Захист інформації

УДК 003.26:004.056.55

В.Г. Бабенко[1], Н.В. Лада[2]

[1] *Одеська національна академія зв'язку ім. О.С. Попова, Одеса*
[2] *Черкаський державний технологічний університет, Черкаси*

СИНТЕЗ І АНАЛІЗ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ДОДАВАННЯ ЗА МОДУЛЕМ ДВА

В статті здійснено синтез та аналіз групи операцій дворозрядного криптографічного додавання за модулем два. Доведено, що синтезована група операцій є групою перестановок та показана її придатність для використання в алгоритмах криптографічного перетворення. В результаті дослідження встановлено, що множину операцій криптографічного додавання за модулем два можливо застосовувати для практичного використання для розширення кількості операцій криптографічного перетворення інформації.

Ключові слова: *криптографічні алгоритми, операції криптографічного перетворення, операція додавання за модулем два, комутативність, еквівалентність, група перестановок.*

Вступ

Постановка проблеми. У сучасному інформаційному суспільстві велику загрозу конфіденційності та цілісності інформації представляє кіберзлочинність. Зростання кількості кібератак та доступність програмно-технічних засобів для їх реалізації зумовлює необхідність розробки сучасних засобів інформаційної безпеки громадян та держави в цілому.

Отже, актуальною задачею є створення та вдосконалення систем захисту інформації, зокрема алгоритмів криптографічного захисту, що в більшості випадків є базовим ядром таких систем. На даний час основним питанням, що підлягає вирішенню, є збільшення об'ємів інформації, що може оброблятися функціями криптографічного перетворення. Одним з підходів вирішення даної проблеми є застосування матричних обчислень.

Саме тому особливу увагу приділено технології виконання матричної операції криптографічного перетворення великої розмірності за допомогою формування на її основі декількох матричних операцій меншої розмірності з подальшою можливістю застосування даної технології для розробки криптоалгоритмів.

Основою функції криптографічного перетворення є базова операція. Тому для вирішення сформульованої проблеми необхідно провести синтез та дослідження множини операцій дворозрядного криптографічного додавання за модулем два з точністю до перестановки, обґрунтувати можливість застосування виявленої групи операцій в якості операції криптографічного додавання за модулем два.

Аналіз останніх досліджень і публікацій. В [1] запропоновано застосовувати матричні операції криптографічного перетворення та криптопримітиви побудовані на основі них для алгоритмів захисту інформаційних ресурсів.

В [1, 2] доведено, що застосування матричних операцій криптографічного перетворення підвищує швидкодію обробки даних в криптосистемах за рахунок паралельного процесу виконання операції криптоперетворення.

Отримані результати наукових досліджень в [2] підтверджують, що складність виконання матричних операцій криптографічного перетворення напряму залежить від кількості операндів. Тому одним із варіантів рішення даної проблеми є можливість представлення матричної операції великої розмірності у вигляді декількох операцій меншої розмірності, які виконуватимуться набагато швидше, тому що їх складність в рази менша.

Мета роботи – здійснити синтез групи операцій дворозрядного криптографічного додавання за модулем два та провести аналіз щодо придатності її використання в алгоритмах криптографічного перетворення.

Основний матеріал

Операцію дворозрядного криптографічного додавання за модулем два можна представити як $F_{\mathrm{mod}\,2} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$, де $x_i, y_i \in \{0,1\}$ – розряди інформації відповідно, $i \in \{1,2\}$, $\oplus$ – операція додавання за модулем два.

Виходячи з наведеної моделі операції можна побудувати групу аналогічних операцій з точністю до перестановки. Результати синтезу даних операцій наведені в табл. 1, де F_i – і-та операція криптографічного додавання, $i \in \{1..24\}$, так як дана операція має 4 операнди, то $i = 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Для проведення подальшого аналізу синтезованих операцій доцільно ввести нумерацію операцій, яка необхідна для спрощення дослідження результатів синтезу.

