УДК 004.056.55:004.312.2

О.Г. Мельник

Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси

МОДЕЛЮВАННЯ ДИСКРЕТНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У даній статті проведено класифікацію прямих та обернених елементарних функцій розширеного матричного криптографічного перетворення, формалізовано правила отримання прямої та оберненої елементарних функцій, а також сформульовано загальний вираз для отримання елементарної функції розширеного матричного криптографічного перетворення інформації. Проведені дослідження дозволяють моделювати елементарні функції розширеного матричного криптографічного перетворення інформації будь-якої розрядності.

Ключові слова: *захист інформації, криптографічне перетворення інформації, розширене матричне перетворення, елементарна функція.*

Вступ

Актуальність проблеми. Створення умов для гармонійного розвитку інформаційної інфраструктури – пріоритетне завдання будь-якої держави в інформаційній сфері. Але разом з підвищенням цінності інформації зростає й необхідність її захисту, оскільки отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести значних збитків державі, представляють собою особливу загрозу інтересам держави. Тому постійна увага повинна приділятися розробці та впровадженню нових методів захисту інформації.

Сучасні рішення багатьох проблем захисту інформації немислимі без використання криптографічних методів [1], що відрізняються від інших методів швидкодією апаратного забезпечення, яке безпосередньо реалізує перетворення інформації. Одним із варіантів удосконалення існуючих та розробки нових криптоалгоритмів є дослідження елементарних функцій, що можуть застосовуватися для реалізації криптографічного перетворення даних.

Аналіз останніх досліджень. В статтях [2, 3] представлено результати проведених обчислювальних експериментів щодо знаходження елементарних функцій для криптографічного перетворення інформації, а в [4] проведено аналіз базових спеціалізованих трирозрядних логічних функцій, що дозволив виявити основну закономірність процесу побудови моделей трирозрядних операцій криптографічного перетворення інформації.

Серед останніх досліджень і публікацій варто також виділити [5], де здійснено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності самих функцій та способу перетворення інформації елементарними функціями кожної групи.

Проте в даних дослідженнях не проводився аналіз елементарних функцій розширеного матричного криптографічного перетворення інформації, що дозволив би розробити правила для визначення кількості елементарних функцій будь-якої розрядності.

Мета роботи полягає в розробці підходу, що дозволить моделювати елементарні функції розширеного матричного криптографічного перетворення інформації будь-якої розрядності.

Виклад основного матеріалу

Аналіз прямих елементарних функцій розширеного матричного криптографічного перетворення [6] показав, що лише один аргумент входить до складу всіх трьох доданків логічного додавання. Класифікуємо ці елементарні функції за даною ознакою:

- функції на основі x_1:

$$f_{30} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3,$$
$$f_{75} = x_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3,$$
$$f_{120} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3,$$
$$f_{45} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3;$$

- функції на основі x_2:

$$f_{54} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3,$$
$$f_{57} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3,$$
$$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3,$$
$$f_{108} = x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3;$$

- функції на основі x_3:

$$f_{86} = \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3,$$
$$f_{89} = \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3,$$
$$f_{101} = x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3,$$
$$f_{106} = x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3.$$

Розглянемо більш детально групу функцій на основі x_1. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_1, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_2 має різні знаки інверсії;
- в другому і третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_1 має інший знак інверсії, ніж в першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_2. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому завжди присутні x_2, x_3;
- в третьому завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_1 має різні знаки інверсії;
- в другому і третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_2 має інший знак інверсії, ніж в першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_3. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_1 має різні знаки інверсії;
- в другому і третьому доданках x_2 має різні знаки інверсії;
- в третьому доданку x_3 має інший знак інверсії, ніж в першому та другому доданках.

З чотирьох варіантів елементарних функцій у трьох із них аргумент, на основі якого будується операція, представлений прямим аргументом, а в другому варіанті – інверсним.

Можливо, розподіл на прямі та обернені функції відповідно до порядку номеру функцій не зовсім коректний. Перевіримо це на основі аналізу обернених функцій.

Як видно з обернених функцій розширеного матричного криптографічного перетворення, лише один аргумент входить до складу всіх трьох доданків логічного додавання. Класифікуємо ці елементарні функції за даною ознакою:

- функції на основі x_1:

$$f_{225} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot x_3;$$
$$f_{180} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3;$$
$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3;$$
$$f_{210} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3;$$

- функції на основі x_2:

$$f_{201} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3;$$
$$f_{198} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3;$$
$$f_{156} = x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3;$$
$$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3;$$

- функції на основі x_3:

$$f_{169} = \overline{x}_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot x_3;$$
$$f_{166} = \overline{x}_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3;$$
$$f_{154} = x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3;$$
$$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3.$$

Розглянемо більш детально групу функцій на основі x_1. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_1, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_2 має різні знаки інверсії;
- в другому й третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_1 має інший знак інверсії, ніж у першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_2. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_1 має різні знаки інверсії;
- в другому й третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_2 має інший знак інверсії, ніж у першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_3. Можна зробити такі висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_1 має різні знаки інверсії;
- в другому і третьому доданках x_2 має різні знаки інверсії;
- в третьому доданку x_3 має інший знак інверсії, ніж у першому та другому доданках.

