УДК 004.056.55:004.312.2

В.Г. Бабенко

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

ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ СКОЛЬЗЯЩЕГО ШИФРОВАНИЯ

В работе предлагается использование матричных операций криптографического преобразования для распараллеливания процесса реализации примитива скользящего шифрования. Доказано, что функции преобразования элементов скользящего шифрования являются рекуррентными последовательностями и могут быть применены для синтеза матричных операций криптографического преобразования. Показано, что использование матричных операций для многократного упрощенного скользящего шифрования позволяет сократить количество элементарных операций, реализующих криптографическое преобразование данных.

Ключевые слова: *параллельная реализация, логическое скользящее шифрование, примитив, матричная операция криптографического преобразования.*

Введение

Постановка проблемы. В современных условиях развития информационных технологий большая значимость и недостаточная как теоретическая так и практическая решенность задачи повышения быстродействия криптографического преобразования данных в системах обработки и передачи информации определяет несомненную важность проведения исследований, которые могут быть основой для создания скоростных криптографических методов.

Таким образом, разработка и реализация быстродействующих программно-аппаратных средств защиты информации на основе криптографических алгоритмов напрямую связана со скоростью выполнения арифметических и логических операций, лежащих в основе алгоритмов. Одним из перспективных направлений решения задачи увеличения скорости реализации таких операций является параллельное выполнение криптографических преобразований над большим количеством информации.

Анализ последних исследований и публикаций. Последнее время много публикаций посвящено матричным операциям криптографического преобразования, которые позволяют выполнять шифрование данных параллельно [1 – 4].

В алгоритмах „Симметричный блочный алгоритм криптографического преобразования информации с динамически-управляемыми параметрами шифрования” и „Блочный симметричный алгоритм криптографического преобразования информации с динамично управляемым процессом стохастической замены криптографических примитивов”, представленных на открытый конкурс симметричных блоч-

ных криптографических алгоритмов [5], впервые были использованы примитивы скользящего шифрования [6, 7]. Основным недостатком данных примитивов является их последовательная реализация.

Исходя из этого, **цель статьи** заключается в разработке моделей параллельной реализации примитивов скользящего шифрования.

Основной материал

Процесс реализации примитива логического скользящего шифрования (ЛСК) может быть представлен следующей структурной схемой алгоритма формирования рис. 1 [6, 7], где x_i, y_i – i -е элементы входных и выходных данных соответственно, оператор $\oplus$ – поразрядное сложение по $\mathrm{mod}\,2$, R' – элемент раундового ключа.

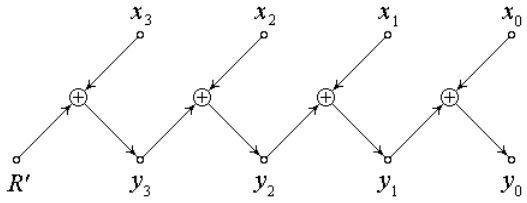

Рис. 1. Структурная схема алгоритма реализации примитива ЛСК

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

$$y_3 = x_3 \oplus R';$$
$$y_2 = x_2 \oplus y_3;$$
$$y_1 = x_1 \oplus y_2;$$
$$y_0 = x_0 \oplus y_1.$$

Проведем исследование возможности параллельной реализации примитива ЛСК (рис. 1) без учета раундового ключа R'. Параллельная реализация возможна на основе использования матричных операций криптографического преобразования [1 – 4].

Рассмотрим матричную модель операции упрощенного скользящего шифрования.

Упрощенное скользящее шифрование преобразует последовательность x_k в y_k, тогда

$$\begin{aligned} y_1 &= x_1;\\ y_2 &= x_1 \oplus x_2;\\ y_3 &= x_1 \oplus x_2 \oplus x_3;\\ y_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4;\\ y_5 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5;\\ &\ldots\ldots\ldots\\ y_n &= x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n. \end{aligned} \qquad (1)$$

Функция преобразования одного элемента скользящего шифрования может быть описана моделью, представленной рекуррентной последовательностью

$$y_n = y_{n-1}. \oplus x_n. \qquad (2)$$

Данная модель позволяет получить матричную операцию криптографического преобразования для параллельной реализации примитива.

