УДК 004.056.055

В. А. Лужецкий, д. т. н., проф.; А. В. Остапенко

БЛОЧНЫЙ ШИФР НА ОСНОВЕ ПСЕВДОНЕДЕТЕРМИНИРОВАННОЙ ПОСЛЕДОВАТЕЛЬНОСТИ КРИПТОПРИМИТИВОВ

Предложен новый подход к реализации блочного шифра, который основан на использовании псевдонедетерминированных последовательностей криптопримитивов и разбиении сообщения на блоки различной длины на каждом из раундов преобразования.

Ключевые слова: *симметричные блочные шифры, криптография, псевдонедетерминированные последовательности.*

Вступление

Постоянно растущие требования к шифрам, учет ими особенностей современной элементной базы, создание новых видов атак обуславливает потребность в разработке и исследовании новых подходов к построению блочных шифров.

Согласно реализации функции шифрования выделяют блочные шифры, построенные на основе сетей Фейстеля (Feistel network) [1, 2, 3], чередования процедур перестановок и подстановок (SP-сетей) [1, 4, 5], структуры «квадрат» (Square) [1, 6] и управляемых операций [7].

Блочные шифры на основе сети Фейстеля имеют недостатки с точки зрения скорости и простоты выполнения операций, поскольку за один раунд шифруется только половина блока входящего сообщения [8]. Использование табличных замен качественно влияет на скорость шифрования, основанного на SP-сетях и структуре «квадрат» (Square).

Цель работы

Целью работы является повышение скорости блочного шифрования данных при обеспечении заданного уровня криптографической стойкости путем разработки блочного шифра на основе псевдонедетерминированной последовательности криптопримитивов.

Постановка задач

Любой блочный шифр может быть описан такой алгебраической моделью:

$$\sum = \{\mathbf{M}, \mathbf{K}, \mathbf{C}, \mathbf{E}, \mathbf{D}\},$$

где $\mathbf{M} = \{m_j\}$ – множество открытых сообщений $(j = j \ldots J)$; $\mathbf{K} = \{k_i\}$ – множество ключей $(i = i \ldots I)$; $\mathbf{C} = \{c_j\}$ – множество криптограмм; $\mathbf{E} = \{E_{ki}\}$ – множество алгоритмов зашифрования; $\mathbf{D} = \{D_{ki}\}$ – множество алгоритмов расшифрования.

Множество **E** образуется отображением **M**×**K**→**C**, при этом E_{ki} описывается функцией $F(k_i, m_j)$. Отображение **C**×**K**→**M** образует множество **D** алгоритмов расшифрования. Отдельные алгоритмы расшифрования D_{ki} описываются функцией $F^{-1}(k_i, m_j)$.

Как правило, алгоритмы зашифрования и расшифрования являются итерационными и состоят из последовательности R преобразований (раундов) [9]. Причем в каждом раунде преобразования используется отдельный раундовый ключ k_r, получаемый из общего секретного ключа $k \in \mathbf{K}$. Исходя из этого, криптограмма $c \in \mathbf{C}$ для открытого сообщения $m \in \mathbf{M}$ и ключа k получается как результат выполнения последовательности раундовых преобразований:

$$c_r = F(k_r, c_{r-1}), \quad (1)$$

где c_r – зашифрованные данные после r-го преобразования $\left(c_1 = m, c = c_R, r = \overline{1 \ldots R}\right)$; $F(k_r, c_{r-1})$ – функция раундового преобразования.

Соответственно открытый текст m для криптограммы c и ключа k получается как результат преобразования:

$$m_r = F^{-1}(k_r, m_{r-1}), \quad (2)$$

где m_r – расшифрованные данные после r-го преобразования $(m_1 = c, m = m_R)$.

Алгебра секретных систем, описанная в работе К. Шеннона [9, 10], раскрывает два способа комбинирования секретных систем с целью получения новой секретной системы.

