© Babenko V., Melnyk O., Stabetska T. The synthesis of nonlinear operations for cryptographic transformation // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 143-147.

СИНТЕЗ НЕЛІНІЙНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Віра Бабенко[1], Ольга Мельник[2], Тетяна Стабецька[3]

[1]Одеська національна академія зв'язку ім. О.С. Попова, Україна
[2]Академія пожежної безпеки імені Героїв Чорнобиля, Україна
[3]Черкаський державний технологічний університет, Україна

БАБЕНКО Віра Григорівна, к.т.н.

Рік та місце народження: 1984 рік, м. Золотоноша, Черкаська область, Україна.
Освіта: Черкаський державний технологічний університет, 2006 рік.
Посада: докторант Одеської національної академії зв'язку ім. О.С. Попова з 2011 року.
Наукові інтереси: криптографічні методи захисту інформації.
Публікації: більше 50 наукових публікацій, серед яких монографії, навчально-методичні розробки, навчальні посібники, наукові статті.
E-mail: zolot_verba@rambler.ru

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 ім. Богдана Хмельницького, 2010 рік.
Посада: доцент кафедри будівельних конструкцій з 2012 року.
Наукові інтереси: методи та засоби побудови комп'ютеризованих систем прогнозування, розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 30 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: melnyk_olja_2012@mail.ru

СТАБЕЦЬКА Тетяна Анатоліївна

Рік та місце народження: 1987 рік, м. Біла Церква, Київська область, Україна.
Освіта: Черкаський національний університет ім. Богдана Хмельницького, 2010 рік.
Посада: аспірант Черкаського державного технологічного університету з 2012 року.
Наукові інтереси: розробка математичних методів захисту інформації та їх реалізація на основі операцій криптографічного перетворення.
Публікації: 5 наукових публікацій.
E-mail: tatiana_ami@ukr.net

Анотація. *У даній статті розроблені правила синтезу нелінійних операцій прямого та оберненого криптографічного перетворення, а також формалізовано модель побудови елементарних функцій розширеного матричного криптографічного перетворення. З використанням матричних моделей, що описують операції розширеного матричного криптографічного перетворення, які синтезовані на основі різних аргументів, отримано загальне правило синтезу доповнення. Застосування даних правил забезпечує синтез обернених операцій розширеного матричного криптографічного перетворення з будь-якою кількістю доповнень. На конкретних прикладах підтверджено коректність застосування отриманих правил для операції розширеного матричного криптографічного перетворення синтезованої на основі трьох замін. Застосування отриманих правил формує основний підхід щодо побудови операцій розширеного матричного криптографічного перетворення інформації. Дані результати можуть знайти своє практичне застосування при розробці програмно-апаратних засобів для систем захисту інформації.*

Ключові слова: *елементарні функції, нелінійна операція криптографічного перетворення, обернена операція, операція розширеного матричного перетворення.*

Постановка проблеми

Криптографічні методи та засоби захисту інформації є основними базовими складовими систем інформаційної безпеки в сучасних умовах технічного розвитку. В свою чергу поширення інформаційних технологій у сфери життя та зростання обсягів інформації, що обробляється та передається, вимагає постійного вдосконалення властивостей стійкості та швидкодії криптографічних алгоритмів, що застосовуються. Базою будь-якого криптоалгоритму є функції перетворення інформації, що синтезуються згідно визначених математичних правил та властивостей та забезпечують обмеження несанкціонованого доступу до інформації, а також контроль за зміною її змісту.

Отже задача вдосконалення криптоалгоритмів напряму пов'язана з вдосконаленням або пошуком нових функцій криптографічного перетворення, застосування яких надасть можливість покращити властивості відомих криптоалгоритмів та забезпечить достатній рівень стійкості систем захисту.

Таким чином, перспективним напрямком досліджень можна вважати пошук та синтез функцій криптографічного перетворення інформації з заданими властивостями, застосування яких забезпечить конфіденційність інформації користувача.

Аналіз останніх досліджень і публікацій

Серед останніх досліджень і публікацій варто виділити: [1], де проведено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності елементарних функцій та способу перетворення ними інформації, та [2,3], де було розглянуто синтез операцій криптографічного перетворення на основі елементарних функцій розширеного матричного представлення.

Проте в даних дослідженнях не було сформульовано та математично обґрунтовано правил побудови оберненої операції розширеного матричного криптографічного перетворення.

