© Rudnytskyi V., Opiskiy I., Melnyk O., Pustovit M. Synthesis of group operations strong stable cryptographic encode for construction stream cipher // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, pp. 195-200.

DOI: 10.18372/2225-5036.24.13430

СИНТЕЗ ГРУПИ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ ДЛЯ ПОБУДОВИ ПОТОКОВИХ ШИФРІВ

Володимир Рудницький[1], Іван Опірський[2], Ольга Мельник[3], Михайло Пустовіт[3]

[1]Черкаський державний технологічний університет
[2] Національний університет «Львівська Політехніка»
[3]Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України

РУДНИЦЬКИЙ Володимир Миколайович, д.т.н., проф.

Рік та місце народження: 1962 рік, м. Золотоноша, Черкаська область, Україна.
Освіта: Харківське вище військове командно-інженерне училище 1984 рік.
Посада: завідувач кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету з 2018 року.
Наукові інтереси: розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного кодування; створення засобів обчислювальної техніки з необхідними рівнями надійності та захищеності.
Публікації: більше 200 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, патенти на винаходи, навчально-методичні розробки, навчальні посібники.
E-mail: RVN_2008@ukr.net

ОПІРСЬКИЙ Іван Романович, д.т.н., доц.

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: доцент кафедри захисту інформації з 2016 року.
Наукові інтереси: методи і засоби технічного захисту інформації, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки,прогнозування несанкціонованого доступу, математичні методи та моделі захисту інформації, спецвимірювання.
Публікації: понад 100 наукових публікацій, серед яких наукові статті, колективні монографія, навчальні посібники, тези та матеріали доповідей на конференціях, навчально-методичні праці
E-mail: iopirsky@gmail.com

МЕЛЬНИК Ольга Григорівна, к.т.н., с.н.с.

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 безпеки об'єктів будівництва та охорони праці Черкаського інституту пожежної безпеки імені Героїв Чорнобиля НУЦЗ України з 2012 року.
Наукові інтереси: методи та засоби побудови комп'ютеризованих систем прогнозування пожеж, розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 60 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, патенти та авторські свідоцтва, навчально-методичні розробки, навчальні посібники.
E-mail: melnyk.olja.2014@gmail.com

ПУСТОВІТ Михайло Олександрович

Рік та місце народження: 1984 рік, м. Дніпропетровськ, Україна.
Освіта: Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, 2006 рік.
Посада: старший викладач кафедри техніки та засобів цивільного захисту Черкаського інституту пожежної безпеки імені Героїв Чорнобиля НУЦЗ України з 2016 року.
Наукові інтереси: розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного кодування; створення систем підтримки прийняття рішень для фахівців органів і підрозділів цивільного захисту.
Публікації: більше 40 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, навчально-методичні розробки, навчальні посібники.
E-mail: m.pustovit@gmail.com

Анотація. *В даній статті проведено дослідження можливості синтезу груп дворозрядних операцій, що відповідають вимогам строгого стійкого кодування для потокового шифрування з точністю до перестановки з обмеженням дворозрядними операціями. За результатами дослідження синтезовано групу дворозрядних операцій строгого стійкого криптографічного кодування з точністю до перестановки.*
Визначено, що реалізація одноопераднних операцій у системах потокового шифрування може проводитись лише шляхом їх поєднання в двохоперандну операцію, в якій вибір операції першого операнда буде визначатися другим операндом. Було проведено перетворення отриманих операцій для спрощення їхнього представлення. Для цього було застосовано технологію побудови двохоперандних операцій криптографічного перетворення інформації. Встановлено взаємозв'язки між операціями при їх застосуванні для прямого та оберненого криптоперетворення. Застосування синтезованої групи операцій для вдосконалення методу підвищення стійкості та надійності потокових шифрів забезпечить збільшення варіативності алгоритму та максимальну невизначеність результатів шифрування, оскільки кожен біт вхідної інформації буде змінено з ймовірністю одна друга.

Ключові слова: *потокове шифрування, дворозрядні операції, строге стійке кодування, двохоперандні операції, криптостійкість.*

Актуальність проблеми дослідження.

Інформація на сьогодні розглядається як стратегічний продукт. Якісно та кількісно зріс обсяг інформаційних потоків, що циркулюють у комп'ютерних мережах і системах.

