УДК 003.26:004.056.55

Р.П. Мельник

Академія пожежної безпеки імені Героїв Чорнобиля, Черкаси

ЗАСТОСУВАННЯ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Розроблено метод реалізації операцій розширеного матричного криптографічного перетворення інформації. Побудовано структурну схему реалізації операцій розширеного матричного криптографічного перетворення та синтезовано функціональну схему модуля, що реалізує дані операції. Проведено розрахунок кількості операцій. За допомогою пакету статистичних тестів NIST STS здійснено оцінку ефективності використання операцій розширеного матричного перетворення для криптографічного захисту інформації.

Ключові слова: *захист інформації, трирозрядні елементарні функції, синтез операцій, операції розширеного матричного представлення.*

Вступ

Постановка проблеми. За останні декілька десятиліть відбулися якісні зміни в процесах управління на всіх ієрархічних рівнях за рахунок інтенсивного впровадження сучасних інформаційних технологій. Їх швидкий розвиток призвів до зростання цінності інформації як для суспільства взагалі, так і для кожної окремої людини зокрема. Водночас стала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій. Саме тому в Україні все більше уваги приділяється проблемам захисту інформації та інформаційній безпеці.

Проблема захисту інформації актуальна для всіх відомств, організацій та підприємств, в тому числі й для Державної служби України з надзвичайних ситуацій, де конфіденційність інформації має величезне значення як для безпеки людей, так і для забезпечення національної безпеки в цілому. Сучасні темпи розвитку інформаційних технологій вимагають від структурних підрозділів ДСНС України високого рівня захисту конфіденційної інформації. Тому важливим завданням на сьогодні є постійне підвищення якості систем захисту інформації, якого можна досягти за допомогою розвитку одного з основних напрямків захисту інформації – криптографічного захисту.

Одним з шляхів вдосконалення існуючих криптографічних систем захисту інформації та розробки нових криптографічних алгоритмів є розширення спектру операцій, на основі яких вони будуються.

Перспективним напрямком розвитку криптографічних систем захисту інформації є використання розширеного матричного представлення операцій криптографічного перетворення для інформаційних систем ДСНС України.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити: [1, 2], де представлено результати проведеного обчислювального експерименту по знаходженню елементарних функцій для криптографічного перетворення інформації, та [3], де на основі отриманих вибіркових експериментальних даних і запропонованого альтернативного способу запису основних елементарних функцій проведено аналіз базових спеціалізованих трирозрядних логічних функцій, який дозволив виявити основну закономірність процесу побудови моделей трирозрядних операцій криптографічного перетворення інформації.

Але в даних дослідженнях не було розглянуто питання щодо реалізації операцій розширеного матричного криптографічного перетворення.

Мета статті полягає у розробці методу синтезу систем захисту інформації на основі використання операцій розширеного матричного представлення та проведенні оцінки його ефективності.

Виклад основного матеріалу

Для практичного використання операцій розширеного матричного криптографічного перетворення необхідно розробити структурну схему реалізації операцій розширеного матричного криптографічного перетворення та дослідити їх криптостійкість.

На рис. 1 представлено розроблену структурну схему реалізації операцій розширеного матричного криптографічного перетворення, де КД1, КД2 – комутатори даних, які забезпечують перестановку біт або блоків даних в залежності від згенерованої операції; МРМП – модулі розширеного матричного перетворення, які забезпечують виконання операцій розширеного матричного перетворення; $К_{m1}$, $К_{m2}$, $К_{k1}$, $К_{k2}$ – групи команд на відповідний модуль / комутатор; x_{1-8} – вхідні дані; y_{1-8} – вихідні дані.

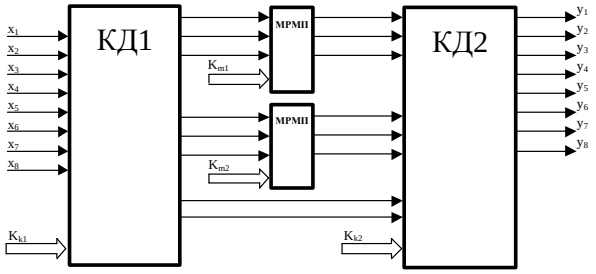

Рис. 1. Структурна схема реалізації операцій розширеного матричного криптографічного перетворення

На рис. 2 представлена функціональна схема модуля розширеного матричного криптографічного перетворення представлена.

