ПРИБОРЫ И СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

УДК 003.26
DOI: 10.17586/0021-3454-2019-62-4-320-330

СИММЕТРИЧНАЯ КРИПТОГРАФИЧЕСКАЯ СИСТЕМА С ОБЩЕЙ ПАМЯТЬЮ, ОСНОВАННАЯ НА РЕКУРРЕНТНЫХ БАЗИСАХ В ЗАДАЧЕ УКЛАДКИ РЮКЗАКА*

А. В. Александров, И. И. Сорокин

Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых, 600000, Владимир, Россия
E-mail: alex_izi@mail.ru

В терминах базисов возвратных последовательностей и им соответствующих сигнатур для задачи об укладке рюкзака выделен класс двоичных возвратных базисов $\mathfrak{R}$, характеризующийся более медленным ростом по сравнению с двоичными. Включение базисов в этот класс обеспечивает уход от атаки редукции базиса Костера—Лагариаса—Одлыжко и дает плотность укладки за пределами интервала (0,1). Конструкции таких базисов использованы для построения блочного симметричного алгоритма шифрования, использующего общую память у Отправителя и Получателя в модели К. Шеннона секретной связи. Алгоритм также использует режим зацепления блоков шифртекста и порождает соответствующую хеш-функцию. Приведен аддитивный протокол создания симметричного ключа.

Ключевые слова: *общая память, задача об укладке рюкзака, разреженные рюкзаки, плотность укладки Костера—Лагариаса—Одлыжко, блочный шифр с режимом зацепления блоков, хеш-функция, криптографический протокол*

В работах [1, 2] для задач шифрования предложено использовать линейно-рекуррентные соотношения возвратных последовательностей (по терминологии Алексея Ивановича Маркушевича [3]). Для этого элементы возвратных последовательностей используются в качестве базиса $\{f\}_1^n$ в классической задаче об укладке рюкзака: для произвольного $S \in N$ найти e_i такие, что

$$S = \sum_{i=1}^{n} e_i f_i; \quad e_i = 0 \quad \text{или} \quad 1.$$

Зафиксируем $m \geq 1$ глубину возвратной последовательности. Для порождения элементов базиса $\{f\}_1^n$ задачи о рюкзаке используем рекуррентное соотношение

$$f_n = \sum_{j=1}^{m} C_j f_{n-j},\ n > m,\ C_1 \neq 0,\ C_j \geq 0,\ C_j \in Z,\ f_s = (f_1, ..., f_m), \tag{1}$$

*Работа выполнена при поддержке Российского Фонда Фундаментальных Исследований грант № 18-01-00596 А.

здесь $\left(f_s = (f_1,...,f_m) - m\right)$ — вектор начальных (стартовых) значений, возвратная последовательность определяется сигнатурой $C = "C_1C_2...C_m"$. Случай $m = 1$ и сигнатура $C = "C_1", C_1 > 1$ порождают в (1) оператор умножения на число и, в частности, охватывают базисы позиционных систем счисления с основаниями $k \in N, k > 1, k = C_1, f_s = 1$. Общепринятой двоичной системе счисления в (1) соответствуют параметры $m = 1, C_1 = 2$ и $f_s = 1$.

В общем случае формула (1) охватывает широкий класс возвратных базисов задачи об укладке, в том числе и обобщенных рюкзаков, где каждый элемент базиса в задаче можно использовать более одного раза. Формула (1) описывает также и супервозрастающие возвратные базисы, которые были использованы в качестве основы для построения асимметричной двоичной схемы шифрования Меркла—Хеллмана [4]. Можно показать, что супервозрастающие возвратные базисы Меркла—Хеллмана порождаются соотношением (1) с $C = "C_1C_2...C_m", C_1 \geq 2$. На основе общего представления (1) для обобщенных рюкзаков в статье [5] приведены схема модульного умножения Меркла—Хеллмана с целью создания пары открытого и закрытого ключа в асимметричной криптографической системе и опубликован GeneralKnapsackCode — GKC.

