ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 621. 391
DOI: 10.17586/0021-3454-2017-60-1-5-9

АЛГОРИТМИЧЕСКИЕ И СТАТИСТИЧЕСКИЕ СВОЙСТВА РАЗРЕЖЕННОЙ РЮКЗАЧНОЙ КРИПТОСИСТЕМЫ С ОБЩЕЙ ПАМЯТЬЮ

А. В. Александров, А. Д. Метлинов

Владимирский государственный университет им. А. Г. и Н. Г. Столетовых,
600000, Владимир, Россия
E-mail: lexlotr@gmail.com

Для базисов возвратных последовательностей конечного порядка определены асимптотические и алгоритмические свойства разреженных рюкзачных криптосистем, обеспечивающих плотность укладки вне интервала (0,1). Конструкция таких криптосистем использована для построения блочного шифра в режиме зацепления блоков. Приведены результаты сравнительного анализа скоростных и статистических характеристик алгоритма шифрования с известными стандартами блочного шифрования.

Ключевые слова: *общая память, скоростные характеристики, рюкзачная криптосистема, разреженные рюкзаки, общая память, плотность укладки, атака Костера — Одлыжко, блочный шифр с режимом зацепления блоков*

В работе [1] была представлена не совсем традиционная модель криптографической симметричной системы с общей памятью, основанная на задаче об укладке рюкзака. В настоящей статье приведены некоторые обобщения этой модели, возникающие при более общем подходе к использованию возвратных (линейно-рекуррентных) последовательностей порядка $m \geq 2$ в качестве базиса укладки рюкзака; также определены статистические свойства криптосистемы для $m = 2$.

В работе американских специалистов [2] представлен аналогичный подход, основанный на возвратных базисах без использования общей памяти и в общей постановке, охватывающей также криптосистемы Меркла — Хеллмана:

$$f_i = \sum_{j=1}^{m} C_j f_{i-j}\,,\ S = C_1 C_2 \ldots C_m, \qquad (1)$$

здесь $S =$ „$C_1 \ldots C_m$“ — сигнатура базиса задачи об укладке рюкзака, C_i — суть положительные целые числа, при этом существуют лексикографические условия, дополняющую формулу (1).

Как отмечено в работах [1, 2], для последовательности (1) существуют варианты базисов, для которых плотность укладки рюкзака

$$\rho = \max_{i=1\ldots n} \frac{n}{\log_2 f_i} > 1 \qquad (2)$$

и известная атака Костера — Одлыжко на задачу о рюкзаке неприменима (здесь n — длина двоичного вектора). Рюкзаки, соответствующие условию (1), назовем разреженными, они описываются только сигнатурами вида $S =$ „$11 \ldots 1$“ и не зависят от их начальных значений.

Обозначим общую память пары Sender, Receiver (отправитель и получатель сообщений в двустороннем канале связи) как $D = \{d_1, d_2, \ldots, d_n\}$ и для двоичного вектора $e = (e_i)$ длиной n определим параметр $d_e = \sum(e_i d_i)$. Для целого числа примем $m \geq 2$ и, согласно (1), сигнатуру S= „1….1“. Для создания базиса задачи о рюкзаке используем линейно-рекуррентные последовательности конечного порядка m:

$$f_1(d_e)=1, f_2(d_e)=1, \ldots, f_m(d_e)= d_e; f_i(d_e)= f_{i-1}(d_e)+f_{i-2}(d_e)+\ldots+f_{i-m}(d_e) \text{ при } i>m. \quad (3)$$

Такие последовательности, называемые также возвратными, достаточно хорошо изучены. При m=2 получаем последовательности Фибоначчи. Относительно свойств базисов справедливы следующие утверждения.

Утверждение 1. Для любого целого числа S справедливо однозначное представление

$$S = \left(\sum k_i f_i(d_e)\right) + \Delta(S, d_e), \; i = 1, \ldots, l, \quad (4)$$

с двоичными элементами k_i и некоторым остаточным слагаемым $\Delta\left(S, d_e\right)$ относительно „жадного“ алгоритма, „просматривающего“ элементы базиса сверху вниз.

