УДК 004.056.55

Т.В. Дахно, В.М. Рудницький

Черкаський державний технологічний університет, Черкаси

КЛАСИФІКАЦІЯ ТРЬОХРОЗРЯДНИХ СПЕЦІАЛІЗОВАНИХ ЛОГІЧНИХ ФУНКЦІЙ ЗА СКЛАДНІСТЮ РЕАЛІЗАЦІЇ

Дана стаття присвячена розробці класифікації трьохрозрядних спеціалізованих логічних функцій представлених у вигляді множин за складністю реалізації. Одним з рішень даної задачі є визначення множин логічних функцій через об'єднання декількох класифікованих по складності та кількості змінних у функції. В результаті виконання досліджень визначено множину логічних функцій, яка за складністю реалізації може бути використана при побудові перспективних систем криптографічного захисту інформації.

Ключові слова: *криптографія, захист інформації, складність, кількість змінних, множина.*

Вступ

Постановка проблеми. Причиною бурхливого розвитку криптографії, як науки, з одного боку, є використання комп'ютерних мереж, зокрема глобальної мережі Internet, по яких передають великі обсяги інформації державного, військового, комерційного та приватного змісту, що не допускає можливості доступу до неї сторонніх осіб, а з іншого, – нових потужних обчислювальних засобів обчислень, що зробили можливою дискредитацію низки криптографічних систем [1].

Ще однією з причин виникнення криптографії є зростання темпів розповсюдження персональних комп'ютерів та розвиток засобів обробки інформації, що призвели до різкого збільшення об'ємів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерних систем; концентрування в єдиних базах даних інформації різного призначення та різної належності; різного розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи.

В зв'язку з цим гостро постає проблема захисту інформації, інтерес до якої обумовлений ще й стрімким впровадженням обчислювальної техніки в такі сфери, як біржова та банківська справа, страхування, медицина та інші [2].

Аналіз останніх досліджень і публікацій. За останні роки збільшилася кількість публікацій для криптографічних систем захисту інформації. Але в даних публікаціях основна увага приділяється дослідженню двохрозрядних логічних функцій [3 – 5].

Мета статті полягає у розробці класифікації трьох розрядних спеціалізованих логічних функцій за складністю реалізації.

Основний матеріал

Повна множина трьохрозрядних логічних функцій складається з 256 логічних функцій серед яких лише 70 функцій можуть бути використані в системах криптографічних перетворень. Подальше дослідження буде направлене на аналіз і визначення характеристик даних функцій.

Складність дискретного пристрою визначається кількістю входів логічних елементів. На основі дискретної моделі пристрою по кількості операцій та аргументів можна визначити складність пристрою.

Класифікуємо отримані внаслідок обчислювального експерименту результати по таких критеріях:

- складність;
- кількість змінних у функції.

Результати класифікацій досліджуваних логічних функцій в залежності від їх складності представимо у вигляді множин (елементами множини є коди цифр в двійковій системі числення) наведені нижче:

$$M_1^{скл} = \{15, 51, 85, 170, 204, 240\};$$

$$M_5^{скл} = \{27, 29, 39, 46, 53, 58, 60, 71, 78, 83, 90, 92, 102, 114, 116, 139, 141, 153, 163, 165, 172, 177, 184, 195, 197, 202, 209, 216, 226, 228\};$$

$$M_8^{скл} = \{23, 43, 77, 113, 142, 178, 212, 232\};$$

$$M_9^{скл} = \{30, 54, 57, 75, 86, 89, 99, 101, 106, 108, 120, 135, 147, 149, 154, 156, 166, 169, 180, 198, 201, 210, 225\};$$

$$M_{11}^{скл} = \{45\};$$

$$M_{15}^{скл} = \{105, 150\}.$$

Перевіримо правильність класифікацій функцій по складності, за допомогою об'єднання множин. Класифікація буде вважатися правильною, якщо в результаті об'єднання результуюча множина буде включати всі 70 елементів.

Результат об'єднання приведено нижче:

$$M_1^{скл} \cup M_5^{скл} \cup M_8^{скл} \cup M_9^{скл} \cup M_{11}^{скл} \cup$$

$$\cup M_{15}^{скл} = \{15, 23, 27, 29, 30, 39, 43, 45, 46, 51,$$
$$53, 54, 57, 58, 60, 71, 75, 77, 78, 83, 85, 86, 89, 90,$$
$$92, 99, 101, 102, 105, 106, 108, 113, 114, 116, 120,$$
$$135, 139, 142, 141, 147, 149, 150, 153, 154, 156,$$
$$163, 165, 166, 169, 170, 172, 177, 178, 180, 184,$$
$$195, 197, 198, 201, 202, 204, 209, 210, 212, 216,$$
$$225, 226, 228, 232, 240\}.$$

Виходячи зі складності функцій для практичної реалізації краще всього використовуються функції з найменшою складністю.

