УДК 004.056.55 : 004.312.2

Т.А. Стабецька

Черкаський державний технологічний університет, Черкаси

УМОВИ НЕВИРОДЖЕНОСТІ НЕЛІНІЙНИХ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ, ЩО МІСТЯТЬ НЕПОВНІ ФУНКЦІЇ РМКП

Сформульовано умови невиродженості нелінійних операцій розширеного матричного криптографічного перетворення n-ої розрядності, у складі яких є неповні функції розширеного матричного криптографічного перетворення (РМКП). На прикладі показано застосування отриманих умов та коректність методу побудови оберненої операції розширеного матричного криптографічного перетворення 4-ої розрядності.

Ключові слова: *нелінійні операції РМКП, неповні функції РМКП, доповнення функцій РМКП.*

Вступ

Постановка проблеми. У наш час розвитку інформаційних ресурсів мало хто не зустрічався з проблемою захисту особистих даних від несанкціонованого доступу та втручанням у роботу власних комп'ютерних систем та мереж. Це призводить до матеріальних збитків, спричинених збоями та уповільненням роботи як окремих комерційних організацій так і цілих структур державного управління. На заваді таким втручанням стають криптографічні методи, які забезпечують належний захист інформаційних ресурсів. Оскільки характеристиками таких методів є стійкість та швидкодія, тому важливим напрямком досліджень є робота над розвитком та удосконаленням цих показників.

Однією з умов підвищення швидкодії криптоалгоритмів є використання операцій криптографічного перетворення великих розрядностей. Вони будуються на основі спеціальних логічних функцій, які визначають розрядність криптографічної операції.

Аналіз останніх досліджень та публікацій. У попередніх роботах було досліджено операції РМКП, побудовані на основі повних функцій розширеного матричного криптографічного перетворення і отримано умови невиродженості таких операцій [1]. Проте їх стає недостатньо, коли операція РМКП містить неповні функції розширеного матричного криптографічного перетворення. Тому виникає потреба сформулювати додаткові умови, які забезпечать невиродженість операцій такого типу.

Метою статті є отримання умов невиродженості операцій розширеного матричного криптографічного перетворення, у складі яких є неповні функції РМКП.

Основний матеріал

У загальному вигляді функції розширеного матричного криптографічного перетворення:

$$f_n = x_i \oplus a_i \tilde{x}_j \tilde{x}_k ... \tilde{x}_l \tilde{x}_m, \qquad (1)$$

де $i, j, k, l, m \in [1, ..., n]$ $n \in N$, $i \neq j \neq k \neq l \neq m$, $a_t, x_t \in [0,1]$, $t \in \{i, j, k, l, m\}$; x_t – операнди-розряди інформації; $\tilde{x}_t$ – операнди-розряди інформації, які можуть входити у доповнення у прямому та інверсному вигляді; a_t – коефіцієнти доповнень елементарних функцій, які визначають наявність заміни елементарної функції на функцію розширеного матричного криптографічного перетворення. Другий доданок у рівності (1) називається доповненням функції розширеного матричного криптографічного перетворення. Розрізняють повні та неповні доповнення функцій розширеного матричного криптографічного перетворення. Для коректного викладу подальшого матеріалу введемо деякі поняття і означення.

О.1. Функція розширеного матричного криптографічного перетворення називається функцією n-ої розрядності, якщо вона перетворює n розрядів інформації у процесі криптографічного перетворення.

О.2. Доповнення функції розширеного матричного криптографічного перетворення n-ої розрядності називається повним, якщо воно складається з (n – 1) -го аргументу.

О.3. Доповнення функції розширеного матричного криптографічного перетворення n-ої розрядності називається неповним, якщо воно складається менше ніж з (n – 1) -го аргументу.

О.4. Функція розширеного матричного криптографічного перетворення називається повною, якщо її доповнення є повним.

О.5. Функція розширеного матричного криптографічного перетворення називається неповною, якщо її доповнення є неповним.