Повторное упрощенное скользящее шифрование преобразует последовательность y_k в z_k:

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

Подставив в выражение (3) выражение (1), получим:

$$\begin{aligned} z_1 &= x_1;\\ z_2 &= x_1 \oplus (x_1 \oplus x_2);\\ z_3 &= x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3);\\ z_4 &= x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4);\\ &\ldots\ldots\ldots\\ z_n &= x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3) \oplus \ldots\ldots \oplus\\ &\oplus (x_1 \oplus x_2 \oplus \ldots\ldots \oplus x_n). \end{aligned}$$

Преобразовав, получим:

$$\begin{aligned} z_1 &= x_1;\\ z_2 &= x_2;\\ z_3 &= x_1 \oplus x_3;\\ z_4 &= x_2 \oplus x_4;\\ z_5 &= x_1 \oplus x_3 \oplus x_5;\\ z_6 &= x_2 \oplus x_4 \oplus x_6;\\ &\ldots\ldots\ldots\\ z_{2k-1} &= x_1 \oplus x_3 \oplus x_5 \oplus \ldots\ldots \oplus x_{2k-1};\\ z_{2k} &= x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \ldots\ldots \oplus x_{2k}. \end{aligned} \qquad (4)$$

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

$$z_n = z_{n-2} \oplus x_n, \qquad (5)$$

при начальных условиях $z_1 = x_1$ и $z_2 = x_2$.

Трехкратное упрощенное скользящее шифрование преобразует последовательность z_k в l_k.

$$\begin{aligned} l_1 &= z_1;\\ l_2 &= z_1 \oplus z_2;\\ l_3 &= z_1 \oplus z_2 \oplus z_3;\\ l_4 &= z_1 \oplus z_2 \oplus z_3 \oplus z_4;\\ l_5 &= z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5;\\ &\ldots\ldots\ldots\\ l_n &= z_1 \oplus z_2 \oplus z_3 \oplus \ldots\ldots \oplus z_n. \end{aligned} \qquad (6)$$

Подставим в выражение (6) выражение (4), получим:

$$
\begin{aligned}
l_1 &= x_1;\\
l_2 &= x_1 \oplus x_2;\\
l_3 &= x_2 \oplus x_3;\\
l_4 &= x_3 \oplus x_4;\\
l_5 &= x_1 \oplus x_4 \oplus x_5;\\
l_6 &= x_1 \oplus x_2 \oplus x_5 \oplus x_6;\\
l_7 &= x_2 \oplus x_3 \oplus x_6 \oplus x_7;\\
l_8 &= x_3 \oplus x_4 \oplus x_7 \oplus x_8;\\
l_9 &= x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_9;\\
l_{10} &= x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_9 \oplus x_{10};\\
l_{11} &= x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11};\\
&\ldots\ldots\ldots
\end{aligned}
\qquad (7)
$$

Функция преобразования одного элемента трехкратного скользящего шифрования может быть описана рекуррентной последовательностью

$$l_n = l_{n-4} \oplus x_{n-1} \oplus x_n, \qquad (8)$$

при начальных условиях

$$l_1 = x_1,\ l_2 = x_1 \oplus x_2,\ l_3 = x_2 \oplus x_3,\ l_4 = x_3 \oplus x_4.$$

Четырехкратное упрощённое скользящее шифрование преобразует последовательность l_k в j_k.

$$
\begin{aligned}
j_1 &= l_1;\\
j_2 &= l_1 \oplus l_2;\\
j_3 &= l_1 \oplus l_2 \oplus l_3;\\
j_4 &= l_1 \oplus l_2 \oplus l_3 \oplus l_4;\\
j_5 &= l_1 \oplus l_2 \oplus l_3 \oplus l_4 \oplus l_5;\\
&\ldots\ldots\ldots\\
j_n &= l_1 \oplus l_2 \oplus l_3 \oplus \ldots\ldots \oplus l_n.
\end{aligned}
\qquad (9)
$$

