$$

де $i,j,k,l,m,p,q,r,s,t \in [1,\ldots,n]$, $n \in N$.

Для проведення подальшого доведення для операції оберненого перетворення $(n+1)$-ї розрядності, опишемо аналітично процес виконання даної рівності. При цьому, для визначеності, змінні в розширеннях елементарних функцій і послідовність множників третього доданку розташуємо в порядку зростання індексів змінних, на основі яких синтезовані дані елементарні функції.

Отже, рівність (6) запишеться у вигляді:

$$\begin{gathered} x_i \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_n \oplus \ldots \oplus \\ \oplus \left(\widetilde{x}_1 \oplus \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n\right)\left(\widetilde{x}_2 \oplus \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n\right) \otimes \ldots \otimes \\ \otimes \left(\widetilde{x}_{i-1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-2} \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n\right)\left(\widetilde{x}_{i+1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \widetilde{x}_{i+2} \otimes \ldots \otimes \widetilde{x}_n\right) \otimes \ldots \otimes \\ \otimes \left(\widetilde{x}_{n-1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_n\right) \otimes \ldots \otimes \\ \otimes \left(\widetilde{x}_n \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_{n-1}\right) = \\ = x_i \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_n \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_n \oplus \\ \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_{n-1} \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_{n-1} \oplus \\ \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_n \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-2} \widetilde{x}_n \oplus \ldots \oplus \\ \oplus \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \oplus \\ \oplus \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \oplus \\ \oplus\ \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \otimes \ldots \otimes \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} = x_i \end{gathered} \qquad (7)$$

Рівність (7) показує, яким чином відбувається процес перетворення закодованої інформації в початкову при дії операції оберненого перетворення n-ї розрядності на операцію прямого перетворення n-ї розрядності. У ній другий і третій доданки обнуляються згідно з властивостями логічної суми $X \oplus X = 0$, а всі інші також перетворюються в нуль, виходячи з властивостей логічного добутку $\overline{X} \otimes X = 0$, оскільки за припущенням у них відбувається входження хоча б однієї пари однойменних множників-змінних із різним інверсним значенням.

4. Покажемо, що теорема справджується для операції оберненого перетворення $(n+1)$-ї розрядності. Тобто, побудована згідно з вимогами теореми, операція оберненого перетворення $\overline{F}_d^{(n+1)}$ задовольняє рівність: $\overline{F}_d^{(n+1)} \otimes \overline{F}_k^{(n+1)} = \overline{F}_r^{(n+1)}$.

Це означає, що для довільного рядка операції оберненого перетворення виконується рівність:

$$\begin{gathered} x_i \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \oplus \\ \left(\widetilde{x}_1 \oplus \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1}\right)\left(\widetilde{x}_2 \oplus \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1}\right) \otimes \ldots \otimes \\ \otimes \left(\widetilde{x}_{i-1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-2} \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1}\right)\left(\widetilde{x}_{i+1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \widetilde{x}_{i+2} \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1}\right) \otimes \ldots \otimes \\ \otimes \left(\widetilde{x}_{n-1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1}\right)\left(\widetilde{x}_n \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_{n+1}\right) \otimes \\ \otimes \left(\widetilde{x}_{n+1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n\right) = \\ = x_i \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \oplus \\ \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \oplus \\ \oplus \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_{n+1} \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_{n+1} \oplus \\ \oplus\ \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1} \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1} \oplus \ldots \oplus \\ \oplus \ldots \oplus \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \oplus \\ \oplus \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_{i-1} \widetilde{x}_{i+1} \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n-1} \widetilde{x}_n \widetilde{x}_{n+1} \oplus \ldots \oplus \\ \oplus \widetilde{x}_2 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_{n+1} \widetilde{x}_1 \widetilde{x}_3 \otimes \ldots \otimes \widetilde{x}_n \widetilde{x}_{n+1} \otimes \ldots \otimes \widetilde{x}_1 \widetilde{x}_2 \otimes \ldots \otimes \widetilde{x}_i \otimes \ldots \otimes \widetilde{x}_n = x_i \end{gathered} \qquad (8)$$

Другий і третій доданки обнуляються, виходячи з властивості логічної суми $X \oplus X = 0$. До четвертого доданка рівності (8) входять усі елементи 4-го доданка рівності (7), а також множник $\widetilde{x}_n$. Оскільки четвертий доданок рівності (7) за припущенням дорівнює нулю, то приєднання до нього додаткового множника $\widetilde{x}_n$ не змінює його значення. Отже, відповідний доданок рівності (8) також перетворюється в нуль.

