УДК 004.056.55:004.312.2 **doi: 10.26906/SUNZ.2019.5.055**

Н. В. Лада[1], С. Г. Козловська[2], В. М. Зажома[3], С. В. Висоцький[1]

[1] Черкаський державний технологічний університет, Черкаси, Україна
[2] Східноєвропейського університету економіки і менеджменту, Черкаси, Україна
[3] Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля, Черкаси, Україна

СИНТЕЗ АПАРАТНИХ ЗОСОБІВ РЕАЛІЗАЦІЇ ГРУП СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ ПОТОКОВОГО ШИФРУВАННЯ

Стаття присвячена розробці технології синтезу апаратних засобів для генерації груп симетричних двохоперандних двохрозрядних криптографічних операцій для підвищення якості потокового шифрування. Наведено результати дослідження по реалізації симетричних операцій потокового шифрування. Розроблено функціональні схеми пристроїв генерації і застосування груп операцій додавання за модулем два, та чотири. Дані групи операцій можуть застосовуватися, як окремо, так і сумісно. Застосування розроблених апаратних засобів при вдосконаленні реалізації методу підвищення стійкості та надійності потокового шифрування забезпечує збільшення варіативності шифрування в п’ять раз.

Ключові слова: криптографічне кодування, потокове шифрування, синтез груп криптоперетворення, додавання за модулем, функціональна схема.

Вступ

Постановка проблеми. На сьогоднішній день в світі відбувається глобальна інформатизація суспільства. Особливо актуальними стають питання високоефективного захисту інформації, особливо криптографічного. Крім того, сучасні тенденції постійного збільшення обсягів інформації та швидкості її обробки та передачі, обумовлені розвитком нових інформаційних технологій, вимагають відповідного розвитку засобів потокового шифрування [1-3].

Сучасні наукові дослідження в сфері криптографічного захисту інформації все більше уваги приділяють розвитку потокових шифрів, зокрема пов'язаному з вирішенням задач апаратної генерації високоякісних псевдовипадкових послідовностей та побудови нових логічних операцій криптографічного перетворення інформації, дослідженням їх побудови або використанням арифметичних операцій з різними модулями [1, 4].

Аналіз останніх досліджень і публікацій. Проведений аналіз методів синтезу одноопераднних операцій криптографічного перетворення інформації показав що не залежно від операцій які синтезуються, алгоритм синтезу можна поділити на блок синтезу одноопераднних операцій базової групи, блок синтезу операцій перестановки, блок синтезу операцій інверсії [5, 6]. Дані блоки доповнюють один одного і розширяють кількість операцій. Особливості реалізації кожного методу синтезу операцій визначається особливостями синтезу операцій базової групи. Технічній реалізації одноопераднних операцій присвячено ряд робіт [7–12]. Особливої уваги заслуговують дослідження присвячені та синтезу апаратних засобів генерації одноопераднних операцій [13, 14]. Проте синтезу апаратних засобів генерації груп двохоперандних операцій не приділялося достатньої уваги.

Метою роботи є розробка технології синтезу апаратних засобів для генерації груп симетричних двохоперандних двохрозрядних криптографічних операцій для підвищення якості потокового шифрування.

Основний матеріал

Для досягнення поставленої мети в процесі аналізу методів синтезу математичних груп симетричних двохоперандних двохрозрядних операцій потокового шифрування на основі додавання за модулем два і додавання за модулем чотири [2, 15] встановлено наступне:

- синтез двохоперандних операцій проводиться аналогічно синтезу одноопераднних операцій шляхом побудови операцій базової групи, поєднанням операцій базової групи з групою операцій перестановок та поєднання отриманої групи операцій з групою операцій інверсії;
- синтез групи двохоперандних операцій реалізується на основі групи одноопераднних операцій, шляхом поєднання однакових одноопераднних операцій обробки першого та другого операнда;
- методи синтезу базових груп симетричних двохоперандних двохрозрядних операцій потокового шифрування на основі додавання за модулем два і додавання за модулем чотири відрізняються правилами поєднання однакових одноопераднних операцій;
- правила поєднання операцій базової групи з операціями групи перестановки та групи інверсій аналогічні правилам поєднання при синтезі одноопераднних операцій.

