УДК 004.056.55:004.312.2

В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький

Черкаський державний технологічний університет, Черкаси

МЕТОД СИНТЕЗУ МАТРИЧНИХ МОДЕЛЕЙ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ТА ДЕКОДУВАННЯ ІНФОРМАЦІЇ

В роботі запропонований математичний апарат, який покладений в основу розробки методу синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Також виявлені та сформульовані вимоги на існування матриць операцій криптографічного кодування та декодування інформації, виконання яких забезпечує для кожної операції (матриці) кодування існування оберненої операції (матриці) декодування.

Ключові слова: *матрична модель, операція криптографічного кодування, матриця декодування.*

Вступ

Постановка проблеми. На сьогоднішній день є великий інтерес до створення швидкісних криптографічних методів, які дають змогу вирішувати найважливіші проблеми захищеної автоматизованої обробки і передачі даних в реальному часі. Висока значимість та недостатня практична вирішеність задачі підвищення швидкодії криптографічного перетворення інформації визначає безперечну важливість такого дослідження, а розгляд питань, пов'язаних з даною тематикою, носить як теоретичну, так і практичну значимість у сучасних умовах. Беручи до уваги те, що швидкісні криптографічні перетворення даних є найефективнішим засобом забезпечення таких характеристик безпеки інформаційних ресурсів як конфіденційність та цілісність, то безумовно перспективним напрямком досліджень є розробка методів підвищення продуктивності криптографічних систем.

Аналіз останніх досліджень і публікацій. Провівши аналіз останніх досліджень та публікацій, слід відмітити [1, 2], в яких проведено синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення відповідно до заданої функції кодування.

В [3] був запропонований метод синтезу операцій криптографічного перетворення на основі додавання за модулем два зі збереженням інформативності. Багато публікацій присвячено питанням синтезу криптографічних примітивів, проте не існує математичного апарату для побудови операцій кодування та декодування інформації, а також відсутні методи обчислення матриці декодування з заданої матриці кодування. Саме тому вирішення даної задачі є практично необхідним для подальшої розробки теоретичних основ реалізації технології побудови дискретних пристроїв для криптосистем на основі запропонованого методу.

Мета статті полягає у розробці методу синтезу матричних моделей операцій криптографічного кодування та декодування інформації.

Основний матеріал

В загальному виді операції криптографічного кодування побудовані на основі додавання за модулем два будуть описані наступною моделлю:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus c_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus c_2 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus c_n \end{pmatrix}, \qquad (1)$$

де $a_{ij}, c_i, x_i \in [0,1]; \ i = 1..n,$

n – кількість розрядів інформації; $x_1...x_n$ – операнди-розряди інформації відповідно; a_{ij} – коефіцієнти матриці кодування; c_i – ознака наявності групи операцій інверсії; $\oplus$ – операція "сума по mod 2".

Якщо операція криптографічного кодування без врахування групи операцій інверсії задана виразом:

$$\vec{F}_k = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \end{pmatrix}, \qquad (2)$$

тоді операція криптографічного декодування буде задана виразом:

$$\vec{F}_d = \begin{pmatrix} b_{11}y_1 \oplus b_{12}y_2 \oplus ... \oplus b_{1n}y_n \\ b_{21}y_1 \oplus b_{22}y_2 \oplus ... \oplus b_{2n}y_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ b_{n1}y_1 \oplus b_{n2}y_2 \oplus ... \oplus b_{n\,n}y_n \end{pmatrix}, \qquad (3)$$

де b_i – коефіцієнти матриці декодування; y_i – операнди-розряди інформації, які отримані в результаті застосування операції кодування

$$\left(y_i = \vec{F}_k(x_i)\right)$$

відповідно.

Тоді результатом виконання операції декодування повинен бути вираз, що має такий запис:

$$\vec{F}_r = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ \dots & \dots & \dots & \dots \\ & & & a_{nn}x_n \end{pmatrix}, \qquad (4)$$

де $\vec{F}_r$ – еталонна матриця або матриця-результат; $x_1 \dots x_n$ – початкові операнди-розряди інформації; $a_{ij} = 1$ при $i = j$, тому що потрібно забезпечити невиродженість перетворення.

Тобто повинна виконуватись умова $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$, а також відсутні перестановки рядків матриці.