В работах [6, 7] на основе двоичных фиксированных сигнатур $C = "C_1,...,C_m"$, $C_1 = 1$, $C_j = 0$ или 1, $j = 2,...,m$, с произвольными начальными значениями $f_s = (f_1,...,f_m)$ представлен алгоритм симметричного блочного шифра с общей памятью у Отправителя и Получателя. В частности, в работе [6] приведены оценки выходных характеристик (скоростных и частотных) алгоритма блочного шифра для сигнатур вида $C = "11"$, а в [7] выделен класс $\Re$ разреженных возвратных базисов с произвольными стартовыми значениями, характеризующихся медленным ростом по отношению к двоичному базису в задаче о рюкзаке.

В работе [6] показано, что возвратные рюкзаки класса $\Re$, имеющие при больших значениях $n \in N$ асимптотическую плотность

$$\rho_f(n) = \frac{n}{\max_{i=1..n} \log_2 f_i} > 1, \tag{2}$$

позволяют избежать атаки редукции базиса Костера—Лагариса—Одлыжко. Такая атака успешно взламывает супервозрастающие рюкзаки с плотностью $0 < \rho_f(n) < 0,94...$ [8]. Детальному анализу возможностей атаки редукции базиса на супервозрастающие базисы общего порядка для обобщенных рюкзаков посвящена статья [9] .

Задача настоящей статьи — привести полное описание архитектуры алгоритма шифрования для всех возможных двоичных сигнатур класса $\Re$ на основе общего представления вида (1).

Сопоставим выражению (1) характеристический многочлен

$$p(z) = z^m - \sum_{j=1}^{m} C_j z^{m-j} \tag{3}$$

и сопровождающую $(m \times m)$-матрицу

$$\mathrm{A}_f = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 1 \\ C_m & C_{m-1} & ... & ... & ... & \mathrm{C}_1 \end{pmatrix}. \tag{4}$$

Можно показать, что справедливо следующее утверждение.

Утверждение 1

Матрица A_f с начальным вектором $f_s = (f_1,...,f_m)$ описывает алгебраическую процедуру порождения элементов базиса, при этом в базис задачи об укладке включены числа, определенные последней m-м компонентом произведений

$$f_1 = A_f \times f_s, f_2 = A_f^2 \times f_s, \dots f_n = A_f^n \times f_s. \quad (5)$$

Спектр матрицы A_f над полем C комплексных чисел $\sigma\left(\mathrm{A}_f\right) = \{\lambda_1,...,\lambda_r\}, r \le m$ совпадает с множеством корней характеристического многочлена (2) с учетом их кратностей.

Обозначим корни уравнения (3) $\lambda_1,\dots,\lambda_r$ кратности $\ell_1,...,\ell_r$, $\ell_1 + ... + \ell_r = m$. Так как коэффициенты сигнатуры $C = "C_1,...,C_m"$ в (1) целые, то $p(\bar{z}) = \overline{p(z)}$, откуда непосредственно можно заключить, что для любого комплексного корня λ_i кратности ℓ_i существует комплексно-сопряженный корень $\overline{\lambda_i}$ той же кратности.

Утверждение 2. Пусть сигнатура в (1) состоит из неотрицательных целых $C_1 \ne 0,\ C_j \ge 0,\ C_j \in Z$. Тогда характеристический многочлен (3) имеет в наборе корней наибольший по модулю вещественный положительный простой корень $\lambda \in R, |\lambda| \ge |\lambda_j|,\ j = 1,\dots,r$, обозначим его $\varphi_m(C), C = "C_1 \dots C_m"$. Все оставшиеся корни многочлена (3) расположены в круге $|z| \le q < \varphi_m(C)$.

