

УДК 003.26:004.056.55

В.Г. Бабенко

Одесская национальная академия связи им. А.С. Попова, Одесса

ОПТИМИЗАЦИЯ МАТРИЧНЫХ ОПЕРАЦИЙ СКОЛЬЗЯЩЕГО ШИФРОВАНИЯ

В статье проведено исследование примитивов скользящего шифрования и внесено предложение по оптимизации матричных операций криптографического преобразования, которые их реализуют. Показано, что элементы раундового ключа, сформированные одним и тем же алгоритмом, при многократном скользящем шифровании не приводят к повышению криптостойкости. Предложенная оптимизация позволяет уменьшить аппаратную сложность реализации примитивов скользящего шифрования, построенных на основе матричных операций, за счет сокращения количества операций сложения по модулю 2.

Ключевые слова: матричные операции, криптографическое преобразование, оптимизация, скользящее шифрование.

Введение

Постановка проблемы. Самым эффективным средством сокрытия данных для информационных систем считается шифрование. Его реализация базируется на использовании криптоалгоритмов, которые возможно выполнить как программно так и аппаратно. Степень защиты данных определяется непосредственно криптостойкостью используемого алгоритма шифрования, которая в свою очередь зависит от набора и последовательности выполнения операций или преобразований, на основе которых он реализован.

В связи с увеличением объемов обрабатываемой информации актуальной задачей становится повышение быстродействия криптоалгоритмов. Одним из вариантов решений данной задачи можно назвать параллельную реализацию криптографических преобразований с помощью использования в алгоритмах матричных операций.

Анализ последних исследований и публикаций. Операции криптографического преобразования, такие как сложение по модулю и перестановки, могут быть представлены как матричные операции криптографического преобразования [1, 2].

Одной из достоинств операций матричного криптографического преобразования есть возможность их параллельной реализации [3].

Реализация примитивов скользящего шифрования на основе матричных операций имеет ряд особенностей, которые не исследовались [4].

Цель статьи – на основе исследования примитивов скользящего шифрования оптимизировать реализующие их матричные операции криптографического преобразования.

Основной материал

Структурные схемы процесса реализации примитива прямого левостороннего скользящего шифрования (прямого левостороннего ЛСК рис. 1) и примитива прямого правостороннего скользящего

шифрования (прямого правостороннего ЛСК рис. 2) имеют вид соответственно, где x_i , y_i – i -ые элементы входных и выходных данных соответственно, а m_1 – элемент раундового ключа [4].

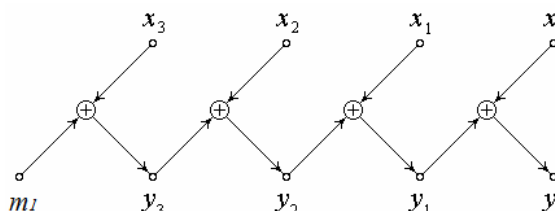


Рис. 1. Структурная схема алгоритма реализации примитива прямого левостороннего ЛСК

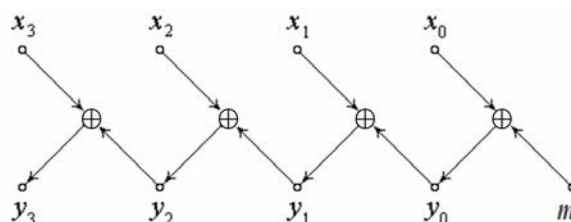


Рис. 2. Структурная схема алгоритма реализации примитива прямого правостороннего ЛСК

Схеме преобразования, приведенной на рис. 1, отвечает система линейных модульных уравнений:

$$\begin{aligned} y_3 &= x_3 \oplus m_1; \\ y_2 &= x_2 \oplus y_3; \\ y_1 &= x_1 \oplus y_2; \\ y_0 &= x_0 \oplus y_1. \end{aligned} \quad (1)$$

Причем в данном случае операции в (1) выполняются поразрядно над каждой парой смежных операндов.

