УДК 004.056.55:004.312.2

Р.П. Мельник[1], В.Г. Бабенко[2], С.В. Гончар[1]

[1]*Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси*
[2]*Черкаський державний технологічний університет, Черкаси*

УДОСКОНАЛЕНИЙ МЕТОД СИНТЕЗУ РОЗШИРЕНИХ МАТРИЧНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ДЛЯ КРИПТОПЕРЕТВОРЕННЯ ДАНИХ

У даній статті розроблено метод синтезу т-розрядних розширених матричних елементарних функцій, синтезовано моделі прямої та оберненої т-розрядної елементарної функції розширеного матричного перетворення в дискретному представленні. Проведені дослідження показали значний ріст кількості елементарних функцій розширеного матричного перетворення в залежності від розрядності моделі криптоперетворення.

Ключові слова: *криптографічний захист інформації, метод синтезу, елементарна функція, розширене матричне криптографічне перетворення.*

Вступ

Актуальність проблеми. Стрімкий розвиток інформаційних систем, комп'ютеризація та впровадження новітніх технологій в усі сфери діяльності суспільства й держави в цілому значно прискорює та удосконалює роботу організацій, підприємств, установ усіх форм власності. Однак, такий розвиток несе в собі цілий ряд загроз, пов'язаних з порушеннями конфіденційності, цілісності та доступності інформації, які, в свою чергу, призводять до різних втрат, у тому числі й фінансовим. Тому важливою проблемою є постійне підвищення якості систем захисту інформації.

Надійний захист інформаційно-телекомунікаційних систем від злочинних посягань можливо забезпечити лише шляхом впровадження системи комплексного захисту інформації, яка включає в себе застосування криптографічних та технічних засобів захисту, а також виконання ряду організаційних та організаційно-технічних заходів. На відміну від інших методів, криптографічні 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 збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії [1, 2].

Вдосконалити існуючі криптографічні системи захисту інформації та розробити нові криптографічні алгоритми можна за допомогою розширення спектра операцій, на основі яких вони будуються [3, 4].

Аналіз останніх досліджень. Серед останніх досліджень і публікацій варто виділити: [5, 6], де розроблено метод реалізації операцій розширеного матричного криптографічного перетворення інформації та здійснено оцінку ефективності використання даних операцій для криптографічного захисту інформації, та [7, 8], в яких доведено, що використання розширених матричних функцій криптографічного перетворення підвищує швидкодію обробки даних в криптосистемах за рахунок паралельного процесу виконання операцій криптоперетворення.

Але в даних дослідженнях не було розглянуто питання щодо розробки методу синтезу трирозрядних розширених матричних елементарних функцій для криптоперетворення даних більшої розрядності, що й робить тему дослідження актуальною.

Мета роботи полягає в розробці методу синтезу трирозрядних розширених матричних елементарних функцій для криптографічного перетворення даних більшої розрядності, для чого потрібно знайти повну множину трирозрядних розширених матричних елементарних функцій та загальну кількість трирозрядних елементарних функцій розширеного матричного перетворення.

Виклад основного матеріалу

Приклади використання методу синтезу трирозрядних розширених матричних елементарних функцій наведені в [9], по аналогії можна отримати метод синтезу трирозрядних розширених матричних елементарних функцій для криптоперетворення даних більшої розрядності. Для цього необхідно модифікувати розроблений метод синтезу в наступній редакції:

1. На основі узагальнених правил синтезу прямих трирозрядних розширених матричних елементарних функцій (вираз: $f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l)$) шляхом перебору значень i, j, l, де $i \in [1, 2, \ldots, n]$, $j \in [1, 2, \ldots, n]$, $l \in [1, 2, \ldots, n]$ за умови $i \neq j \neq l$; $j < l$, отримати n основних трирозрядних розширених матричних елементарних функцій.

2. На основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$, де, $\hat{x}_j \in [x_j, \overline{x}_j]$, $\hat{x}_l \in [x_l, \overline{x}_l]$, підставивши отримані набори в три основні трирозрядні розширені матричні елементарні функції, отримати повну множину прямих трирозрядних розширених матричних елементарних функцій.

3. На основі узагальнених правил синтезу обернених трирозрядних розширених матричних елементарних функцій (вираз: $f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \oplus 1$), інвертувавши множину прямих трирозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, буде отримана множина обернених розширених матричних елементарних функцій.