Тому, розташуємо множини від найбільш пріоритетних до найменш в наступному порядку:

$$M_1^{скл}; M_5^{скл}; M_8^{скл}; M_9^{скл}; M_{11}^{скл}; M_{15}^{скл}.$$

Результати класифікацій досліджуваних логічних функцій в залежності від кількості змінних:

$$M_1^{к-ть\ зм.} = \{15, 51, 85, 170, 204, 240\};$$

$$M_2^{к-ть\ зм.} = \{60, 90, 102, 153, 165, 195\};$$

$$M_3^{к-ть\ зм.} = \{23, 27, 29, 30, 39, 43, 45, 46, 53, 54,$$
$$57, 58, 71, 75, 77, 78, 83, 86, 89, 92, 99, 101, 105,$$
$$106, 108, 113, 114, 116, 120, 135, 139, 142, 141,$$
$$147, 149, 150, 154, 156, 163, 166, 169, 172, 177,$$
$$178, 180, 184, 197, 198, 201, 202, 209, 210, 212,$$
$$216, 225, 226, 228, 232\}.$$

Тепер перевіримо правильність класифікацій функцій по кількості змінних у функції за допомогою того ж об'єднання множин.

Результатом такого об'єднання повинно бути 70 елементів.

В результаті було отримано:

$$M_1^{к-ть\ зм.} \cup M_2^{к-ть\ зм.} \cup M_3^{к-ть\ зм.} = \{15, 23,$$
$$27, 29, 30, 39, 43, 45, 46, 51, 53, 54, 57, 58, 60, 71,$$
$$75, 77, 78, 83, 85, 86, 89, 90, 92, 99, 101, 102, 105,$$
$$106, 108, 113, 114, 116, 120, 135, 139, 142, 141,$$
$$147, 149, 150, 153, 154, 156, 163, 165, 166, 169,$$
$$170, 172, 177, 178, 180, 184, 195, 197, 198, 201,$$
$$202, 204, 209, 210, 212, 216, 225, 226, 228, 232,$$
$$240\}.$$

Виходячи з вимог лавинного ефекту, який забезпечує залежність вихідного значення розряду від максимально можливої функції вхідного розряду, по рівню пріоритету множини будуть розташовуватися в наступному порядку:

$$M_3^{к-ть\ зм.}; M_2^{к-ть\ зм.}; M_1^{к-ть\ зм}.$$

Проведемо пошук логічних функцій, які при максимальній кількості розрядів, забезпечували найменшу складність реалізації.

Розглянемо множину логічних функцій з найменшою складністю:

$$M_1^{скл} \cap M_1^{к-ть\ зм.} = \{15, 51, 85, 170, 204, 240\};$$

$$M_1^{скл} \cap M_2^{к-ть\ зм.} = \varnothing;$$

$$M_1^{скл} \cap M_3^{к-ть\ зм.} = \varnothing.$$

Лише функції, які залежать від однієї змінної мають в перетині з даною множиною не пусту множину.

Розглянемо наступну множину логічних функцій:

$$M_5^{скл} \cap M_1^{к-ть\ зм.} = \varnothing;$$

$$M_5^{скл} \cap M_2^{к-ть\ зм.} = 60, 90, 102, 153, 165, 195$$

$$M_5^{скл} \cap M_3^{к-ть\ зм.} = \{27, 29, 39, 46, 53,$$
$$58, 60, 71, 78, 83, 90, 92, 102, 114, 116, 139,$$
$$141, 153, 163, 165, 172, 177, 184, 195, 197,$$
$$202, 209, 216, 226, 228\}.$$

В результаті було визначено дві множини, які в перетині з даною множиною дають не пусту множину.

Причому, перетин множин

$$M_5^{скл} \cap M_3^{к-ть\ зм.}$$

задовольняє лавинному ефекту і є не складною для реалізації.