З чотирьох варіантів елементарних функцій у трьох із них аргумент, на основі якого будується операція, представлений прямим аргументом, а в

другому варіанті – інверсним. Виходячи з результатів дослідження прямих та обернених розширених матричних елементарних функцій, для спрощення алгоритму синтезу елементарних функцій було б доцільно поміняти три прямі елементарні функції з трьома оберненими функціями. Дана заміна елементарних функцій не призведе до зміни кількості операцій криптографічного перетворення на основі розширеного матричного перетворення, при цьому може призвести до спрощення алгоритмів побудови самих операцій криптоперетворення.

Виходячи з пропозиції формування прямих функцій в залежності від прямого значення основного аргументу, а обернених – з оберненого значення основного аргументу, формалізуємо правила отримання прямої та оберненої елементарної функції:

- пряма функція:

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l , \qquad (1)$$

де x – пряме значення аргументу; $\overline{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\overline{\hat{x}}$ – інверсне до будь-якого значення аргументу; за умови: $i \in [1,2,3]$; $j \in [1,2,3]$; $l \in [1,2,3]$; $i \neq j \neq l$;

- обернена функція:

$$f = \overline{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee x_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l . \qquad (2)$$

Виходячи з формул (1) та (2), сформулюємо загальний вираз для отримання елементарних функцій криптографічного перетворення:

$$f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \overline{\hat{x}}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l , \qquad (3)$$

де $\hat{x}_i$ – змінні, що можуть приймати прямі або інверсні значення.

Вирази (1) – (3) можна вважати формалізованим записом методу синтезу елементарних функцій розширеного матричного перетворення для криптографічного перетворення інформації.

Вирази (1) – (3) дозволяють:

- синтезувати прямі трирозрядні елементарні функції або обернені трирозрядні елементарні функції, чи повну множину трирозрядних елементарних функцій;

- синтезувати прямі або обернені трирозрядні елементарні функції, чи повну множину елементарних функцій будь-якої розрядності;

- визначити кількість елементарних функцій будь-якої розрядності.

Висновки

Проведена класифікація елементарних функцій розширеного матричного криптографічного перетворення, розроблені правила отримання елементарних функцій дозволили розробити підхід для моделювання елементарних функцій розширеного матричного криптографічного перетворення інформації будь-якої розрядності.

Список літератури

1. Криптографическое кодирование: коллективная монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – 240 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». – 2012. – № 3-4. – С. 77–79.

3. Бабенко В.Г. Дослідження групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Новітні технології – для захисту повітряного простору: мат-ли VIII наук. конф. Харківського університету Повітряних Сил імені Івана Кожедуба, 18-19 квітня 2012 року. – Харків: ХУПС ім. І. Кожедуба, 2012. – С. 218.

4. Рудницкий С.В. Криптографическое преобразование информации на основе трехразрядных логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Вере-тельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4. – С. 119–122.

5. Бабенко В.Г. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В.Г. Бабенко, О.Г. Мельник, Р.П. Мельник // Безпека інформації. – 2013. – С. 56–59.

Надійшла до редколегії 29.01.2015

Рецензент: д-р техн. наук проф. В.М. Рудницький, Черкаський національний технологічний університет, Черкаси.

МОДЕЛИРОВАНИЕ ДИСКРЕТНЫХ ЭЛЕМЕНТАРНЫХ ФУНКЦИЙ ДЛЯ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

О.Г. Мельник

В данной статье проведена классификация прямых и обратных элементарных функций расширенного матричного криптографического преобразования, формализовано правила получения прямой и обратной элементарной функций, а также сформулировано общее выражение для получения элементарной функции расширенного матричного криптографического преобразования информации. Проведенные исследования позволяют моделировать элементарные функции расширенного матричного криптографического преобразования информации любой разрядности.

Ключевые слова: *защита информации, криптографическое преобразование информации, расширенное матричное преобразование, элементарная функция.*

MODELING OF DISCRETE ELEMENTARY FUNCTIONS FOR CRYPTOGRAPHIC TRANSFORMATION

O.H. Melnyk

In this paper was classificated direct and inverse elementary functions of expanded matrix cryptographic transformation, formalized rules for obtaining the forward and reverse elementary functions, and formulated a general expression for the getting of elementary function of the extended matrix of cryptographic transformation of information. The studies allow modeling of elementary functions expanded matrix cryptographic transformation of information of different digits.

Keywords: *protection of information, cryptographic transformation of information, expanded matrix transformation, an elementary function.*