Способ, который называется «взвешенная сумма» состоит из предварительного выбора системы T_i с некоторой вероятностью p_i. После того как выбор сделан, система T_i используется в соответствии с ее определением. При этом новая система имеет множество отображений, она состоит из совокупности всех множеств отображения, использованных секретных систем с вероятностями их использования, равными произведению вероятности выбора этих отображений и вероятности выбора секретной системы:

$$S = \sum_{i=1}^{n} p_i \cdot T_i, \ \sum_{i=1}^{n} p_1 = 1, \quad (3)$$

где S – комбинированная секретная система; T_i – i-ая секретная система из набора n секретных систем; p_i – вероятность выбора i-ой секретной системы.

Полный ключ системы S указывает на то, какая из систем используется и с каким ключом.

Способ «произведение» состоит из последовательного применения секретных систем, при условии, что система T_{i+1} имеет область определения (пространство языка) такую, что ее можно сравнить с областью определения (пространством криптограмм) системы T_i то есть:

$$S = \prod_{i=1}^{n} T_i. \quad (4)$$

При этом полный ключ системы S состоит из ключей всех используемых систем.

Анализ рассмотренных подходов к построению блочных шифров показывает, что шифры на основе сети Фейстеля, SP-сети, структуры «квадрат» могут быть описаны как произведение секретных систем (3), при этом T_i можно рассматривать как раунд преобразования.

Блочные шифры на основе управляемых операций можно описать произведением систем (3). В этом случае в каждом раунде выполняются различные преобразования с фиксированной последовательностью, но с переменными параметрами операций. Например, выполнение операции циклического сдвига вправо на 3 разряда в первом раунде и на 7 разрядов во втором.

Эти преобразования описываются одной и той же функцией, но в качестве аргументов используются результаты предварительного преобразования и раундовый ключ. То есть алгоритм блочного шифра является детерминированным.

Поскольку набор и последовательность выполнения операций являются детерминированными, криптографическая стойкость рассмотренных блочных шифров определяется размером ключа, сложностью выполняемых операций или количеством раундов при использовании простых операций.

Для уменьшения количества раундов, а значит повышения скорости шифрования, при

использовании набора простых операций, предлагается применять недетерминированную последовательность операций (с точки зрения злоумышленника), которая определяется секретным ключом.

Поскольку при шифровании будет использоваться определенный набор алгоритмов, в которых последовательность выполняемых операций определяется ключом, то в дальнейшем эти алгоритмы будем называть псевдонедетерминированными. Такой подход к шифрованию приводит к тому, что злоумышленнику необходимо перебрать все возможные алгоритмы шифрования.

Идея построения блочного шифра

Предлагается строить блочный шифр на основе использования псевдонедетерминированных алгоритмов. В общем случае они состоят из набора функций преобразований $F_1, F_2, \ldots F_L$ и операций, которые с использованием секретного ключа k формируют последовательность $a(1), a(2), \ldots, a(i)$ [10].

Процедура зашифрования открытого сообщения c использованием k заключается в применении функций F в порядке, определяемом последовательностью $a(i)$:

$$c = F_k(m) = F_{a(i)}(\ldots(Fa(2)(Fa(1)(m)))\ldots) \quad (5)$$

Таким образом, алгоритм шифрования на основе псевдонедетерминированных последовательностей криптопримитивов состоит из известных преобразований, позволяющих теоретически оценить стойкость шифра, согласно правилу Керкоффа, но порядок их применения определяется секретным ключом k и является недетерминированным процессом с точки зрения криптоаналитика.

Идея предлагаемого подхода заключается в том, что преобразования в каждом из раундов состоят из элементарных преобразований (криптопримитивов), набор и последовательность выполнения которых определяются некоторым множеством признаков, которые формируются из ключевой информации.