Утверждение 2. Алгоритмическая сложность представления (2) оценивается величиной $O(\log S)$ равномерно при выборе параметров базиса с $m \geq 2$, d_e.

Утверждение 3. Асимптотика роста последовательности $\{f_i(d_e)\}$ при больших значениях индекса „i“ не зависит от начальных значений базиса в формуле (1) и определяется наибольшим вещественным значением корня $\alpha_f(m)$ соответствующего выражениям (3) характеристического уравнения $x^m - x^{m-1} - \ldots - 1 = 0$. Вид асимптотики:

$$f_n = O(\alpha_n(f)^n). \quad (5)$$

Последовательность корней $\alpha_f(m)$ монотонно возрастает по параметру m и ограничена сверху значением 2. Для любого $m \geq 2$ асимптотика роста обеспечивает плотность укладки рюкзака за пределами интервала (0,1).

Подтверждением того, что представление (4), строго говоря, не единственно, являются примеры для базиса Фибоначчи. Однако известный „жадный“ алгоритм, „просматривающий“ элементы базиса сверху вниз, всегда дает единственное представление (4) с некоторым остаточным слагаемым Δ. При $e \equiv 0$ представление (4) вырождается при n = 2 в представление Цекендорфа. В этом случае $\Delta \equiv 0$ равномерно по всему натуральному ряду чисел.

Значения корней асимптотики роста и соответствующих плотностей укладки для m = 2...10 приведены в табл. 1. Значения $\rho(m)$ вычисляются непосредственно при подстановке выражения (5) в формулу (2).

Таблица 1

m	$\alpha_f(m)$	$\rho(m)$
2	1,618033989	1,44042009
3	1,839	1,137758063
4	1,927	1,056684161
5	1,965	1,0261364
6	1,983	1,012468881
7	1,9919	1,005889259
8	1,99603	1,002874837
9	1,99802	1,00143102
10	1,99901	1,000714821

Введение термина „разреженные рюкзаки“ обусловлено не только значением плотности укладки, но и еще одним обстоятельством, вытекающим из утверждений 1—3 и свойств представлений Цекендорфа. Очевидно, что для разложения (4) натурального числа при фиксиро-

ванном m существует запретная комбинация битов вида „0111…1“, которую можно заменить комбинацией „10...0“. Следовательно, вероятности появления соответственно 0 и 1 в представлении (4) не равны. Количество нулей превышает количество единиц, причем тем больше, чем больше параметр m. В силу этого при построении схемы шифрования данный эффект необходимо скрывать. Решение в этом случае — режим блочной работы шифра с зацеплением блоков.

Для базисов второго порядка, гарантирующих наибольшее отклонение значения плотности укладки от интервала (0,1), разработана конструкция блочного шифра в режиме зацепления блоков и построена соответствующая ему хеш-функция, формируемая посредством XOR-свертки шифрованных блоков открытого текста. Статистика этой программы детально изучена.

На основе представления (4) построен масштабируемый блочный симметричный шифр с несколькими режимами работы, в том числе режимом кодовой книги (рис. 1) и режимом зацепления блоков (рис. 2).

