УДК 004.056.55
DOI: 10.17586/0021-3454-2015-58-5-344-350

СИММЕТРИЧНАЯ РЮКЗАЧНАЯ КРИПТОСИСТЕМА С ОБЩЕЙ ПАМЯТЬЮ И ПЛОТНОСТЬЮ УКЛАДКИ БОЛЬШЕ ЕДИНИЦЫ

А. В. Александров, А. Д. Метлинов

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

Предложен вариант симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы, которая устойчива к L^3-атаке, полиномиальной по своей скорости, разработанной Лагариасом и Одлыжко для взлома рюкзачных схем шифрования со сверхвозрастающими базисами. На основе протоколов с общей памятью разработаны алгоритмы шифрования и дешифрования, в основе работы которых лежат базисы типа Фибоначчи и их обобщения.

Ключевые слова: *рюкзачная криптосистема, общая память, L^3-атака, открытый канал связи, статистические свойства, алгоритмы.*

Введение. С развитием информационных технологий проблема усовершенствования систем, отвечающих за конфиденциальность информации, приобретает особую значимость. В этой связи использование криптосистем на базе рюкзачных схем представляется обоснованным.

Задача о ранце в криптографии [1], на основе которой американскими криптографами Мерклом и Хеллманом был разработан асимметричный алгоритм шифрования с открытым ключом, широко известна. Для представления чисел и шифрования сообщений использовалось решение задачи об укладке ранца, которая в общем виде является NP-полной.

К настоящему времени известно множество версий рюкзачных криптосистем; это объясняется тем, что по сравнению с другими схемами шифрования, использующими длинную целочисленную арифметику, рюкзачные системы обладают повышенными скоростными характеристиками алгоритмов шифрования и дешифрования. Однако все существующие на сегодняшний день рюкзачные криптосистемы взломаны или признаны потенциально небезопасными. Одна из основных причин этого — низкая плотность укладки рюкзака

$$\rho(a) = \frac{k}{\max_{1 \le i \le k} \log_2 a_k}, \qquad (1)$$

где k — количество элементов рюкзачного базиса, a_k — максимальный из всех элементов базиса.

Параметр (1) введен Лагариасом и Одлыжко [2] при проектировании ими алгоритма L^3-атаки; там же доказаны и приведены примеры полиноминальной по сложности атаки на рюкзачные криптосистемы, успешно взламывающей почти все криптографические рюкзаки с плотностью укладки менее 0,6463. Идея L^3-атаки состоит в том, чтобы преобразовать параметры задачи о рюкзаке в базис для некоторой целочисленной решетки в конечномерных целочисленных пространствах, после чего найти в этом базисе короткий вектор с помощью L^3-алгоритма редукции базиса решетки. Существует большая вероятность того, что с помощью найденного короткого вектора можно осуществить обратное решение этой задачи. В работе [3] с помощью более точных оценок влияние L^3-атаки расширено на интервал $0<\rho<0{,}940$. Из строго доказанных в работе [3] результатов следует, что чем больше величина ρ, тем меньше вероятность успеха осуществления L^3-атаки на данную рюкзачную криптосистему. При $\rho > 0{,}9408$ проведение L^3-атаки на рюкзачную криптосистему затруднено, но также

возможно. Однако утверждение, что L^3-атаку можно распространить на все супервозрастающие базисы в интервале 0<ρ<1, в работе [3] строго не доказано, но, по-видимому, верно.

Оценка асимптотики роста рюкзачных базисов. Оценим асимптотику роста рюкзачных базисов, используемых при разработке алгоритмов передачи сообщений, на основе вариации симметричной рюкзачной криптосистемы в рамках криптографических двусторонних протоколов с общей памятью, оценим также скорость работы алгоритмов.

Определение. Супервозрастающей последовательностью называется целочисленная последовательность $f_n, n = 1, \ldots, k$, для любого индекса i которой всегда выполняется условие $f_{i+1} > \sum_{j=1}^{i} f_j$. Очевидно, что минимальной последовательностью, для которой выполняется это условие, является последовательность степеней двойки: $\{1, 2^1, 2^2, \ldots, 2^n\}$.

Пусть n — достаточно большое натуральное число. Сформируем последовательность положительных целых попарно отличных друг от друга чисел: $\{a\}_1^n = (a_1, \ldots, a_n)$, и определим относительно пары $\{a\}_1^n$ и $\{e\}_1^n = (e_1, \ldots, e_n)$ линейную форму над полем Галуа GF_2:

$$< e, a >= \sum_{i=1}^{n} e_i a_i , \tag{2}$$

где e_i принадлежит GF_2.