Криптографічні операції розширеного матричного криптографічного перетворення синтезуються на основі вибраних функцій РМКП та являють собою композицію відповідних функцій перетворення.

Для забезпечення правильності та коректності перетворення інформації, необхідно використовувати лише невироджені операції криптографічного пе-

ретворення. Розглянувши процес побудови обернених операцій РМКП [2], проведено аналогію з утворенням обернених операцій, синтезованих на основі неповних функцій розширеного матричного криптографічного перетворення. В результаті було помічено, що коли однойменні змінні у доповненнях функцій РМКП входять в операцію з різними інверсними значеннями, то такі операції можна застосувати для криптографічного перетворення інформації. При цьому повинні виконуватись умови невиродженості для операцій РМКП, отримані в [1].

Таким чином, зроблено висновок, що для операцій РМКП, що містять у своєму складі неповні функції розширеного матричного криптографічного перетворення, умови невиродженості можна сформулювати так. Нелінійна операція розширеного матричного криптографічного перетворення n-ої розрядності, що містить неповні функції криптографічного перетворення, є невиродженою, якщо вона:

1. Складається лише з тих функцій РМКП, у доповненнях яких менше ніж $(n-2)$ однойменні змінні мають однакове інверсне значення.

2. Доповнення всіх функцій криптографічного перетворення, на основі яких побудована дана операція, повинні мати у своєму складі хоча б по одній однойменній змінній з різними інверсними значеннями.

Приклад. Побудувати операцію розширеного матричного криптографічного оберненого перетворення для операції прямого криптоперетворення:

$$\overline{F}_k^4 = \begin{pmatrix} x_3 \oplus x_1\overline{x}_2 \\ x_1 \oplus x_2\overline{x}_3x_4 \\ x_4 \oplus x_2x_3 \\ x_2 \end{pmatrix}. \qquad (2)$$

Покажемо, що для даної операції виконуються умови невиродженості. Оскільки маємо операцію 4-ї розрядності, то для виконання першої умови потрібно, щоб менше ніж дві однойменні змінні мали однакове інверсне значення. Доповнення функцій другого і третього рядків мають лише по одній змінній x_2 з однаковим інверсним значенням. Тому перша умова виконана. Друга умова також задовольняється, оскільки для змінної $\overline{x}_2$, доповнення функції першого рядка, присутні однойменні інвертовані змінні x_2 у доповненнях функцій другого та третього рядків. Доповнення функцій другого і третього рядків містять змінні x_3 та $\overline{x}_3$, які забезпечують виконання умови невиродженості. У 4-му рядку знаходиться елементарна функція x_2, яка не є функцією РМКП.

Позначимо рядки операції (2), змінними y_1, y_2, y_3, y_4 відповідно:

$$\overline{F}_k^4 = \begin{pmatrix} x_3 \oplus x_1\overline{x}_2 \\ x_1 \oplus x_2\overline{x}_3x_4 \\ x_4 \oplus x_2x_3 \\ x_2 \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \\ \to y_4 \end{matrix}. \qquad (3)$$

Побудуємо обернену операцію розширеного матричного криптографічного перетворення, використовуючи створений метод синтезу обернених операцій РМКП [2, 3]. Таким чином, операція оберненого перетворення матиме вигляд:

$$\overline{F}_d^4 = \begin{pmatrix} y_2 \oplus \overline{y}_1y_3y_4 \\ y_4 \\ y_1 \oplus y_2\overline{y}_4 \\ y_3 \oplus y_1y_4 \end{pmatrix}.$$

Перевірка:

1) $$y_2 \oplus \overline{y}_1y_3y_4 =$$
$$= x_1 \oplus x_2\overline{x}_3x_4 \oplus (\overline{x}_3 \oplus x_1\overline{x}_2)(x_4 \oplus x_2x_3)x_2 =$$
$$= x_1 \oplus x_2\overline{x}_3x_4 \oplus x_2\overline{x}_3x_4 \oplus x_1\overline{x}_2x_2x_4 \oplus$$
$$\oplus x_2x_2x_3\overline{x}_3 \oplus x_1\overline{x}_2x_2x_2x_3 = x_1;$$

