Теоретичні основи розробки систем озброєння

УДК 621.391: 004.056.55

В.Г. Бабенко, С.В. Рудницький

Черкаський державний технологічний університет

СИНТЕЗ ФУНКЦІЙ ПЕРЕКОДУВАННЯ ДЛЯ ГРУПИ ТРЬОХРОЗРЯДНИХ КРИПТОГРАФІЧНИХ ОПЕРАЦІЙ

В роботі проведено синтез вектор-функцій трьох змінних для криптографічного перетворення інформації. Показано залежність порядку застосування логічних операцій криптографічного перетворення для процесу кодування-декодування інформації. Отримано математичні моделі функцій перекодування, які забезпечать підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Ключові слова: *криптографічне перетворення, логічна операція, кодування, перекодування.*

Вступ

Постановка проблеми. В зв'язку з створенням квантових комп'ютерів надзвичайно гостро постало питання криптостійкості системи захисту інформації. Обробка трьох бітів а порівнянні з двома бітами на 50% збільшує кількість інформації, що обробляється за один відрізок часу. До того ж збільшення кількості операцій криптографічного перетворення напряму пов'язане з криптостійкістю системи. На сьогодні трьохрозрядні операції криптоперетворення досліджені недостатньо, хоча вони складають значну частину операцій криптоперетворення. Використання спеціалізованих операцій криптоперетворення дозволяє не лише підвищити криптостійкість, а також швидкість обробки інформації. Виходячи з цього, проблема пошуку, дослідження та використання нових операцій криптографічного перетворення для симетричних та несиметричних шифрів є актуальною та перспективною.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто насамперед виділити [1], де був запропонований загальний підхід для формалізації структури множини логічних операцій кодування. В [2] проведена систематизація спеціалізованих логічних функцій придатних для криптографічного перетворення інформації. Далі в [3, 4] наведено узагальнений опис алгоритму кодування повідомлення з допомогою логічних функцій, доведено коректність процедур кодування і декодування, а також запропонований метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Проте, в проаналізованих наукових працях досліджувалися лише функції кодування та декодування інформації в групі двохрозрядних операцій криптографічного перетворення, не розглядалася можливість визначення функції кодування, декодування та синтез функції перекодування в групі трьохрозрядних операцій криптографічного перетворення.

Мета статті полягає у побудові математичної моделі пристроїв перекодування та декодування в системах захисту інформації з трьохрозрядними операціями криптографічного кодування.

Основний матеріал

На сьогоднішній день недостатньо досліджені можливості використання логічних функцій трьох і більше змінних в криптоперетвореннях з метою збільшення кількості інформації при обробці її загальновживаними криптографічними алгоритмами, де ключова послідовність формується із тексту самого повідомлення, що підлягає шифруванню.

Дослідимо трьохрозрядні логічні функції задані наступною алгебраїчною системою:

$$\begin{cases} x_1^* = a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \oplus b_1; \\ x_2^* = a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \oplus b_2;, \\ x_3^* = a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}x_3 \oplus b_3, \end{cases} \quad (1)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; x_1, x_2, x_3 – операнди-розряди відповідно; $\oplus$ – операція "сума по mod 2".

Будь-яку систему алгебраїчних рівнянь можливо зобразити у матричному вигляді. Тоді отримаємо:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \oplus b_2 \\ a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}x_3 \oplus b_3 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \\ a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}x_3 \end{pmatrix} * \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \quad (2)$$

$$= \bar{F}_a \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} * \bar{F}_b \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix},$$

де $\vec{F}$ – це вектор-функція трьох змінних, причому $\vec{F}_a, \vec{F}_b$ – базова та інверсії вектор-функції відповідно.

При проведенні дослідження задамо обмеження: розглянемо випадок коли $b_i = 0$, тобто операція інверсії відсутня, $a_{ij} = 1$ 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 (2).

Синтезуємо логічні функції трьох змінних для криптоперетворення шляхом заміни однієї, двох або трьох змінних на суму по модулю двох чи трьох змінних.

Результати синтезу представлені в табл. 1.

