Теоретичні основи розробки систем озброєння

УДК 004.056.55:004.312.2

В.Г. Бабенко[1], О.Г. Мельник[2], Р.П. Мельник[2]

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси*

МУЛЬТИОПЕРАЦІЙНЕ БАГАТОРАЗОВЕ КОВЗНЕ ШИФРУВАННЯ

У даній статті синтезовано моделі багаторазового застосування восьмиелементного прямого правостороннього примітиву ковзного шифрування. На основі рекурентних залежностей даних моделей отримано узагальнений вираз рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінною раундовою операцією, а також узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінними операціями в раунді. У роботі запропоновано спосіб синтезу моделей мультиопераційних примітивів багаторазового ковзного шифрування на основі рекурентних послідовностей, застосування якого дозволить підвищити практичну та теоретичну криптостійкість примітивів ковзного шифрування.

Ключові слова: *рекурентна послідовність, примітив прямого правостороннього ковзного шифрування, багаторазове ковзне шифрування, синтез, матричні моделі, раунд, узагальнена модель, мультиопераційність.*

Вступ

Постановка проблеми. Сьогодні в світі актуальним питанням є проблема захисту інформації та інформаційного простору. Це питання постійно розглядається на найвищому рівні держав та підлягає постійному оновленню, як на законодавчому, так і програмно-апаратному рівні, адже від цього залежить безпека держави, її військові, економічні, соціальні та приватні ресурси.

На технічному рівні одним із варіантів вирішення проблеми захисту інформації є створення швидкодіючих програмно-апаратних засобів захисту інформації на основі різноманітних криптографічних алгоритмів.

Розробка та реалізація швидкодіючих програмно-апаратних засобів захисту інформації на основі криптоалгоритмів безпосередньо пов'язана зі швидкістю виконання арифметичних і логічних операцій, що лежать в основі алгоритмів.

Криптостійкість алгоритму шифрування, що використовується, безпосередньо визначає ступінь захисту даних, і, в свою чергу, залежить від набору й послідовності виконання операцій або перетворень, на основі яких даний алгоритм реалізований. Водночас збільшення обсягів інформації, яка обробляється, актуалізує завдання підвищення швидкодії криптоалгоритмів. Тому паралельна реалізація криптографічних перетворень за допомогою використання в алгоритмах саме матричних операцій багаторазового перетворення інформації на основі примітивів ковзного шифрування є одним із можливих варіантів вирішення даної задачі.

Аналіз останніх досліджень і публікацій. У статтях [1, 2] пропонується спосіб паралельної реалізації примітиву ковзного шифрування на основі використання матричних операцій криптографічного перетворення, а також оптимізація даних матричних операцій шляхом паралельного застосування елементів раундового ключа. Показано, що використання оптимізованих матричних операцій криптографічного перетворення для реалізації примітивів ковзного шифрування дає можливість підвищити швидкість виконання криптографічного перетворення. Способи та рекомендації щодо застосування матричних операцій криптографічного перетворення на основі суми за модулем для шифрування інформації запропоновані в [3]. Але в даних дослідженнях не розглядалось питання синтезу мультиопераційних примітивів ковзного шифрування для проведення багаторазових перетворень на їх основі. Тому побудова рекурентних моделей багаторазового криптопримітиву ковзного шифрування зі змінними операціями в раунді є актуальним.

Мета роботи полягає в синтезі моделей мультиопераційного багаторазового ковзного шифрування на основі рекурентних послідовностей.

Виклад основного матеріалу

Восьмиелементний примітив прямого правостороннього ковзного шифрування перетворює послідовність x_i у y_i, $i = 1..8$.

Реалізація примітиву восьмиелементного прямого правостороннього ковзного шифрування, описується як

$$y_1 = x_1 \oplus m_1;\ \ y_2 = x_2 \oplus y_1;$$
$$y_3 = x_3 \oplus y_2;\ \ y_4 = x_4 \oplus y_3;$$
$$y_5 = x_5 \oplus y_4;\ \ y_6 = x_6 \oplus y_5;$$
$$y_7 = x_7 \oplus y_6;\ \ y_8 = x_8 \oplus y_7.$$

Рекурентна послідовність, яка описує операцію восьмиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \qquad (1)$$

де $y_0^1 = m_1$ та $i \in \{1, \dots, 8\}$.