До 5-го доданку рівності (8) входять також усі елементи четвертого доданка рівності (7), а також множник $\widetilde{x}_{n+1}$, який не впливає на результат добутку. Тому п'ятий доданок рівності (8) також перетворюється в нуль. Аналогічно, всі інші доданки виразу (8) також обнуляються, виходячи з вищенаведених міркувань. Таким чином показано, що ця теорема справджується для операції оберненого перетворення $(n + 1)$-ї розрядності.

Тому теорема є правильною для операції оберненого перетворення довільної розрядності. Теорему доведено.

Отже, доведено коректність побудованого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення. Покажемо застосування цього методу на прикладі.

Приклад. Нехай операція розширеного матричного криптографічного прямого перетворення задана матрицею:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3\overline{x}_4 \\ x_1 \oplus \overline{x}_2\overline{x}_3 x_4 \\ x_4 \oplus x_1\overline{x}_2 x_3 \\ x_3 \oplus x_1 x_2 x_4 \end{pmatrix} \tag{9}$$

Побудуємо для неї операцію розширеного матричного криптографічного оберненого перетворення.

Позначимо рядки матриці (9) змінними y_1, y_2, y_3, y_4 відповідно:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3\overline{x}_4 \\ x_1 \oplus \overline{x}_2\overline{x}_3 x_4 \\ x_4 \oplus x_1\overline{x}_2 x_3 \\ x_3 \oplus x_1 x_2 x_4 \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \\ \to y_4 \end{matrix} \tag{10}$$

1. Побудуємо лінійну операцію оберненого перетворення для лінійної операції прямого перетворення $\overline{F}_k = \begin{pmatrix} x_2 \\ x_1 \\ x_4 \\ x_3 \end{pmatrix}$. Вона матиме вигляд: $\overline{F}_d^{lin} = \begin{pmatrix} y_2 \\ y_1 \\ y_4 \\ y_3 \end{pmatrix}$.

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

$$\overline{F}_d = \begin{pmatrix} y_2 \oplus \widetilde{y}_1\widetilde{y}_3\widetilde{y}_4 \\ y_1 \oplus \widetilde{y}_2\widetilde{y}_3\widetilde{y}_4 \\ y_4 \oplus \widetilde{y}_1\widetilde{y}_2\widetilde{y}_3 \\ y_3 \oplus \widetilde{y}_1\widetilde{y}_2\widetilde{y}_4 \end{pmatrix} \tag{11}$$

3. Розставивши знаки інверсії, згідно з вимогами теореми, отримаємо операцію оберненого перетворення, яка матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_2 \oplus \overline{y}_1 y_3\overline{y}_4 \\ y_1 \oplus y_2\overline{y}_3\overline{y}_4 \\ y_4 \oplus y_1 y_2 y_3 \\ y_3 \oplus \overline{y}_1 y_2 y_4 \end{pmatrix} \tag{12}$$

