УДК 004.056.55:004.312.2

С.В. Голуб[1], В.Г. Бабенко[2], С.В. Рудницький[2]

[1]*Черкаський національний університет, Черкаси*
[2]*Черкаський державний технологічний університет, Черкаси*

МЕТОД СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ НА ОСНОВІ ДОДАВАННЯ ЗА МОДУЛЕМ ДВА

В роботі запропонований метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох елементарних функцій зі збереженням інформативності. Також докладно описані етапи синтезу трьохрозрядних операцій криптографічного перетворення на основі операції додавання за модулем два.

Ключові слова: *криптографічне перетворення, базова операція, кодування, декодування.*

Вступ

Постановка проблеми. Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи та засоби захисту інформації.

Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має представляти собою сукупність організаційно-технічних та криптографічних заходів.

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, створеного за певними математичними законами, з метою виключити доступ до даної інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольної отримання інформації з боку тих же самих осіб.

Аналіз останніх досліджень і публікацій. Аналітичний огляд останніх досліджень та публікацій показує, що забезпечити конфіденційність інформації користувача дозволяє використання спеціалізованих логічних операцій, які можливо використовувати для підвищення оперативності доступу до конфіденційних інформаційних ресурсів [1 – 3], на основі виконання операції перекодування. Це дозволяє зменшити час доступу до конфіденційних інформаційних ресурсів за рахунок заміни етапів декодування та кодування у форматі користувача на етапі перекодування, а також, підвищити конфіденційність збереження інформації за рахунок обмеження доступу до конфіденційних інформаційних ресурсів.

В [3] був запропонований метод підвищення оперативності криптографічного перетворення інформації на основі використання запропонованих спеціалізованих логічних операцій для систем захисту інформації та доведено, що застосування його дозволяє збільшити швидкість обробки інформації від 1,57 до 2,92 разів залежно від часу отримання ключа та розрядності перетворення.

Проте на сьогоднішній день недостатньо досліджені можливості використання операцій криптографічного перетворення трьох і більше змінних на основі логічних операцій замість операцій криптографічного додавання за модулем два.

Вирішення даної задачі є практично необхідним як на сучасному етапі розвитку систем захисту інформації, так і для подальшої перспективи.

Мета статті полягає розробці етапів синтезу трьохрозрядних операцій криптографічного перетворення на основі додавання за модулем два.

Основний матеріал

При проведенні дослідження обмежимося операціями криптографічного перетворення побудованими на основі додавання за модулем два.

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

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}, \qquad (1)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція "сума по mod 2".

Дослідимо трьохрозрядні операції криптографічного перетворення побудовані на основі додавання за модулем два та розширимо отримані результати на довільну кількість розрядів. Обмеження за кількістю розрядів ($n = 3$) пов'язане із задіянням ресурсів для проведення обчислювального експерименту. Адже для проведення дослідження створено програмне забезпечення, що здійснює синтез набору операцій криптографіного перетворення із заданою кількістю розрядів. За результатами обчислювального експерименту кількість операцій криптографічного перетворення побудованих на основі моделі (1) складає 1344 операції.

Загальна кількість операцій криптографічного кодування (N) утворюється поєднанням базових операцій ($N_б$), операцій перестановки ($N_п$) та операцій інверсії (N_i) [4].

Визначимо кількість трьохрозрядних базових операцій криптографічного кодування. Так як $N = N_б \cdot N_п \cdot N_i = N_б \cdot 3! \cdot 2^3 = 1344$, де $N_б$ - кількість базових операцій, $N_п$ - кількість операцій перестановки, N_i - кількість операцій інверсії. Тоді визнчимо, що $N_б = 28$.

Отже, необхідно побудувати 28 базових операцій.

Для синтезу двохрозрядних операцій криптографічного кодування було використано операцію заміщення [4]. Слід відмітити що базова група операцій не відповідає вимогам до математичної групи операцій.

В попередньому дослідженні [5] способів запису криптографічних операцій перетворення інформації були введені позначення та визначення, які використаємо для даного дослідження теж.

Основні елементарні функції:

$$f_1^{(1)}(x_1, x_2, ..., x_N),$$

$$f_2^{(2)}(x_1, x_2, ..., x_N),$$

$$f_m^{(N)}(x_1, x_2, ..., x_N) -$$

функції перетворення першого, другого та N-го розряду інформації відповідно, що являють собою дискретні логічні функції. Кожна функція відображає правило-залежність перетвореного значення розряду від всіх N початкових значень розрядів інформації.

N – кількість розрядів інформації, що беруть участь в процесі криптографічного перетворення, а m – це номер функції перетворення, що застосовується, $m = 1..M$, де M – загальна можлива кількість N-розрядних функцій криптографічного перетворення.