Розглянемо докладніше процес знаходження операції (матриці) декодування:

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) \\ \dots \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ \dots & \dots & \dots & \dots \\ & & & a_{nn}x_n \end{pmatrix}. \qquad (5)$$

Даний процес можна зобразити такими етапами реалізації:

1. Знайдемо перший рядок матриці декодування:

$$b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus$$
$$\oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \oplus \quad \cdot$$
$$\oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) = a_{11}x_1$$

Так як $x_1 = 1$, а $x_j = 0$ при $j \neq 1$, тоді b_{1i} є рішенням системи рівнянь:

$$\begin{cases} b_{11}a_{11} \oplus b_{12}a_{21} \oplus \dots \oplus b_{1n}a_{n1} = 1 \\ b_{11}a_{12} \oplus b_{12}a_{22} \oplus \dots \oplus b_{1n}a_{n2} = 0 \\ \dots \\ b_{11}a_{1n} \oplus b_{12}a_{2n} \oplus \dots \oplus b_{1n}a_{nn} = 0 \end{cases}.$$

2. Знайдемо другий рядок матриці декодування:

$$b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus$$
$$\oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \oplus \quad .$$
$$\oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) = a_{22}x_2$$

Так як $x_2 = 1$, а $x_j = 0$ при $j \neq 2$, тоді b_{2i} є рішенням системи рівнянь:

$$\begin{cases} b_{21}a_{11} \oplus b_{22}a_{21} \oplus \dots \oplus b_{2n}a_{n1} = 0 \\ b_{21}a_{12} \oplus b_{22}a_{22} \oplus \dots \oplus b_{2n}a_{n2} = 1 \\ \dots \\ b_{21}a_{1n} \oplus b_{22}a_{2n} \oplus \dots \oplus b_{2n}a_{nn} = 0 \end{cases}.$$

3. Знайдемо n-ий рядок матриці декодування:

$$b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n) \oplus$$
$$\oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n) \oplus \dots \oplus \quad .$$
$$\oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \dots \oplus a_{nn}x_n) = a_{nn}x_n$$

Так як $x_n = 1$, а $x_j = 0$ при $j \neq n$, тоді b_{ni} є рішенням системи рівнянь:

$$\begin{cases} b_{n1}a_{11} \oplus b_{n2}a_{21} \oplus \dots \oplus b_{nn}a_{n1} = 0 \\ b_{n1}a_{12} \oplus b_{n2}a_{22} \oplus \dots \oplus b_{nn}a_{n2} = 0 \\ \dots \\ b_{n1}a_{1n} \oplus b_{n2}a_{2n} \oplus \dots \oplus b_{nn}a_{nn} = 1 \end{cases}.$$

Розглянемо приклади побудови операції криптографічного декодування.

Приклад 1. Якщо операція криптографічного кодування задана матрицею $\vec{F}_k = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, тоді підставивши значення $a_{11} = 1$, $a_{12} = 0$, $a_{21} = 1$ та $a_{22} = 1$ в вираз (5) отримаємо:

$$\vec{F}_d = \begin{pmatrix} b_{11}x_1 \oplus b_{12}x_1 \oplus b_{12}x_2 \\ b_{21}x_1 \oplus b_{22}x_1 \oplus b_{22}x_2 \end{pmatrix} = \begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix}.$$

Для знаходження першого рядка матриці декодування розв'яжемо систему рівнянь:

$$\begin{cases} b_{11} \oplus b_{12} = 1 \\ b_{12} = 0 \end{cases} = \begin{cases} b_{11} = 1 \\ b_{12} = 0 \end{cases}.$$

Для знаходження другого рядка матриці декодування розв'яжемо систему рівнянь:

$$\begin{cases} b_{21} \oplus b_{22} = 0 \\ b_{22} = 1 \end{cases} = \begin{cases} b_{21} = 1 \\ b_{22} = 1 \end{cases}.$$

Отримана операція криптографічного декодування буде задана матрицею $\vec{F}_d = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Приклад 2. Якщо операція криптографічного кодування задана матрицею $\vec{F}_k = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, тоді підставивши значення a_{ij} в вираз (5) отримаємо:

$$\vec{F}_d = \begin{pmatrix} b_{11}x_1 \oplus b_{11}x_3 \oplus b_{12}x_1 \oplus b_{12}x_2 \oplus b_{13}x_2 \\ b_{21}x_1 \oplus b_{21}x_3 \oplus b_{22}x_1 \oplus b_{22}x_2 \oplus b_{23}x_2 \\ b_{31}x_1 \oplus b_{31}x_3 \oplus b_{32}x_1 \oplus b_{32}x_2 \oplus b_{33}x_2 \end{pmatrix} = \begin{pmatrix} x_1 & & \\ & x_2 & \\ & & x_3 \end{pmatrix}.$$

Для знаходження першого рядка матриці декодування розв'яжемо систему рівнянь:

$$\begin{cases} b_{11} \oplus b_{12} = 1 \\ b_{12} \oplus b_{13} = 0 \\ b_{11} = 0 \end{cases} = \begin{cases} b_{11} = 0 \\ b_{12} = 1 \\ b_{13} = 1 \end{cases}.$$