Регулярные и возмущенные базисы

Определение. Последовательность $\{f\}_1^n$ в (5) называется *регулярным возвратным базисом задачи о рюкзаке,* если начальные значения $f_s = \left(f_{s1},...,f_{sm}\right)$ таковы, что в (5) $f_1 = 1$, в противном случае базис называется *возмущенным возвратным*. В этом случае можно положить $f_1 = 1 + d$, где d — начальное возмущение.

Для регулярных базисов справедлива следующая теорема.

Теорема 1 [2]**.** Пусть базис $\{f\}_1^n$ регулярен и отношение (1) имеет сигнатуру $C = "C_1,...,C_m",\ C_1 \ne 0,\ C_i \ge 0,\ C_i \in Z$. Тогда любое натуральное число *S* имеет единственное представление

$$S = \left[\alpha_p \alpha_{p-1} ... \alpha_0\right]_f = \sum_{i=1}^{p} \alpha_{i-1} f_i \quad (6)$$

в рюкзачном базисе $\{f\}_1^n,\ \alpha_i \in N,\ \alpha_i < \max C_j,\ C_j \in C = "C_1 ... C_m"$ с дополнительными ограничениями на комбинации соседних цифр, которые определяются по значениям сигнатуры $C = "C_1,...,C_m"$. Алгоритмическая сложность жадного алгоритма вычисления (6) оценивается величиной $O(\log S)$.

Единственность представления понимается по отношению к жадному рекурсивному алгоритму, просматривающему опорные точки $\{\nu_{i,n}\}$, однозначно определяемые по $\{f\}_1^n$. Ограничения на комбинации цифр следующие: последовательность цифр и их комбинации (кортежей) в (6) не содержит комбинаций, лексикографически больших либо равных сигнатуре $C = "C_1,...,C_m"$.

Доказательство теоремы громоздко, поэтому обозначим только его этапы. Частные случаи теоремы 1 для последовательности Фибоначчи доказаны Цекендорфом, а для единичных сигнатур вида $C = "11...1"$ — Н. Утгофф.

Первый этап. Следуя работе [2], сопоставим сигнатуре $C = "C_1C_2...C_m"$ число $A = \sum_i C_i$ и соответственно базовый набор строк $B = \{St_0, \cdots St_{A-1}\}$ по следующему правилу:

$St_0 = 0$, для $i > 0$, St_i состоят из всех строк $1 \le l \le m$, таких, что $0 \le St_i < C_1 \ldots C_l$ в лексикографическом порядке.

В общем случае множество $B = \{St_0, \cdots St_{A-1}\}$ обладает свойством префикса. Приведем примеры:

Пример 1. Базис Фибоначчи Пусть $C = "11"$ Тогда $B = \{St_0 = 0, St_1 = 10\}$

Пример 2. Обобщенный базис Фибоначчи 3-го порядка

Пусть $C = "111"$ Тогда $B = \{St_0 = 0, St_1 = 10, St_2 = 110\}$

Пример 3. Обобщенный базис Фибоначчи *m*-го порядка

Пусть $C = "\underbrace{111\ldots1}_{m}"$ Тогда $B = \left\{ St_0 = 0, St_1 = 11, St_2 = 110, \ldots, St_{m-1} = \underbrace{1\ldots10}_{m-1} \right\}$.

Пример 4.

Пусть $C = "2401"$. $A = 7$

Тогда $B = \{0,1, 20, 21, 22, 23, 2400\}$

Для базового набора строк $B(C_1 \ldots C_m)$ на множестве натуральных чисел определим опорное множество точек $St\{\nu_{i,n}\}$ согласно следующему правилу:

Если $St_i \in B, St_i = C_1C_2 \ldots C_{k-1}l$, где $0 \le l < C_k$, то для любого элемента базиса $\{f_n\}$ в (1) положим $\nu_{i,n} = C_1 f_n + C_2 f_{n-1} + \ldots C_{k-1} f_{n-k+2} + l\, f_{n-k+1}$. При $n<m$, определить $\nu_{i,n}$ можно по соответствующим начальным значениям.