Найважливішою складовою сучасного інформаційного суспільства є глобальні інформаційні мережі й системи, серед яких найбільшої популярності набула глобальна мережа Інтернет. Проте глобальні інформаційні системи, поряд з позитивними впливами на суспільство, несуть також нові негативні впливи та потенційні загрози. Передусім це стосується нових можливостей несанкціонованого доступу до інформації, її корегування, або просто пошкодження та знищення. На сьогодні світове співтовариство вже усвідомило, що міжнародна інформаційна безпека є глобальною проблемою, розв'язання якої суттєво впливає на існування людства. Однією з найбільш актуальних задач, від вирішення якої залежить комфортне існування єдиного інформаційного простору, є випереджаючий розвиток комп'ютерної криптографії. Для інтенсифікації розвитку даного напряму постійно проводяться як державні, так і міжнародні конкурсні відбори алгоритмів претендентів на стандарти криптографії, в тому числі і постквантові.

Аналіз останніх досліджень і публікацій.

Серед напрямів розвитку комп'ютерної криптографії останнім часом активно розвивається синтез і аналіз операцій криптографічного кодування інформації, що забезпечують теоретико-інструментальну базу для побудови нових та вдосконалення існуючих [1]. Синтез даних операцій ґрунтується на використанні логічних функцій і поєднує в собі досягнення як систем захисту інформації, так і комп'ютерної інженерії. По своїй сутності дані операції представляють собою формалізовані багатоваріантні моделі підстановок, реалізація яких забезпечує високу ефективність як захисту інформації, так і застосування обчислювальної техніки при їх реалізації [2, 3].

Наукова новизна даного дослідження полягає в синтезі груп дворозрядних операцій, що відповідають вимогам строгого стійкого криптографічного кодування для потокового шифрування з точністю до перестановки. Застосування синтезованої групи операцій для вдосконалення методу підвищення стійкості та надійності потокових шифрів забезпечить збільшення варіативності алгоритму та максимальну невизначеність результатів шифрування.

Метою роботи є синтез і аналіз групи операцій строгого стійкого криптографічного кодування для побудови систем потокового шифрування.

Основна частина.

При дослідженні можливості синтезу груп дворозрядних операцій, що відповідають вимогам ССК для потокового шифрування з точністю до перестановки обмежимося дворозрядними операціями.

Множина дворозрядних операцій ССК включає в себе чотири операції [6], а саме:

$$F_1 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}; \quad F_2 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix};$$

$$F_3 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}; \quad F_4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix},$$

де $x_1, x_2 \in \{0, 1\}$ – значення біт вхідної інформації.

Реалізація даних одноопераднних операцій у системах потокового шифрування може проводитись лише шляхом їх поєднання в двохоперандну операцію, в якій вибір операції першого операнда буде визначатися другим операндом. Наприклад,

$$O_1^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \quad (1)$$

де $x_1, x_2 \in \{0,1\}$ – значення біт вхідної інформації, $\gamma_1, \gamma_2 \in \{0,1\}$ – значення біт гамуючої послідовності, $y_1, y_2 \in \{0,1\}$ – значення біт вихідної інформації.

Перетворимо операцію (1) для спрощення її представлення. Для цього застосуємо технологію побудови двохоперандних операцій криптографічного перетворення інформації:

$$O_1^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases}$$

Виходячи з цього,

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}. \quad (2)$$

Побудуємо обернену операцію за умови, що при прямому й оберненому перетворенні гамуючі послідовності повинні бути ідентичними.

Відповідно до [4] можна констатувати наступне:

– якщо $F_1 = F_1^k$ тоді $F_1^d = F_2^k = F_2$;

– якщо $F_2 = F_2^k$ тоді $F_2^d = F_1^k = F_1$;

– якщо $F_3 = F_3^k$ тоді $F_3^d = F_4^k = F_4$;

– якщо $F_4 = F_4^k$ тоді $F_4^d = F_3^k = F_3$.

З урахуванням відповідності між прямими й оберненими одноопераднними операціями, обернену операцію для (1) можна представити:

$$O_1^d = \begin{cases} \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} y_2 \oplus 1 \\ y_1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \quad (3)$$

Перетворимо операцію (3) для спрощення її представлення:

$$O_1^d = \begin{cases} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases},$$

Виходячи з цього,

$$O_1^d = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \quad (4)$$

Обернена операція (4) до операції (1) була отримана шляхом перестановки одноопераднних операцій F_1 і F_2. Використаємо дану перестановку одноопераднних операцій F_1 і F_2 в двохоперандній операції (1) для побудови нової двохоперандної операції криптоперетворення [7]:

$$O_2^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}. \quad (5)$$

Перетворимо операцію (5) для спрощення її представлення:

$$O_2^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases}.$$

Виходячи з цього,

$$O_2^k = \begin{bmatrix} x_1 \cdot \bar{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \bar{\gamma}_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}. \quad (6)$$