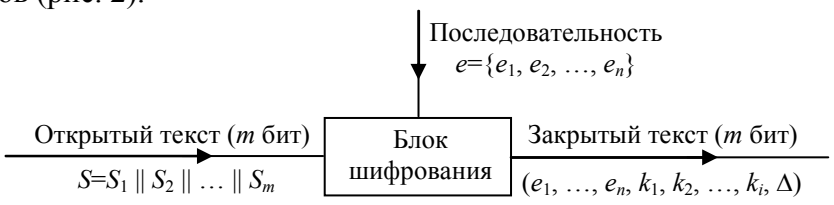

Рис. 1

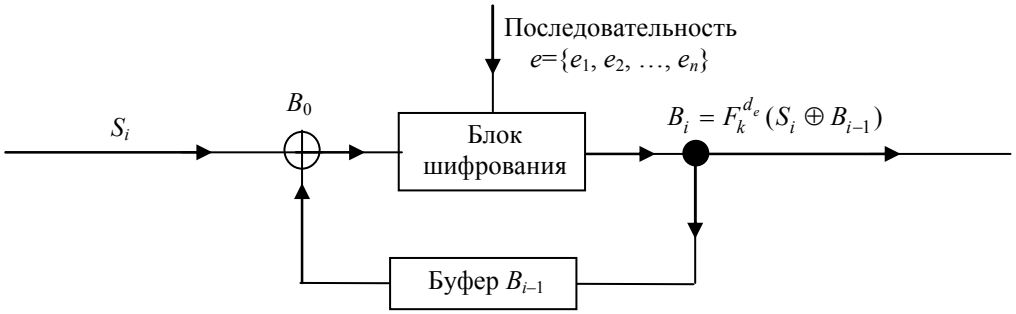

Рис. 2

Пусть в представлении (4) l — достаточно большое натуральное число и $\overline{S}$ — максимально возможное натуральное число. Пусть S — любой двоичный файл произвольной длины. Зададим конкатенацию блоков $S = S_1 \parallel S_2 \parallel \ldots \parallel S_m$, где $S_i \in \mathrm{GF}_2$ и длина каждого блока, за исключением последнего, фиксирована (см. рис. 1). Считая эти условия выполненными равномерно по всем индексам $S_i \le \overline{S}$, для каждого блока применим представление (4). При этом определяются функция шифрования блока $F_k\left(d_e, S\right)$ и функция дешифрования $F_k^{-1}\left(d_e, \left[e_1, \ldots, e_n, k_1, \ldots, k_l, \Delta_2\right]\right)$.

В режиме зацепления блоков (см. рис. 2) каждый блок S_i открытого текста, кроме вектора инициализации, побитово складывается по модулю 2 с предыдущим результатом шифрования. Пусть B_0 — вектор инициализации (блок формируется с помощью определенного одностороннего алгоритма на основе общей памяти), тогда

$$B_i = F_k^{d_e}(S_i \oplus B_{i-1}), \tag{6}$$

где i — номер текущего блока, $F_k^{d_e}$ — алгоритм шифрования, соответствующий функции $F_k\left(d_e, S\right)$.

В реализованной конструкции блочного шифра длина блока текста равна 64 битам, максимально возможный размер общей памяти оценивается в 2^{64} бит и $\Delta_{max} = 3$ бита.

Для оценивания скорости работы алгоритма блочный шифр был протестирован по двум направлениям. Первый тест — на скорость шифрования и сравнение с соответствующими скоростями работы криптосистем Меркла — Хеллмана и базиса Цекендорфа. В ходе тестирования было выбрано 10 различных типов файлов (сжимаемых и несжимаемых). Для каждой из трех криптосистем и для каждого типа файла проведено по 30 контрольных экспериментов (всего порядка 1000), результаты которых показали, что спроектированный алгоритм шифрования криптосистемы с общей памятью работает в среднем на 25—28 % быстрее, чем криптосистема Меркла — Хеллмана, и на 7—9 % быстрее, чем рюкзак, в основе которого лежит базис Цекендорфа (табл. 2).

Таблица 2

Номер файла	Тип и размер файла	Скорость шифрования, с		
		Разработанный алгоритм	Криптосистема Меркла — Хеллмана	Базис Цекендорфа
1	*.txt (~200 кб)	1,2	1,4	1,2
2	*.txt (~2 Мб)	16	22	17
3	*.bmp (~8 Мб)	31	40	62
4	*.gif (~1 Мб)	7	9	9
5	*.exe (~3 Мб)	21	26	20
6	*.mp3 (~5 Мб)	27	31	27
7	*.mp4 (~20 Мб)	95	147	99
8	*.html (~400 кб)	1	3	1
9	*.rar (~1 Мб)	8	11	8
10	*.7z (~2 Мб)	13	20	15

При втором тестировании подтверждено существование определенной статистической закономерности влияния значения S и битовой структуры части ключа $e = \{e_1, e_2, \ldots, e_n\}$ на наличие или отсутствие коэффициента Δ [3—5].