Очевидно, что для фиксированного n семейство $\{\nu_{i,n}\}$ монотонно $\nu_{1,n} < \nu_{2,n} < \ldots < \nu_{A-1,n} < \nu_{2,n+1}$.

Второй этап. Для базового набора строк $B(C_1 \ldots C_m)$ на множестве натуральных чисел определим опорное множество точек $St\{\nu_{i,n}\}$ согласно следующему правилу:

Если $St_i \in B, St_i = C_1C_2 \ldots C_{k-1}l$, где $0 \le l < C_k$, то для любого элемента базиса $\{f_n\}$ в (1) положим $\nu_{i,n} = C_1 f_n + C_2 f_{n-1} + \ldots C_{k-1} f_{n-k+2} + l\, f_{n-k+1}$. Очевидно, что для фиксированного n семейство $\{\nu_{i,n}\}$ обладает монотонным свойством $\nu_{1,n} < \nu_{2,n} < \ldots < \nu_{A-1,n} < \nu_{2,n+1}$.

Третий этап. Выполнение жадного алгоритма, просматривающего элементы последовательности $\{\nu_{i,n}\}$ сверху вниз.

```
Function H (S, m: integer; C: string) recursive;
 {If S<f1 then exit;
R:=""; i:=1;j:=1;
while (νi,j≤ S) do {
while (j<A) do {
get fi,νi,j;
```

```
j:=j+1; i:=i+1}
j:=1 }
R:=R+St_i
S:=S-ν_i,j
}
Return H (R: integer)
```

Можно строго доказать, что алгоритм для регулярных базисов завершает свою работу с финальным значением S=0.

Заметим, что для базиса Фибоначчи значения $\{\nu_{i,n}\}$ совпадают со значениями $\{f_n\}$, и теорема 1 совпадает с кодом Цекендорфа. Это было использовано в [1, 6] для возмущенных базисов.

Следствие теоремы 1. Пусть начальный вектор в (5) произволен, и базис задачи о рюкзаке построен так же, как и в теореме 1, с той разницей, что $f_1 = 1 + d$,
тогда

$$S = \left[\alpha_p \alpha_{p-1} \ldots \alpha_0\right]_f + \Delta(d, f) = \sum_{i=1}^{p} \alpha_{i-1} f_i + \Delta(d, f), \tag{8}$$

с теми же условиями лексикографической ограниченности на комбинации цифр, как и в условии теоремы 1. Однозначность представления (8) понимается по отношению к выходным значениям Н-алгоритма, при этом значение $\Delta(d, f)$ определяется ненулевым значением по завершении работы Н-алгоритма.

Обозначим $\Re$ класс возвратных базисов (5), для которых в асимптотике при больших n в (5) $\rho_f(n) > 1$. Можно показать [7]: это при больших значениях n равносильно тому, что

$$\rho_f(n) > 1 \Leftrightarrow 1 < \varphi_m(C) < 2 .$$

$\Re$ естественно называть классом базисов разреженных рюкзаков, поскольку двоичные представления натурального числа в них содержат в среднем в $\rho_f(n)$ раз больше битов по сравнению с аналогичными битовыми представлениями в двоичной системе счисления, для которой $\{f_n\} = 2^{n-1}$, $\varphi_m(C = "2") = 2$, и равномерно по n: $\rho_f(n) = 1$.

Из описания класса $\Re$ разреженных рюкзаков, порожденных возвратными последовательностями (1), получим теорему.