В результаті виконаної перестановки було отримано нову операцію (6), що відповідає вимогам ССК. Знайдемо обернену операцію для O_2^k. Для цього, переставивши в ній одноопераднні операції F_1 і F_2 місцями, отримаємо:

$$O_2^d = \begin{cases} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 0 \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 0; \gamma_2 = 1 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 0 \\ \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}, \text{ якщо } \gamma_1 = 1; \gamma_2 = 1 \end{cases},$$

$$O_2^d = \begin{bmatrix} y_1 \cdot \bar{\gamma}_1 \oplus y_2 \cdot \gamma_1 \\ y_1 \cdot \gamma_1 \oplus y_2 \cdot \bar{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \gamma_1 \oplus \gamma_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \quad (7)$$

На основі виразів (2), (4), (6) і (7) можна побачити, що: $O_1^k = O_2^d$; $O_2^k = O_1^d$; $O_1^d = O_2^k$; $O_2^d = O_1^k$.

Аналіз отриманих результатів дозволив зробити припущення, що, застосувавши всі перестановки одноопераднних операцій $F_1 - F_4$, отримаємо 24 операції криптографічного перетворення інформації, які відповідають вимогам ССК.

Результати побудови та аналізу операцій на основі перестановок одноопераднних операцій наведені в табл. 1. Дані операції будемо називати двохопераднними операціями з точністю до перестановки, що відповідають вимогам ССК.

Група двохопераднних операцій з точністю до перестановки, які відповідають вимогам ССК, наведена в табл. 1 таким чином, що кожна пара з 24 операцій – це дві взаємопов'язані операції даної групи. Якщо одна з даної пари операцій буде використана для прямого криптоперетворення, то інша операція забезпечить виконання оберненого криптоперетворення, про що свідчать залежності між операціями.

Найбільш доцільне та ефективне застосування групи синтезованих операцій можливе при вдосконаленні методу підвищення стійкості та надійності потокових шифрів [8]. Застосування даних операцій може бути реалізовано на основі двох варіантів: збільшення кількості операцій, які реалізують даний метод, що забезпечить додаткове збільшення варіативності алгоритму потокового шифрування, і, як наслідок, збільшиться криптостійкість; застосування синтезованої групи операцій замість дванадцяти операцій додавання по модулю два з точністю до перестановки, що також забезпечить збільшення варіативності алгоритму, а також забезпечить максимальну невизначеність результатів шифрування, оскільки кожен біт вхідної інформації буде змінено з ймовірністю одна друга.

Таблиця 1

Результати синтезу та аналізу двохоперандних операцій з точністю до перестановки, що відповідають вимогам ССК