Таблиця 1

Множина операцій

Модель операції	Модель операції	Модель операції	Модель операції
$F_1 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$F_2 = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}$	$F_3 = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$	$F_4 = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$
$F_5 = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}$	$F_6 = \begin{vmatrix} x_1 \oplus y_2 \\ y_1 \oplus x_2 \end{vmatrix}$	$F_7 = \begin{vmatrix} y_1 \oplus x_2 \\ x_1 \oplus y_2 \end{vmatrix}$	$F_8 = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix}$
$F_9 = \begin{vmatrix} x_1 \oplus x_2 \\ y_2 \oplus y_1 \end{vmatrix}$	$F_{10} = \begin{vmatrix} x_1 \oplus y_1 \\ y_2 \oplus x_2 \end{vmatrix}$	$F_{11} = \begin{vmatrix} y_2 \oplus x_2 \\ x_1 \oplus y_1 \end{vmatrix}$	$F_{12} = \begin{vmatrix} y_2 \oplus y_1 \\ x_1 \oplus x_2 \end{vmatrix}$
$F_{13} = \begin{vmatrix} y_1 \oplus x_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$F_{14} = \begin{vmatrix} y_1 \oplus y_2 \\ x_2 \oplus x_1 \end{vmatrix}$	$F_{15} = \begin{vmatrix} x_2 \oplus x_1 \\ y_1 \oplus y_2 \end{vmatrix}$	$F_{16} = \begin{vmatrix} x_2 \oplus y_2 \\ y_1 \oplus x_1 \end{vmatrix}$
$F_{17} = \begin{vmatrix} x_2 \oplus x_1 \\ y_2 \oplus y_1 \end{vmatrix}$	$F_{18} = \begin{vmatrix} x_2 \oplus y_1 \\ y_2 \oplus x_1 \end{vmatrix}$	$F_{19} = \begin{vmatrix} y_2 \oplus y_1 \\ x_2 \oplus x_1 \end{vmatrix}$	$F_{20} = \begin{vmatrix} y_2 \oplus x_1 \\ x_2 \oplus y_1 \end{vmatrix}$
$F_{21} = \begin{vmatrix} y_1 \oplus x_1 \\ y_2 \oplus x_2 \end{vmatrix}$	$F_{22} = \begin{vmatrix} y_1 \oplus x_2 \\ y_2 \oplus x_1 \end{vmatrix}$	$F_{23} = \begin{vmatrix} y_2 \oplus x_1 \\ y_1 \oplus x_2 \end{vmatrix}$	$F_{24} = \begin{vmatrix} y_2 \oplus x_2 \\ y_1 \oplus x_1 \end{vmatrix}$

Так як представлені в табл. 1 операції можуть розглядатися як одна операцією з точністю до перестановки, то вони зберігають всі властивості операції дворозрядного криптографічного додавання за модулем два та відрізняються лише результатами їх виконання.

Так як операція дворозрядного криптографічного додавання за модулем два є базовою для багатьох функцій перетворення криптографічних алгоритмів, то можемо запропонувати, що її можливо замінити на будь-яку іншу операцію із тих, що отримані в результаті синтезу (табл. 1).

В той же час, можемо констатувати, що синтезована множина операцій характеризується надлишковістю, адже в ній присутні операції, які володіють властивісю комутативності.

Тому виникає потреба у скороченні кількості операцій, що утворюють множину операцій дворозрядного криптографічного додавання за модулем два.

Це можливо за рахунок виявлення та викреслення таких операцій, що мають властивість комутативності [3, ст. 41], тобто

$$x \oplus y = c,$$

$$y \oplus x = c,$$

звідси

$$x \oplus y = y \oplus x.$$

А це означає, що результат застосування двох різних операцій однаковий.

Провівши аналіз отриманої множини операцій, було виявлено такі комутативні пари операцій табл. 2.

Таблиця 2

Комутативні моделі операцій

Відповідні пари моделей операцій		
$F_6 \cong F_2$	$F_{13} \cong F_1$	$F_{19} \cong F_8$
$F_7 \cong F_3$	$F_{14} \cong F_8$	$F_{20} \cong F_2$
$F_9 \cong F_5$	$F_{15} \cong F_5$	$F_{21} \cong F_1$
$F_{10} \cong F_1$	$F_{16} \cong F_4$	$F_{22} \cong F_3$
$F_{11} \cong F_4$	$F_{17} \cong F_5$	$F_{23} \cong F_2$
$F_{12} \cong F_8$	$F_{18} \cong F_3$	$F_{24} \cong F_4$

Скоротивши кількість синтезованих операцій, отримаємо основні операції групи – табл. 3.