Аналогичным образом могут быть построены и системы линейных модульных алгебраических уравнений для прямого правостороннего ЛСК.

Для дальнейшего исследования ограничимся левосторонним ЛСК, так как правостороннее выполняется аналогично.

Скользящее шифрование преобразовывает последовательность x_k в y_k , где n - количество элементов информации, а $x_1^* = x_1 \oplus m_1$:

$$\begin{aligned} y_1 &= x_1^*; \\ y_2 &= x_1^* \oplus x_2; \\ y_3 &= x_1^* \oplus x_2 \oplus x_3; \\ y_4 &= x_1^* \oplus x_2 \oplus x_3 \oplus x_4; \\ y_5 &= x_1^* \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5; \\ &\dots \\ y_n &= x_1^* \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n \end{aligned} \quad (2)$$

или

$$\begin{aligned} y_1 &= x_1 \oplus m_1; \\ y_2 &= x_1 \oplus x_2 \oplus m_1; \\ y_3 &= x_1 \oplus x_2 \oplus x_3 \oplus m_1; \\ y_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1; \\ y_5 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1; \\ &\dots \\ y_n &= x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n \oplus m_1. \end{aligned}$$

Функция преобразования одного элемента скользящего шифрования может быть описана рекуррентной последовательностью

$$y_n = y_{n-1} \oplus x_n.$$

Примитив скользящего шифрования построен на основе полученной рекуррентной последовательности и может быть представлен в виде матричной модели

$$F(x) = \begin{bmatrix} x_1 \oplus m_1 \\ x_1 \oplus x_2 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1 \\ \dots \\ x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n \oplus m_1 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ \dots \\ x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} m_1 \\ m_1 \\ m_1 \\ m_1 \\ m_1 \\ \dots \\ m_1 \end{bmatrix}.$$

Результат шифрования состоит из поразрядного сложения по модулю 2 результатов выполнения блока обработки информации и блока обработки раундового ключа, причем блок обработки ключа может быть описан такой рекуррентной последовательностью

$$m_n = m_{n-1}.$$

Рассмотрим повторное скользящее шифрование, которое преобразует последовательность y_k в z_k .

$$\begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_1 \oplus y_2 \oplus m_2; \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus m_2; \\ z_4 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus m_2; \\ z_5 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus m_2; \\ &\dots \\ z_n &= y_1 \oplus y_2 \oplus y_3 \oplus \dots \oplus y_n \oplus m_2; \end{aligned} \quad (3)$$

Подставим в выражение (3) выражение (2) получим:

$$\begin{aligned} z_1 &= x_1 \oplus m_1 \oplus m_2; \\ z_2 &= x_2 \oplus m_2; \\ z_3 &= x_1 \oplus x_3 \oplus m_1 \oplus m_2; \\ z_4 &= x_2 \oplus x_4 \oplus m_2; \\ z_5 &= x_1 \oplus x_3 \oplus x_5 \oplus m_1 \oplus m_2; \\ z_6 &= x_2 \oplus x_4 \oplus x_6 \oplus m_2; \\ &\dots \\ z_{2k-1} &= x_1 \oplus x_3 \oplus x_5 \oplus \dots \oplus x_{2k-1} \oplus m_1 \oplus m_2; \\ z_{2k} &= x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \dots \oplus x_{2k} \oplus m_2. \end{aligned}$$