С точки зрения секретных систем по Шеннону данный блочный шифр можно представить как комбинацию «взвешенной суммы» (3) и «произведения» (4) то есть:

$$S = \prod_{i=1}^{n} \left(\sum_{j=1}^{m} p_{ij} \cdot T_{ij}\right), \sum_{j=1}^{m} p_{ij} = 1.$$

Исходя из вышеизложенного, предлагается такая модель блочного шифра:

$$\sum = \{\mathbf{M}, \mathbf{K}, \mathbf{F_E}, \mathbf{F_D}, \mathbf{Q}, \mathbf{P}, \mathbf{C}\}, \quad (6)$$

где $\mathbf{M} = \{m_j\}$ – множество открытых сообщений; $\mathbf{K} = \{k_i\}$ – множество ключей; $\mathbf{F_E} = \{F_{Eki}\}$ – множество функций преобразования для зашифрования; $\mathbf{F_D} = \{F_{Dki}\}$ – множество функций преобразования для расшифрования; $\mathbf{Q} = \{q_p\}$ – множество признаков $(p = 1 \ldots P)$; $\mathbf{B} = \{b_h\}$ – множество базовых операций $(h = 1 \ldots H)$; $\mathbf{C} = \{c_j\}$ – множество криптограмм.

Главными аспектами разработки предложенного подхода являются реализация функции формирования признаков **Q** и реализация выбора базовых операций **B**.

Признак $q \in \mathbf{Q}$ определяет набор операций **B**, которые составляют раундовую функцию F, поэтому преобразование на определенном этапе алгоритма будет иметь вид:

$$P_r = F_q(c_q, k_r),$$

где P_r – раундовое преобразование; F_q – функция раундового преобразования определена по признаку q; c_q – информация, которая обрабатывается в текущем раунде.

Таким образом, алгоритм блочного шифрования **A** может быть представлен совокупностью раундовых преобразований P_r, функции, преобразования которых и структура обрабатываемых ими данных зависят от признаков q:

$$\mathbf{A} = \{P_1, P_2, \ldots, P_R\}.$$

Процесс формирования признака преобразования предусматривает выделение на каждом этапе зашифрования с ключевой информации (текущего раундового подключа k_r) таких признаков:

- количество подблоков Q_{pb};
- разрядность подблока Q_{rb} (бит);
- вид функции раундового преобразования Q_{vp}.

Каждый из этих признаков является некоторым целым числом в заданных пределах.

Структура обрабатываемого блока для данного шифра состоит из определенного количества подблоков переменной длины. При этом количество блоков и их длина определяются признаками Q_{pb} и Q_{rb}. С учетом этого длина блока:

$$N_b = Q_{pb} \cdot Q_{rb}.$$

На рис. 1 изображен пример разбиения обрабатываемой информации на блоки переменной длины.

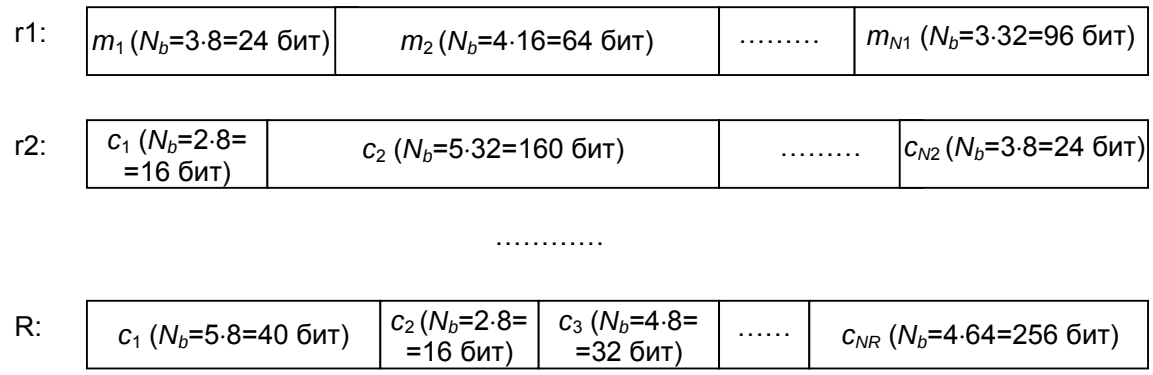


Рис.1. Схема разбиения на блоки переменной длины

Особенности предлагаемого подхода обуславливают большое количество возможных модификаций алгоритмов блочного шифрования. С помощью выбранного диапазона значений признаков может быть построено N_m различных алгоритмов для одного раунда преобразования:

$$N_m = Q_{pb} \cdot Q_{rb} \cdot Q_{vp}.$$

Неопределенность для злоумышленника конкретной последовательности криптопримитивов в конкретном алгоритме шифрования и большое количество возможных модификаций последовательностей делают практически невозможным предварительное исследование статистических свойств каждой из них, что значительно усложняет задачу криптоанализа.