Повторне восьмиелементне ковзне шифрування перетворює послідовність y_i у z_i за умови: m_2 – вхідний раундовий ключ, $m_2 = y_8$. Підставивши відповідні вирази, отримаємо:

$$z_1 = x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8;$$
$$z_2 = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus m_1;$$
$$z_3 = x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8;$$
$$z_4 = x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus m_1;$$
$$z_5 = x_2 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8;$$
$$z_6 = x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus x_8 \oplus m_1;$$
$$z_7 = x_2 \oplus x_4 \oplus x_6 \oplus x_8;$$
$$z_8 = x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus m_1.$$

Рекурентна послідовність, яка описує операцію дворазового восьмиелементного прямого правостороннього ковзного шифрування, має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \qquad (2)$$

де $y_0^2 = y_8^1$ та $i \in \{1, \dots, 8\}$.

Триразове восьмиелементне ковзне шифрування перетворює послідовність z_i у l_i за умови, що $m_3 = z_8$ – вхідний раундовий ключ даного етапу шифрування, та описується моделлю:

$$l_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus m_1;$$
$$l_2 = x_2 \oplus x_3 \oplus x_5 \oplus x_7;$$
$$l_3 = x_3 \oplus x_4 \oplus x_6 \oplus x_8;$$
$$l_4 = x_1 \oplus x_4 \oplus x_5 \oplus x_7 \oplus m_1;$$
$$l_5 = x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_8 \oplus m_1;$$
$$l_6 = x_2 \oplus x_3 \oplus x_6 \oplus x_7;$$
$$l_7 = x_3 \oplus x_4 \oplus x_7 \oplus x_8;$$
$$l_8 = x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus m_1.$$

Рекурентна послідовність, яка описує операцію триразового восьмиелементного прямого правостороннього ковзного шифрування, має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \qquad (3)$$

де $y_0^3 = y_8^2$ та $i \in \{1, \dots, 8\}$.

Чотириразове восьмиелементне ковзне шифрування перетворює послідовність l_i у j_i, де $m_4 = l_8$ – вхідний раундовий ключ даного етапу шифрування. Підставивши відповідні вирази, отримаємо:

$$j_1 = x_2 \oplus x_5 \oplus x_6;$$
$$j_2 = x_3 \oplus x_6 \oplus x_7;$$
$$j_3 = x_4 \oplus x_7 \oplus x_8;$$
$$j_4 = x_1 \oplus x_5 \oplus x_8 \oplus m_1;$$
$$j_5 = x_2 \oplus x_6;$$
$$j_6 = x_3 \oplus x_7;$$
$$j_7 = x_4 \oplus x_8;$$
$$j_8 = x_1 \oplus x_5 \oplus x_7 \oplus m_1.$$

Рекурентна послідовність, яка описує операцію чотириразового восьмиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \qquad (4)$$

де $y_0^4 = y_8^3$ та $i \in \{1, \dots, 8\}$.

На основі виразів (1) – (4) отримано узагальнений вираз рекурентної послідовності для опису виконання багаторазового прямого правостороннього ковзного шифрування:

$$y_i^k = y_{i-1}^k \oplus y_i^{k-1}, \qquad (5)$$

де $y_0^k = y_d^{k-1}$ та $i \in \{1, \dots, d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування (або кількість разів застосування примітиву ковзного шифрування), а d – розрядність перетворення.

Дані рекурентні послідовності дійсні для багаторазового прямого правостороннього ковзного шифрування, синтезованого на основі додавання за модулем 2. А при синтезі прямого правостороннього примітиву ковзного шифрування можуть бути використані й інші операції, наприклад, додавання за модулем 2^n. Тоді узагальнену модель багаторазового прямого правостороннього примітиву ковзного шифрування на основі рекурентної послідовності можливо записати як:

$$y_i^k = y_{i-1}^k (\nabla) y_i^{k-1}, \qquad (6)$$

де $y_0^k = y_d^{k-1}$, $i \in \{1, \dots, d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування; d – розрядність перетворення, а (∇) – двохоперандна криптографічна операція.

Крім того, операція, яка використовується для реалізації багаторазового криптопримітиву ковзного шифрування може змінюватися на будь-якому раунді зашифрування. Виходячи з цього, узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінною раундовою операцією запишемо, як:

$$y_i^k = y_{i-1}^k (\nabla_k) y_i^{k-1}, \qquad (7)$$

де $y_0^k = y_d^{k-1}$, $i \in \{1, \dots, d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування; d – розрядність перетворення; (∇_k) – двохоперандна криптографічна операція для k-го раунду.