4. Об'єднавши множини прямих і обернених елементарних функцій буде отримана повна множина трирозрядних розширених матричних елементарних функцій.

Визначимо кількість елементарних функцій розширеного матричного перетворення будь-якої розрядності.

Кількість елементарних функцій розширеного матричного перетворення визначається:

$$K_П = K_O = 12 \cdot C_n^3 = \frac{12n!}{3!(n-3)!}, \qquad (1)$$

де $K_П$ – кількість прямих елементарних функцій; K_O – кількість обернених елементарних функцій; C – кількість сполучень із n по 3; n – кількість розрядів; 3 – розрядність функцій.

Загальна кількість трирозрядних елементарних функцій розширеного матричного перетворення визначається:

$$K_\Sigma = K_П + K_O = 24 \cdot C_n^3. \qquad (2)$$

Розширені матричні елементарні функції можуть бути не лише трирозрядними.

Метод синтезу m-розрядних розширених матричних елементарних функцій полягає в наступному:

1. На основі виразу:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot ... \cdot \hat{x}_q) \qquad (3)$$

шляхом перебору значень i, j, l, … , q, де $i \in [1, 2, ..., n]$, $j \in [1, 2, ..., n]$, $l \in [1, 2, ..., n]$, …, $q \in [1, 2, ..., n]$ за умови:

$$i \neq j \neq l \neq ... \neq q;\ j < l < ... < q,$$

отримати основні n–розрядні розширені матричні елементарні функції.

2. На основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$, …, $\hat{x}_q$ де, $\hat{x}_j \in [x_j, \overline{x}_j]$, $\hat{x}_l \in [x_l, \overline{x}_l]$, … , $\hat{x}_q \in [x_q, \overline{x}_q]$, підставивши отримані набори основні трирозрядні розширені матричні елементарні функції, отримати повну множину прямих трирозрядних розширених матричних елементарних функцій.

3. На основі виразу:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot ... \cdot \hat{x}_q) \oplus 1, \qquad (4)$$

інвертувавши множину прямих трирозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, буде отримана множина обернених розширених матричних елементарних функцій.

4. Об'єднавши множини прямих і обернених елементарних функцій буде отримана повна множина трирозрядних розширених матричних елементарних функцій.

Кожна із синтезованих m-розрядних елементарних функцій розширеного матричного перетворення може бути використана в криптографії, тому що для виразів (3) та (4) будуть справедливі співвідношення:

$$\sum_{x=0}^{2^m-1} (x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot ... \cdot \hat{x}_q)) = C_{2^m}^{2^{m-1}};$$

$$\sum_{x=0}^{2^m-1} (x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot ... \cdot \hat{x}_q) \oplus 1) = C_{2^m}^{2^{m-1}}.$$

Виходячи з виразу (3), можна синтезувати модель прямої m-розрядної елементарної функції розширеного матричного перетворення в дискретному представленні:

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee ... \vee x_i \cdot \hat{x}_q \vee \vee \left(\overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l \cdot ... \cdot \overline{\hat{x}}_q\right). \qquad (5)$$

де $i \in [1, 2, ..., n]$, $j \in [1, 2, ..., n]$, $l \in [1, 2, ..., n]$, …, $q \in [1, 2, ..., n]$ за умов:

$$i \neq j \neq l \neq ... \neq q \ \text{ і } \ j < l < ... < q.$$

На основі правил синтезу прямих елементарних функцій (вираз: $f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l$ [9]) та виходячи з виразу (3), можна синтезувати модель оберненої m-розрядної елементарної функції розширеного матричного перетворення в дискретному представленні:

$$f = \overline{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee ... \vee \overline{x}_i \cdot \hat{x}_q \vee \vee \left(x_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l \cdot ... \cdot \overline{\hat{x}}_q\right).$$

Кількість m-розрядних елементарних функцій розширеного матричного перетворення визначається:

$$K_П = K_O = 2^{m-1} \cdot m \cdot C_n^m = \frac{2^{m-1} \cdot m \cdot n!}{m!(n-m)!}. \qquad (6)$$

Загальна кількість m-розрядних елементарних функцій розширеного матричного перетворення на основі виразу (6) визначається:

$$K_{\Sigma} = K_{П} + K_{О} = \\ = 2 \cdot 2^{m-1} \cdot m \cdot C_{n}^{m} = \frac{2^{m} \cdot m \cdot n!}{m!(n-m)!}. \quad (7)$$

Для криптографічного перетворення m-розрядної інформації можуть бути використані елементарні функції розрядності від 3 до n.