Теорема 2. По отношению к двоичным кортежам класс $\Re$ разреженных возвратных базисов классической задачи о рюкзаке описывается следующими условиями:

$$m \geq 1,\ C_1 = 1,\ C_j \in \{0,1\},\ 1 < j \leq m.$$

Асимптотика роста последовательности $\{f\}_1^n$ в (5) при больших n определяется оценками

$$n \geq n_0;\ f_n = O\left(\varphi_m^n(C)\right), \text{ а также } \frac{f_{n+k}}{f_n} \approx \varphi_m^k(C), \quad k = 1, 2, \ldots , \tag{9}$$

При больших n значение $\rho_f = \dfrac{1}{\log_2 \varphi_m(c)}$ не зависит от начальных значений рекуррентности (1).

Следствие теоремы 2. Пусть базис $\{f\}_1 \in \Re$ является возмущенным. Тогда для любой $C = "C_1,...,C_m" \in \Re$, любого заданного возмущения d существует такое $n_0(C,d) \in N$ (может быть достаточно большое), что $\forall n > n_0\ \rho_f(n) > 1$.

Заметим, что для регулярных базисов следствие теоремы 2 несправедливо.

Проиллюстрируем этот факт графиками изменения плотности с увеличением n для знаменитой рекуррентной последовательности Фибоначчи. На рис. 1 приведен график изменения плотности со стартовым возмущением d=50, на рис. 2 — график изменения плотности классического базиса Фибоначчи.

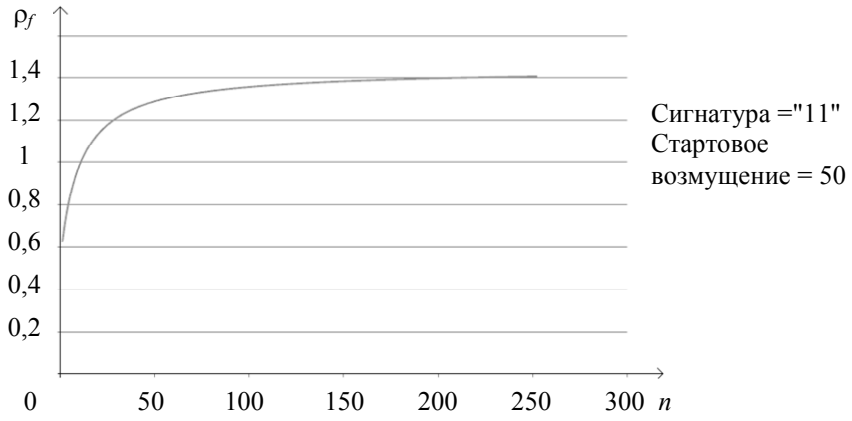

Рис. 1

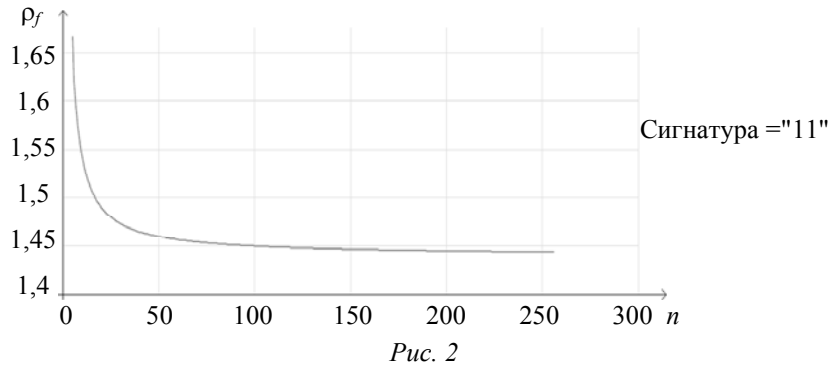

Рис. 2

Пусть $D = \{d_1...d_n\}$ — заранее согласованное множество данных, находящееся на устройствах отправителя А и получателя В в модели К. Шеннона секретной связи. Назовем множество $D = \{d_1...d_n\}$ общей памятью криптографической системы. В качестве предварительного ключа выберем вектор $E = \{e_1...e_n\}$, $e_i \in GF_2$; $E \neq 0$, и сформируем ключевой параметр

