УДК 004.056.55:004.312.2

СИНТЕЗ МОДЕЛИ ОБРАТНОЙ НЕЛИНЕЙНОЙ ОПЕРАЦИИ РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Н. Рудницкий, доктор технических наук, профессор
Черкасский государственный технологический университет, Черкассы (Украина)
С.В. Пивнева, кандидат педагогических наук,
доцент кафедры «Высшая математика и математическое моделирование»
Тольяттинский государственный университет, Тольятти (Россия)
В.Г. Бабенко, кандидат технических наук, докторант
Одесская национальная академия связи им. А.С. Попова, Одесса (Украина)
Т.А. Стабецкая, аспирант
Черкасский государственный технологический университет, Черкассы (Украина)
К.В. Король, аспирант
Тольяттинский государственный университет, Тольятти (Россия)

Ключевые слова: трехразрядные логические функции; операция криптографического преобразования; матричная модель; обратная операция; операция расширенного матричного преобразования.

Аннотация: В данной работе получена модель синтеза нелинейной операции расширенного матричного криптографического преобразования на основе одной замены, а также сформулирована и доказана теорема о построении обратной операции расширенного матричного криптографического преобразования при наличии одной замены.

Операции, использующиеся для криптографического преобразования, должны быть стойкими к линейному криптоанализу, поэтому они должны обладать свойством нелинейности.

Для синтеза операций расширенного матричного криптографического преобразования был использован определенный набор трехразрядных логических функций, которые получены на основе вычислительного эксперимента с помощью специального программного обеспечения. Проведена классификация данных функций за аргументами, которые образовывают первое слагаемое, и получены три базовые группы соответственно.

Основным преимуществом операций расширенного матричного криптопреобразования является одно из их главных свойств – нелинейность, которое и влечет за собой сложность нахождения операций обратного преобразования.

При анализе обобщенной матричной модели операции расширенного матричного криптографического преобразования, образованной на основе замены одной строки основной элементарной функцией расширенного матричного представления, показано, что матрицу, которая описывает операцию расширенного матричного преобразования, можно представить в виде суммы по модулю 2 линейной матрицы преобразования и нелинейной матрицы расширений.

Доказано, что последовательность индексов расширения образовывает возрастающую последовательность. Сформулировано главное правило синтеза расширения, и получены основные этапы процесса синтеза модели обратной нелинейной операции криптографического преобразования.

Использование предложенных нелинейных операций расширенного матричного криптографического преобразования позволяет расширить множество операций для построения систем криптографической защиты информации и повысить их криптостойкость путем дополнительного использования данных операций.

На сегодняшний день, как показал анализ наиболее распространенных криптоалгоритмов, основные преобразования, которые они используют, строятся на основе таких операций: сложение по модулю, подстановки, перестановки, сдвиги. Если расширить количество операций, на основе которых строятся криптоалгоритмы, и доказать, что эти операции создают разные математические группы, то это даст разработчикам новые средства для создания новых и совершенствования существующих криптосистем.

В [1; 2] была определена группа логических функций, которая теоретически может повысить качество работы систем защиты информации при условии создания на их основе операций криптопреобразования [3]. Для данной группы операций были разработаны методы синтеза операций криптопреобразования на основе замены и исключения [3; 4].

Основным преимуществом операций расширенного матричного криптопреобразования является одно из их главных свойств – нелинейность, которое и влечет за собой сложность нахождения операций обратного преобразования.

Цель работы: для операции расширенного матричного криптографического преобразования разработать правила построения обратной операции и доказать их корректность применения.

В результате вычислительного эксперимента с помощью специального программного обеспечения для дальнейшего синтеза операций криптографического преобразования была найдена группа трехразрядных логических функций, которые представлены:

$$f_{30} = x_1 \oplus (x_2 \cdot x_3);\ \ f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3);\ \ f_{54} = x_2 \oplus (x_1 \cdot x_3);$$

$$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3);\ \ f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3);\ \ f_{86} = x_3 \oplus (x_1 \cdot x_2);$$

$$f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2);\ \ f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3);\ \ f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2);$$

$$f_{106} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2);\ \ f_{108} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3);\ \ f_{120} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3).$$

Классифицируем эти функции за аргументами, которые образовывают первое слагаемое.