Наступне об'єднання множин має вигляд:

$$M_8^{скл} \cap M_1^{к-ть\ зм.} = \varnothing;$$

$$M_8^{скл} \cap M_2^{к-ть\ зм.} = \varnothing;$$

$$M_8^{скл} \cap M_3^{к-ть\ зм.} = \{23, 43, 77, 113, 142, 178,$$
$$212, 232\}.$$

В результаті було отримано лише одну множину, яка в перетині з даною множиною дає не пусту множину, але складність реалізації такої множини є складною:

$$M_9^{скл} \cap M_1^{к-ть\ зм.} = \varnothing;$$

$$M_9^{скл} \cap M_2^{к-ть\ зм.} = \varnothing;$$

$$M_9^{скл} \cap M_3^{к-ть\ зм.} = \{30, 54, 57, 75, 86, 89, 99,$$
$$101, 106, 108, 120, 135, 147, 149, 154, 156, 166,$$
$$169, 180, 198, 201, 210, 225\}.$$

Визначена множина задовольняє лавинному ефекту, але, так як і попередня множина, є досить складною для реалізації. Далі були розглянуті такі перетини:

$$M_{11}^{скл} \cap M_1^{к-ть\ зм.} = \varnothing;$$

$$M_{11}^{скл} \cap M_2^{к-ть\ зм.} = \varnothing;$$

$$M_{11}^{скл} \cap M_3^{к-ть\ зм.} = \{45\};$$

$$M_{15}^{скл} \cap M_1^{к-ть\ зм.} = \varnothing;$$

$$M_{15}^{скл} \cap M_2^{к-ть\ зм.} = \varnothing;$$

$$M_{15}^{скл} \cap M_3^{к-ть\ зм.} = \{105, 150\}.$$

Дані множини мають в своєму перетині малу кількість логічних функцій, що не забезпечує потрібний рівень захисту інформації.

Проаналізувавши результати перетину множин було визначено, що функції зі складністю

$$M_8^{скл}, M_9^{скл}, M_{11}^{скл}, M_{15}^{скл}$$

задовольняють лавинному ефекту, але є складними для реалізації.

Одним з найкращих результатів дає множина $M_5^{скл}$, яка має найменшу складність і забезпечує умови досягнення лавинного ефекту.

Висновки

В результаті виконання даних досліджень було отримано такі результати:

1. Класифікацій досліджуваних логічних функцій та визначення їх правильності в залежності від складності за допомогою об'єднання множин.

2. Класифікацій досліджуваних логічних функцій та визначення їх правильності в залежності від кількості змінних за допомогою об'єднання множин.

3. Визначення логічних функцій, які при максимальній кількості розрядів, забезпечували найменшу складність реалізації.

4. Визначення множини, яка має найменшу складність і найкращий лавинний ефект.

Список літератури

1. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.

2. Яремчук Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей: монографія / Ю.Є. Яремчук. – Вінниця: Книга-Вега, 2002. – 136 с.

3. Бабенко В.Г. Вибір наборів кодів команд для підвищення надійності та швидкодії систем захисту інформації / В.Г. Бабенко // Захист інформації з обмеженим доступом та автоматизація її обробки: матеріали наук.-техн. конф. студентів та аспірантів, 12-13 лютого 2009 р.: зб. тез доп. – К.: НАУ, 2009. – С. 5-6.

4. Миронець І.В. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів / І.В. Миронець, В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2010. – Вип. 5 (86). – С. 15-19.

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

Надійшла до редколегії 16.09.2010

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

КЛАССИФИКАЦИЯ ТРЕХРАЗРЯДНЫХ СПЕЦИАЛИЗИРОВАННЫХ ЛОГИЧЕСКИХ ФУНКЦИЙ ПО СЛОЖНОСТИ РЕАЛИЗАЦИИ

Т.В. Дахно, В.Н. Рудницкий

Данная статья посвящена разработке классификации трехразрядных специализированных логических функций представленных в виде множеств по сложности реализации. Одним из решений данной задачи является определение множеств логических функций через объединение нескольких классифицированных по сложности и количеству переменных в функции. В результате выполнения исследований определено множество логических функций, которое по сложности реализации может быть использовано при построении перспективных систем криптографической защиты информации.

Ключевые слова: *криптография, защита информации, сложность, количество переменных, множество.*

THE THREE-DIGIT SPECIALIZED LOGICAL FUNCTIONS CLASSIFICATION ON THE COMPLEXITY OF IMPLEMENTATION

T.V. Dahno, V.N. Rudnitsky

This article is devoted to developing the three-digit specialized logic functions classification. These functions are represented as sets on the complexity of implementation. One solution of this problem is to define functions sets by combining several classified functions on the complexity and number of variables. As a result of doing research the logic functions sets, which can be used in the construction of perspective cryptographic security information systems on the complexity of implementation are determined.

Keywords: *cryptography, information security, complexity, number of variables, set.*