дискретного логарифма эллиптической кривой над полем GF(p). Освещены аспекты применения устройств ППВМ, в которых вычисления основаны на использовании системы остаточных классов Радемахера-Крестенсона и параллельного суммирования.
Ключевые слова: *информационно-управляющая система, эллиптическая кривая, функциональная безопасность, живучесть, система остаточных классов Радемахера-Крестенсона.*

Отримано *28 січня 2013 року*, затверджено редколегією *4 березня 2013 року*

КЛАСИФІКАЦІЯ ТРИРОЗРЯДНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Віра Бабенко[1], Ольга Мельник[2], Руслан Мельник[2]

[1] Одеська національна академія зв'язку ім. О.С. Попова, Україна
[2]Академія пожежної безпеки імені Героїв Чорнобиля, Україна

БАБЕНКО Віра Григорівна, к.т.н.

Рік та місце народження: 1984 рік, м. Золотоноша, Черкаська область, Україна.
Освіта: Черкаський державний технологічний університет, 2006 рік.
Посада: докторант Одеської національної академії зв'язку ім. О.С. Попова з 2011 року.
Наукові інтереси: криптографічні методи захисту інформації.
Публікації: більше 40 наукових публікацій, серед яких монографії, навчально-методичні розробки, навчальні посібники, наукові статті.
E-mail: zolot_verba@rambler.ru

МЕЛЬНИК Ольга Григорівна, к.т.н.

Рік та місце народження: 1987 рік, м. Черкаси, Україна.
Освіта: Академія пожежної безпеки імені Героїв Чорнобиля, 2009 рік; Черкаський національний університет імені Богдана Хмельницького, 2010 рік.
Посада: доцент кафедри будівельних конструкцій з 2012 року.
Наукові інтереси: методи та засоби побудови комп'ютеризованих систем прогнозування, розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 30 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: melnyk_olja_2012@mail.ru

МЕЛЬНИК Руслан Павлович

Рік та місце народження: 1987 рік, м. Ульяновка, Кіровоградська область, Україна.
Освіта: Академія пожежної безпеки імені Героїв Чорнобиля, 2009 рік.
Посада: ад'юнкт з 2010 року.
Наукові інтереси: розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 15 наукових публікацій.
E-mail: indigo211212@gmail.com

Анотація. *У даній статті представлено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності елементарних функцій та способу перетворення інформації елементарними функціями кожної групи.*

Ключові слова: *трирозрядні елементарні функції, матричні операції, розширені матричні операції, схема реалізації.*

Постановка проблеми

На сьогоднішній день вважається, що забезпечення інформаційної безпеки повинно носити комплексний характер, тому пропонуються нові комплексні рішення для захисту інформаційних ресурсів. Проте організація інформаційної безпеки повинна носити не просто комплексний характер, але ще й засновуватися на всебічному аналізі можливих наслідків, при якому важливо не упустити будь-які суттєві аспекти [1].

Напрями забезпечення безпеки інформації – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особистості.

Однією із складових інженерно-технічного напряму захисту інформації є криптографічні засоби захисту – апаратні, програмні та програмно-апаратні засоби, які реалізують захист інформації за допомогою криптографічних перетворень, які, в свою чергу, є основою криптографічних методів, що створюються з метою виключення несанкціонованого доступу до інформації та її незаконного отримання.

Криптографічний захист інформації розвивається в двох напрямах: шифрування та кодування. Поєднання цих напрямів можливе на основі використання логічних операцій криптографічного перетворення інформації.

Аналіз останніх досліджень і публікацій

Серед останніх досліджень і публікацій варто виділити: [2, 3], де представлено результати проведеного обчислювального експерименту по знаходженню повного набору елементарних функцій для криптографічного перетворення інформації та проведено розрахунок кількості елементарних функцій в залежності від розрядності, та [4], де було розглянуто основні способи запису трирозрядних основних елементарних функцій та криптографічних операцій на їх основі.

Проте в даних дослідженнях не було здійснено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації. Саме це й робить тему дослідження актуальною.

Мета статті полягає у проведенні класифікації трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності елементарних функцій та способу перетворення ними інформації.

Виклад основного матеріалу

У результаті проведеного обчислювального експерименту [5], основна задача якого полягала у виявленні та зборі інформації про логічні функції декількох змінних, за допомогою методів мінімізації [2] виявлені елементарні логічні функції були формалізовані та класифіковані по складності та по виду представлення (прямий чи інверсний). Класифікація формалізованих результатів обчислювального експерименту приведена в табл. 1.