Таблиця 1

Відібрані результати синтезу функції трьох змінних з заміною операндів

Блок 1			
Функції кодування-декодування			
$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
Блок 2			
Функції		Функції	
Кодування	Декодування	Кодування	Декодування
$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$\vec{F} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$\vec{F} = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$		

Відмітимо, що в блоці 1 зображені функції, які при кодуванні та декодуванні співпадають, а в блоці 2 вказані попарно функція кодування та декодування відповідно.

Представлення (2) свідчить про те, що вектор-функція утворена з поєднання двох логічних операцій: базової логічної операції, що позначається як матриця-стовпець $\bar{F}_a\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ та операції інверсії з позначенням як $\bar{F}_b\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$.

Як бачимо в формулі (2) поєднання цих логічних операцій показано як послідовне виконання їх в певному порядку. Таке послідовне виконання логічних операцій ми визначили як композиція операцій.

Крім цього представлення (2) дає змогу розглядати базову операцію та операцію інверсії окремо. Враховуючи це, для розширення множини синтезованих спеціалізованих функцій додатково можна ввести логічну операцію перестановки.

Крім цього, в процесі дослідження виявилось, що при композиції даних операцій важливе значення відіграє їх порядок застосування. Наприклад, якщо для процесу кодування названі операції виконувались в заданому порядку, то для процесу декодування потрібно їх виконувати відповідно в зворотному рис. 1.

В [4] реалізований метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних операцій для криптографічного перетворення шляхом введення логічних операцій перекодування.

Даний метод дозволив зменшити час доступу до інформації за рахунок заміни процесу «декодування-кодування» процесом безпосереднього «перекодування».

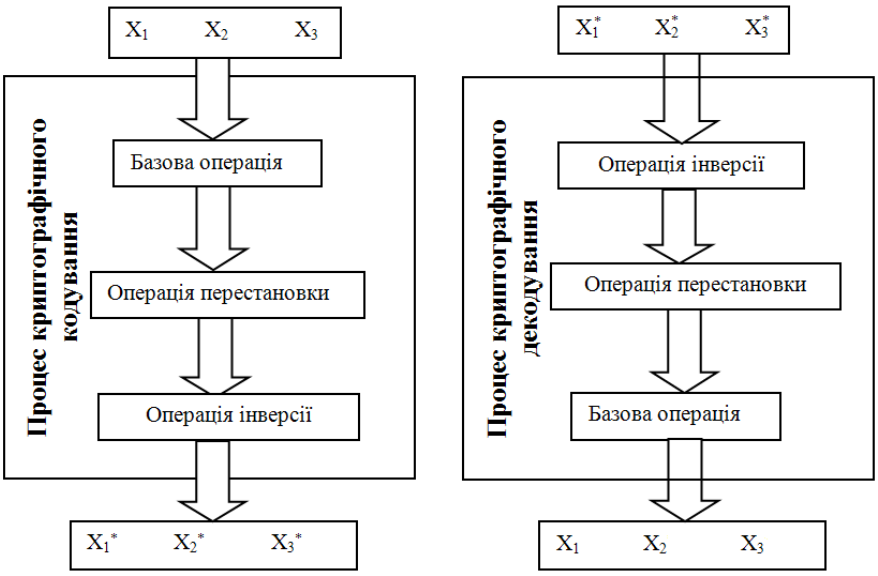

Рис. 1. Криптографічні перетворення процесу кодування-декодування інформації

По аналогії з попередньою роботою, в якій здійснили побудову функцій перекодування в групі двохрозрядних логічних операцій, в даній роботі проведений синтез функцій перекодування на основі застосування групи трьохрозрядних логічних операцій криптографічного перетворення без врахування інверсій.

Узагальнений результат з позначенням вхідних та вихідних параметрів моделювання наведений в табл. 3.

Криптографічні перетворення, що реалізують функції перекодування f_1, f_2, f_3 на основі трьозрозрядних логічних операцій, для першого рівняння системи (1) набудуть вигляду:

Таблиця 3

Позначення моделі функції перекодування в групі трьохрозрядних логічних операцій

Кодування			Перекодування (декодування)		
x_1	x_2	x_3	f_1	f_2	f_3
x_4	x_5	x_6	f_4	f_5	f_6
x_7	x_8	x_9	f_7	f_8	f_9

$f_1 = \bar{x}_6 \cup \bar{x}_8$;

$f_2 = x_2\bar{x}_3 \cup x_2\bar{x}_8 \cup \bar{x}_2x_3x_8$;

$f_3 = \bar{x}_2x_3 \cup x_3\bar{x}_6 \cup x_2\bar{x}_3x_6$.

