УДК 004.056.55:004.312.2

В.Г. Бабенко[1], Р.П. Мельник[2], С.В. Гончар[2]

[1] *Черкаський державний технологічний університет, Черкаси,*
[2] *Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси*

РОЗРОБКА МЕТОДІВ СИНТЕЗУ ТРИРОЗРЯДНИХ РОЗШИРЕНИХ МАТРИЧНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ

Проведено вивчення груп прямих та обернених елементарних функцій розширеного матричного криптографічного перетворення, а також отримано правила їх синтезу. Розроблено методи синтезу трирозрядних розширених матричних елементарних функцій в дискретному та модульно-дискретному представленнях.

Ключові слова: *захист інформації, криптографічне перетворення, трирозрядна розширена матрична елементарна функція, дискретне представлення, модульно-дискретне представлення.*

Вступ

Актуальність проблеми. Сучасний світ характеризується тенденцією постійного росту ролі інформації. З підвищенням цінності інформації відповідно зростає й важливість та необхідність її захисту. Одним із можливих способів захисту інформації під час її передачі та зберігання є використання криптографічних методів захисту. Задача вдосконалення криптоалгоритмів полягає в покращенні існуючих та пошуку нових функцій криптографічного перетворення, застосування яких дає можливість забезпечити достатній рівень стійкості систем криптоперетворення даних.

Таким чином, перспективним напрямом досліджень можна вважати пошук і синтез функцій криптографічного перетворення інформації, застосування яких дозволить розширити кількість операцій криптоперетворення і, як наслідок, підвищити стійкість криптоалгоритмів.

Аналіз останніх досліджень. В [1, 2] запропоновано застосовувати розширені матричні функції криптографічного перетворення і криптопримітиви, побудовані на їх основі, для алгоритмів захисту інформаційних ресурсів. У [3, 4] доведено, що використання розширених матричних функцій криптографічного перетворення підвищує швидкодію обробки даних в криптосистемах за рахунок паралельного процесу виконання операцій криптоперетворення. Проте в даних дослідженнях не були достатньо вивчені прямі та обернені елементарні функції розширеного матричного криптографічного перетворення, що не дозволяло сформулювати методи їх синтезу. Саме це й робить тему дослідження актуальною.

Мета роботи полягає в розробці методів синтезу трирозрядних розширених матричних елементарних функцій в дискретному та модульно-дискретному представленнях, для чого необхідно провести дослідження груп прямих та обернених елементарних функцій розширеного матричного крипографічного перетворення.

Виклад основного матеріалу

У [2, 5] проведено дослідження та систематизацію трирозрядних розширених матричних елементарних функцій, де встановлено, що лише один аргумент в дискретному представленні елементарних функцій входить до складу всіх трьох логічних доданків. За цією ознакою проведено класифікацію цих елементарних функцій та виділено з них прямі та обернені. Розглянемо більш детально групу прямих елементарних функцій на основі x_1:

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

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

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

$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3.$$

Як видно з наведеного представлення:

- перший логічний доданок $x_1 \cdot x_2$;
- другий логічний доданок $x_2 \cdot x_3$;
- третій логічний доданок $x_1 \cdot x_2 \cdot x_3$;
- x_1 в першому та другому доданках прямий, а в третьому доданку інверсний;
- x_2 в першому і третьому доданках має різні знаки інверсії;
- x_3 в другому і третьому доданках має різні знаки інверсії.

Формалізуємо наведені правила:

$$f = x_1 \cdot \hat{x}_2 \vee x_1 \cdot \hat{x}_3 \vee \overline{x}_1 \cdot \overline{\hat{x}}_2 \cdot \overline{\hat{x}}_3, \qquad (1)$$

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.

Розглянемо більш детально групу обернених елементарних функцій на основі x_1:

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

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

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

$$f_{225} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot x_3.$$

Правила побудови обернених елементарних функцій на основі x_1 від побудови прямих елементарних функцій відрізняються лише тим, що x_1 в першому та другому доданках представлено інверсним значенням, а в третьому доданку – прямим значенням. Формалізовані правила синтезу обернених елементарних функцій на основі x_1 будуть представлені моделлю:

$$f = \overline{x}_1 \cdot \hat{x}_2 \vee \overline{x}_1 \cdot \hat{x}_3 \vee x_1 \cdot \overline{\hat{x}}_2 \cdot \overline{\hat{x}}_3 . \qquad (2)$$

Об'єднавши вирази (1) і (2) будуть отримані правила синтезу прямих і обернених елементарних функцій на основі x_1:

$$f = \hat{x}_1 \cdot \hat{x}_2 \vee \hat{x}_1 \cdot \hat{x}_3 \vee \overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2 \cdot \overline{\hat{x}}_3 . \qquad (3)$$

По аналогії можна отримати формалізовані правила прямих елементарних функцій на основі x_2:

$$f = \hat{x}_1 \cdot x_2 \vee x_2 \cdot \hat{x}_3 \vee \overline{\hat{x}}_1 \cdot \overline{x}_2 \cdot \overline{\hat{x}}_3 . \qquad (4)$$