$$d_e = \sum_{i=1}^{n} e_i d_i,$$

зададим $m \geq 2$ и сигнатуру $C \in \Re$. Обозначим S — открытый текст произвольной длины относительно двоичной меры Хартли. Зададим конкатенацию блоков двоичного представления $S = S_1 \| S_2 \| ... \| S_l$. Длина каждого блока, за исключением последнего, фиксирована. Для каждого блока S_i применим представление (8) с ключевым значением $d_e = \sum_{i=1}^{n} e_i d_i$, обозначим в $F_{d_e}^{+1}(S_i) = \left(\alpha_p \alpha_{p-1} ... \alpha_0, \Delta_2\right)$ и в качестве разделителя между $\alpha_p \alpha_{p-1} ... \alpha_0$ и Δ_2 используем сигнатуру, лексикографически большую, чем выбрана для построения базиса в (8), и той же дли-

ны. Согласно следствию теоремы 2, можно считать, что битовые размеры двоичных форм S_i, и $F_{d_e}^{+1}(S_i) = \left(\alpha_p \alpha_{p-1} ... \alpha_0, \Delta_2\right)_i$ равны.

С учетом смещенной статистики нулей и единиц в форме (8), наследуемой из теоремы 1, используем режим зацепления блоков, где блок открытого текста S_i, кроме вектора инициализации побитно складывается по модулю 2 с результатом шифрования предыдущих блоков. Пусть B_0 — вектор инициализации. Положим

$$B_i = F_{de}^{+1}(S_i \oplus B_{i-1}), \quad i = 1, 2...l, \tag{10}$$

и выходными значениями алгоритма шифрования считаем конкатенацию блоков

$$F_{d_e}^{+1}(S) = B = B_1 \| B_2 \| ... \| B_l. \tag{11}$$

Алгоритм шифрования представлен на рис. 3, *а* ($F_{de}^{+1}(B_i)$ — блок зашифрованного текста; S_i — открытый текст; $\oplus$ — XOR).

Легко показать, что алгоритм дешифрования происходит по схеме, представленной на рис. 3, *б* (функция дешифрования $F_{de}^{-1}(F_{de}^{+1}(B_{i+1}))$ определяется формулой суммирования в (8); $F_{de}^{+1}(B_i)$ — блок зашифрованного текста; S_{i+1} — блок открытого текста; $\oplus$ — XOR).

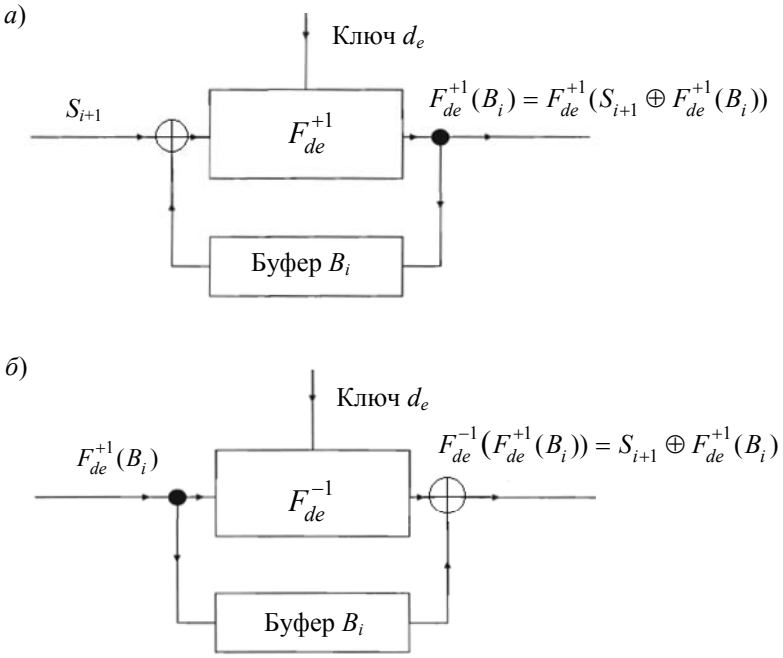

Рис. 3

Наконец, свяжем с (11) хеш-функцию $H_{d_e}(S) = B_l$, которую легко получить на стадии шифрования в режиме сцепления блоков. С учетом сцепления блоков, функция $H_d(S) = B_l$ зависит от всех битов значения *S*. Сформулируем, основываясь на работе [7], теорему.