Виходячи з цього апаратні засоби формування групи симетричних двохоперандних двохрозрядних операцій потокового шифрування повинні включати схему формування базових операцій, схему реалізації операцій перестановок та схему реалізації операцій інверсій.

Синтез базової групи симетричних двохоперандних двохрозрядних операцій потокового шифрування на основі додавання за модулем два проводиться з враховуванням взаємозв’язків між одноопераднними операціями обробки операндів, які описуються моделлю $F = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. Моделі симетричних двохоперандних двохрозрядних операцій базової

групи які необхідно реалізувати в пристрої генерації групи операцій додавання за модулем два такі:

$$O_{1б}^{\oplus 2} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (1)$$

$$O_{2б}^{\oplus 2} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (2)$$

$$O_{3б}^{\oplus 2} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}. \quad (3)$$

Виходячи з виразів (1-3) апаратні засоби формування групи операцій повинні включати блок формування двохоперандних операцій із одноопераднних. В даному випадку він повинен об'єднувати, шляхом додавання за модулем два, бітів операндів з однаковими номерами. На основі даного підходу побудовано функціональну схему пристрою реалізації груп операцій додавання за модулем два представлену на рис. 1.

Побудована функціональна схема пристрою розбита на чотири функціонально незалежні модулі: блок формування двохоперандних операцій на основі одноопераднних шляхом додавання відповідних розрядів операндів за модулем два (об'єднуються відповідні розряди першого операнда x_1 і x_2, з відповідними розрядами другого операнда k_1 і k_2); схеми формування операцій базової групи (схема працює в залежності від значень команди управління заданої вхідними сигналами z_1 і z_2); схеми управління перестановками (перестановка задається значенням вхідного сигналу z_3) ; та схеми управління інверсіями (наявність інверсій виходів визначається сигналами управління z_4 і z_5). Три останні схеми умовно можна поєднати в об'єднаний блок формування групи операцій. Функціональна схема пристрою реалізації груп операцій додавання за модулем два працює наступним чином: при подачі на входи інформації та сигналів управління на виході буде результат виконання операції заданої сигналами управління.

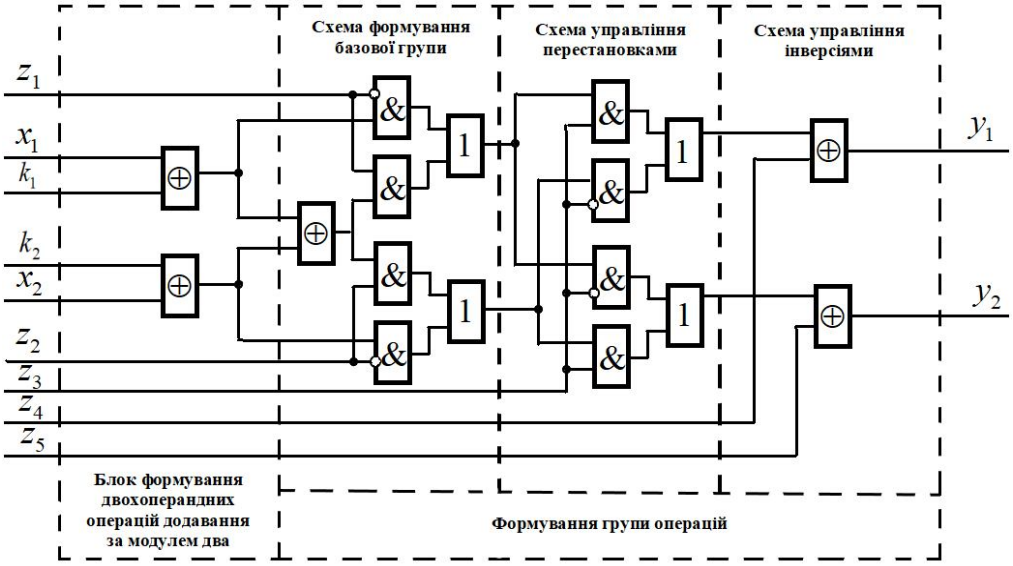

Рис. 1. Функціональна схема пристрою реалізації груп операцій додавання за модулем два