I группа: функции на основе x_1: $f_{30} = x_1 \oplus (x_2 \cdot x_3)$;

$f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3)$; $f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3)$; $f_{120} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3)$.

В общем виде основную элементарную функцию, которая используется для синтеза операции расширенного матричного криптографического преобразования, на основе x_1 можно представить:

$$f = x_1 \oplus (\tilde{x}_2 \cdot \tilde{x}_3), \quad (1)$$

где – $\tilde{x}$ аргумент с неизвестным значением инверсии.

II группа: функции на основе x_2: $f_{54} = x_2 \oplus (x_1 \cdot x_3)$;

$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3)$; $f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3)$; $f_{108} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3)$.

III группа: функции на основе x_3: $f_{86} = x_3 \oplus (x_1 \cdot x_2)$;

$f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2)$; $f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2)$; $f_{106} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2)$.

В общем виде основную элементарную функцию для синтеза операции расширенного матричного криптографического преобразования на основе x_2, а также на основе x_3 можно представить соответственно:

$$f = x_2 \oplus (\tilde{x}_1 \cdot \tilde{x}_3), \; f = x_3 \oplus (\tilde{x}_1 \cdot \tilde{x}_2). \quad (2)$$

Исходя из выражений (1, 2), правила получения прямой элементарной функции для трехразрядной операции будут формализованы выражением $f = x_i \oplus (\tilde{x}_j \cdot \tilde{x}_k)$ при условии, что $i, j, k \in [1,2,3]$, $i \neq j \neq k$ где $\tilde{x}$ – аргумент с неизвестным значением инверсии.

Рассмотрим операции криптографического преобразования информации на основе замены элементарной функции первой строки функцией расширенного матричного представления:

$$\bar{F}_k = \begin{pmatrix} x_i \oplus x_j x_k \\ x_j \\ x_k \end{pmatrix}; \; \bar{F}_k = \begin{pmatrix} x_i \oplus \bar{x}_j x_k \\ x_j \\ x_k \end{pmatrix};$$

$$\bar{F}_k = \begin{pmatrix} x_i \oplus x_j \bar{x}_k \\ x_j \\ x_k \end{pmatrix}; \; \bar{F}_k = \begin{pmatrix} x_i \oplus \bar{x}_j \bar{x}_k \\ x_j \\ x_k \end{pmatrix},$$

где $i, j, k \in [1,2,3]$, и $j < k$.

Следовательно, можно записать общий вид модели операции:

$$\bar{F}_k = \begin{pmatrix} x_i \oplus \tilde{x}_j \tilde{x}_k \\ x_j \\ x_k \end{pmatrix},$$

где $\tilde{x}_j$, $\tilde{x}_k$ – аргументы с неизвестным значением инверсии, причем $j < k$.

Аналогично, модели операций криптографического преобразования информации на основе одной замены элементарных функций второй и третьей строк представлены соответственно:

$$\bar{F}_k = \begin{pmatrix} x_i \\ x_j \oplus \tilde{x}_i \tilde{x}_k \\ x_k \end{pmatrix}, \; \bar{F}_k = \begin{pmatrix} x_i \\ x_j \\ x_k \oplus \tilde{x}_i \tilde{x}_j \end{pmatrix}.$$

В общем виде операция расширенного матричного криптографического преобразования, образованная на основе замены одной строки основной элементарной функцией расширенного матричного представления, может быть представлена в таком виде:

$$\bar{F}_k = \begin{pmatrix} x_i \oplus a_1 \tilde{x}_j \tilde{x}_k \\ x_j \oplus a_2 \tilde{x}_i \tilde{x}_k \\ x_k \oplus a_3 \tilde{x}_i \tilde{x}_j \end{pmatrix}, \quad (3)$$

где a_1, a_2, a_3 – коэффициенты, определяющие наличие расширения в основной элементарной функции, один из которых равняется 1, а другие равны нулю.