Формалізовані правила синтезу обернених елементарних функцій на основі x_2 будуть описані як

$$f = \hat{x}_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot \hat{x}_3 \vee \overline{\hat{x}}_1 \cdot x_2 \cdot \overline{\hat{x}}_3 . \qquad (5)$$

Об'єднавши вирази (4) і (5), будуть отримані правила синтезу прямих і обернених елементарних функцій на основі x_2:

$$f = \hat{x}_1 \cdot \hat{x}_2 \vee \hat{x}_2 \cdot \hat{x}_3 \vee \overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2 \cdot \overline{\hat{x}}_3 . \qquad (6)$$

Результати формалізації правил синтезу елементарних функцій на основі x_3 такі:

- прямі елементарні функції на основі x_3:

$$f = \hat{x}_1 \cdot x_3 \vee \hat{x}_2 \cdot x_3 \vee \overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2 \cdot \overline{x}_3 ; \qquad (7)$$

- обернені елементарні функції на основі x_3:

$$f = \hat{x}_1 \cdot \overline{x}_3 \vee \hat{x}_2 \cdot \overline{x}_3 \vee \overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2 \cdot x_3 ; \qquad (8)$$

- прямі та обернені елементарні функції на основі x_3:

$$f = \hat{x}_1 \cdot \hat{x}_3 \vee \hat{x}_2 \cdot \hat{x}_3 \vee \overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2 \cdot \overline{\hat{x}}_3 . \qquad (9)$$

Узагальнимо на основі виразів (1), (4), (7) правила синтезу прямих елементарних функцій:

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l , \qquad (10)$$

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: $i \in [1,2,3]$; $j \in [1,2,3]$; $l \in [1,2,3]$; $i \neq j \neq l$.

На основі виразів (2), (5), (8) формалізуємо правила синтезу прямих елементарних функцій:

$$f = \overline{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee x_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l \qquad (11)$$

Синтез повної множини прямих та обернених елементарних функцій базується на виразах (3), (6), (9) і в загальному випадку може бути описаний:

$$f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \overline{\hat{x}}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l \qquad (12)$$

Вирази (10) – (12) створюють основу метода синтезу трирозрядних розширених матричних елементарних функцій в дискретному представленні, сутність якого полягає в наступному:

1. Виходячи з задач проектування визначити, які формалізовані правила необхідно використати:

- при синтезі множини прямих трирозрядних розширених матричних елементарних функцій необхідно використати вираз (10);

- при синтезі множини обернених трирозрядних розширених матричних елементарних функцій необхідно використати вираз (11);

- при синтезі повної множини трирозрядних розширених матричних елементарних функцій необхідно використати вираз (12).

2. На основі перебору значень i, j, l, де $i \in [1,2,3]$, $j \in [1,2,3]$, $l \in [1,2,3]$ за умови $i \neq j \neq l$, $j < l$ отримати три основні трирозрядні розширені матричні елементарні функції;

- на основі виразу (10):

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l ;$$

$$f = x_j \cdot \hat{x}_i \vee x_j \cdot \hat{x}_l \vee \overline{x}_j \cdot \overline{\hat{x}}_i \cdot \overline{\hat{x}}_l ;$$

$$f = x_l \cdot \hat{x}_j \vee x_l \cdot \hat{x}_i \vee \overline{x}_l \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_i ;$$

- на основі виразу (11):

$$f = \overline{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee x_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l ;$$

$$f = \overline{x}_j \cdot \hat{x}_i \vee \overline{x}_j \cdot \hat{x}_l \vee x_j \cdot \overline{\hat{x}}_i \cdot \overline{\hat{x}}_l ;$$

$$f = \overline{x}_l \cdot \hat{x}_j \vee \overline{x}_l \cdot \hat{x}_i \vee x_l \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_i ;$$

- на основі виразу (12):

$$f = \hat{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee \overline{\hat{x}}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l ;$$

$$f = \hat{x}_j \cdot \hat{x}_i \vee \hat{x}_j \cdot \hat{x}_l \vee \overline{\hat{x}}_j \cdot \overline{\hat{x}}_i \cdot \overline{\hat{x}}_l ;$$

$$f = \hat{x}_l \cdot \hat{x}_j \vee \hat{x}_l \cdot \hat{x}_i \vee \overline{\hat{x}}_l \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_i ;$$

На основі перебору значень інверсії $\hat{x}_i$, $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_i \in [x_i, \overline{x}_i]$, $\hat{x}_j \in [x_j, \overline{x}_j]$, $\hat{x}_l \in [x_l, \overline{x}_l]$, підставивши отримані набори в три основні трирозрядні розширені матричні елементарні функції, можна отримати повну множину трирозрядних розширених матричних елементарних функцій відповідно до задачі синтезу. По аналогії з синтезом елементарних функцій в дискретному представленні розглянемо синтез операцій криптографічного перетворення на основі модульно-дискретного представлення елементарних функцій. Як видно з елементарних функцій розширеного матричного перетворення [2], лише один аргумент входить до першого доданку за модулем.

Класифікація елементарних функцій в дискретному і модульно-дискретному представленнях повністю співпадає. Виходячи з цього, можна стверджувати, що класифікації елементарних функцій не залежать від способів запису та представлення.