Кількість m-розрядних елементарних функцій розширеного матричного перетворення можна отримати на основі виразу (7):

$$K_{\Sigma} = \sum_{m=3}^{n} \frac{2^{m} \cdot m \cdot n!}{m!(n-m)!} \quad (8)$$

Аналіз виразу (8) показує значний ріст кількості елементарних функцій розширеного матричного перетворення в залежності від розрядності моделі криптоперетворення.

Висновки

Проведені дослідження дозволили розробити метод синтезу на основі трирозрядних розширених матричних елементарних функцій для криптографічного перетворення даних більшої розрядності, що, в свою чергу, забезпечить підвищення якості функціонування систем захисту інформаційних ресурсів на основі розширеного матричного криптографічного перетворення, а також дасть можливість забезпечити необхідні значення швидкості шифрування та криптостійкості.

Список літератури

1. Криптографическое кодирование: коллективная монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – 240 с.

2. Криптографическое кодирование: методы и средства реализации (часть 2): моногр. / 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.

3. Бабенко В.Г. Визначення множини трирозрядних елементарних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький, Р.П. Мельник // Теоретичний і науково-практичний журнал інженерної академії України «Вісник інженерної академії України». – 2012. – № 3-4. – С. 77-79.

4. Бабенко В.Г. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В.Г. Бабенко, О.Г. Мельник, Р.П. Мельник // Безпека інформації. – 2013. – С. 56-59.

5. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 9 (107). – С. 145-147.

6. Мельник Р.П. Використання розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник, О.Г. Мельник // Проблеми інформатизації: мат-ли II міжнар. наук.-техн. конф., 25-26 листопада 2014 р. – Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. – С. 11.

7. Бабенко В.Г. Параллельная реализация нелинейного расширенного матричного криптографического преобразования // В.Г. Бабенко, С.В. Пивнева, О.Г. Мельник, Р.П. Мельник // Вектор науки Тольяттинского государственного университета. – 2014. – № 3 (29). – С. 17-20.

8. Бабенко В.Г. Оцінка ефективності використання операцій криптографічного перетворення / В.Г. Бабенко, Р.П. Мельник, С.В. Гончар // Вісник інженерної академії України. – Вип. 2. – 2014. – С. 39-41.

9. Мельник Р.П. Методи та засоби синтезу операцій розширеного матричного криптографічного перетворення : дис. канд. техн. наук : 05.13.21 / Р.П. Мельник. – Черкаси, 2013. – 178 с.

Надійшла до редколегії 17.02.2015

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД СИНТЕЗА РАСШИРЕННЫХ МАТРИЧНЫХ ЭЛЕМЕНТАРНЫХ ФУНКЦИЙ ДЛЯ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ

Р.П. Мельник, В.Г. Бабенко, С.В. Гончар

В данной статье разработан метод синтеза m-разрядных расширенных матричных элементарных функций, синтезированы модели прямой и обратной m-разрядной элементарной функции расширенного матричного преобразования в дискретном представлении. Проведенные исследования показали значительный рост количества элементарных функций расширенного матричного преобразования в зависимости от разрядности модели криптопреобразования.

Ключевые слова: *криптографическая защита информации, метод синтеза, элементарная функция, расширенное матричное криптографическое преобразование.*

AN IMPROVED METHOD FOR THE SYNTHESIS OF EXTENDED MATRIX OF ELEMENTARY FUNCTIONS FOR CRYPTOGRAPHIC TRANSFORMATION OF DATA

R.P. Melnyk, V.G. Babenko, S.V. Gonchar

In this paper was develop a method for the synthesis of m-capacity extended matrix of elementary functions, synthesized model of direct and inverse m-capacity unit features an expanded matrix transformation in a discrete representation. Studies have shown a significant increase in the number of elementary functions expanded matrix transformation depending on the bit patterns cryptographic transformation.

Keywords: *cryptographic protection of information, method of synthesis, elementary function, advanced cryptographic transformation matrix.*