УДК 004.056.55:004.312.2

В.Г. Бабенко,
кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДЛЯ СИНТЕЗУ КРИПТОАЛГОРИТМІВ

У статті наведені способи синтезу ефективних криптоалгоритмів на основі використання операцій криптографічного перетворення інформації, запропоновано підходи до розрахунків параметрів отриманих алгоритмів. Здійснений аналіз показників ефективності застосування запропонованих структур криптоалгоритмів показав, що використання операцій криптографічного перетворення на макро- та мікрорівнях забезпечує підвищення криптостійкості та швидкості реалізації алгоритмів криптографічного захисту інформації.

Ключові слова: *криптографічний алгоритм, операція криптографічного перетворення, час виконання, швидкість реалізації, криптостійкість, складність реалізації, структура операції, макро- та мікрорівень використання операцій.*

В статье приведены способы синтеза эффективных криптоалгоритмов на основе использования операций криптографического преобразования информации, предложены подходы к расчетам параметров полученных алгоритмов. Проведенный анализ показателей эффективности применения предложенных структур криптоалгоритмов показал, что использование операций криптографического преобразования на макро- и микроуровнях обеспечивает повышение криптостойкости и скорости реализации алгоритмов криптографической защиты информации.

Ключевые слова: *криптографический алгоритм, операция криптографического преобразования, время выполнения, скорость реализации, криптостойкость, сложность реализации, структура операции, макро- и микроуровень использования операций.*

The paper presents methods for the synthesis of efficient cryptographic algorithms based on the use of cryptographic transformation operations of information, approaches to calculating the parameters of the received algorithms are proposed. The analysis of indicators of the effectiveness of the proposed structures of cryptographic algorithms has shown that the use of cryptographic transformation operations at the macro- and micro levels enhances the reliability and speed of an implementation of algorithms for cryptographic protection of information.

Keywords: *cryptographic algorithm, cryptographic transformation operation, execution time, the speed of implementation, cryptographic, implementation complexity, the structure of operation, macro and micro-level of operations use.*

Діяльність сучасного суспільства безпосередньо пов'язана із введенням, збереженням, обробкою та виведенням інформації, зокрема персональної. У свою чергу, використання автоматизованих систем обробки інформації у всіх сферах діяльності суспільства має як ряд переваг, так і призводить до виникнення низки проблем, одною з яких на цей час є проблема інформаційної безпеки. Широке

запровадження автоматизованих засобів обробки інформації, зокрема комп'ютерних систем, зумовлює залежність суспільства від ступеня безпеки інформаційних технологій, що застосовуються. Безпека комп'ютерних систем давно виокремлена як самостійний напрям наукових досліджень. Особливу увагу за цьому напряму присвячено криптографії, адже криптографічні алгоритми вважаються одним із найефективніших засобів захисту інформації. На цьому етапі науково-технічного прогресу стрімкий розвиток інформаційних технологій не тільки вимагає розробки нових криптографічних алгоритмів, що зможуть забезпечити якісний захист інформації, але й зумовлює нові вимоги щодо вдосконалення та ефективного застосування вже наявних.

Таким чином, на сьогодні однією з актуальних проблем інформаційної безпеки є підвищення ефективності засобів криптографічного захисту інформації.

Згідно з дослідженнями К. Шеннона [1] повторне використання криптоалгоритмів, що базуються на операціях, які належать різним групам, підвищує криптостійкість. Виходячи з цього, при побудові крипоталгоритмів доцільно використовувати операції криптоперетворення, які належать різним математичним групам. Серед останніх досліджень і публікацій варто звернути увагу на [2; 3], де представлено методи синтезу матричних моделей операцій для криптографічного перетворення інформації, а також способи застосування синтезованих матричних операцій для криптографічного захисту інформації. У роботах [4; 5] була доведена ефективність застосування матричних та розширених матричних операцій криптографічного перетворення інформації, побудованих на основі арифметичних операцій за різними модулями, які належать різним математичним групам.