Базовые операции для псевдонедетерминированного блочного шифра

Для построения псевдонедетерминированного алгоритма авторами предлагается множество базовых операций B, состоящих из двух видов операций: однооперандных и двооперандных.

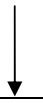
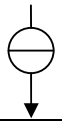
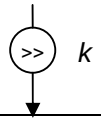
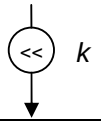
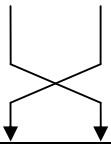
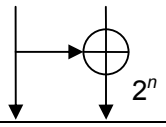
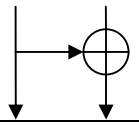
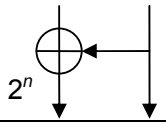
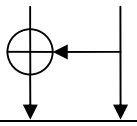
Однооперандные операции выполняются над одним подблоком данных (циклический

сдвиг на k бит, инвертирование, отсутствие преобразования). Двооперандные операции выполняются над двумя подблоками данных (добавление по модулю 2, добавление по модулю 2n, перестановка подблоков).

Схематическое обозначение предложенного набора базовых операций и их мнемоническое описание приведены в табл. 1.

Таблица 1

Базовые операции

Название операции	Схематическое обозначение	Мнемоническое обозначение
Одноопераднные операции		
Отсутствие преобразования		NOP
Инвертирование данных		NOT
Циклический сдвиг вправо на k бит		LLC
Циклический сдвиг влево на k бит		RLC
Двооперандные операции		
Перестановка блоков		PR
Двооперандные левосторонние операции		
Добавление по модулю 2^n		L^n
Добавление по модулю 2		L^2
Двооперандные правосторонние операции		
Добавление по модулю 2^n		R^n
Добавление по модулю 2		R^2

Вышеописанные операции дают возможность построить большое количество криптопримитивов и их модификаций для оперирования в блочном шифре.

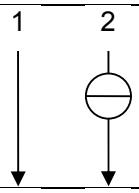
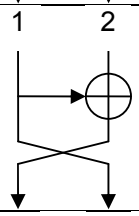
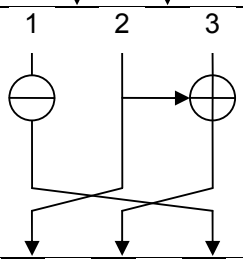
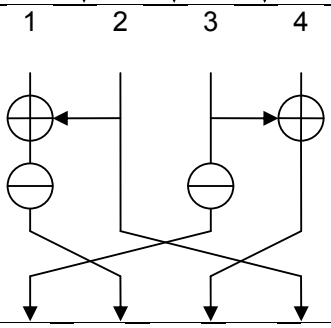
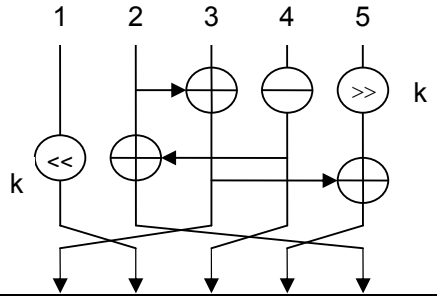
Рассмотрим варианты возможных преобразований блочного шифра с использованием представленного набора базовых операций. Для этого введем некоторые обозначения:

P – преобразования; O_a – выполнение одноопернандной операции над подблоком a $\left(a = 1 \ldots Q_{pb}\right)$; D_{ab} – выполнение двуопернандной операции над подблоками a и b $\left(b = 1 \ldots Q_{pb}, b \rangle a\right)$; PR_{ab} – перестановка подблоков a и b; $||$ – параллельное выполнение действий; $\rightarrow$ – последовательное выполнение действий.