Анализируя матричную модель операции (3), можно утверждать, что матрица, которая описывает операцию расширенного матричного преобразования, подается в виде суммы по модулю 2 линейной матрицы преобразования и расширенной нелинейной матрицы преобразования:

$$\bar{F}_k = \bar{F}_k^{lin} \oplus \bar{F}_k^{nonlin},$$

где $\bar{F}_k^{lin} = \begin{pmatrix} x_i \\ x_j \\ x_k \end{pmatrix}$,

а $\bar{F}_k^{nonlin} = \begin{pmatrix} a_1 \tilde{x}_j \tilde{x}_k \\ a_2 \tilde{x}_i \tilde{x}_k \\ a_3 \tilde{x}_i \tilde{x}_j \end{pmatrix}$.

Введем понятие индекса строки. Индекс строки – это индекс слагаемого линейной матрицы преобразования. Доказано, что последовательность индексов расширения образовывает возрастающую последовательность.

Правило синтеза расширения следующее: для того чтобы образовать расширение одной из строк матрицы, которая обозначает операцию расширенного матричного преобразования, с помощью двух других, нужно выполнить логическое умножение этих строк, инвертируя при этом те строки, индексы которых совпадают с индексами инвертированных переменных.

Из вышеизложенного следует, что синтез модели обратной нелинейной операции криптографического преобразования состоит в следующем.

Теорема 1. Для того чтобы построить для операции расширенного матричного криптографического преоб-

разования $\overline{F}_k$ операцию обратного преобразования $\overline{F}_d$, нужно:

1. Построить линейную операцию обратного преобразования в матричном представлении;

2. Построить соответствующие расширения, учитывая, что прямые расширения переходят в прямые, инверсные в инверсные, а в смешанных расширениях порядок инвертирования сохраняется, если последовательность индексов расширения совпадает с последовательностью индексов соответствующих строк матричной модели для операции преобразования, и изменяется в противном случае.

Доказательство. Рассмотрим одну из возможных операций преобразования. Для других доказательство аналогичное.

Пусть дана матрица, которая описывает операцию расширенного преобразования $\overline{F}_k = \begin{pmatrix} x_i \oplus x_j \overline{x}_k \\ x_j \\ x_k \end{pmatrix}$. Каждая строка матрицы $\overline{F}_k$ представляет собой операнд-разряд информации, который получен в результате применения основной элементарной функции преобразования, т. е. $y_i = F_k(x_i)$.

Обозначим строки матрицы $\overline{F}_k$ переменными y_1, y_2, y_3 соответственно:

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

Прежде всего строится матрица для линейной операции обратного преобразования. Она определяет порядок расположения переменных y_i, $i \in [1,2,3]$ в искомой операции обратного преобразования. Потом строятся соответствующие расширения таким образом, чтобы в результате преобразования строк матрицы $\overline{F}_k$ согласно указанным преобразованиям в матрице $\overline{F}_d$ образовалась диагональная матрица, составленная из переменных x_i, x_j, x_k.

Для того чтобы получить переменную x_i, нужно с помощью строк с j-м и k-м индексами образовать выражение расширения $x_j \overline{x}_k$ и выполнить суммирование по модулю 2 со строкой i-го индекса.

Тогда получим $x_i \oplus x_j \overline{x}_k \oplus x_j \overline{x}_k = x_i$.

При использовании переменных y_1, y_2, y_3 образование переменной x_i будет иметь вид $y_1 + y_2 \overline{y}_3$.

Если же в матрице, которая описывает операцию преобразования, последовательность индексов расширения не будет совпадать с последовательностью индексов соответствующих строк, т. е. последовательность индексов соответствующих строк образовывает убывающую последовательность, то порядок инвертирования изменится, что обусловлено установленным порядком расположения переменных в расширении.

Теорема доказана.

Данная теорема обеспечивает синтез обратных операций расширенного матричного криптографического преобразования и может найти свое практическое применение при разработке программно-аппаратных средств для систем защиты информации.