Проте в цих дослідженнях не було здійснено синтезу криптоалгоритмів з ефективним використанням операцій криптографічного перетворення та опис взаємозалежностей між показниками цих алгоритмів криптографічного захисту інформації.

Метою дослідження є розробка стратегії синтезу криптоалгоритмів на основі застосування операцій криптографічного перетворення для покращання показників ефективності засобів захисту інформаційних ресурсів.

Можливо прийняти, що шифрування кожного вхідного повідомлення полягає в послідовному виконанні над ним декількох елементарних шифрувальних перетворень. У такому випадку формування конкретного алгоритму шифрування можна задати шляхом задання залежності почерговості виконання елементарних перетворень від секретного ключа [6].

Виходячи з цього, криптографічний алгоритм можна представити як послідовність операцій криптографічного перетворення інформації $Y=f(X)$ де $f=[F_1, F_2,...,F_n]$, тоді:

$$Y = F_n(...(F_2(F_1(X)))) \qquad (1)$$

Графічно криптографічний алгоритм зображено в загальному вигляді на рис. 1.

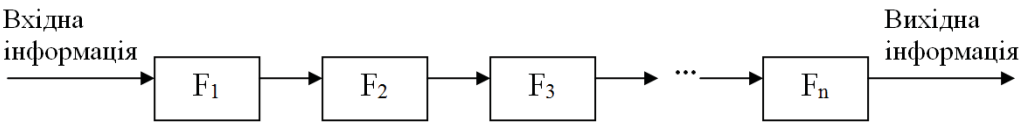

Рис. 1. Графічна структура криптографічного алгоритму

Для забезпечення максимальної криптостійкості повинна виконуватися основна вимога до вибору операцій, а саме: будь-які дві обрані операції, що виконуються послідовно, не належать одній групі. Наприклад: матричні операції, розширені (нелінійні) матричні операції, операції перестановки, керовані інформацією, та інші.

Кожна операція криптографічного перетворення $F_i(x)$ має складену функціональну структуру, яка охоплює всю обрану групу операцій та забезпечує реалізацію однозначно визначеної на основі ключової послідовності операції перетворення.

Структура операції перетворення криптографічного алгоритму наведена на рис. 2.

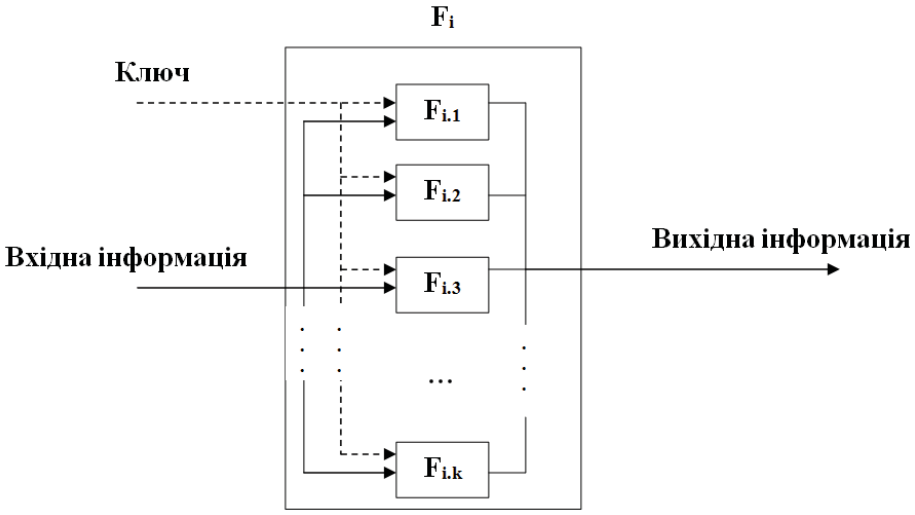

Рис. 2. Структура операції перетворення

Складність реалізації будь-якої операції $F_{i,j}$ однакова, тому складність операції криптографічного перетворення дорівнює складності виконуваної операції:

$$C(F_i) = C(F_{i.j}), \quad j = 1..k\,. \tag{2}$$

Звідси складність криптографічного алгоритму (рис. 1) розраховується як сума складностей реалізації кількості операцій криптографічного перетворення, тому що виконання операцій здійснюється послідовно:

$$C_{ALG} = \sum_{i=1}^{n} C(F_i) = \sum_{i=1}^{n} C(F_{i.j}) = C(F_{1.j}) + C(F_{2.j}) + ... + C(F_{n.j})\,, \tag{3}$$

де, j=1..k, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення ($F_{i,}$ i=1..n);

k – кількість операцій групи, що реалізує операцію перетворення.

Оскільки є лише єдиний виключний випадок, коли $C(F_{1.j}) = C(F_{2.j}) = ... = C(F_{n.j})$, то складність алгоритму розраховуватиметься як $C_{ALG} = n \times C(F_{i.j})$.

Тобто в загальному випадку всі операції криптографічного перетворення мають різну складність, тому діє залежність, описана в (3).

Час виконання будь-якої операції $F_{i,j}$ однаковий, тому час виконання операції криптографічного перетворення дорівнює часу виконання однієї операції:

$$Time(F_i) = Time(F_{i.j}), \quad j = 1..k. \tag{4}$$

Звідси час виконання криптографічного алгоритму (рис. 1) розраховується як сума часу виконання операцій в алгоритмі криптографічного перетворення, тому що операції виконуються послідовно:

$$Time_{ALG} = \sum_{i=1}^{n} Time(F_i) = \sum_{i=1}^{n} Time(F_{i.j}) = Time(F_{1.j}) + Time(F_{2.j}) + ... + Time(F_{n.j}), \tag{5}$$

де j=1..k, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення (F_i,i=1..n); k – кількість операцій групи, що реалізує операцію перетворення.

Швидкість реалізації операції перетворення обернено пропорційна часу виконання та складності.

Виходячи з цього, швидкість реалізації алгоритму визначається як:

$$V_{ALG} = \frac{1}{Time_{ALG}} = \frac{1}{Time(F_{1.j}) + Time(F_{2.j}) + ... + Time(F_{n.j})} = \frac{1}{\sum_{i=1}^{n} Time(F_{i.j})}. \tag{6}$$

Час виконання операції прямо пропорційний складності її реалізації, тоді $Time(F_i) = k_i \cdot C(F_i)$. Визначимо час реалізації криптоалгоритму, виходячи із його складності:

$$Time_{ALG} = \sum_{i=1}^{n} k_i \cdot C(F_{i.j}) = k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + ... + k_n \cdot C(F_{n.j}). \tag{7}$$

Враховуючи зазначене вище, швидкість виконання криптоалгоритму визначатиметься як:

$$V_{ALG} = \frac{1}{\sum_{i=1}^{n} k_i \cdot C(F_{i.j})} = \frac{1}{k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + ... + k_n \cdot C(F_{n.j})}. \tag{8}$$

Криптостійкість операції F_i визначається як криптостійкість $F_{i,j}$, тому що операції, які реалізують F_i, належать одній групі. Повторне використання операції F_i не призводить до збільшення криптостійкості. Оскільки операції алгоритму не створюють єдиної математичної групи та виконуються послідовно, то криптостійкість алгоритму визначається як добуток значень криптостійкості операцій:

$$K_{ALG} = \prod_{i=1}^{n} K(F_i) = \prod_{i=1}^{n} K(F_{i.j}) = K(F_{1.j}) \cdot K(F_{2.j}) \cdot ... \cdot K(F_{n.j}). \tag{9}$$

Структура паралельного виконання операції перетворення криптографічного алгоритму над блоком інформації наведена на рис. 3.