Синтез групи операцій додавання за модулем чотири відрізняється від синтез групи операцій додавання за модулем два побудовою операцій базової групи на основі моделі $F = \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$:

$$O_{1б}^{\oplus 4} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (4)$$

$$O_{2б}^{\oplus 4} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (5)$$

$$O_{2б}^{\oplus 4} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (6)$$

$$O_{3б}^{\oplus 4} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}. \quad (7)$$

Виходячи з (4-6) апаратні засоби формування групи операцій додавання за модулем чотири можна представити функціональною схемою рис. 2. Дана функціональна схема відрізняється від рис. 1 лише блоком формування двохоперандних операцій за модулем. Даний блок забезпечує поєднання операцій відповідно до методу синтезу групи другої операцій. Схеми формування групи операцій залишені без зміни. Функціонування даної схеми аналогічно попередній. Об'єднавши під управлінням сигналу z_6 поєднання блоків формування двохоперандних операцій додавання за модулем два та чотири було отримано функціональну схему пристрою реалізації груп операцій додавання за модулями два та чотири (рис. 3).

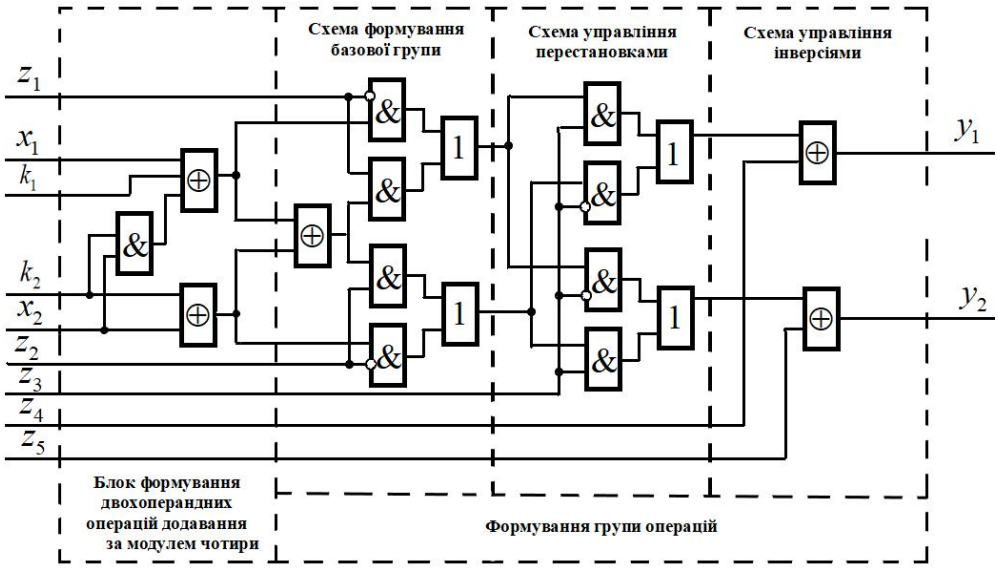

Рис. 2. Функціональна схема пристрою реалізації груп операцій додавання за модулем чотири