В данной работе сформулировано и доказано правило построения обратной операции расширенного матричного криптографического преобразования на основе одной замены. Использование предложенных нелинейных операций расширенного матричного криптографического преобразования позволяет расширить множество операций для построения систем криптографической защиты информации и повысить их криптостойкость путем дополнительного использования данных операций.

СПИСОК ЛИТЕРАТУРЫ

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. Рудницкий С.В., Мельник Р.П., Веретельник В.В. Криптографическое преобразование информации на основе трехразрядных логических функций // Вектор науки Тольяттинского государственного университета. 2012. № 4. С. 119–122.
3. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації // Системи обробки інформації. 2012. № 9. С. 145–147.
4. Мельник Р.П. Методи та засоби синтезу операцій розширеного матричного криптографічного перетворення : дис. … канд. техн. наук. Черкаси, 2013. 178 с.

REFERENCES

1. Babenko V., Melnik O., Melnik R. Classification of three-digit elementary functions for cryptographic transformation of the information. *Ukrainian Scientific Journal of Information Security*, 2013, vol. 19, no. 1, pp. 56–59.
2. Rudnitsky S.V., Melnik R.P., Veretelnik V.V. Cryptographic transformation of information on the basis three-digit logic functions. *Vektor nauki Tolyattinskogo gosudarstvennogo universiteta*, 2012, no. 4, pp. 119–122.
3. Melnik R.P. Application of operations extended matrix cryptographic transformations for information security. *Information processing systems*, 2012, no. 9, pp. 145–147.
4. Melnik R.P. *Methods and tools for the synthesis of matrix operations advanced cryptographic transformation*. Diss. kand. tech. nauk. Cherkasi, 2013, 178 p. (in Ukr.).

SYNTHESIS OF MODEL OF REVERSE NONLINEAR OPERATION OF EXTENDED MATRIX CRYPTOGRAPHIC TRANSFORMATION

V.N. Rudnicki, Doctor of Engineering, Professor
Cherkassy State Technological University, Cherkassy (Ukraine)
S.V. Pivneva, candidate of pedagogic sciences,
Assistant professor of the Department «Higher Mathematics and Mathematic Modeling»
Togliatti State University, Togliatti (Russia)
V.G. Babenko, candidate of technical sciences, doctoral student
Odessa National Academy of Communication named after O.S. Popov, Odessa (Ukraine)
T.A. Stabetskaya, postgraduate student
Cherkassy State Technological University, Cherkassy (Ukraine)
K.V. Korol, postgraduate student
Togliatti State University, Togliatti (Russia)

Keywords: three-digit logical functions; operation of cryptographic transformation; matrix model; reverse operation; operation of extended matrix transformation.

Annotation: The operations used for cryptographic transformations should be strong to linear cryptanalysis, so they must have the property of non-linearity.

To synthesize the operations of extended matrix cryptographic transformation the authors used a particular set of three-digit logical functions obtained on the basis of simulation experiment using special software. A classification of these functions following the arguments that produce the first term was carried out and three basic groups were respectively received.

The main advantage of the extended matrix cryptographic transformation operations is one of their main properties - non-linearity, which causes the difficulty of identifying of reverse transformation operations.

The analysis of generalized matrix model of expanded matrix cryptographic transformation operations formed by the replacement of one line of basic elementary function of extended matrix representation showed that the matrix describing the operation of the extended matrix transformation can be represented as the modulo 2 sum of linear matrix transformation and the nonlinear matrix extensions. The experiment proved that the sequence of extension indices forms the increasing sequence. The authors laid down the main rule of extension synthesis and obtained the basic stages of the process of synthesis of the model of reverse nonlinear operation of cryptographic transformation.

The article presents the model of synthesis of nonlinear operation of extended matrix cryptographic transformation on the base of one substitution, and formulates and proved a theorem on the construction of reverse operation of extended matrix cryptographic transformation using one substitution.

The applying of proposed nonlinear operations of extended matrix cryptographic transformation allows to extend a number of operations for construction of cryptographic information protection systems and to improve their cryptographic strength by additional use of these operations.