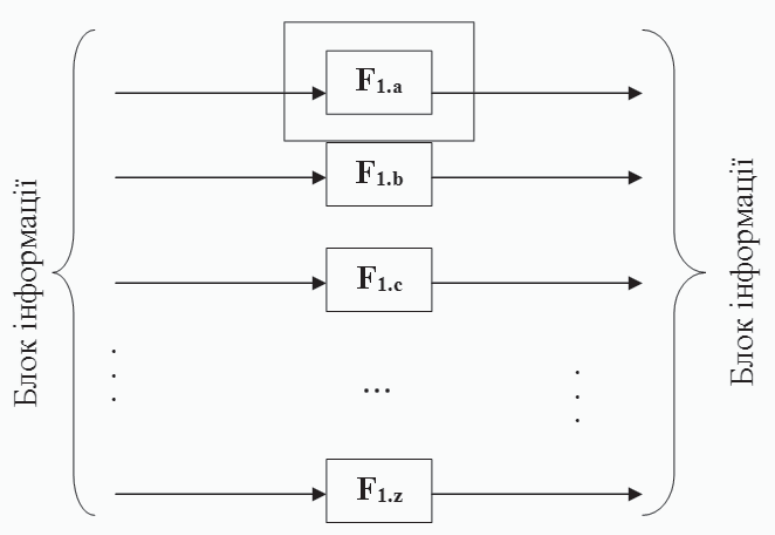

Рис. 3. Графічна структура паралельного виконання операції перетворення блоку інформації

Криптографічний алгоритм може складатися із операцій різної розрядності, що забезпечує підвищення криптостійкості перетворення, тому що операції, які мають різну кількість змінних, належать до різних груп операцій.

Крім того, при такому криптоалгоритмі забезпечуються властивості розсіювання та перемішування, оскільки розряди інформації кожного з підблоків (при перетворенні блоку інформації він розбивається на підблоки згідно з розрядністю операцій, які будуть над ними виконуватися) будуть мати вплив на значення кінцевого результату. Структурна схема взаємозв'язків для виконання послідовності операцій, в якій кожна наступна операція має іншу розрядність, наведена на рис. 4. У цій структурній схемі зображені операції над 8 та 5 операндами.

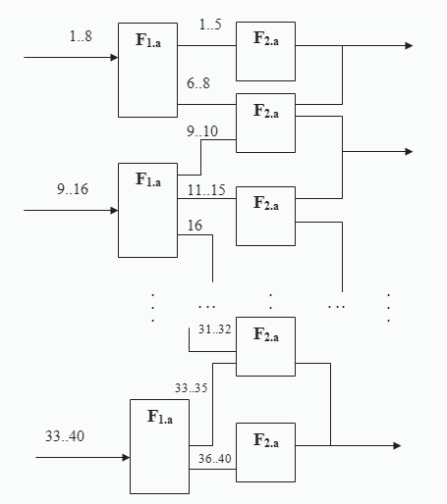

Рис. 4. Графічна структура виконання операції перетворення блоків інформації різної розрядності

Зазначена схема застосування операцій криптографічного перетворення функціонально може бути використана для заміни однієї операції над 40 операндами.

Для порівняння операцій з різною кількістю операндів можна визначати їх складність та час виконання через максимально можливу кількість операндів в операції. Тоді умовна складність реалізації послідовності операцій над 8 та 5 операндами буде не більше ніж 13. А складність операції над 40 операндами дорівнює 40. Умовний час виконання операцій буде 13 та 40 відповідно.

У результаті проведеного дослідження було встановлено, що найефективніше здійснювати вибір кількості змінних для операцій як прості числа, що забезпечує досягнення оптимальної складності алгоритма.