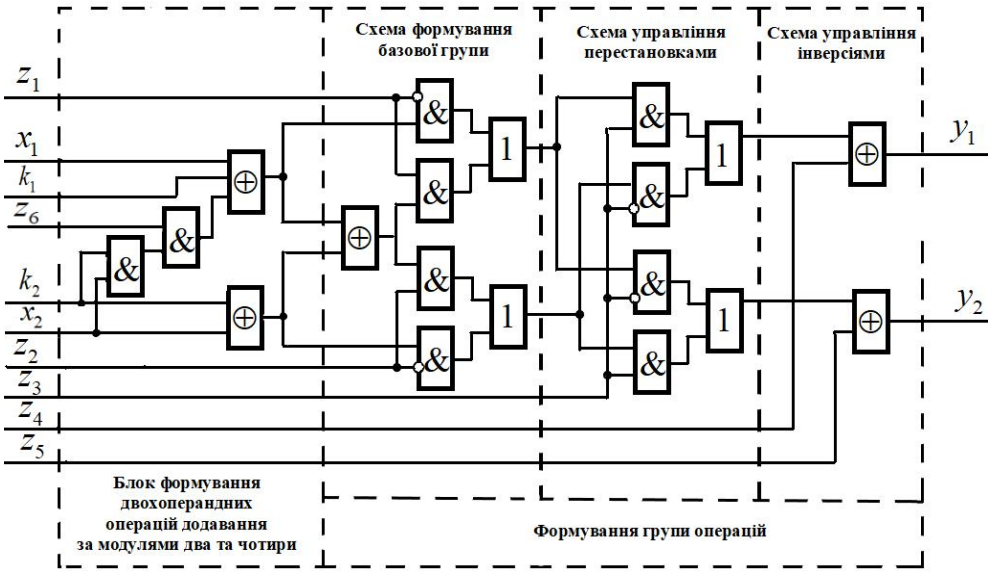

Рис. 3. Функціональна схема пристрою реалізації груп операцій додавання за модулями два та чотири

Дана функціональна схема реалізує 48 симетричних двохрозрядних двохоперандних операцій криптоперетворення замість 24, що реалізують дві попередні функціональні схеми.

В процесі дослідження було встановлено, що побудований пристрій доцільно застосовувати в блоці криптоперетворення інформації при реалізації методу підвищення стійкості та надійності потокового шифрування [3].

В процесі дослідження встановлено що сумісне застосування операцій збільшує кількість операцій з 12 до 60, і як наслідок, в 5 раз збільшує варіативність алгоритму потокового шифрування.

Висновки

Побудова апаратних засобів генерації математичних груп симетричних двохоперандних двохрозрядних операцій потокового шифрування по аналогії повинна відображати концепцію синтезу математичних груп операцій і включати в себе побудову блоків генерації операцій базової групи, генерації операцій перестановки та генерації операцій інверсії.

Розроблено функціональну схему пристрою реалізації груп операцій додавання за модулем два, яка реалізує синтез 24 симетричних операцій потокового шифрування в залежності від сигналів управління. Розроблено функціональну схему апаратного синтезу 24 симетричних операцій потокового шифрування на основі додавання за модулем чотири. Розроблено функціональну схему пристрою сумісної реалізації груп операцій додавання за модулем два та модулем чотири.

Розглянутий підхід до побудови розглянутих апаратних засобів можна трактувати як технологію синтезу апаратних засобів генерації груп симетричного двохоперандних двохрозрядних операцій потокового шифрування. Застосування розроблених апаратних засобів при вдосконаленні реалізації методу підвищення стійкості та надійності потокового шифрування забезпечує збільшення варіативності шифрування в 5 раз.