Для знаходження другого рядка матриці декодування розв'яжемо систему рівнянь:

$$\begin{cases} b_{21} \oplus b_{22} = 0 \\ b_{22} \oplus b_{23} = 1 \\ b_{21} = 0 \end{cases} = \begin{cases} b_{21} = 0 \\ b_{22} = 0 \\ b_{23} = 1 \end{cases}.$$

Для знаходження третього рядка матриці декодування розв'яжемо систему рівнянь:

$$\begin{cases} b_{31} \oplus b_{32} = 0 \\ b_{32} \oplus b_{33} = 0 \\ b_{31} = 1 \end{cases} = \begin{cases} b_{31} = 1 \\ b_{32} = 1 \\ b_{33} = 1 \end{cases}.$$

Отримана операція криптографічного декодування буде задана матрицею:

$$\vec{F}_d = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

На основі проведених досліджень були сформовані вимоги до існування операцій (матриць) кодування-декодування:

1. Матриця повинна бути не виродженою (відсутні нульові рядки $\sum_{j=1}^{n} a_{ij} > 0$, чи нульові стовбці $\sum_{i=1}^{n} a_{ij} > 0$);

2. В матриці відсутні однакові рядки: $(\sum_{j=1}^{n} (a_{ij} \oplus a_{lj}) > 0)$;

3. Сума по модулю два двох чи декількох рядків не повторює існуючий рядок матриці:

$$\sum_{j=1}^{n} (a_{ij} \oplus a_{lj} \oplus a_{hj} \oplus ... \oplus a_{uj}) > 0.$$

Відповідність цим вимогам забезпечує наявність розв'язку виразу (5) і як наслідок існування для кожної операції (матриці) кодування оберненої операції (матриці) декодування.

Висновки

В даній роботі запропоновано спосіб побудови математичної моделі матриці декодування з відомої матриці кодування на основі операції суми за модулем два.

Також виявлені та сформульовані обмеження на існування матриць операцій криптографічного кодування та декодування інформації.

В дослідженні запропонований математичний апарат, який покладений в основу розробки методу синтезу матричних моделей операцій криптографічного кодування та декодування інформації.

До того ж, на прикладах моделей матриць двох та трьохрозрядних операцій криптографічного перетворення інформації підтверджена коректність застосування запропонованого методу.

Список літератури

1. Бабенко В.Г. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення / В.Г. Бабенко, С.В. Рудницький // Моделирование, идентификация, синтез систем управления: сб. тезисов пятнадцатой Международной науч.-техн. конф.. 9 – 16 сентября 2012. – Донецк: Изд. Института прикладной математики и механики НАН Украины, 2012. – С. 190-191.

2. Бабенко В.Г. Дослідження групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Восьма наукова конф. ХУПС ім. І. Кожедуба "Новітні технології – для захисту повітряного простору": Тези доповідей: 18-19 квітня 2012 року. – Х.: ХУПС, 2012. – С. 218.

3. Голуб С.В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С.В. Голуб, В.Г. Бабенко, С.В. Рудницький // Зб. наук. пр. «Системи обробки інформації». – Х.: ХУПС ім. І. Кожедуба. – 2012. – Вип. 3(101). – Том 1. – С. 119-122.

4. Гантмахер Ф.Р. Гантмахер. Теория матриц / Ф.Р. Гантмахер. – М.: Наука, 1966. – 576 с.

Надійшла до редколегії 23.08.2012

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ» Харків.

МЕТОД СИНТЕЗА МАТРИЧНЫХ МОДЕЛЕЙ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ

В.М. Рудницкий, В.Г. Бабенко, С.В. Рудницкий

В работе предложен математический аппарат, который положен в основу разработки метода синтеза матричных моделей операций криптографического кодирования и декодирования информации. Также выявлены и сформулированы требования на существование матриц операций криптографического кодирования и декодирования информации, выполнение которых обеспечивает для каждой операции (матрицы) кодирования существование обратной операции (матрицы) декодирования.

Ключевые слова: *матричная модель, операция криптографического кодирования, матрица декодирования.*

THE SYNTHESIS METHOD OF MATRIX MODELS OF CRYPTOGRAPHIC OPERATIONS DATA ENCODING AND DECODING

V.M. Rudnitsky, V.G. Babenko, S.V. Rudnitsky

The authors propose a mathematical tool which is the basis of developing a synthesis method of matrix models of cryptographic operations encoding and decoding data. Also identify and formulate the requirements for the existence of matrix operations cryptographic encoding and decoding, which ensures that each operation (matrix) encoding there is an inverse operation (matrix) decoding.

Keywords: *matrix model, the operation of cryptographic encoding, matrix decoding.*