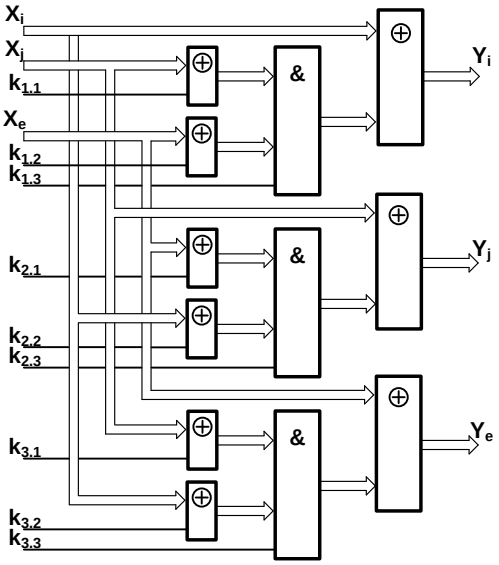

Рис. 2. Функціональна схема модуля розширеного матричного криптографічного перетворення

Операція криптографічного перетворення відповідно до функціональної схеми реалізації буде виконуватися за час переключення п'яти логічних елементів. Виходячи з запропонованої реалізації операцій розширеного матричного представлення, кількість операцій, які можуть бути використані для шифрування інформації (S_t) буде визначатися:

$$S_t = \left(2016^{K_{mo}}\right)^{K_c},$$

де K_{mo} – кількість матричних операцій криптографічного перетворення, K_c – кількість циклів криптографічного перетворення, яка визначається як $_c$ = m/n, де m – довжина вхідної інформації, n – довжина блоку даних, який обробляється за один цикл.

Розрахунок кількості операцій для шифрування інформації в залежності від кількості операцій в циклі та кількості циклів перетворення приведено в табл. 1. Результати програмної реалізації алгоритму перетворення даних на основі операцій розширеного матричного представлення було оцінено за допомогою статистичних тестів NIST STS.

Результати перетворення псевдовипадкової послідовності генератора RANDOM, невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти, та перетворення текстового файлу представлені в табл. 2.

Реалізація операцій розширеного матричного криптографічного перетворення відповідає вимогам програмного пакету статистичного тестування NIST STS. Практичне використання операцій розширеного матричного криптографічного перетворення, виходячи з проведених досліджень, проводиться на основі гамуючої послідовності.

Застосуємо метод підвищення швидкості шифрування, сутність якого полягає в використанні гамуючої послідовності як послідовного набору команд виконання випадково вибраної підмножини операцій криптоперетворення. Необхідно відмітити що криптостійкість (z) використання даного методу визначається як $z = z_г \cdot z_o$, де $z_г$ – криптостійкість гамуючої послідовності, z_o – криптостійкість послідовностей операцій криптоперетворення.

Криптостійкість і швидкість шифрування визначаються параметрами: n_k – розрядність команди виконання послідовностей операцій криптоперетворення, $K_{оп}$ – кількість операцій в послідовності, яка реалізує команду.

Підмножина випадково вибраних операцій для реалізації методу визначається як $П_o = 2^{n_k} \cdot K_{on}$. Практична криптостійкість залежить від розрядності пароля $R_П = (2^{n_k} \cdot K_{on}) \log_2 2016$ і буде пропорціональною величині $z_o = 2^{R_П}$.

Наприклад, якщо $n_k = 4$, а $K_{оп} = 4$, тоді $П_o = 64$, $R_П = 64 \cdot \log_2 2016 = 704$ і $z_o = 2^{704}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в 2^{704} раз пропорційно.