Розглянемо більш детально групу прямих елементарних функцій на основі x_1:

$$f_{30} = x_1 \oplus (x_2 \cdot x_3) ; \quad f_{45} = x_1 \oplus (x_1 \cdot \overline{x}_3) ;$$

$$f_{75} = x_1 \oplus (\overline{x}_2 \cdot x_3) ; \quad f_{135} = x_1 \oplus (\overline{x}_2 \cdot \overline{x}_3) .$$

Формалізовані правила синтезу прямих елементарних функцій на основі x_1 будуть описані виразом:

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3), \qquad (13)$$

де x – пряме значення аргументу; $\overline{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\overline{\overline{x}}$ – інверсне до будь-якого значення аргументу.

Формалізовані правила синтезу обернених елементарних функцій на основі x_1 будуть описані як

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3) \oplus 1.$$

По аналогії формалізовані правила синтезу прямих елементарні функції на основі x_2 та x_3 будуть описані відповідно виразами:

$$f = x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3); \quad f = x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2).$$

Правила синтезу обернених елементарних функцій на основі x_2 та x_3 будуть описані відповідно як

$$f = x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3) \oplus 1; \quad f = x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2) \oplus 1.$$

Узагальнені правила синтезу прямих трирозрядних розширених матричних елементарних функцій будуть описані виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l), \qquad (14)$$

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

Узагальнені правила синтезу обернених трирозрядних розширених матричних елементарних функцій будуть описані виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \oplus 1 \qquad (15)$$

Вирази (14), (15) дозволяють розробити метод синтезу трирозрядних розширених матричних елементарних функцій в модульно-дискретному представленні. Сутність розробленого методу полягає в такому:

1. На основі виразу (14) шляхом перебору значень i, j, l де $i \in [1,2,3]$, $j \in [1,2,3]$, $l \in [1,2,3]$ за умови: $i \neq j \neq l$; $j < l$ отримати три основні трирозрядні розширені матричні елементарні функції.

2. На основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$ де $\hat{x}_j \in [x_j, \overline{x}_j]$, $\hat{x}_l \in [x_l, \overline{x}_l]$, підставивши отримані набори в три основні трирозрядні розширені матричні елементарні функції, отримати повну множину із 12 прямих трирозрядних розширених матричних елементарних функцій.

3. На основі виразу (15), інвертувавши множину прямих трирозрядних розширених матричних елементарних функцій шляхом додавання по модулю два, буде отримана множина обернених розширених матричних елементарних функцій.

4. Об'єднавши множини прямих і обернених елементарних функцій буде отримана повна множина із 24 трирозрядних розширених матричних елементарних функцій.

Висновки

Дослідження елементарних функцій в дискретному та модульно-дискретному представленнях дозволили розробити методи їх синтезу. Подальші дослідження будуть направлені на отримання методу синтезу трирозрядних розширених матричних елементарних функцій для криптоперетворення даних більшої розрядності.

Список літератури

1. Криптографическое кодирование: коллективная монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Харьков: Изд-во ООО «Щедрая усадьба плюс», 2014. – 240 с.

2. Мельник Р.П. Метод захисту конфіденційної інформації як складова управління інформаційною безпекою ДСНС України / Р.П. Мельник, О.Г. Мельник, С.В. Гончар, В.Г. Бабенко // Системи обробки інформації. – 2014. – Вип. 4 (120). – С. 145–148.

3. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник // Системи обробки інформації. – 2012. – № 9 (107). – С. 145–147.

4. Бабенко В.Г. Оцінка ефективності використання операцій криптографічного перетворення / В.Г. Бабенко, Р.П. Мельник, С.В. Гончар // Вісник інженерної академії України. – Вип. 2. – 2014. – С. 39-41.

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.

РАЗРАБОТКА МЕТОДОВ СИНТЕЗА ТРЕХРАЗРЯДНЫХ РАСШИРЕННЫХ МАТРИЧНЫХ ЭЛЕМЕНТАРНЫХ ФУНКЦИЙ

В.Г. Бабенко, Р.П. Мельник, С.В. Гончар

В данной статье проведено изучение групп прямых и обратных элементарных функций расширенного матричного криптографического преобразования, а также получено правила их синтеза. Разработаны методы синтеза трехразрядных расширенных матричных элементарных функций в дискретном и модульно-дискретном представлениях.

Ключевые слова: *защита информации, криптографическое преобразование, трехразрядная расширенная матричная элементарная функция, дискретное представление, модульно-дискретное представление.*

DEVELOPMENT OF SYNTHESIS METHODS THREE-DIGIT EXTENDED MATRIX ELEMENTARY FUNCTIONS

V.G. Babenko, R.P. Melnyk, S.V. Gonchar

This article studied groups of direct and inverse elementary functions expanded cryptographic transformation matrix, and also acquired the rights for their synthesis. Methods of synthesis of three-digit extended matrix of elementary functions in discrete and module-discrete representation.

Keywords: *information security, cryptographic transformation, three-digit extended matrix elementary function, discrete representation, modular discrete representation.*