Спроектированные алгоритмы шифрования и дешифрования работают значительно быстрее, чем в аналогичных рюкзачных криптосистемах. Это позволяет сделать вывод о возможности применения разработанных алгоритмов в комплексе с другими стандартами, такими как AES, DES и ГОСТ 1989.

СПИСОК ЛИТЕРАТУРЫ

1. *Александров А. В., Метлинов А. Д.* Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы // Изв. вузов. Приборостроение. 2015. Т. 58, № 5. С. 344—350.

2. *Hamlin N., Krishnamoorthy B., Webb W.* A knapsack-like code using recurrence sequence representations // Fibonacci Quarterly. 2015. N 1 (53). P. 24—33.

3. *Александров А. В., Метлинов А. Д.* О симметричных рюкзачных криптографических системах с разреженной плотностью укладки // Материалы Пятой Междунар. науч. конф. „Современные методы и проблемы теории операторов и гармонического анализа и их приложения V“. Ростов-на-Дону: Изд. центр ДГТУ, 2015. С. 150—151.

4. *Александров А. В., Метлинов А. Д., Зимников А. С.* О семействе рюкзачных блочных шифров с общей памятью и плотностью укладки больше единицы и хеш-функций на их основе // Сб. науч. тр. II Междунар. науч.-практ. конф. „Информационная безопасность в свете Стратегии Казахстан — 2050“. 2014. С. 31—35.

5. *Александров А. В., Метлинов А. Д.* К вопросу об особенностях реализации симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы // XXXIII Всерос. НТК „Проблемы эффективности и безопасности функционирования сложных технических и информационных систем“: Сб. тр. Серпухов, 2014.

Сведения об авторах

Алексей Викторович Александров — канд. физ.-мат. наук, доцент; ВлГУ, кафедра информатики и защиты информации; E-mail: alex_izi@mail.ru

Александр Дмитриевич Метлинов — аспирант; ВлГУ, кафедра информатики и защиты информации; E-mail: lexlotr@gmail.com

Рекомендована кафедрой информатики и защиты информации

Поступила в редакцию 28.08.16 г.

Ссылка для цитирования: *Александров А. В., Метлинов А. Д.* Алгоритмические и статистические свойства разреженной рюкзачной криптосистемы с общей памятью // Изв. вузов. Приборостроение. 2017. Т. 60, № 1. С. 5—9.

ALGORITHMIC AND STATISTICAL PROPERTIES OF SPARSE KNAPSACK CRYPTOSYSTEM WITH SHARED MEMORY

A. V. Aleksandrov, A. D. Metlinov

Vladimir State University, 600000, Vladimir, Russia
E-mail: lexlotr@gmail.com

Asymptotic and algorithmic properties of sparse backpack cryptosystems, providing the packing density outside the interval (0,1), are determined in terms of basis of finite-order recurrent sequences. Design of such cryptosystems is used to construct a block cipher in blocks engagement mode. Results of analysis of speed and statistical properties of the encryption algorithm as compared to the known standards of block cipher are presented.

Keywords: shared memory, speed characteristics, cryptosystem, sparse knapsack, packing density, L^3- attack, block cipher in blocks engagement mode

Data on authors

Alexey V. Aleksandrov — PhD, Associate Professor; Vladimir State University, Department of Information and Information Security; E-mail: alex_izi@mail.ru

Alexander D. Metlinov — Post-Graduate Student; Vladimir State University, Department of Information and Information Security; E-mail: lexlotr@gmail.com

For citation: *Aleksandrov A. V., Metlinov A. D.* Algorithmic and statistical properties of sparse knapsack cryptosystem with shared memory // Izv. vuzov. Priborostroenie. 2017. Vol. 60, N 1. P. 5—9 (in Russian).

DOI: 10.17586/0021-3454-2017-60-1-5-9