2) $$y_4 = x_2;$$

3) $$y_1 \oplus y_2\overline{y}_4 = x_3 \oplus x_1\overline{x}_2 \oplus (x_1 \oplus x_2\overline{x}_3x_4)\overline{x}_2 =$$
$$= x_3 \oplus x_1\overline{x}_2 \oplus x_1\overline{x}_2 \oplus \overline{x}_2x_2\overline{x}_3x_4 = x_3;$$

4) $$y_1 \oplus y_2\overline{y}_4 = x_3 \oplus x_1\overline{x}_2 \oplus (x_1 \oplus x_2\overline{x}_3x_4)\overline{x}_2 =$$
$$= x_4 \oplus x_2x_3 \oplus x_2x_3 \oplus x_1\overline{x}_2x_2 = x_4.$$

Висновки

У статті сформульовано умови невиродженості операцій розширеного матричного криптографічного перетворення n-ої розрядності, у складі яких присутні неповні функції РМКП, а на прикладі показано практичне застосування отриманих умов та коректність вибраного методу побудови обернених нелінійних операцій розширеного матричного криптографічного перетворення n-ої розрядності.

Список літератури

1. Бабенко В.Г. Построение нелинейных операций расширенного матричного криптографического преобразования / В.Г. Бабенко, О.Г. Мельник, Т.А. Стабецкая // Криптографическое кодирование: коллективная монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – С. 41-55.

2. 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. – Х.: ХУ ПС, 2013. – Вип. 6 (122). – С. 118-121.

3. Стабецька Т.А. Математичне обґрунтування узагальненого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення / Т.А. Стабецька // Наукові праці. – Вип. 238 (250). Комп'ютерні технології. – Миколаїв : Вид-во ЧДУ ім. Петра Могили, 2014. – С. 110-114.

4. Фомичев В.М. Дискретная математика и криптология. Курс лекций / В.М. Фомичев; под общ. ред. д-ра физ.-мат. наук Н.Д. Подуфалова.. – М.: ДИАЛОГ-МИФИ, 2003 – 400 с.

Надійшла до редколегії 11.11.2015

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «ХПІ», Харків.

УСЛОВИЯ НЕВЫРОЖДЕННОСТИ НЕЛИНЕЙНЫХ ОПЕРАЦИЙ РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ, КОТОРЫЕ СОДЕРЖАТ НЕПОЛНЫЕ ФУНКЦИИ РМКП

Т.А. Стабецкая

Сформулированы условия невырожденности нелинейных операций расширенного матричного криптографического преобразования n-й разрядности, в составе которых есть неполные функции расширенного матричного криптографического преобразования (РМКП). На примере показано применение полученных условий и корректность метода построения обратной операции расширенного матричного криптографического преобразования 4-й разрядности.

Ключевые слова: *нелинейные операции РМКП, неполные функции РМКП, дополнения функций РМКП.*

NONDEGENERACY CONDITION NONLINEAR OPERATION OF EXPANDED MATRIX CRYPTOGRAPHIC TRANSFORMATIONS, WHICH CONTAIN INCOMPLETE FUNCTIONS EMCT

T.A. Stabetskaya

In this paper formulated the conditions of nondegeneracy of nonlinear operations expanded matrix cryptographic transformation n-th digit capacity, which contain incomplete functions of expanded matrix cryptographic transformation (EMCT). The example shows the application of the conditions obtained and correctness of the method of constructing an expanded matrix reverse operation of cryptographic transformation of the 4th digit capacity.

Keywords: *nonlinear operation EMCT, incomplete function EMCT, additions of functions EMCT.*