Теорема 3. Пусть $e = (e_1 ... e_n) \neq 0$ — набор битов, определяющий для $d_e = \sum_{i=1}^{n} e_i d_i$ выбор подмножества общей памяти для пары (Отправитель, Получатель). $\{f_{de}\}_1^n$ — разреженный базис симметричной рюкзачной криптосистемы, и $H_{de}(S)$ — соответствующая ей хеш-функция, полученная XOR-сверткой из блочного шифра $F_k(S)$, построенного на базисе

$\{f_{de}\}_1^n$. Тогда: $H_{de}(S)$ — односторонняя хеш-функция. Поскольку $H_{de}(S)$ — однозначно идентифицирует пару (Отправитель, Получатель) за счет выбора параметра d_e, то в случае передачи пакета $(S, H_{de}(S))$ в канале связи функция $H_{de}(S)$ контролирует целостность значения *S*, в частности эффективно противостоит атакам подмены текста *S* в канале связи, в том числе атакам типа Man in the middle (MITM).

Противник в канале связи может находиться в пассивном *PP* и активном *PA* режимах. Первый режим соответствует прослушиванию всего трафика между абонентами A и B в модели Шеннона секретной связи. *PA* означает, что противник, пользуясь слабостью аутентификации, может заменять сообщения, проводя между A и B атаку MITM в модели безопасности Долев—Яо [12].

Пусть $D = \{d_1 ... d_n\}$ — согласованное заранее множество, находящееся на устройствах A и B. В качестве предварительного ключа выберем вектор $E = \{e_1 ... e_n\}$, $e_i \in GF_2$; $E \neq 0$.

Следуя обозначениям [11], приведем аддитивный протокол создания сеансового ключа. Далее *m* — размер блока в блочном шифре, ключ d_e принимает значения k_{AB} или k_{BA}, где первый символ индекса показывает, на какой стороне в канале связи вырабатывается симметричный ключ.

Протокол 1:

1) $\mathrm{A} \to \mathrm{B} : E = \{e_1 ... e_n\} \neq 0$;

2) $\mathrm{A} : k_{\mathrm{AB}} = \sum e_i d_i \bmod 2^m$;

3) $\mathrm{B} : k_{\mathrm{BA}} = \sum e_i d_i \bmod 2^m$.

Можно показать, что *PP*, перехватывая вектор *E,* не получает информации о значении сеансового ключа $k_{\mathrm{AB}} = k_{\mathrm{BA}}$, так как не имеет доступа к общей памяти. Нами построены такие примеры значений $D = \{d_1 ... d_n\}$, при которых множества сеансовых ключей, которые можно получить в алгоритме 1, не пересекается с множеством предварительных ключей, отличных от нуля. Из этого, в частности, следует, что предварительный ключ можно передавать в канале связи открыто.

Для противодействия активному противнику, воспользуемся уникальностью хеш-функции $H_{d_e}(S)$ теоремы, модифицируя алгоритм 1. Пусть d_e — предыдущий сеансовый ключ, и верхний символ в обозначении хеш-функции $H^X{}_{d_e}(S)$ указывает, на какой стороне вырабатывается это значение участником протокола $X \in \{\mathrm{A},\mathrm{B}\}$. Приведем алгоритм формирования нового симметричного ключа.