Дві системи лінійних рівнянь називаються еквівалентними, якщо довільний розв'язок однієї з них є розв'язком іншої та навпаки (тобто якщо вони мають одну і ту ж множину розв'язків).

Очевидно, що поняття еквівалентності володіє властивістю симетричності, тобто якщо A~B, то B~A [3, с. 69].

В ході дослідження основних операцій групи (табл. 3), встановлено, що використання еквівалентних систем (операцій) призводить до перестановки результатів шифрування в криптографії, тому вони можуть використовуватися при розробці криптографічних алгоритмів.

Таблиця 3

Основні операції

Модель операції
$F_1 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$
$F_2 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$
$F_3 = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$
$F_4 = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$
$F_5 = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}$

Крім цього операція F_5 не придатна для застосування в матричних операціях криптографічного перетворення, тому що її застосування призведе до втрати інформації.

Аналіз властивостей операцій в табл. 1 показав, що з 24 синтезованих операцій лише перші 5 відрізняються результатами свого виконання, всі інші повторюють їх результати.

В результаті дослідження встановлено, що множину операцій дворозрядного криптографічного додавання за модулем два придатну для практичного використання розширено на три операції.

Висновки

Провели аналіз синтезованих на основі перестановок операцій і за допомогою знаходження комутативних операцій виділили в якості основних 4 операції дворозрядного криптографічного додавання за модулем два. Так як отримана множина операцій є групою перестановок G_4, то дана група має точно такі властивості як і додавання за модулем два. Тому отримана в дослідженні група операцій дворозрядного криптографічного додавання за модулем два може розширити кількість операцій, що застосовуються у блокових та потокових шифрах.

Список літератури

1. Криптографическое кодирование: методы и средства реализации: монография / В.Н. Рудницкий, С.В. Пивнева, В.Г. Бабенко, И.В. Миронец и др. – Тольятти: Тольят. гос. ун-т, 2013. – 196 с.

2. Рудницький В.М. Алгебраїчна структура множини логічних операцій кодування / В.М. Рудницький, В.Г. Бабенко, Д.А. Жиляєв // Наука і техніка Повітряних Сил Збройних Сил України: наук.-техн. журн. – Х.: ХУПС ім. І. Кожедуба. – 2011. – № 2 (6). – С. 112-114.

3. Ильин В.А. Линейная алгебра: Учеб. для вузов / В.А. Ильин, Э.Г. Позняк. – 4-е изд. – М.: Нака. Физматлит, 1999. – 296 с.

Надійшла до редколегії 3.03.2014

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

СИНТЕЗ И АНАЛИЗ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО СЛОЖЕНИЯ ПО МОДУЛЮ ДВА

В.Г. Бабенко, Н.В. Лада

В статье осуществлен синтез и анализ группы операций двухразрядного криптографической сложения по модулю два. Доказано, что синтезированная группа операций является группой перестановок и показана ее пригодность для использования в алгоритмах криптографического преобразования. В результате исследования установлено, что множество операций криптографической сложения по модулю два можно применять для практического использования для расширения количества операций криптографического преобразования информации.

Ключевые слова: *криптографические алгоритмы, операции криптографического преобразования, операция сложения по модулю два, коммутативность, эквивалентность, группа перестановок.*

SYNTHESIS AND ANALYSIS OF OPERATIONS OF CRYPTOGRAPHIC ADDITION MODULO TWO

V.G. Babenko, N.V. Lada

In this article the synthesis and analysis of group 2-digit cryptographic operations of addition modulo two have been done. We prove that the synthesized group of operations is the permutation group and shown its suitability for use in cryptographic transformation algorithms. The study found that many cryptographic operations of addition modulo two can be used for practical applications to expand the number of operations of a cryptographic transformation of the information.

Keywords: *cryptographic algorithms, operations of cryptographic transformation, the operation of addition modulo two, the commutativity, the equivalence, group of permutations.*