Мета статті полягає в формалізації матричної моделі нелінійної операції криптографічного перетворення та розробці правил синтезу прямих та обернених операцій.

Виклад основного матеріалу

При розробці криптографічних засобів захисту інформації неабияку зацікавленість виявляють до нелінійних функцій перетворення. Функція перетворення, яка не може бути описана поліномом $f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n$, $n = 1, 2, ...$ є нелінійною [4, ст. 58-59].

Виходячи з цього елементарні функції виду

$$f = x_i \oplus \left(x_j \cdot x_k \right), \qquad (1)$$

забезпечують побудову нелінійних операцій криптографічного перетворення.

За результатами обчислювального експерименту було встановлено, що операція криптографічного перетворення, побудована на основі функцій виду (1) обов'язково повинна мати операнди x_j та x_k в прямому та інверсному представленні.

Розглянемо синтез операцій криптографічного перетворення на основі заміни трьох елементарних функцій на функції розширеного матричного перетворення.

Згідно отриманої в [5] моделі синтезу нелінійної операції розширеного матричного криптографічного перетворення на основі двох замін синтезуємо операцію криптографічного перетворення.

Першою елементарною функцією повинна бути функція розширеного матричного перетворення операції на основі x_1:

$$f = x_1 \oplus \left(\hat{x}_2 \cdot \hat{x}_3 \right), \qquad (2)$$

де $\hat{x}$ - це аргумент, що може приймати будь-яке значення інверсії.

Друга функція на основі x_2 має інверсне значення x_3 першої функції, x_1 може приймати будь-яке значення.

Виходячи з цього, друга елементарна функція матиме представлення

$$f = x_2 \oplus \left(\hat{x}_1 \cdot \bar{\hat{x}}_3 \right). \qquad (3)$$

Третя функція на основі x_3 має інверсне значення x_1, x_2 приймає інверсне значення x_2 другого елемента доповнення першої елементарної функції.

Виходячи з цього, третя елементарна функція матиме представлення

$$f = x_3 \oplus \left(\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2 \right). \qquad (4)$$

Враховуючи вирази (2), (3), (4), операція криптографічного перетворення при синтезі, починаючи з першої елементарної функції, має вигляд:

$$\bar{F}_k = \begin{pmatrix} x_1 \oplus \left(\hat{x}_2 \cdot \hat{x}_3 \right) \\ x_2 \oplus \left(\hat{x}_1 \cdot \bar{\hat{x}}_3 \right) \\ x_3 \oplus \left(\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2 \right) \end{pmatrix}. \qquad (5)$$

По аналогії, якщо почати синтез з другої функції, отримаємо:

$$\bar{F}_k = \begin{pmatrix} x_1 \oplus \left(\hat{x}_2 \cdot \bar{\hat{x}}_3 \right) \\ x_2 \oplus \left(\hat{x}_1 \cdot \hat{x}_3 \right) \\ x_3 \oplus \left(\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2 \right) \end{pmatrix}. \qquad (6)$$

По аналогії, якщо почати синтез з третьої функції, отримаємо:

$$\bar{F}_k = \begin{pmatrix} x_1 \oplus \left(\bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3 \right) \\ x_2 \oplus \left(\bar{\hat{x}}_1 \cdot \hat{x}_3 \right) \\ x_3 \oplus \left(\hat{x}_1 \cdot \hat{x}_2 \right) \end{pmatrix}. \qquad (7)$$

Вирази (5)-(7) дозволяють синтезувати операції прямого криптографічного перетворення на основі розширеного матричного представлення.

Як бачимо, матричні моделі (5)-(7) можливо представити у вигляді суми двох матриць: матриці

аргументів, яка є лінійною, та нелінійної матриці доповнень.

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

Правило синтезу доповнення наступне: для того, щоб утворити доповнення 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 процес побудови матричної моделі оберненої операції полягає в наступному. Для того, щоб побудувати для операції розширеного матричного криптографічного перетворення з трьома доповненнями матричну модель операції оберненого криптографічного перетворення, потрібно виконати дії, описані наступними правилами:

Правило 1. Побудувати лінійну операцію оберненого перетворення у матричному представленні.

Правило 2. Побудувати відповідні три 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.

Здійснимо перевірку результатів застосування отриманих правил для синтезу нелінійних операцій криптографічного перетворення. Розглянемо одну з можливих операцій перетворення. Нехай дано матрицю, яка описує операцію розширеного перетворення

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

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

Позначимо рядки матриці $\overline{F_k}$ змінними y_1, y_2, y_3 відповідно.