$x_1, x_2, ..., x_N$ – значення першого, другого, N-го розрядів інформації відповідно.

Відомо, що $x_1, x_2, x_N \in \{0;1\}$, а відповідно і значення дискретних логічних функцій

$$f_1^{(1)}, f_2^{(2)}, ..., f_m^N \in \{0;1\}.$$

Криптографічні операції або елементарні функції синтезуються на основі вибраних основних елементарних функцій та являють собою композицію відповідних функцій перетворення:

$$F_{1,2,...,m} = (f_1^{(1)}, f_2^{(2)}, ..., f_m^N).$$

Основні елементарні функції $f_1^{(1)}, f_2^{(2)}, ..., f_m^N$ утворюють групу. Тобто виконується властивість суперпозиції: серед множини основних елементарних функцій можна знайти відповідні набори пар функцій таких, що

$$f_1^N(f_2^N(x_1, x_2, ..., x_N)) = (x_1, x_2, ..., x_N).$$

Тобто множину основних елементарних функцій, з яких формуються криптографічні операції, можливо використовувати як для кодування, так і для декодування відповідно.

Надалі будемо називати такі відповідні пари як криптографічна операція кодування F^k та криптографічна операція декодування F^d інформації відповідно.

В [6] доведено, що для синтезу трьохрозрядних операцій криптографічного перетворення на основі моделі (1) можуть використовуватися наступні елементарні логічні операції:

$$f_{15} = x_1; \quad (2)$$

$$f_{51} = x_2; \quad (3)$$

$$f_{85} = x_3; \quad (4)$$

$$f_{60} = x_1 \oplus x_2; \quad (5)$$

$$f_{90} = x_1 \oplus x_3; \quad (6)$$

$$f_{102} = x_2 \oplus x_3; \quad (7)$$

$$f_{105} = x_1 \oplus x_2 \oplus x_3. \quad (8)$$

В основу методу синтезу базових операцій криптографічного перетворення на основі заміщення по аналогії з [4] виберемо операцію повторення інформації (нульову операцію). Тоді операції криптографічного кодування та декодування будуються як:

$$F^k_{15,51,85} = F^d_{15,51,85} = (f^1_{15},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}. \quad (9)$$

При введенні заміни необхідно враховувати збереження інформативності при виконанні операції криптографічного перетворення, так елементарна функція $f_{60} = x_1 \oplus x_2$ може заміняти $f_{15} = x_1$ та $f_{51} = x_2$, а елементарну функцію $f_{85} = x_3$ заміняти не може, інакше має місце випадок, коли при перетворенні втрачається значення x_3, що допустити ні в якому разі не можна.

Провівши заміну елементарних функцій в операції (9) однією з елементарних функцій (5) – (8) отримаємо:

$$F^k_{60,51,85} = F^d_{60,51,85} = (f^1_{60},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix};$$

$$F^k_{15,60,85} = F^d_{15,60,85} = (f^1_{15},\ f^2_{60},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix};$$

$$F^k_{90,51,85} = F^d_{90,51,85} = (f^1_{90},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix};$$

$$F^k_{15,51,90} = F^d_{15,51,90} = (f^1_{15},\ f^2_{51},\ f^3_{90}) = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix};$$

$$F^k_{15,102,85} = F^d_{15,102,85} = (f^1_{15},\ f^2_{102},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};$$

$$F^k_{15,51,102} = F^d_{15,51,102} = (f^1_{15},\ f^2_{51},\ f^3_{102}) = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{105,51,85} = F^d_{105,51,85} = (f^1_{105},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix};$$

$$F^k_{15,105,85} = F^d_{15,105,85} = (f^1_{15},\ f^2_{105},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix};$$

$$F^k_{15,51,105} = F^d_{15,51,105} = (f^1_{15},\ f^2_{51},\ f^3_{105}) = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}.$$

Провівши заміну двох елементарних функцій в операції (9) двома елементарними функцій (5) – (8), та вилучивши з базових операцій поєднання базових операцій та операцій перестановки отримаємо:

$$F^k_{15,60,105} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};\ F^d_{15,60,102} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{15,90,105} = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};\ F^d_{15,102,60} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix};$$

$$F^k_{105,51,60} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_2 \end{pmatrix};\ F^d_{102,51,90} = \begin{pmatrix} x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix};$$

$$F^k_{105,51,102} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};\ F^d_{90,51,102} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{105,102,85} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};\ F^d_{60,102,85} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};$$

$$F^k_{105,90,85} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_3 \end{pmatrix};\ F^d_{102,60,85} = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix};$$

$$F^k_{15,60,102} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix};\ F^d_{15,60,105} = \begin{pmatrix} x_1; \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{15,102,90} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix};\ F^d_{15,105,90} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix};$$

$$F^k_{15,60,90} = F^d_{15,60,90} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{pmatrix};$$

$$F^k_{60,51,102} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};\ F^d_{60,51,105} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{90,51,102} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};\ F^d_{105,51,102} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{60,51,90} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix};\ F^d_{60,51,105} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{60,102,85} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};\ F^k_{105,102,85} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};$$

$$F^k_{90,102,85} = F^k_{90,102,85} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix};$$

$$F^k_{90,60,85} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix};\ F^d_{90,105,85} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}.$$