Обозначим верхнюю грань представления (2) как $t_a = \sum a_i$. Последовательность $\{a\}_1^n$ относительно формы (2) образует на множестве $[1, t_a]$ базис над GF_2, если для любого k из $[1, t_a]$ существует единственное представление

$$k =< e_k, a > \tag{3}$$

с некоторым набором $e_k \in GF_2^n$.

Задача о ранце состоит в том, чтобы в рамках представления (3) при заданном базисе $\{a\}_1^n$ и известном k найти $\{e\}_1^n = (e_1, \ldots, e_n)$.

Очевидно, что свойство базисности относительно формы (2) инвариантно к перестановке элементов последовательности $\{a\}_1^n$, поэтому, не ограничивая общности, считаем, что базисная последовательность всегда возрастающая. Основным в теории двоичной связи и двоичного кодирования является базис степеней двойки, однако он не является единственным.

Рассмотрим базис Фибоначчи, определяемый последовательностью $\{f\}_1^n$, $f_1 = 1$, $f_2 = 2$, $f_i = f_{i-1} + f_{i-2}$, где $i \geq 3$. Разложение натурального числа по базису Фибоначчи в общем случае свойством единственности не обладает, однако хорошо известна *теорема Цекендорфа* о том, что любое число k, отличное от нуля, можно единственным образом записать в виде линейной формы (2) над GF_2, при этом в правой части уравнения (2) отсутствуют пары соседних элементов базиса Фибоначчи.

Соответствующие теореме Цекендорфа разложения любого известного числа k по базису с логарифмической сложностью по k реализуются с помощью рекурсивного „жадного“ однопроходного алгоритма.

Лемма 1. Для любого супервозрастающего базиса $\{a\}_1^n$ при больших значениях n асимптотика роста оценивается величиной $O(a^n)$, $a \geq 2$, в частности, если существует решение задачи (3), то плотность укладки удовлетворяет оценке $0 < \rho < 1$.

Асимптотика роста базиса Фибоначчи хорошо известна. Введем обозначение для золотого сечения $\varphi = \dfrac{1+\sqrt{5}}{2}$.

Лемма 2. Для базиса Фибоначчи $\{f\}_1^n$ при больших значениях n асимптотика роста имеет оценку $f_n = O(\varphi^n)$. При этом показатель плотности укладки для задачи (3) оценивается величиной $\rho_f = \dfrac{1}{\log_2 \varphi} \approx 1{,}4404$.

Из лемм 1 и 2 непосредственно выводятся оценки мер Хартли, определяющие количество бит информации, необходимых для создания равномерного двоичного кода с использованием соответствующих базисов над GF_2.

Лемма 3. Число $k \in [1, t_a]$. Тогда информационный битовый объем $|k|$ относительно формы (3) над GF_2 оценивается с помощью меры Хартли:

$$|k| = \lceil \log_a (t_a) \rceil, \tag{4}$$

где прямые полускобки в правой части выражения (4) определяют наименьшее целое число, большее или равное значению логарифма, а основание $a > 1$ определяется асимптотикой роста базисной последовательности $\{a\}_1^n$.

В частности, для базиса Фибоначчи вышеприведенная оценка справедлива при $a = \varphi$. Для базиса, состоящего из степеней двойки, оценка (4) хорошо известна при $a = 2$.

На основе оценки (4) формируются оценки двоичного объема данных, представленных в указанных базисах, т.е. справедливо соотношение

$$w = \frac{A}{B} = \frac{\log_2 2}{\log_2 \varphi} \sim 1{,}44, \tag{5}$$

где A — размер сообщения, бит, — оценка меры Хартли для данных, представленных в двоичном базисе; B — размер пакета, бит, — оценка тех же данных, но в базисе Фибоначчи.

Соотношение (5) можно непосредственно вывести из определения (1), применяя представление (3) для базиса Фибоначчи; в частности, соотношение (5) показывает, что применением базисов типа Фибоначчи позволяет выйти за пределы соотношения $0 < \rho < 1$ при оценке плотности укладки.

Протоколы с общей памятью и рюкзачная криптосистема на основе базиса типа Фибоначчи. Пусть Sender и Receiver — соответственно отправитель и получатель сообщений в двустороннем канале связи. Обозначим через $D = \{d_1, d_2, \ldots, d_n\}$ исходную согласованную совокупность документов, имеющихся и у отправителя, и у получателя. Назовем это множество общей памятью. Соответствующие конфиденциальные протоколы передачи, использующие общую память, предложены в работе [4] для изучения свойств двусторонних SMT-протоколов. Наличие общей памяти далее будет использовано для расширения ключевого пространства алгоритма шифрования и создания параметризованных базисов типа Фибоначчи.