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

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 $\overline{F}_k$ згідно з вказаними перетвореннями у матриці $\overline{F}_d$, 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 $x_j x_k$ та виконати логічне додавання за модулем 2 з рядком i-го індексу. Тоді отримаємо:

$$x_i \oplus x_j x_k \oplus \left(x_j \oplus \overline{x}_i \overline{x}_k\right) \otimes \left(x_k \oplus x_i \overline{x}_j\right) =$$
$$= x_i \oplus x_j x_k \oplus x_j x_k \oplus x_j x_i \overline{x}_j \oplus \overline{x}_i \overline{x}_k x_k \oplus$$
$$\oplus \overline{x}_i \overline{x}_k x_i \overline{x}_j = x_i \oplus x_j x_k \oplus x_j x_k = x_i.$$

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

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

Тоді отримаємо:

$$x_j \oplus \overline{x}_i \overline{x}_k \oplus \overline{\left(x_i \oplus x_j x_k\right)} \otimes \overline{\left(x_k \oplus x_i \overline{x}_j\right)} =$$
$$= x_j \oplus \overline{x}_i \overline{x}_k \oplus \left(\overline{x}_i \oplus x_j x_k\right)\left(\overline{x}_k \oplus x_i \overline{x}_j\right) =$$
$$= x_j \oplus \overline{x}_i \overline{x}_k \oplus \overline{x}_i \overline{x}_k \oplus \overline{x}_i x_i \overline{x}_j \oplus x_j x_k \overline{x}_k \oplus$$
$$\oplus x_j x_k x_i \overline{x}_j = x_j \oplus \overline{x}_i \overline{x}_k \oplus \overline{x}_i \overline{x}_k = x_j.$$

Використовуючи змінні y_1, y_2, y_3, синтез змінної x_j матиме вигляд: $y_2 + \overline{y}_1 \overline{y}_3$.

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

Тоді отримаємо:

$$x_k \oplus x_i \overline{x}_j \oplus \left(x_i \oplus x_j x_k\right) \overline{\left(x_j \oplus \overline{x}_i \overline{x}_k\right)} =$$
$$x_k \oplus x_i \overline{x}_j \oplus \left(x_i \oplus x_j x_k\right)\left(\overline{x}_j \oplus \overline{x}_i \overline{x}_k\right) =$$
$$= x_k \oplus x_i \overline{x}_j \oplus x_i \overline{x}_j \oplus x_i \overline{x}_i \overline{x}_k \oplus x_j x_k \overline{x}_j \oplus$$
$$\oplus x_j x_k \overline{x}_i \overline{x}_k = x_k \oplus x_i \overline{x}_j \oplus x_i \overline{x}_j = x_k.$$

Використовуючи змінні y_1, y_2, y_3, синтез змінної x_k матиме вигляд: $y_3 + y_1 \overline{y}_2$.

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.

Приклад. Побудувати матричну модель операції декодування для матриці

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

Позначимо рядки матриці змінними y_1, y_2, y_3 відповідно:

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

Побудуємо лінійну матрицю оберненого перетворення для матриці $\overline{F}_l = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}$. Вона є оберненою матрицею до $\overline{F}_l$ і утворюється в процесі

транспонування даної. Таким чином лінійна матриця оберненого перетворення матиме вигляд:

$$\overline{F}_l^{-1} = \begin{pmatrix} y_2 \\ y_3 \\ y_1 \end{pmatrix}.$$

Доповнення для y_1 отримуємо в результаті логічного множення другого і третього рядків, розташувавши множники таким чином, щоб послідовність індексів рядків утворила зростаючу послідовність: $y_2 y_3$;

Доповнення для y_2 отримуємо в результаті логічного множення інвертованих першого і третього рядків, розташувавши множники таким чином, щоб послідовність індексів рядків утворила зростаючу послідовність: $\overline{y}_1 \overline{y}_3$;

Доповнення для y_3 будуємо аналогічно. Воно матиме вигляд: $y_1 \overline{y}_2$.