Провівши заміну трьох елементарних функцій в операції (9) трьома елементарними функцій (5) – (8), та вилучивши з базових операцій поєднання базових операцій та операцій перестановки отримаємо:

$$F^k_{90,60,105} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};\ F^d_{105,90,102} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{90,102,105} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};\ F^d_{102,90,105} = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};$$

$$F^k_{60,102,105} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix};\ F^d_{102,105,90} = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}.$$

В результаті заміни одної, двох або трьох елементарних функцій в операції (9) функцій (5) – (8), та вилучивши з базових операцій поєднання базових операцій та операцій перестановки отримано всі 28 базових операцій.

В результаті проведеного дослідження можна сформулювати метод синтезу операцій криптографічного перетворення на основі додавання за модулем два, який полягає в наступному:

– в операції повтору інформації заміною одної, або декількох елементарних функцій отримати розширену базову групу операцій криптографічного перетворення;

– вибракувавши з розширеної групи базових операцій поєднання базових операцій та операцій перестановки отримати базову групу операцій криптографічного перетворення;

– виконавши над кожною операцією базової групи операції перестановки елементарних функцій отримати групу операцій заміщення та перестановки;

– виконавши над кожною операцією групи операцій заміщення та перестановки операції інверсії елементарних функцій отримати повну групу операцій криптографічного перетворення на основі додавання за модулем два.

За результатами обчислювального експерименту група операцій заміщення та перестановки, а також група операцій криптографічного перетворення на основі додавання за модулем два являються математичними групами операцій.

Висновки

В роботі запропонований метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох елементарних функцій зі збереженням інформативності.

Доведено, що базова група операцій окремо не відповідає вимогам до математичної групи операцій, а група операцій заміщення та перестановки, а також група операцій криптографічного перетворення на основі додавання за модулем два являються математичними групами операцій.

Список літератури

1. Рудницький В.М. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Системи управління, навігації та зв'язку: зб. наук. пр. – К.: ЦНДІ НіУ, 2010. – Вип. 2 (14). – С. 118-122.

2. Рудницький В.М. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Вісник Черкаського державного технологічного університету. – 2010. – Вип. № 3. – С. 60-65.

3. Бабенко В.Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: дис.... канд. техн. наук: 05.13.21. – Черкаси, 2009. – 166 с.

4. Бабенко В.Г. Алгоритми вибору логічних функцій для криптографії / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Сучасні інформаційні системи. Проблеми та тенденції розвитку: зб. матеріалів 2-ої міжнар. наук. конф. – Х.: ХНУРЕ, 2007. – С. 423-424.

5. Бабенко В.Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В.Г. Бабенко, Р.П. Мельник, С.В. Рудницький // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2012.– Вип. 3(101) – С. 115-118.

6. Бабенко В.Г. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Системи озброєння і військова техніка: наук. журнал. – Х.: ХУПС, 2012. – Вип. 1 (29). – С. 112-115.

Надійшла до редколегії 8.02.2012

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

МЕТОД СИНТЕЗА ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ СЛОЖЕНИЯ ПО МОДУЛЮ ДВА

С.В. Голуб, В.Г. Бабенко, С.В. Рудницкий

В работе предложен метод синтеза базовых операций криптографического преобразования на основе замещения одного или нескольких элементарных функций с сохранением информативности. Также подробно описаны этапы синтеза трехразрядных операций криптографического преобразования на основе операции сложения по модулю два.

Ключевые слова: *криптографическое преобразование, базовая операция, кодирование, декодирование.*

THE METHOD OF SYNTHESIS OF THE OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATIONS ON THE BASIS OF ADDITION MODULO TWO

S.V. Golub, V.G. Babenko, S.V. Rudnitsky

In this paper we propose a method for the synthesis of the basic operations of cryptographic transformations based on the substitution of one or more elementary functions with preservation of information content. Also described in detail the stages of the synthesis three-digit operations of cryptographic transformation based on the operation of addition modulo two.

Keywords: *cryptographic transformation, basic operation, encoding, decoding.*