Операції криптоперетворення		Примітки
$O_1^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \overline{\gamma_1 \oplus \gamma_2} \end{bmatrix}$	$O_2^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \overline{\gamma}_2 \end{bmatrix}$	$O_1^k = O_2^d;\ O_2^k = O_1^d;$ $O_1^d = O_2^k;\ O_2^d = O_1^k.$
$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \\ x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \\ \overline{\gamma}_1 \end{bmatrix}$	$O_4^k = \begin{bmatrix} x_1 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \\ x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \overline{\gamma}_2 \end{bmatrix}$	$O_3^k = O_4^d;\ O_4^k = O_3^d;$ $O_3^d = O_4^k;\ O_4^d = O_3^k.$
$O_5^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_2 \\ \gamma_2 \end{bmatrix}$	$O_6^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \\ x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma_1 \oplus \gamma_2} \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}$	$O_5^k = O_6^d;\ O_6^k = O_5^d;$ $O_5^d = O_6^k;\ O_6^d = O_5^k.$
$O_7^k = \begin{bmatrix} x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \\ x_1 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \\ \overline{\gamma}_1 \end{bmatrix}$	$O_8^k = \begin{bmatrix} x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \\ x_1 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_2 \\ \gamma_2 \end{bmatrix}$	$O_7^k = O_8^d;\ O_8^k = O_7^d;$ $O_7^d = O_8^k;\ O_8^d = O_7^k.$
$O_9^k = \begin{bmatrix} x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \\ x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \overline{\gamma}_2 \end{bmatrix}$	$O_{10}^k = \begin{bmatrix} x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \\ x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma_1 \oplus \gamma_2} \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}$	$O_9^k = O_{10}^d;\ O_{10}^k = O_9^d;$ $O_9^d = O_{10}^k;\ O_{10}^d = O_9^k.$
$O_{11}^k = \begin{bmatrix} x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \\ x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_2 \\ \gamma_2 \end{bmatrix}$	$O_{12}^k = \begin{bmatrix} x_1 \cdot \gamma_1 \oplus x_2 \cdot \overline{\gamma}_1 \\ x_1 \cdot \overline{\gamma}_1 \oplus x_2 \cdot \gamma_1 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \overline{\gamma_1 \oplus \gamma_2} \end{bmatrix}$	$O_{11}^k = O_{12}^d;\ O_{12}^k = O_{11}^d;$ $O_{11}^d = O_{12}^k;\ O_{12}^d = O_{11}^k.$
$O_{13}^k = \begin{bmatrix} x_1 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \\ x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_1 \\ \gamma_1 \end{bmatrix}$	$O_{14}^k = \begin{bmatrix} x_1 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \\ x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot \overline{(\gamma_1 \oplus \gamma_2)} \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_2 \\ \gamma_2 \end{bmatrix}$	$O_{13}^k = O_{14}^d;\ O_{14}^k = O_{13}^d;$ $O_{13}^d = O_{14}^k;\ O_{14}^d = O_{13}^k.$
$O_{15}^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \\ x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \\ \overline{\gamma}_1 \end{bmatrix}$	$O_{16}^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \\ x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \oplus \gamma_2 \\ \overline{\gamma_1 \oplus \gamma_2} \end{bmatrix}$	$O_{15}^k = O_{16}^d;\ O_{16}^k = O_{15}^d;$ $O_{15}^d = O_{16}^k;\ O_{16}^d = O_{15}^k.$
$O_{17}^k = \begin{bmatrix} x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \\ x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \\ \overline{\gamma}_1 \end{bmatrix}$	$O_{18}^k = \begin{bmatrix} x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \\ x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma_1 \oplus \gamma_2} \\ \gamma_1 \oplus \gamma_2 \end{bmatrix}$	$O_{17}^k = O_{18}^d;\ O_{18}^k = O_{17}^d;$ $O_{17}^d = O_{18}^k;\ O_{18}^d = O_{17}^k.$
$O_{19}^k = \begin{bmatrix} x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \\ x_1 \cdot (\overline{\gamma_1 \oplus \lambda_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_1 \\ \gamma_1 \end{bmatrix}$	$O_{20}^k = \begin{bmatrix} x_1 \cdot (\gamma_1 \oplus \gamma_2) \oplus x_2 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \\ x_1 \cdot (\overline{\gamma_1 \oplus \gamma_2}) \oplus x_2 \cdot (\gamma_1 \oplus \gamma_2) \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \overline{\gamma}_2 \end{bmatrix}$	$O_{19}^k = O_{20}^d;\ O_{20}^k = O_{19}^d;$ $O_{19}^d = O_{20}^k;\ O_{20}^d = O_{19}^k.$
$O_{21}^k = \begin{bmatrix} x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \\ x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \end{bmatrix} \oplus \begin{bmatrix} \gamma_2 \\ \overline{\gamma}_2 \end{bmatrix}$	$O_{22}^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \\ x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \gamma_1 \\ \overline{\gamma}_1 \end{bmatrix}$	$O_{21}^k = O_{22}^d;\ O_{22}^k = O_{21}^d;$ $O_{21}^d = O_{22}^k;\ O_{22}^d = O_{21}^k.$
$O_{23}^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \\ x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_2 \\ \gamma_2 \end{bmatrix}$	$O_{24}^k = \begin{bmatrix} x_1 \cdot \overline{\gamma}_2 \oplus x_2 \cdot \gamma_2 \\ x_1 \cdot \gamma_2 \oplus x_2 \cdot \overline{\gamma}_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{\gamma}_1 \\ \gamma_1 \end{bmatrix}$	$O_{23}^k = O_{24}^d;\ O_{24}^k = O_{23}^d;$ $O_{23}^d = O_{24}^k;\ O_{24}^d = O_{23}^k.$

Висновки.

На основі проведеного дослідження було синтезовано групу дворозрядних операцій строгого стійкого криптографічного кодування з точністю до перестановки. Встановлено взаємозв'язки між операціями при їх застосуванні для прямого та оберненого криптоперетворення. Застосування синтезованої групи операцій для вдосконалення методу підвищення стійкості та надійності потокових шифрів забезпечить збільшення варіативності алгоритму й максимальну невизначеність результатів шифрування.