Покажемо, що побудована операція криптографічного перетворення (12) дійсно є оберненою операцією для операції прямого перетворення (9). Для цього опишемо процес виконання дій кожного рядка:

$$\begin{aligned}
&1)\quad y_2 \oplus \overline{y}_1 y_3\overline{y}_4 = x_1 \oplus \overline{x}_2\overline{x}_3 x_4 \oplus \left(\overline{x}_2 \oplus x_1\overline{x}_3\overline{x}_4\right)\left(x_4 \oplus x_1\overline{x}_2 x_3\right)\left(\overline{x}_3 \oplus x_1 x_2 x_4\right) = \\
&= x_1 \oplus \overline{x}_2\overline{x}_3 x_4 \oplus \overline{x}_2\overline{x}_3 x_4 \oplus \overline{x}_2 x_4 x_1 x_2 x_4 \oplus \overline{x}_2\overline{x}_3 x_1\overline{x}_2 x_3 \oplus \overline{x}_3 x_4 x_1\overline{x}_3\overline{x}_4 \oplus \overline{x}_2 x_1\overline{x}_2 x_3 x_1 x_2 x_4 \oplus \\
&\oplus x_4 x_1\overline{x}_3\overline{x}_4 x_1 x_2 x_4 \oplus \overline{x}_3 x_1\overline{x}_3\overline{x}_4 x_1\overline{x}_2 x_3 \oplus x_1\overline{x}_3\overline{x}_4 x_1\overline{x}_2 x_3 x_1 x_2 x_4 = x_1\,; \\
&2)\quad y_1 \oplus y_2\overline{y}_3\overline{y}_4 = x_2 \oplus x_1\overline{x}_3\overline{x}_4 \oplus \left(x_1 \oplus \overline{x}_2\overline{x}_3 x_4\right)\left(\overline{x}_4 \oplus x_1\overline{x}_2 x_3\right)\left(\overline{x}_3 \oplus x_1 x_2 x_4\right) = \\
&= x_2 \oplus x_1\overline{x}_3\overline{x}_4 \oplus x_1\overline{x}_3\overline{x}_4 \oplus x_1\overline{x}_4 x_1 x_2 x_4 \oplus x_1\overline{x}_3 x_1\overline{x}_2 x_3 \oplus \overline{x}_3\overline{x}_4\overline{x}_2\overline{x}_3 x_4 \oplus x_1 x_1\overline{x}_2 x_3 x_1 x_2 x_4 \oplus \\
&\oplus \overline{x}_4\overline{x}_2\overline{x}_3 x_4 x_1 x_2 x_4 \oplus \overline{x}_3\overline{x}_2\overline{x}_3 x_4 x_1\overline{x}_2 x_3 \oplus \overline{x}_2\overline{x}_3 x_4 x_1\overline{x}_2 x_3 x_1 x_2 x_4 = x_2\,; \\
&3)\quad y_4 \oplus y_1 y_2 y_3 = x_3 \oplus x_1 x_2 x_4 \oplus \left(x_2 \oplus x_1\overline{x}_3\overline{x}_4\right)\left(x_1 \oplus \overline{x}_2\overline{x}_3 x_4\right)\left(x_4 \oplus x_1\overline{x}_2 x_3\right) = \\
&= x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_4 \oplus x_2 x_1 x_1\overline{x}_2 x_3 \oplus x_2 x_4\overline{x}_2\overline{x}_3 x_4 \oplus x_1 x_4 x_1\overline{x}_3\overline{x}_4 \oplus x_2\overline{x}_2\overline{x}_3 x_4 x_1\overline{x}_2 x_3 \oplus \\
&\oplus x_1 x_1\overline{x}_3\overline{x}_4 x_1\overline{x}_2 x_3 \oplus x_4 x_1\overline{x}_3\overline{x}_4\overline{x}_2\overline{x}_3 x_4 \oplus x_1\overline{x}_3\overline{x}_4\overline{x}_2\overline{x}_3 x_4 x_1\overline{x}_2 x_3 = x_3\,; \\
&4)\quad y_3 \oplus \overline{y}_1 y_2 y_4 = x_4 \oplus x_1\overline{x}_2 x_3 \oplus \left(\overline{x}_2 \oplus x_1\overline{x}_3\overline{x}_4\right)\left(x_1 \oplus \overline{x}_2\overline{x}_3 x_4\right)\left(x_3 \oplus x_1 x_2 x_4\right) = \\
&= x_4 \oplus x_1\overline{x}_2 x_3 \oplus x_1\overline{x}_2 x_3 \oplus x_1\overline{x}_2 x_1 x_2 x_4 \oplus \overline{x}_2 x_3\overline{x}_2\overline{x}_3 x_4 \oplus x_1 x_3 x_1\overline{x}_3\overline{x}_4 \oplus \overline{x}_2\overline{x}_2\overline{x}_3 x_4 x_1 x_2 x_4 \oplus \\
&\oplus x_1 x_1\overline{x}_3\overline{x}_4 x_1 x_2 x_4 \oplus x_3 x_1\overline{x}_3\overline{x}_4\overline{x}_2\overline{x}_3 x_4 \oplus x_1\overline{x}_3\overline{x}_4\overline{x}_2\overline{x}_3 x_4 x_1 x_2 x_4 = x_4\,.
\end{aligned}$$