Таким чином матриця оберненого перетворення матиме вигляд:

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

Дійсно, при перевірці отримаємо:

$$\overline{F}_k(\overline{F}_d) = \begin{pmatrix} x_3 \oplus x_1 x_2 \\ x_1 \oplus \overline{x}_2 \overline{x}_3 \\ x_2 \oplus \overline{x}_1 x_3 \end{pmatrix} \left(\begin{pmatrix} y_2 \oplus \overline{y}_1 \overline{y}_3 \\ y_3 \oplus y_1 \overline{y}_2 \\ y_1 \oplus y_2 y_3 \end{pmatrix} \right) =$$

$$= \begin{pmatrix} x_1 \oplus \overline{x}_2 \overline{x}_3 \oplus (\overline{x}_3 \oplus x_1 x_2)(\overline{x}_2 \oplus \overline{x}_1 x_3) \\ x_2 \oplus \overline{x}_1 x_3 \oplus (\overline{x}_3 \oplus x_1 x_2)(\overline{x}_1 \oplus \overline{x}_2 \overline{x}_3) \\ x_3 \oplus x_1 x_2 \oplus (x_1 \oplus \overline{x}_2 \overline{x}_3)(x_2 \oplus \overline{x}_1 x_3) \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 & & \\ & x_2 & \\ & & x_3 \end{pmatrix}.$$

Отже, можемо стверджувати, що результати підтвердили коректність застосування отриманих правил. Застосування даних правил забезпечує синтез обернених операцій розширеного матричного криптографічного перетворення з будь-якою кількістю доповнень.

Дані результати можуть знайти своє практичне застосування при розробці програмно-апаратних засобів для систем захисту інформації.

Висновки

У статті отримана формалізована матрична модель нелінійної операції криптографічного перетворення, сформульовані правила побудови доповнень елементарних функцій перетворення та синтезу нелінійних операцій прямого та оберненого криптографічного перетворення в загальному випадку. Застосування отриманих правил формує основний підхід щодо побудови операцій розширеного матричного криптографічного перетворення інформації.

Література

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

[2] Бабенко В.Г., Мельник Р.П., Рудницкий С.В. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления // Информационные системы и технологии: управление и безопасность : сб. статей Первой междунар. заочной научно-практ. конф. – Тольятти: Изд-во ПВГУС, 2012. – С. 67–77.

[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] Фомичев В.М. Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра ф.-м.н. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003-400 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. – 2013. – Вип. 3(27). – С. 117-119.

УДК 003.26:004.056.55 (045)

Бабенко В.Г., Мельник О.Г., Стабецкая Т.А. Синтез нелинейных операций криптографического преобразования

Аннотация. *В данной статье разработаны правила синтеза нелинейных операций прямого и обратного криптографического преобразования, а также формализована модель построения элементарных функций расширенного матричного криптографического преобразования. С использованием матричных моделей, описывающих операции расширенного матричного криптографического преобразования, которые синтезированы на основе различных аргументов, получено общее правило синтеза дополнения. Применение данных правил обеспечивает синтез обратных операций расширенного матричного криптографического преобразования с любым количеством дополнений. На конкретных примерах подтверждено корректность применения полученных правил для операции расширенного матричного криптографического преобразования синтезированной на основе трех замен. Применение полученных правил формирует основной подход к построению операций расширенного матричного криптографического преобразования информации. Данные результаты могут найти свое практическое применение при разработке программно-аппаратных средств для систем защиты информации.*

Ключевые слова: *элементарные функции, нелинейная операция криптографического преобразования, обратная операция, операция расширенного матричного преобразования.*

Babenko V., Melnyk O., Stabetska T. The synthesis of nonlinear operations for cryptographic transformation

Abstract. *In this paper we develop rules for the synthesis of nonlinear direct and reverse cryptographic transformation, as well as formalized the model of construction of elementary functions of extended matrix cryptographic transformation. With the use of matrix models describing the operation extended matrix cryptographic transformation, which were synthesized on the basis of various arguments, a general rule of synthesis of additions. The application of these rules provides a synthesis of reverse operations extended matrix cryptographic transformation with any number of additions. With specific examples confirmed the correctness of the application of received rules for the operation of extended matrix cryptographic transformation synthesized on the basis of three substitutions. The application of the rules generates a basic approach to the construction of the expanded matrix operations cryptographic transformation of the information. These results may find practical application in the development of software and hardware for security systems.*

Key words: *elementary functions, nonlinear operation of cryptographic transformation, reverse operation, the operation of expanded matrix transformation.*

Отримано *08 квітня 2014 року*, затверджено редколегією *20 травня 2014 року*