Так як операції криптоперетворення можуть виконуватися паралельно, то час криптоперетворення буде визначатися лише часом формування n_k розрядів гамуючої послідовності. Тоді збільшення швидкості криптографічного перетворення інформації буде визначатися відношенням розрядності інформації, яка шифрується на основі операцій розширеного матричного перетворення під управлінням гамуючої послідовності до кількості розрядів, над якими виконано гамування. Для нашого прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як:

$$k_v = \frac{3 \cdot K_{оп}}{n_k} = 3.$$

Вибір параметрів n_k і $K_{оп}$ дозволяє забезпечити необхідні значення швидкості шифрування та криптостійкості за рахунок збільшення апаратної та програмної складності системи криптографічного захисту інформації.

Таблиця 1

Розрахунок кількості операцій для шифрування інформації

K_{mo} \ K_c		Кількість циклів			
		1	2	3	4
Кількість операцій в циклі	1	2016	4064256	8193540096	2016^4
	2	4064256	4064256^2	4064256^3	4064256^4
	3	8193540096	8193540096^2	8193540096^3	8193540096^4

Таблиця 2

Оцінка програмної реалізації операцій розширеного матричного представлення

Об’єкти тестування	Кількість тестів, у яких тестування пройшли більш 99 % послідовностей	Кількість тестів, у яких тестування пройшли більш 96 % послідовностей
Генератор RANDOM-РМП	127 (68 %)	189 (100 %)
Криптографічне перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти на основі операцій РМП	132 (70 %)	189 (100 %)
Криптографічне перетворення текстового файлу на основі операцій РМП	127 (68 %)	189 (100 %)

Висновки

Отримали подальший розвиток методи синтезу систем захисту інформації на основі використання операцій розширеного матричного представлення, що забезпечило підвищення криптостійкості та швидкості реалізації алгоритмів за рахунок збільшення апаратної та програмної складності.

Розширене матричне представлення в залежності від параметрів n_k і K_{on} дозволяє збільшити криптостійкість від 10^{32} до 10^{150} раз пропорційно, при зменшенні часу шифрування в 1,5 – 6 раз за рахунок збільшення апаратної та програмної складності системи криптографічного захисту інформації.

Список літератури

1. Бабенко В.Г. Визначення множини трирозрядних елементарних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький, Р.П. Мельник // Теоретичний і науково-практичний журнал інженерної академії України «Вісник інженерної академії України» – К.: Інтерсервіс, 2012. – Вип. 3 (4). – С. 77 – 79.

2. Рудницкий В.Н. Повышение быстродействия систем защиты информации / В.Н. Рудницкий, Р.П. Мельник, О.Г. Мельник // Чрезвычайные ситуации: теория, практика, инновации «ЧС – 2012» : сб. материалов международной НПК. – Гомель : ГГТУ им. П.О. Сухого, 2012. – С. 224.

3. Рудницкий С.В. Криптографическое преобразование информации на основе трехразрядных логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4. – С. 119 – 122.

Надійшла до редколегії 30.10.2012

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ПРИМЕНЕНИЕ ОПЕРАЦИЙ РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Р.П. Мельник

В статье разработан метод реализации операций расширенного матричного криптографического преобразования информации. Построена структурная схема реализации операций расширенного матричного криптографического преобразования и синтезировано функциональную схему модуля, реализующего данные операции. Проведен расчет количества операций. С помощью пакета статистических тестов NIST STS осуществлена оценка эффективности использования операций расширенного матричного преобразования для криптографической защиты информации.

Ключевые слова: *защита информации, трехразрядные элементарные функции, синтез операций, операции расширенного матричного представления.*

APPLICATION OF OPERATIONS EXTENDED MATRIX CRYPTOGRAPHIC TRANSFORMATIONS FOR INFORMATION SECURITY

R.P. Melnyk

In the paper developed a method for the implementation of the extended matrix operations cryptographic transformation of data. The structural scheme of the operations of the extended matrix of cryptographic transformation and synthesized a functional diagram of the module that implements these operations. The calculation of the number of operations. With this package of statistical tests performed NIST STS evaluation of operations over an extended matrix transformation for cryptographic protection of information.

Keywords: *information security, the three-digit elementary functions, synthesis operations, operations expanded matrix representation.*