Аналізуючи структуру синтезованих матричних моделей примітивів багаторазового ковзного шифрування, дійшли висновку, що існує ще один альтернативний варіант забезпечення мультиопераційності примітива. Даний варіант полягає в тому, що операція, яка використовується для реалізації багаторазового криптопримітива ковзного шифрування, може змінюватися деяку визначену кількість разів в середині самого раунду зашифрування. Позначимо операції, що змінюються в раунді як ∇_{k_i}. Тоді максимальна кількість змінних операцій в раунді визначається кількістю елементів примітиву ковзного шифрування:

$$\text{count}_{\max}(\nabla_{k_i}) = d, \text{ так як } i \in \{1, \dots, d\}.$$

Тому узагальнена модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінними операціями в раунді матиме вигляд:

$$y_i^k = y_{i-1}^k(\nabla_{k_i}) y_i^{k-1}, \qquad (8)$$

де $y_0^{k_i} = y_d^{k_i-1}$, $i \in \{1, \dots, d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування; d – розрядність перетворення; ∇_{k_i} – двохоперандна криптографічна операція для перетворення i-го елемента для k-го раунду.

Двохоперандні криптографічні операції, які можуть бути використані при реалізації багаторазового застосування примітивів ковзного шифрування згідно запропонованих рекурентних моделей (6) – (8) потребують більш детального аналізу та дослідження, на що й будуть спрямовані подальші наукові дослідження.

Висновки

У даній статті одержано узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінною раундовою операцією та змінними операціями в раунді. Забезпечення можливості випадкової зміни раундових операцій та операцій безпосередньо в самому раунді дозволить підвищити практичну та теоретичну криптостійкість примітивів ковзного шифрування.

У статті запропоновано спосіб забезпечення мультиопераційності при синтезі моделей примітивів багаторазового ковзного шифрування на основі рекурентних послідовностей.

Список літератури

1. Бабенко В.Г. Параллельная реализация скользящего шифрования / В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – 2013. – Вип. 9 (116) – С. 131-134.

2. Бабенко В.Г. Оптимизация матричных операций скользящего шифрования / В.Г. Бабенко // Системи озброєння і військова техніка: наук. журнал. – 2013. – № 4 (36).– С. 132-135.

3. 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.

Надійшла до редколегії 17.07.2015

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МУЛЬТИОПЕРАЦИОННОЕ МНОГОКРАТНОЕ СКОЛЬЗЯЩЕЕ ШИФРОВАНИЕ

В.Г. Бабенко, О.Г. Мельник, Р.П. Мельник

В данной статье синтезированы модели многократного применения восьмиэлементного прямого правостороннего примитива скользящего шифрования. На основе рекуррентных зависимостей данных моделей получено обобщенное выражение рекуррентной последовательности многократного криптопримитива скользящего шифрования с переменной раундовой операцией, а также обобщенную модель рекуррентной последовательности многократного криптопримитива скользящего шифрования с переменными операциями в раунде. В работе предложен способ синтеза моделей мультиоперационных примитивов многократного скользящего шифрования на основе рекуррентных последовательностей, применение которого позволит повысить практическую и теоретическую криптостойкость примитивов скользящего шифрования.

Ключевые слова: *рекуррентная последовательность, примитив прямого правостороннего скользящего шифрования, многократное скользящее шифрование, синтез, матричные модели, раунд, обобщенная модель, мультиоперационность.*

MULTIPLE MULTIOPERATIONAL SLIDING ENCRYPTION

V.G. Babenko, O.G. Melnyk, R.P. Melnyk

In this article were synthesized models of eight element direct right-primitives sliding encryption of multiple application. On the basis of these models recurrent dependencies obtained by a generalized expression of a recurrent sequence of multiple cryptoprimitive sliding encryption with variable rounder operation, as well as a generalized model of recursive sequence of multiple cryptoprimitive sliding encryption with variable operations in the round. This paper proposes a method of synthesizing models multioperation primitives multiple sliding encryption based on recurring sequences, the application of which will improve the practical and theoretical cryptographic resistance primitives sliding encryption.

Keywords: *recurrent sequence, direct right-primitive sliding encryption, multiple sliding encryption, synthesis, matrix models, round, generalized model, multioperation.*