Подставим в выражение (9) выражение (7), получим:

$$
\begin{aligned}
j_1 &= x_1;\\
j_2 &= x_2;\\
j_3 &= x_3;\\
j_4 &= x_4;\\
j_5 &= x_1 \oplus x_5;\\
j_6 &= x_2 \oplus x_6;\\
j_7 &= x_3 \oplus x_7;\\
j_8 &= x_4 \oplus x_8;\\
j_9 &= x_1 \oplus x_5 \oplus x_9;\\
j_{10} &= x_2 \oplus x_6 \oplus x_{10};\\
j_{11} &= x_3 \oplus x_7 \oplus x_{11};\\
&\ldots\ldots\ldots
\end{aligned}
\qquad (10)
$$

Функция преобразования одного элемента четырехкратного упрощенного скользящего шифрования может быть описана рекуррентной последовательностью

$$j_n = j_{n-4} \oplus x_n, \qquad (11)$$

при начальных условиях

$$j_1 = x_1,\ j_2 = x_2,\ j_3 = x_3,\ j_4 = x_4.$$

Пятикратное упрощённое скользящее шифрование преобразует последовательность j_k в p_k:

$$
\begin{aligned}
p_1 &= j_1;\\
p_2 &= j_1 \oplus j_2;\\
p_3 &= j_1 \oplus j_2 \oplus j_3;\\
p_4 &= j_1 \oplus j_2 \oplus j_3 \oplus j_4;\\
p_5 &= j_1 \oplus j_2 \oplus j_3 \oplus j_4 \oplus j_5;\\
&\ldots\ldots\ldots\\
p_n &= j_1 \oplus j_2 \oplus j_3 \oplus \ldots\ldots \oplus j_n.
\end{aligned}
\qquad (12)
$$

Подставив в выражение (12) выражение (10), получим:

$$
\begin{aligned}
p_1 &= x_1;\\
p_2 &= x_1 \oplus x_2;\\
p_3 &= x_1 \oplus x_2 \oplus x_3;\\
p_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4;\\
p_5 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5;\\
p_6 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6;\\
p_7 &= x_4 \oplus x_5 \oplus x_6 \oplus x_7;\\
p_8 &= x_5 \oplus x_6 \oplus x_7 \oplus x_8;\\
p_9 &= x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9;\\
p_{10} &= x_1 \oplus x_2 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10};\\
p_{11} &= x_1 \oplus x_2 \oplus x_3 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11};\\
p_{11} &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12};\\
&\ldots\ldots\ldots
\end{aligned}
\qquad (13)
$$

Функция преобразования одного элемента пятикратного упрощенного скользящего шифрования может быть описана рекуррентной последовательностью

$$p_n = p_{n-8} \oplus x_{n-3} \oplus x_{n-2} \oplus x_{n-1} \oplus x_n. \qquad (14)$$

Шестикратное упрощённое скользящее шифрование преобразует последовательность p_k в q_k.

$$
\begin{aligned}
q_1 &= p_1;\\
q_2 &= p_1 \oplus p_2;\\
q_3 &= p_1 \oplus p_2 \oplus p_3;\\
q_4 &= p_1 \oplus p_2 \oplus p_3 \oplus p_4;\\
q_5 &= p_1 \oplus p_2 \oplus p_3 \oplus p_4 \oplus p_5;\\
&\ldots\ldots\ldots\\
q_n &= p_1 \oplus p_2 \oplus p_3 \oplus \ldots\ldots \oplus p_n.
\end{aligned}
\qquad (15)
$$

Подставим в выражение (15) выражение (13) получим:

$$
\begin{aligned}
q_1 &= x_1;\\
q_2 &= x_2;\\
q_3 &= x_1 \oplus x_3;\\
q_4 &= x_2 \oplus x_4;\\
q_5 &= x_3 \oplus x_5;\\
q_6 &= x_4 \oplus x_6;\\
q_7 &= x_5 \oplus x_7;\\
q_8 &= x_6 \oplus x_8;
\end{aligned}
$$

$$
\begin{aligned}
q_9 &= x_1 \oplus x_7 \oplus x_9;\\
q_{10} &= x_2 \oplus x_8 \oplus x_{10};\\
q_{11} &= x_1 \oplus x_3 \oplus x_9 \oplus x_{11};\\
q_{12} &= x_2 \oplus x_4 \oplus x_{10} \oplus x_{12};\\
q_{13} &= x_3 \oplus x_5 \oplus x_{11} \oplus x_{13};\\
q_{14} &= x_4 \oplus x_6 \oplus x_{12} \oplus x_{14};\\
&\ldots\ldots\ldots
\end{aligned}
\qquad (16)
$$