Примеры возможных преобразований для разного количества подблоков и их схематическое и мнемоническое описание приведены в табл. 2.

Таблица 2

Обозначения преобразований

Схематическое обозначение	Мнемоническое обозначение
	$P=NOP_1 \| \| NOT_2$
	$P=L^2_{12} \rightarrow PR_{12}$
	$P=(NOT_1 \| \| L^2_{23}) \rightarrow PR\ (PR_{12} \rightarrow PR_{23})$
	$P=(R^2_{12} \| \| L^2_{34}) \rightarrow$ $\rightarrow (NOT_1 \| \| NOP_2 \| \| NOT_3 \| \| NOP_4) \rightarrow$ $\rightarrow PR(PR_{23} \rightarrow PR_{12} \rightarrow PR_{32})$
	$P=(NOP_1 \| \| R^2_{23} \| \| NOT_4 \| \| RLC_5) \rightarrow$ $\rightarrow (LLC_1 \| \| L^2_{24} \| \| R^2_{35}) \rightarrow$ $\rightarrow PR\ (PR_{23} \rightarrow PR_{12} \rightarrow PR_{34} \rightarrow PR_{45})$

Сформированное множество базовых операций **B** является основным для различных по структуре раундовых преобразований, а предложенное мнемоническое описание операций

однозначно определяет их структуру.

Применение вышеизложенной идеи блочного шифра позволяет достичь соответствующего уровня криптографической стойкости блочных шифров с детерминированной структурой, благодаря использованию псевдонедетерминированных последовательностей криптопримитивов. Это позволяет уменьшить количество раундов шифра R и упростить функцию раундового преобразования F, используя операции, которые быстро выполняются на современных процессорах, без потери криптостойкости. Таким образом, достигается увеличение скорости блочного шифрования.

Выводы

Предложен новый подход к реализации блочного шифра, который основан на использовании псевдонедетерминированных последовательностей криптопримитивов и разбиении сообщения на блоки переменной длины на каждом из раундов преобразования. Именно это позволяет усложнить взлом шифра, поскольку необходимо осуществлять перебор всех возможных комбинаций базовых операций на каждом из раундов и всех возможных вариантов разбивки сообщения на блоки и блоков на подблоки.

СПИСОК ЛИТЕРАТУРЫ

1. Аграновский А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2002. – 256 с.

2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 346 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.: ил.

4. Kam J. Structured design of substitution-permutation encryption networks / J. Kam, G. Davida // IEEE Transactions on Computers. – 1979. – Vol. 28, №10. – P. 747.

5. Heys H. Substitution-permutation networks resistant to deferential and linear cryptanalysis / H. Heys, S. Tavares // Journal of Cryptology. – 1996. – Vol. 9, №1. – P.1 – 19.

6. Daemen J. The block cipher SQUARE / J. Daemen, V. Rijmen, L. Knudsen // Fast Software Encryption: FSE'97, Israel, January 1997 / Computer Science. Springer – Verlag. – 1997. – Vol. 1267. – P. 149 – 165.

7. Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов. / Н. А. Молдовян, А. А. Молдовян, М. А. Ефремов. – СПб.: БХВ-Петербург, 2004. – 448 с.

8. Алферов А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузмин. – М.: Гелиос АРВ, 2001. – 479 с.

9. Шеннон К. Работы по теории информации и кібернетики / К. Шеннон – М., 1963. – 829 с.

10. Адигеев М. Г. Введение в криптографію. Ч.1. Основные понятия, задачи и методы криптографии / М. Г. Адигеев. – Ростов-на-Дону: Ростовский гос. ун-т, 2002. – 35 с.

Лужецкий Владимир Андреевич – д. т. н., профессор, заведующий кафедрой защиты информации.

Остапенко Алина Васильевна – аспирант кафедры защиты информации.
Винницкий национальный технический университет.