Сумму всех элементов общей памяти обозначим как $d = \sum d_i$. Кроме того, определим над GF_2 вектор $e = (e_i)$ длиной n и рассмотрим все возможные суммы $d_e = \sum (e_i d_i)$, которые имеют 2^n вариантов.

Выберем параметризованный по d_e базис типа Фибоначчи $\{f(d_e)\}$, определяемый последовательностью $f_1(d_e)=1$, $f_2(d_e)=1+d_e$, $f_i(d_e)= f_{i-1}(d_e)+f_{i-2}(d_e)$ при $i>2$. Для нулевого вектора e получим классический базис Фибоначчи, который обозначим как $\{f(0)\}$.

Асимптотика линейно-рекуррентных последовательностей такого типа определяется соответствующим характеристическим уравнением, совпадает с характеристическим уравнением ряда Фибоначчи и, в частности, не зависит от выбора величины d_e. Поэтому для любого параметризованного базиса $\{f(d_e)\}$ оценки согласно леммам 2 и 3 распределяются равномерно по d_e.

Можно показать, что при использовании рекурсивного „жадного“ алгоритма для любого S справедливо единственное представление

$$S = \left(\sum k_i f_i(d_e)\right) + \Delta(S), i = 1,\ldots,l, \tag{6}$$

где $k_i \in \mathrm{GF}_2$ — элементы ключевой последовательности, $f_i(d_e)$ — элементы базиса, Δ — остаточное слагаемое.

Лемма 4. *D* — общая память пары Sender, Receiver в канале связи, вектор $e = (e_i)$, $i = 1...n$, фиксирован, и существует „жадный“ алгоритм разложения числа S в базисе $\{f(d_e)\}$. Тогда любое натуральное S в представлении (6) единственным образом определяется набором $S = \left(k_1, k_2, \ldots, k_l, \Delta\right)$ относительно базиса $\{f(d_e)\}$.

В лемме 2 была приведена оценка величины ρ для базиса Фибоначчи $\{f(0)\}$. Для параметризованных базисов $\{f(d_e)\}$ справедлив следующий результат.

Теорема. Пусть *D* — общая память пары Sender, Receiver в канале связи и $\{f(d_e)\}$ — параметризованный базис Фибоначчи. Тогда:

a) плотность укладки относительно выражения (6) оценивается как

$$\frac{l}{[\log_2 f_l(0) + \log_2(d+1)]} \le \rho \le \frac{l}{[\log_2 f_l(0)]}, \tag{7}$$

где условие

$$d \le 2^{0,31l} - 1 \tag{8}$$

гарантирует нижнюю оценку плотности в базисе (6);

b) для параметризованных базисов Фибоначчи асимптотика роста оценивается величиной

$$f_n(d_e) = O\left(\varphi^n\right) \tag{9}$$

равномерно по параметру d_e, так что при больших значениях *n* результаты лемм 2 и 3 справедливы для выражения (6).

Доказательство теоремы вытекает из соотношений

$$f_i(d_e) = f_{i-1}(0) + f_{i-2}(0)(1 + d_e), \tag{10}$$

$$f_i(0) \le f_i(d_e) \le f_i(1 + d_e),$$

где неравенство следует непосредственно из выражения (1) с учетом (10); для доказательства утверждения „*b*“ имеем с учетом (10) неравенство $f_i(d_e) \le f_i(0) + f_i(0)(1+d_e)$.

Пусть $\{f(d_e)\}$ — параметризованный базис Фибоначчи. Если числовое значение S удовлетворяет оценке $S < t_{f(d_e)}$ равномерно по d_e, то в рамках приведенной схемы, основанной на общей памяти *D* и форме (6), в параметризованном базисе $\{f(d_e)\}$ устанавливается однозначное представление

$$S \leftrightarrow \left(e_1, \ldots, e_n, k_1, k_2, \ldots, k_l, \Delta\right). \tag{11}$$

Очевидно, что наличие общей памяти при больших значениях l в выражении (6) не влияет на асимптотику роста параметризованных базисов и на оценки мер Хартли. При этом особенно важно — разложение по базисам Фибоначчи и выбор самого базиса непрерывно зависят от параметра d_e. В частности, выбор значений $e_1, \ldots, e_n$ не только соответствующим образом расширяет ключевое пространство в схеме шифрования (11), но и в совокупности со значением S однозначно влияет на последующие значения ключа $k_1, k_2, \ldots, k_l, \Delta$.