ЛІТЕРАТУРА

[1]. В. Бабенко, С. Рудницький, "Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення", *Системи обробки інформації : зб. наук. праць*, № 9 (107), С. 130-139, 2012.

[2]. В. Рудницький, І. Миронець, В. Бабенко, "Систематизація повної множини логічних функцій

для криптографічного перетворення інформації", *Системи обробки інформації : зб. наук. праць*, Вип. 8 (98), С. 184-188, 2011.

[3]. В. Рудницький, В. Бабенко, Д. Жиляєв, "Алгебраїчна структура множини логічних операцій кодування", *Наука і техніка Повітряних Сил Збройних Сил України*, Вип. 2 (6), С. 112-114, 2011.

[4]. В. Рудницький, Л. Шувалова, О. Нестеренко, "Аналіз дворозрядних операцій криптографічного кодування по критерію строгого лавинного ефекту", *Наукові праці Чорноморського державного університету імені Петра Могили. Комп'ютерні технології*, Том 283, № 271, С. 74-77, 2016.

[5]. В. Рудницький, Л. Шувалова, О. Нестеренко, "Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування", *Вісник інженерної академії України*, Вип. 3, С. 105-108, 2016.

[6]. В. Рудницький, Л. Шувалова, О. Нестеренко, "Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування", *Вісник Черкаського державного технологічного університету*, Вип. 1, С. 5-10, 2017.

[7]. В. Рудницький, Н. Лада, С. Козловська, "Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання", *Сучасні інформаційні системи*, Т. 2, № 4, С. 26-30, 2018.

[8]. Н. Лада, С. Козловська, "Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах", *Системи управління, навігації та зв'язку : збірник наукових праць*. Т. 1 (47), С. 127-130, 2018.

УДК 004.421.5: 004.056.55

Рудницкий В.Н., Опирский И.Р., Мельник О.Г., Пустовит М.А. Синтез группы операций строгого устойчивого криптографического кодирования для построения потоковых шифров

Аннотация. *В данной статье проведено исследование возможности синтеза групп двухразрядных операций, отвечающих требованиям строгого устойчивого кодирования для потокового шифрования с точностью до перестановки с ограничением двухразрядными операциями. По результатам исследования синтезировано группу двухразрядных операций строгого устойчивого криптографического кодирования с точностью до перестановки. Определено, что реализация одноопернадных операций в системах потокового шифрования может проводиться только путем их объединения в двухоперандную операцию, в которой выбор операции первого операнда будет определяться вторым операндом. Было проведено преобразование полученных операций для упрощения их представления. Для этого была применена технология построения двухоперандных операций криптографического преобразования информации. Установлены взаимосвязи между операциями при их применении для прямого и обратного криптопреобразования. Применение синтезированной группы операций для совершенствования метода повышения устойчивости и надежности потоковых шифров обеспечит увеличение вариативности алгоритма и максимальную неопределенность результатов шифрования, поскольку каждый бит исходной информации будет изменен с вероятностью одна вторая.*

Ключевые слова: *потоковое шифрование, двухразрядные операции, строгое устойчивое кодирование, двухоперандные операции, криптостойкость.*

Rudnytskyi V., Opiskiy I., Melnyk O., Pustovit M. Synthesis of group operations strong stable cryptographic encode for construction stream cipher

Annotation. *In this article a study was conducted of the possibility of synthesizing groups of two-bit operations that meet the requirements of strict stable coding for stream ciphering up to permutation with the restriction of two-bit operations. According to the results of the study, a group of two-digit operations of strict stable cryptographic coding with a permutation accuracy was synthesized. It is determined that the implementation of single-operand operations in stream encryption systems can only be carried out by combining them into a two-operand operation, in which the choice of the operation of the first operand will be determined by the second operand. Transformation of the received operations was carried out to simplify their presentation. For this, the technology of construction of two-operand operations of cryptographic transformation of information was applied. The interrelationships between operations in their application for direct and inverse crypto-transformation are established. The use of a synthesized group of operations to improve the method of improving the stability and reliability of stream ciphers will increase the variability of the algorithm and maximize the uncertainty of the encryption results, since each bit of the original information will be changed with one-second probability.*

Keywords: *stream encryption, two-bit operations, strict stable coding, two-operand operations, cryptographic resistance.*

Отримано 11 *грудня 2018 року*, затверджено редколегією 16 *грудня 2018 року*