Для другого та третього рівняння f_4, f_5, f_6 та f_7, f_8, f_9 відповідно:

$$f_4 = x_4\overline{x}_6 \cup x_4\overline{x}_7 \cup \overline{x}_4\overline{x}_6\overline{x}_7;$$

$$f_5 = \overline{x}_3 \cup \overline{x}_7;$$

$$f_6 = \overline{x}_3x_6 \cup \overline{x}_4x_6 \cup x_3x_4\overline{x}_6;$$

$$f_7 = x_7\overline{x}_4 \cup x_7\overline{x}_8 \cup \overline{x}_7x_4x_8;$$

$$f_8 = x_8\overline{x}_2 \cup x_8\overline{x}_7 \cup \overline{x}_8x_2x_7;$$

$$f_9 = \overline{x}_2 \cup \overline{x}_4.$$

Отримані математичні моделі дозволяють будувати алгоритми та функціональні схеми пристроїв перекодування, які забезпечать апаратну реалізацію засобів для побудови швидкодіючих систем захисту інформації підвищеної криптостійкості.

Висновки

В статті досліджено групу трьохрозрядних логічних операцій криптографічного перетворення інформації, яка побудована на основі модульної арифметики.

Синтезовано операції кодування та декодування для симетричних та асиметричних криптосистем. На основі математичного моделювання отримано математичні моделі функцій перекодування, які забезпечать підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Отримано моделі для побудови функціональних схем пристроїв, що реалізують операцію перекодування, та є найбільш придатними для реалізації на практиці.

Список літератури

1. *Рудницький В.М. Алгебраїчна структура множини логічних операцій кодування / В.М. Рудницький, В.Г. Бабенко, Д.А. Жиляєв // Наука і техніка Повітряних Сил Збройних Сил України. – 2011. – № 2(6). – С. 112-114.*
2. *Систематизація повної множини логічних функцій для криптографічного перетворення інформації / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Системи обробки інформації. – Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2011. – Вип. 8(98). – С. 184-188.*
3. *Рудницький В.М. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – Вип. 5(86). – С. 15-19.*
4. *Рудницький В.М. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Вісник Черкаського державного технологічного університету. – 2010. – Вип. № 3. – С. 60-65.*
5. *Бабенко В.Г. Декодування інформації в групі двохрозрядних операцій криптографічного перетворення / В.Г. Бабенко, І.В. Миронець, С.В. Рудницький // Системи управління, навігації та зв'язку: зб. наук. пр. – К.: ДП «ЦНДІ навігації і управління» Мінпромполітики, 2011. – Вип. 4(20) – С. 208-212.*

Надійшла до редколегії 20.12.2011

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

СИНТЕЗ ФУНКЦИЙ ПЕРЕКОДИРОВАНИЯ ДЛЯ ГРУППЫ ТРЕХРАЗРЯДНЫХ КРИПТОГРАФИЧЕСКИХ ОПЕРАЦИЙ

В.Г. Бабенко, С.В. Рудницкий

В работе проведен синтез вектор-функций трех переменных для криптографического преобразования информации. Показана зависимость порядка применения логических операций криптографического преобразования для процесса кодирования-декодирования информации. Получены математические модели функций перекодирования, которые обеспечат повышение оперативности доступа к конфиденциальным информационным ресурсам.

Ключевые слова: *криптографическое преобразование, логическая операция, кодирование, перекодирование.*

THE SYNTHESIS OF TRANSCODING FUNCTIONS IN GROUP OF THREE-DIGIT OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATION

V.G. Babenko, S.V. Rudnitsky

In this work were synthesized vector-valued functions of three variables for the cryptographic transformation of data. The dependence of the order of logical operations of cryptographic transformations to the process of encoding-decoding information is shown. The mathematical model of transcoding functions that will provide increased speed of access to confidential information resources is obtained.

Keywords: *cryptographic transformation, logic operation, encoding, transcoding.*