Отже, показано, що побудована операція криптографічного перетворення (12) дійсно є оберненою операцією для операції прямого перетворення (9).

Висновки

У статті проведено математичне обґрунтування узагальненого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення. Також на прикладі моделі матриці чотирьохрозрядної операції розширеного матричного криптографічного перетворення підтверджено коректність застосування запропонованого методу.

ЛІТЕРАТУРА

1. Бабенко В. Г. Синтез нелінійних операцій криптографічного перетворення / В. Г. Бабенко, О. Г. Мельник, Т. А. Стабецька // Безпека інформації: наук. журнал. – К. : НАУ, 2014. – Т. 20. – № 2. – С. 143–147.
2. Бабенко В. Г. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення / В. Г. Бабенко, Т. А. Стабецька // Системи управління навігації та зв'язку. – 2013. – Вип. 3 (27). – С. 117–119.
3. Бабенко В. Г. Построение нелинейных операций расширенного матричного криптографического преобразования / В. Г. Бабенко, О. Г. Мельник, Т. А. Стабецька // Криптографическое кодирование : [коллективная монография] / под редакцией В. Н. Рудницкого, В. Я. Мильчевича. – Х. : Изд-во ООО «Щедрая усадьба плюс», 2014. – С. 41–55.
4. Рудницький В. М. Узагальнений метод синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення / В. М. Рудницький, В. Г. Бабенко, Т. А. Стабецька // Системи обробки інформації. – 2013. – Вип. 6 (122). – С. 118–121.
5. Рудницький В. М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький // Зб. наук. пр. «Кібернетика та системний аналіз». – Х. : ХУПС, 2012. – Вип. 4 (33). – С. 198–200.

Стабецкая Т. А., *Черкасский государственный технологический университет, г. Черкассы, Украина.*

МАТЕМАТИЧЕСКОЕ ОБОСНОВАНИЕ ОБОБЩЁННОГО МЕТОДА СИНТЕЗА ОБРАТНЫХ ОПЕРАЦИЙ НЕЛИНЕЙНОГО РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В данной статье построено математическое обоснование обобщённого метода синтеза обратных операций нелинейного расширенного матричного криптографического преобразования, которые строятся на основе специальных логических нелинейных функций и представляются с помощью матричных моделей. Также на примере показано корректность применения созданного метода синтеза обратных операций нелинейного расширенного матричного криптографического преобразования.

Ключевые слова: *операция прямого преобразования; операция обратного преобразования; матрица дополнений; операция расширенного матричного криптографического преобразования.*

Stabetskaya T. A., *Cherkasy State Technological University, Cherkasy city, Ukraine.*

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

This paper presents constructed a mathematical justification of the generalized method for the synthesis of nonlinear inverse operations expanded matrix cryptographic transformation, built on the basis of specific logical functions extended cryptographic transformation and are represented by the matrix models. Also, the example shows the correct use of established method for the synthesis of nonlinear operations of expanded matrix cryptographic transformation.

Key words: *operation of direct conversion; operation of reverse conversion; matrix additions; operation of expanded matrix cryptographic transformation.*

© Стабецька Т. А., 2014

Дата надходження статті до редколегії 08.12.2014 р.