Функция преобразования одного элемента повторного скользящего шифрования может быть описана рекуррентной моделью

$$z_n = z_{n-2} \oplus x_n.$$

Примитив скользящего шифрования построенный на основе рекуррентной модели и может быть представлен в виде матричной модели

$$F(x) = \begin{bmatrix} x_1 \oplus m_1 \oplus m_2 \\ x_2 \oplus m_2 \\ x_1 \oplus x_3 \oplus m_1 \oplus m_2 \\ x_2 \oplus x_4 \oplus m_2 \\ x_1 \oplus x_3 \oplus x_5 \oplus m_1 \oplus m_2 \\ x_2 \oplus x_4 \oplus x_6 \oplus m_2 \\ \dots \\ x_1 \oplus x_3 \oplus x_5 \oplus \dots \oplus x_{2k-1} \oplus m_1 \oplus m_2 \\ x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \dots \oplus x_{2k} \oplus m_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \\ x_2 \oplus x_4 \\ x_1 \oplus x_3 \oplus x_5 \\ x_2 \oplus x_4 \oplus x_6 \\ \dots \\ x_1 \oplus x_3 \oplus x_5 \oplus \dots \oplus x_{2k-1} \\ x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \dots \oplus x_{2k} \end{bmatrix} \oplus \begin{bmatrix} m_1 \oplus m_2; \\ m_2 \\ m_1 \oplus m_2; \\ m_2; \\ m_1 \oplus m_2; \\ m_2; \\ \dots \\ m_1 \oplus m_2; \\ \oplus m_2; \end{bmatrix}.$$

Блок обработки раундового ключа может быть описан рекуррентной последовательностью

$$m_n = m_{n-2}.$$

Функция преобразования элемента трехкратного скользящего шифрования может быть описана рекуррентной моделью

$$l_n = l_{n-4} \oplus x_{n-1} \oplus x_n.$$

Примитив трехкратного скользящего шифрования построенный на ее основе будет иметь вид

$$F(x) = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ lx_3 \oplus x_4 \\ x_1 \oplus x_4 \oplus x_5 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \\ x_3 \oplus x_4 \oplus x_7 \oplus x_8 \\ x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_9 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_9 \oplus x_{10} \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11} \\ \dots \end{bmatrix} \oplus$$

$$\oplus \begin{bmatrix} m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3; \\ 0; \\ m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3 \\ 0 \\ m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3 \\ \dots \end{bmatrix}.$$

Рекуррентная последовательность, которая описывает блок обработки раундового ключа трехкратного скользящего шифрования представляется как

$$m_n = m_{n-4}.$$

Аналогично получили рекуррентные модели функции преобразования четырехкратного скользящего шифрования и блока обработки раундового ключа соответственно

$$j_n = j_{n-4} \oplus x_n;$$

$$m_n = m_{n-4}.$$

Пятикратное скользящее шифрование преобразует последовательность j_k в p_k .

Рекуррентные последовательности функции преобразования пятикратного скользящего шифро-

вания и блока обработки раундового ключа могут быть описаны в таком виде

$$p_n = p_{n-8} \oplus x_{n-3} \oplus x_{n-2} \oplus x_{n-1} \oplus x_n,$$

$$m_n = m_{n-8}.$$

Шестикратное скользящее шифрование преобразует последовательность p_k в q_k .

Функция преобразования шестикратного скользящего шифрования может быть описана рекуррентной моделью

$$q_n = q_{n-8} \oplus x_{n-2} \oplus x_n.$$

Примитив шестикратного скользящего шифрования представлен матричной моделью

$$F(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \\ x_2 \oplus x_4 \\ x_3 \oplus x_5 \\ x_4 \oplus x_6 \\ x_5 \oplus x_7 \\ x_6 \oplus x_8 \\ x_1 \oplus x_7 \oplus x_9 \\ x_2 \oplus x_8 \oplus x_{10} \\ x_1 \oplus x_3 \oplus x_9 \oplus x_{11} \\ x_2 \oplus x_4 \oplus x_{10} \oplus x_{12} \\ x_3 \oplus x_5 \oplus x_{11} \oplus x_{13} \\ x_4 \oplus x_6 \oplus x_{12} \oplus x_{14} \\ \dots \end{bmatrix} \oplus$$

$$\oplus \begin{bmatrix} m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ m_6 \\ 0 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ \dots \end{bmatrix} \quad (4)$$

Рекуррентная последовательность, которая описывает блок обработки раундового ключа имеет вид

$$m_n = m_{n-8}.$$

Рассмотрим вариант оптимизации примитива скользящего шифрования, реализованный матрич-

ной операцією. Так як $m_1 \oplus m_2 \oplus \dots \oplus m_n = m_k$ і случайные елементи раундового ключа формуються на основі одного і того ж алгоритма, відповідно, улічуючи теорему Шеннона [5], можна утвердити, що повторне застосування елементів раундового ключа не підвищує криптостійкість.