Алгоритм шифрования.

1. Создание общей памяти и числа d_e: пара Sender и Receiver формирует общую память. Одним из вариантов ее организации является возможность использования широковещательной рассылки сообщений по открытым каналам связи. Таким образом, формируется определенная совокупность документов $D = \{d_1 \ldots d_n\}$, $d_i \neq d_j$. После этого Sender и Receiver выбирают значение вектора $\{e\}_1^n$, который определяет d_e и первые n бит симметричного ключа из правой части выражения (11).

2. Выбор поля Галуа: с помощью документов из общей памяти Sender и Receiver выбирают число $p \sim 2^{64}$ и фиксируют GF_p, в котором будут производиться вычисления. Не ограничивая общности, считаем, что числовое значение секрета S принадлежит выбранному GF_p.

3. Sender создает в соответствии с выбранным значением d_e базис типа Фибоначчи $\{f(d_e)\}$, определяемый последовательностью $f_1(d_e)=1$, $f_2(d_e)=1+d_e$, $f_i(d_e)= f_{i-1}(d_e)+f_{i-2}(d_e)$ при $i>2$, до тех пор, пока $f_i(d_e)$ принадлежат выбранному полю Галуа.

4. Полученная ключевая последовательность $(k_1, k_2, \ldots, k_l, \Delta)$ передается получателю.

Таким образом, в силу выражения (6), лемм 2, 3 и теоремы существует логарифмический по скорости алгоритм разложения S в базисе $\{f(d_e)\}$, дающий на выходе значения $k_1, k_2, \ldots, k_l, \Delta$, определяющие симметричный ключ для шифрования и дешифрования.

Алгоритм дешифрования.

1. Аналогично п. 3 алгоритма шифрования Receiver по значениям вектора $\{e\}_1^n$ вычисляет величину d_e, строит базис $\{f(d_e)\}$.

2. Ключ $\{k_1, k_2, \ldots, k_l, \Delta\}$ по формуле (6) восстанавливает секрет S.

Рассмотрим случай, когда числовое значение S выходит за рамки выбранного поля Галуа. Тогда двоичное значение S делится на блоки одинаковой длины, так чтобы числовое значение каждого блока укладывалось в выбранное поле Галуа, а к каждому отдельно взятому блоку применяются описанные выше алгоритмы шифрования и дешифрования.

Реализация алгоритмов и их статистические свойства. В схеме шифрования и дешифрования на основе представлений (6) и (11) не удается аналитически получить минимальное значение Δ и проследить, как выбор параметризованного базиса влияет на величину Δ в выражении (6). Для уточнения взаимосвязи величин d_e и Δ был проведен эксперимент, содержащий следующие шаги.

1. Формирование $GF_p = \{0, 1, \ldots, p-1\}$ и $p \sim 2^{64}$.

2. Выбор вектора $\{e\}_1^n = (e_1, \ldots, e_n)$, с помощью которого из общей памяти $\{d_1, d_2, \ldots, d_n\}$ формируется параметризованный базис $\{f(d_e)\}$.

3. Расчет значения плотности укладки для полученного параметризованного базиса $\{f(d_e)\}$.

4. Решение аддитивной задача разложения секрета с помощью „жадного“ алгоритма для всех целых чисел от 1 до $p-1$.

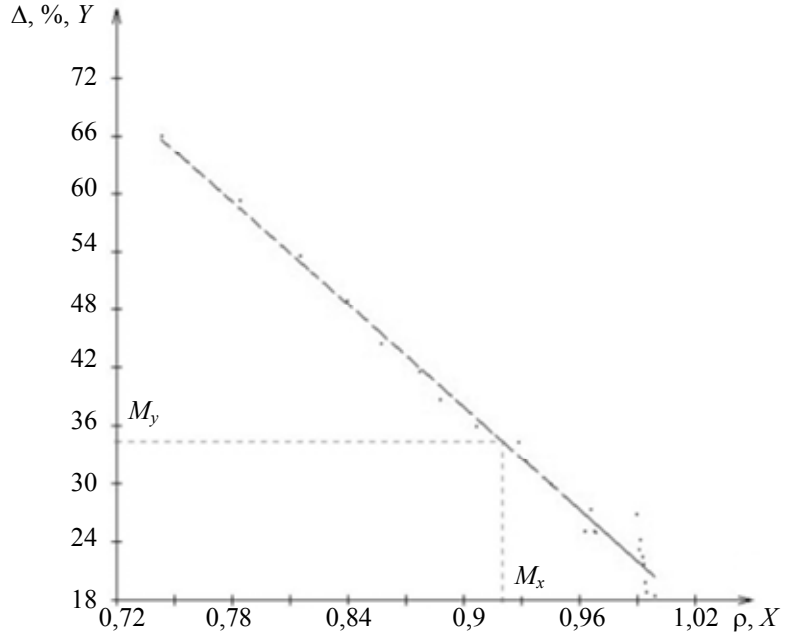
5. Определение количества случаев, когда $\Delta \neq 0$, для всех заданных секретов.