Функция преобразования одного элемента шестикратного упрощенного скользящего шифрования может быть описана рекуррентной последовательностью

$$q_n = q_{n-8} \oplus x_{n-2} \oplus x_n. \qquad (17)$$

На основе выше изложенного можно утверждать, что функции преобразования элементов скользящего шифрования представляются рекуррентными последовательностями (2, 5, 11, 14, 17) и являются частными случаями из всего разнообразия рекуррентных последовательностей, которые могут быть применены для синтеза матричных операций криптографического преобразования.

Выводы

Использование матричных операций криптографического преобразования дает возможность распараллелить процесс реализации примитива скользящего шифрования.

Применение матричных операций для многократного упрощенного скользящего шифрования позволяет сократить количество операций по сравнению с однократным упрощенным скользящим шифрованием, что дает выигрыш как во времени, так и в сложности реализации примитивов.

Также показано, что примитивы скользящего шифрования являются частичным случаем матричных операций построенных на основе ограниченных рекуррентных последовательностей.

Список литературы

1. *Голуб С.В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С.В. Голуб, В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації. – Х.: ХУ ПС ім. І. Кожедуба, 2012. – Вип. 3(101). – Т.1. – С. 119-122.*
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. – Х.: ХУ ПС ім. І. Кожедуба, 2012. – Вип. 4(33). – С. 198-200.*
3. *Бабенко В.Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко , С.В. Рудницький // Системи обробки інформації. – Х.: ХУ ПС ім. І. Кожедуба, 2012. – Вип. 9 (107). – С. 130-139.*
4. *Криптографическое кодирование: методы и средства реализации: монография / Тольят. гос. ун-т. – Тольятти, 2013. – 196 с.*
5. *Повідомлення організаційного комітету по проведенню відкритого конкурсу криптоалгоритмів про припинення прийому заявок на участь у конкурсі. [Електронний ресурс] – Режим доступу до ресурсу: http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=49027&cat_id=38710.*
6. *Белецкий А.Я. Примитивные полиномы в криптографических приложениях / А.Я. Белецкий, А.А. Белецкий, Д.А. Навроцкий, Р.Ю. Кандыба // Сучасний захист інформації. – 2011. – № 4. – С. 5-18.*
7. *Белецкий А.Я. Криптографические примитивы, основанные на методе скользящего кодирования / А.Я. Белецкий, А.А. Белецкий // Вісник СумДУ. – 2006. – № 10. – С. 33-42.*

Поступила в редколлегию 28.10.2013

Рецензент: д-р техн. наук, проф. В.Н. Рудницкий, Черкасский государственный технологический университет, Черкассы.

ПАРАЛЕЛЬНА РЕАЛІЗАЦІЯ КОВЗНОГО ШИФРУВАННЯ

В.Г. Бабенко

У роботі пропонується застосування матричних операцій криптографічного перетворення для розпаралелювання процесу реалізації примітиву ковзного шифрування. Доведено, що функції перетворення елементів ковзного шифрування є рекурентними послідовностями і можуть бути застосовані для синтезу матричних операцій криптографічного перетворення. Показано, що використання матричних операцій для багаторазового спрощеного ковзного шифрування дозволяє скоротити кількість елементарних операцій, що реалізують криптографічне перетворення даних.

Ключові слова: *паралельна реалізація, логічне ковзне шифрування, примітив, матрична операція криптографічного перетворення.*

PARALLEL IMPLEMENTATION OF A SLIDING ENCODING

V.G. Babenko

The paper proposes the use of matrix operations for cryptographic transformation to parallelize the process of realization of the primitive sliding encryption. Proved that the conversion function of the sliding encryption elements are recurrent sequences and can be applied for the synthesis of matrix operations of cryptographic transformations. It is shown that the use of matrix operations for multiple sliding simplified encryption reduces the number of elementary operations that implement cryptographic transformation of data.

Keywords: *parallel implementation, logical sliding encryption, the primitive, matrix operation of cryptographic transformation.*