Таблиця 1

Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації

№ блоку	Пряма елементарна функція			Обернена елементарна функція		
	Код функції		Опис функції	Код функції		Опис функції
1	00001111	15	$f_{15} = x_1$	11110000	240	$f_{240} = \bar{x}_1$
	00110011	51	$f_{51} = x_2$	11001100	204	$f_{204} = \bar{x}_2$
	01010101	85	$f_{85} = x_3$	10101010	170	$f_{170} = \bar{x}_3$
2	00111100	60	$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2$	11000011	195	$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2$
	01011010	90	$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3$	10100101	165	$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3$
	01100110	102	$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10011001	153	$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
3	00011011	27	$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$	11100100	228	$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
	00011101	29	$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	11100010	226	$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$
	00100111	39	$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	11011000	216	$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
	00101110	46	$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	11010001	209	$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$
	00110101	53	$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	11001010	202	$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3$
	00111010	58	$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	11000101	197	$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3$
	01000111	71	$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10111000	184	$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
	01001110	78	$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$	10110001	177	$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
	01010011	83	$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	10101100	172	$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3$
	01011100	92	$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	10100011	163	$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3$
	01110010	114	$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10001101	141	$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
	01110100	116	$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10001011	139	$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
4	00010111	23	$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	11101000	232	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
	00101011	43	$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	11010100	212	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$
	01001101	77	$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	10110010	178	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$
	01110001	113	$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	10001110	142	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$

Продовження таблиці 1

5	00011110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$	11100001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
	00110110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$	11001001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
	00111001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11000110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
	01001011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10110100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
	01010110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$	10101001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
	01011001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10100110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$
	01100011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10011100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
	01100101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10011010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
	01101010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10010101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
	01101100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10010011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
	01111000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10000111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
	00101101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11010010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
6	01101001	105	$f_{105} = x_1 \oplus x_2 \oplus x_3$	10010110	150	$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1$

Дослідження форм представлення трирозрядних основних елементарних функцій та криптографічних операцій на їх основі [4] дало можливість вивчити дані функції та способи їх реалізації, а також провести їх класифікацію, яка представлена на рис. 1.

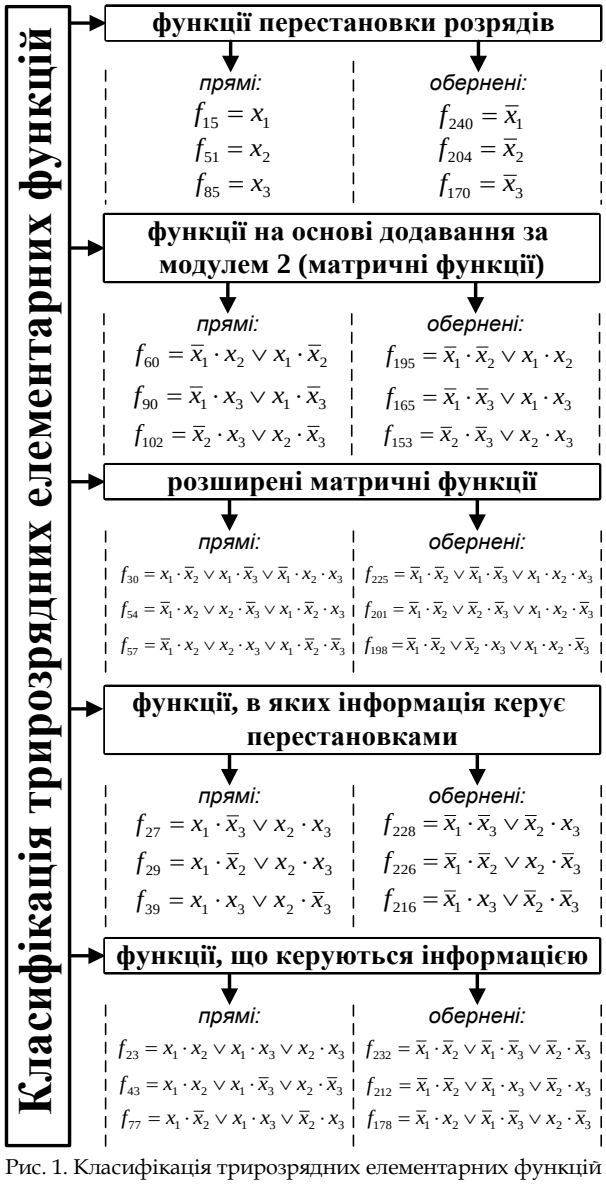

Рис. 1. Класифікація трирозрядних елементарних функцій

Виходячи з аналізу математичних моделей елементарних функцій, можна виділити групу елементарних функцій, які забезпечують перестановки розрядів. Тобто на основі цих елементарних функцій будуються операції криптографічного перетворення, які забезпечують виконання перестановок розрядів інформації, що перетворюємо. До цієї групи функцій відносяться функції з блоку № 1 (табл. 1).

Другу групу представляють елементарні функції, побудовані на основі додавання за модулем 2 (матричні функції) [6]. До цієї групи відносяться елементарні функції з блоку № 2 (табл. 1). Схема реалізації даних функцій показана на рис. 2.