Виходячи з цього, з'явилась можливість оптимізувати операцію криптографічного перетворення блоку обробки раундового ключа без зменшення криптостійкості наступної системою:

$$F(x) = \begin{bmatrix} x_1 \\ x_1 \oplus x_{21} \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ \dots \\ x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ \dots \\ m_L \end{bmatrix},$$

де L - кількість раундів.

Таким чином оптимізована операція дозволяє збільшити швидкість обробки раундового ключа для моделі (4) до 5 раз, а швидкість виконання операцій криптографічного перетворення – до 2 раз відносно реалізації матричної операції, яка реалізує примітив скользящего шифрування.

Висновки

Отримані матричні операції, які реалізують примітиви скользящего шифрування, можуть бути оптимізовані без втрати криптостійкості шляхом паралельного використання елементів раундового ключа.

Дана оптимізація дозволяє зменшити апаратну складність реалізації примітива скользящего шифрування.

з'являється за рахунок скорочення кількості операцій додавання по $\text{mod } 2$.

Як видно з наведених прикладів, підвищення швидкості виконання примітивів скользящего шифрування на основі матричних операцій криптографічного перетворення може бути збільшено приблизно до 2 раз.

Список літератури

1. 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. – Вип. 4 (33). – Х.: ХУПС ім. І. Кожедуба, 2012. – С. 198–200.
2. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Захист інформації: наук.-практ. журнал. – № 3 (56). – К.: НАУ, 2012. – С. 50–56.
3. Бабенко В.Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, В.М. Рудницький // Системи обробки інформації: зб. наук. праць. – № 9 (107). – Х.: ХУПС ім. І. Кожедуба, 2012. – С. 130–139.
4. Белецький А.Я. Криптографічні примітиви, засновані на методі скользящего кодування / А.Я. Белецький, А.А. Белецький // Вісник СумДУ, 2006. – № 10. – С. 33–42.
5. Шеннон К. Роботи по теорії інформації та кібернетикі / К. Шеннон. – М.: Изд-во іноземної літератури, 1963. – 830 с.

Поступила в редакцію 23.10.2013

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

ОПТИМІЗАЦІЯ МАТРИЧНИХ ОПЕРАЦІЙ КОВЗНОГО ШИФРУВАННЯ

В.Г. Бабенко

В статті проведено дослідження примітивів ковзного шифрування та внесено пропозицію щодо оптимізації матричних операцій криптографічного перетворення, які їх реалізують. Показано, що елементи раундового ключа, сформовані одним і тим же алгоритмом, при багатократному ковзному шифруванні не призводять до підвищення криптостійкості. Запропонована оптимізація дозволяє зменшити апаратну складність реалізації примітивів ковзного шифрування, побудованих на основі матричних операцій, за рахунок скорочення кількості операцій додавання за модулем 2.

Ключові слова: матричні операції, криптографічне перетворення, оптимізація, ковзне шифрування.

OPTIMIZATION OF MATRIX OPERATIONS SLIDING ENCRYPTION

V.G. Babenko

The paper investigated the sliding encryption primitives and suggested optimization of matrix operations of cryptographic transformations that implement them. It is shown that the elements of round keys are formed by one and the same algorithm for multiple encryption sliding do not lead to an increase in the reliability. The proposed optimization can reduce the hardware complexity of implementing a sliding encryption primitives that are based on matrix operations, by reducing the number of operations of addition modulo 2.

Keywords: matrix operations, cryptographic transformation, optimization, a sliding encryption.