СПИСОК ЛІТЕРАТУРИ

1. Лада Н.В., Козловська С.Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2018. Т. 1 (47). С. 127-130.
2. Рудницький В.М. Криптографічне кодування: обробка та захист інформації: колективна монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 139 с.
3. Рудницький В.М., Лада Н.В., Бабенко В.Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 184 с.
4. Бабенко В.Г., Лада Н.В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.
5. Бабенко В.Г., Дахно Т.В., Рудницький В.М. Алгоритми синтезу логічних функцій для систем захисту інформації. Інтегровані інформаційні технології та системи (ІІТС-2007). К.:НАУ, 2007. С.46-48
6. Рудницкий В.Н., Пивнева С.В., Бабенко В.Г., Миронец И.В. и др. Криптографическое кодирование: методы и средства реализации: монографія. Тольят. гос. ун-т. Тольятти, 2013. 196 с.
7. Рудницький В.М., Бабенко В.Г. Математичне моделювання дискретних пристроїв для систем інформаційної безпеки. Міжнародна науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2007». Харків: НАУ ім. М.Є. Жуковського «Харківський авіаційний інститут», 2007. С. 227-229.
8. Бабенко В.Г. Параллельная реализация скользящего шифрования. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2013. Вип. 9(116). С. 131-134.
9. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
10. Рудницький В.М., Лада Н.В., Федотова-Півень І.М., Пустовіт М.О. Синтез обернених дворозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Системи та методи обробки інформації. Збірник наукових праць. Київ: ДНДІ МВС України, 2018. Вип. 4(55). С. 76–81.
11. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.
12. Semenov, S., Sira, O., Kuchuk, N. (2018), "Development of graphicanalytical models for the software security testing algorithm", Eastern-European Journal of Enterprise Technologies, Vol 2, No 4 (92), pp. 39-46, DOI: https://doi.org/10.15587/1729-4061.2018.127210
13. Пристрій для виконання логічних операцій криптографічного перетворення. Деклараційний патент на корисну модель 45916 Україна, МПК H03M 13/00. - № u200907997; Заявл. 29.07.2009; Опубл. 25.11.2009, Бюл. № 22.
14. Пристрій для виконання логічних операцій криптографічного перетворення. Деклараційний патент на корисну модель 45917 Україна, МПК H03M 13/00. - № u200907998; Заявл. 29.07.2009; Опубл. 25.11.2009, Бюл. № 22.
15. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. Системи управління, навігації та зв'язку: зб. наук. праць. К., 2012. Вип. 4 (24). С. 85–88.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет «ХПІ», Харків
Received (Надійшла) 12.08.2019
Accepted for publication (Прийнята до друку) 11.09.2019

Синтез аппаратных средств реализации групп симметрических двухоперандных операций поточного шифрования

Н. В. Лада, С. Г. Козловская, В. М. Зажома, С. В. Висоцький

Статья посвящена разработке технологии синтеза аппаратных средств для генерации групп симметричных двухоперандных двухрозрядних криптографических операций для повышения качества потокового шифрования.

Приведены результаты исследования по реализации симметричных операций потокового шифрования. Разработаны функциональные схемы устройств генерации и применения групп операций сложения по модулю два и четыре. Данные группы операций могут применяться как отдельно, так и совместно. Применение разработанных аппаратных средств при совершенствовании реализации метода повышения устойчивости и надежности потокового шифрования обеспечивает увеличение вариативности шифрования в пять раз.

Ключевые слова: криптографическое кодирование, потоковое шифрование, синтез групп криптопреобразования, сложение по модулю, функциональная схема.

Synthesizing the hardware implementation means for groups of symmetric two-operand stream ciphering operations

N. Lada, S. Kozlovska, V. Zazhoma, S. Vysotskyi

The article is devoted to the technology's development for synthesizing the hardware means to generate the groups of symmetric two-operand two-bit cryptographic operations for the quality of stream ciphering improvement. The research results of stream ciphering symmetric operations implementation are presented. The generation and application devices' functional diagrams for groups of modulo-2 and modulo-4 addition operations are developed. These groups of operations can be applied individually as well as jointly. Applying the developed hardware means increases the encryption variability by five times at improving the application of the stream ciphering stability and reliability increasing method.

Keywords: cryptographic coding, streaming encryption, synthesis of cryptoconversion groups, adding by module, functional diagram.