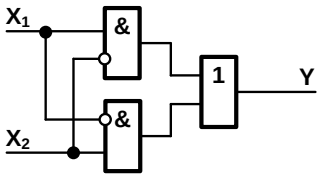

Рис. 2. Схема реалізації функцій на основі додавання за модулем 2 (матричні функції)

Наступну групу представляють розширені матричні функції – це елементарні функції з блоку № 5 (табл. 1), які на сьогоднішній день майже не досліджувалися. Вони накладають додаткову умову на матричне представлення операцій криптографічного перетворення. Схема реалізації розширених матричних функцій наведена на рис. 3.

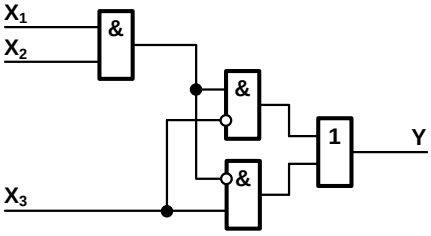

Рис. 3. Схема реалізації розширених матричних функцій

Наступну групу елементарних функцій представляють функцій, в яких інформація керує перестановками. До цієї групи елементарних функцій відносяться функції з блоку № 3 (табл. 1), схема виконання яких показана на рис. 4.

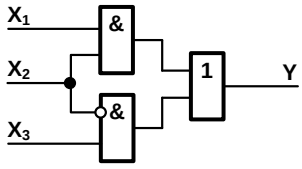

Рис. 4. Схема реалізації функцій, в яких інформація керує перестановками

На основі елементарних функцій з блоку № 3 будуються операції криптографічного перетворення інформації, в яких результат перетворення залежить не лише від функції, а й від інформації, що кодується. Тобто інформація керує процесом перетворення на основі перестановок.

Наступну групу елементарних функцій представляють функції, що керуються інформацією. Ця група елементарних функцій будується на основі елементарних функцій блоку № 4 (табл. 1), схема реалізації яких приведена на рис. 5.

На основі цих елементарних функцій будуються операції криптографічного перетворення інформації, в яких керування процесом перетворення на основі перестановок залежить від значення третього розряду.

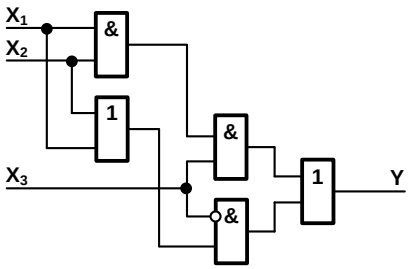

Рис. 5. Схема реалізації функцій, що керуються інформацією

В даному дослідженні ми запропонували класифікацію основних елементарних функцій для криптографічного перетворення, які були отримані та формалізовані в результаті проведеного обчислювального експерименту. За допомогою залежностей, виявлених в ході класифікації, з'явилась можливість провести розподіл основних елементарних функцій на блоки та побудувати схеми для реалізації елементарних функцій кожного такого блоку.

Висновки

Дослідження форм представлення трирозрядних основних елементарних функцій та криптографічних операцій на їх основі дало можливість вивчити дані функції та способи їх побудови, а також провести їх класифікацію і побудову схем реалізації.

Література

[1] Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

[2] Бабенко В.Г. Визначення множини трирозрядних елементарних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький, Р.П. Мельник // Теоретичний і науково-практичний журнал інженерної академії України «Вісник інженерної академії України» – К. «Інтерсервіс». – 2012. – Вип. 3 (4). – С. 77–79.

[3] Рудницкий С. В. Криптографическое преобразование информации на основе трехразрядных логических функцій / С. В. Рудницкий, Р. П. Мельник, В. В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4. – С. 119–122.

[4] Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабен-ко, С. В. Рудницький, Р. П. Мельник // Системи управління, навігації та зв'язку. – 2012. – № 1 (21). – Т. 2.– С. 170–173.

[5] Бабенко В.Г. Технологія визначення спеціальних логічних функцій для систем захисту інформації / В.Г. Бабенко, В.М. Рудницький, Т.В. Дахно // Вісник інженерної академії України. – 2007. – Вип. 3–4. – С. 64–67.

[6] 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». – 2012. – Вип. 3 (101). – Том 1. – С. 119–122.

УДК 003.26:004.056.55 (045)

Бабенко В.Г., Мельник О.Г., Мельник Р.П. Классификация трехразрядных элементарных функций для криптографического преобразования информации

Аннотация. *В данной статье представлена классификация трехразрядных элементарных функций для криптографического преобразования информации в зависимости от сложности элементарных функций и способа преобразования информации элементарными функциями каждой группы.*

Ключевые слова: *трехразрядные элементарные функции, матричные операции, расширенные матричные операции, схема реализации.*

Babenko V.G., Melnyk O.G., Melnyk R.P. Classification of three-digit elementary functions for cryptographic transformation of the information

Abstract. *In the article presents the three-digit classification of elementary functions for cryptographic transformation of the information depending on the complexity of the elementary functions and the method of converting information elementary functions of each group.*

Key words: *three-elementary functions, matrix operations, advanced matrix operations, schematics of implementation.*

Отримано *22 січня 2013 року*, затверджено редколегією *25 лютого 2013 року*