Ще одним зі способів застосування операцій для синтезу криптоалгоритму можна вважати послідовність операцій на основі різних модулів, що теж забезпечує покращання криптографічних властивостей перетворення. У [4] проаналізовані схеми реалізації криптографічного перетворення, що використовують комбінацію операцій на основі різного модуля. Також у [4] показано, що є два способи застосування операцій з різним модулем, коли спочатку криптографічне перетворення відбувається на базі операції, синтезованої на основі суми за модулем 2, а потім застосовується операція, синтезована на основі суми за модулем N та навпаки. В [4] доведено, що для підвищення криптостійкості алгоритму до статистичного криптоаналізу операцію додавання за модулем 2 доцільно використовувати як кінцеву операцію для побудови операцій криптографічного перетворення.

Крім цього, криптографічний алгоритм може здійснюватися послідовністю перетворень, кожне з яких побудоване на основі різних операцій, при цьому послідовне виконання операцій над однаковою кількістю операндів за умови використання операцій з різних математичних груп забезпечує підвищення криптостійкості.

Цей підхід до використання синтезованих операцій криптографічного перетворення дозволяє визначити макро та мікрорівень використання операцій. Наведені вище алгоритми з використанням операцій можна вважати макрорівнем.

Використання операції для реалізації іншої операції – це мікрорівень.

Графічно криптографічний алгоритм на основі різних операцій на мікрорівні зображено в загальному вигляді на рис. 5.

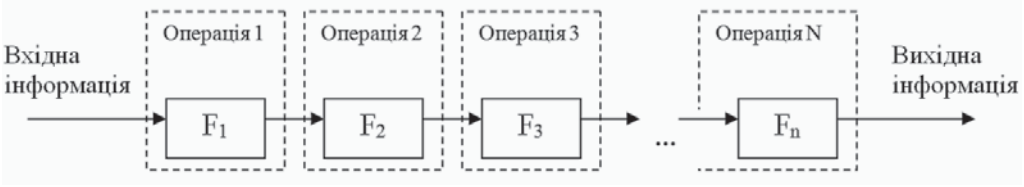

Рис. 5. Графічна структура криптографічного алгоритму з додатковим використання операцій на мікрорівні.

У цьому алгоритмі кожна операція криптографічного перетворення $F_i(x)$, що формує послідовність для виконання перетворення над інформацією, будується на основі вибраної синтезованої операції. При чому для різних операцій криптографічного перетворення $F_i(x)$ вибираються операції на мікрорівні з різних груп.

Подальші дослідження будуть спрямовані на дослідження статистичних властивостей запропонованих криптографічних алгоритмів для аналізу ефективності їх застосування при побудові засобів захисту інформації.

У роботі показано, що використання як криптоалгоритму послідовності операцій криптоперетворення, що належать різним групам, дає змогу покращувати показники криптостійкості цих алгоритмів. Аналіз показників ефективності застосування запропонованих структур криптоалгоритмів показав, що використання операцій криптографічного перетворення забезпечує підвищення криптостійкості та швидкості реалізації алгоритмів криптографічного захисту інформації залежно від способу здійснення криптоперетворення. Наведено взаємозалежності зміни показників ефективності синтезованих криптоалгоритмів, а саме: складності, часу та швидкості виконання, криптостійкості, що забезпечує можливість управління властивостями криптоалгоритму на стадії проектування залежно від поставлених завдань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Шеннон К.* Работы по теории информации и кибернетике / К. Шеннон. – М. : Изд-во иностранной литературы, 1963. – 830 с.

2. *Рудницький В.М.* Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – 2012. – Вип. 4 (33). – С. 198–200.

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.* Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем / В.Г. Бабенко // Системи управління, навігації та зв'язку : зб. наук. пр. – 2012. – Вип. 4 (24). – С. 85–88.

5. Криптографическое кодирование: методы и средства реализации (часть 2) : монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О.Г. Мельник. – Краснодар, 2014. – 224 с.

6. *Молдовян А.А.* Криптографія / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. – СПб. : Издательство "Лань", 2001. – 224 с., илл. – (Учебники для вузов. Специальная литература).

Отримано 01.10.2014.