6. Определение коэффициентов ковариации и корреляции для двух заданных множеств X и Y, где $X = \{x_1, x_2, \ldots, x_n\}$ — множество всех значений ρ, $Y = \{y_1, y_2, \ldots, y_n\}$ — множество случаев появления остаточного слагаемого Δ (в процентах).

Согласно полученным значениям коэффициентов ковариации и корреляции существует определенная статистическая зависимость $\Delta(\rho)$, когда $\Delta \neq 0$, график которой приведен на рисунке.

Кроме того, согласно математически рассчитанному на основе результатов экспериментов значению коэффициента корреляции $|R| \sim 0{,}99$ существует весомая статистическая зави-

симость множества Y от множества X: с возрастанием плотности укладки уменьшается количество случаев появления слагаемого Δ при разложении заданного секрета S с помощью „жадного“ алгоритма.



Обсуждение результатов; заключение. Наличие общей памяти в рассмотренной криптосистеме, конечно, выходит за рамки шенноновской модели симметричного шифрования, однако не противоречит криптографической модели безопасности Долева — Яо [5] при соблюдении двух условий: во-первых, при возможности существования общей памяти и, во-вторых, при безопасной передаче первой части ключа $\{e\}_1^n = (e_1, \ldots, e_n)$, определяющей необходимые для параметризованного базиса разложения.

К достоинствам приведенной криптосистемы можно отнести следующие:

— высокая логарифмическая скорость алгоритмов шифрования и дешифрования, а также масштабируемость длины ключа;

— возможность построения симметричного, масштабируемого по размеру ключа блочного, симметричного шифра с несколькими режимами работы алгоритма, в том числе и режимами зацепления блоков;

— возможность построения на основе блочного шифра с помощью стандартной схемы свертки блоков алгоритма хеширования для контроля достоверности передаваемой информации, где хэш-функция для пары Sender, Receiver строго индивидуальна, поскольку зависит от общей памяти этой и только этой пары.

СПИСОК ЛИТЕРАТУРЫ

1. *Merkle D. R., Hellman M.* Hiding information and signatures in trapdoor knapsacks // Information Theory. IEEE Transactions. 1978. P. 525—530.

2. *Odlyzko A. M., Lagarias J. C.* Solving low-density subset sum problems // J. Association Computing Machinery. 1985. Vol. 32, N 1. P. 229—246.

3. *Coster M. J., Joux A., LaMacchia B. A.* et al. Improved low-density subset sum algorithms // Computational Complexity. 1992. N 2. P. 111—128.

4. *Александров А. В.* Устойчивость SMT-протокола к атакам противника в модели безопасности Долева — Яо // Изв. вузов. Приборостроение. 2012. Т. 55, № 8. С. 60—64.

5. *Dolev D., Yao A.* On the security of public key protocols // IEEE Transact. on Information Theory. 1983. Vol. 29, N 2. P. 198—208.

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 14.07.14 г.

Ссылка для цитирования: *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.

SYMMETRIC KNAPSACK CRYPTOSYSTEM WITH SHARED MEMORY AND THE PACKING DENSITY ABOVE UNIT

A. V. Aleksandrov, A. D. Metlinov

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

A variant of symmetric knapsack cryptosystem with packing density above one is proposed. The latter feature makes the system resistant to L^3-attack with polynomial speed characteristic developed by Lagarias and Odlyzko. The proposed algorithms of encryption and decoding are based on shared memory protocols and use Fibonacci-type basis.

Keywords: knapsack cryptosystem, shared memory, L^3-attack, open communication channel, statistical properties, algorithms.

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

Reference for citation: *Aleksandrov A. V., Metlinov A. D.* Symmetric knapsack cryptosystem with shared memory and the packing density above unit // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2015. Vol. 58, N 5. P. 344—350 (in Russian).

DOI: 10.17586/0021-3454-2015-58-5-344-350