Протокол 2:

1) $\mathrm{A} \to \mathrm{B} : E = \{e_1 ... e_n\} \,||\, H^{\mathrm{A}}_{d_e}(E)$;

2) $\mathrm{B} : H^{\mathrm{B}}_{d_e}(E)$; если $H^{\mathrm{B}}_{d_e}(E) \neq H^{\mathrm{A}}_{d_e}(E)$, то стоп;

3) $\mathrm{A} : k_{\mathrm{AB}} = \sum e_i d_i \bmod 2^m$; $H^{\mathrm{A}}_{d_e}(k_{\mathrm{AB}})$;

4) $\mathrm{B} : k_{\mathrm{BA}} = \sum e_i d_i \bmod 2^m$; $H^{\mathrm{B}}_{d_e}(k_{\mathrm{BA}})$;

5) $\mathrm{A} \to \mathrm{B} : H^{\mathrm{A}}_{d_e}(k_{\mathrm{AB}})$;

6) B: если $H^{\mathrm{A}}_{d_e}(k_{\mathrm{AB}}) = H^{\mathrm{B}}_{d_e}(k_{\mathrm{BA}})$, то $d_e \leftarrow k_{\mathrm{BA}}$, иначе стоп;

7) $\mathrm{B} \to \mathrm{A}$:OK;

8) A : если OK, то $d_e \leftarrow k_{\mathrm{AB}}$.

Легко видеть, что такая модификация протокола 1, в силу теоремы 3, позволяет эффективно противостоять *PA* в канале связи. В самом деле, *PA* на 1-м шаге алгоритма 2 может легко изменить вектор E, однако не может построить функцию $H_{d_e}(E)$, так как не имеет доступа к общей памяти в модели Долев—Яо, хотя и знаком с ее описанием. В то же время абонент B, вычисляя $H^{\mathrm{B}}_{d_e}(E)$, легко может обнаружить факт подмены предварительного ключа $E = (e_1 ..., e_n)$, на 2-м шаге. Противник также может совершить перехват и подмену $H_{d_e}(k_{\mathrm{AB}})$ на 5-м шаге, разрушая протокол создания симметричного ключа, однако этот факт также будет обнаружен без выработки значения OK на 6-м шаге.

Представленная криптографическая система, имеет масштабируемые сменяемые компоненты — общую память, глубину рекуррентности (1), и сигнатуру класса $\Re$. Эти компоненты должны быть недоступны противнику, так же как и симметричный ключ d_e. Именно при таких условиях функции $F^{+1}_{d_e}(S_i) = \left(\alpha_p \alpha_{p-1} ... \alpha_0, \Delta_2\right)_i$ в (8), (11) и соответствующая хеш-функция $H_{de}(S)$ становятся трудновычислимыми для противника, или односторонними. С учетом использования общей памяти, система ограничена в использовании, имеет парный долговременный характер по отношению к отправителю A и получателю B.

Приведенный протокол (13) порождения симметричного ключа на основе общей памяти, хеш-функции $H_{d_e}(S)$ и предварительного ключа сравнительно нов, однако, в отличие от классического протокола Диффи—Хеллмана, эффективно противостоит атакам MITM, проводимой AP в канале связи. Нами рассматриваются варианты встраивания общей памяти и протокола 2 в работу стандартных блочных шифров, участвующих в обеспечении TLS-протоколов передачи данных, что было уже проделано для частного случая сигнатур $C =$ "11" в статье [13].

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., and Webb W.* A Knapsack-Like Code Using Recurrence Sequence Representations // Fibonacci Quarterly. 2015. Vol. 53, N 1. P. 24—33.

3. *Маркушевич А. И.* Возвратные последовательности. М.: Наука, 1983. 48 с.

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

5. *Hamlin N.* Number in Mathematical Cryptography // Open Journal of Discrete Mathematics. 2017. N 7. P. 13—31.

6. *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.

7. *Александров А. В.* Класс разреженных рюкзаков в задаче укладки рюкзака и его некоторых приложениях в секретной связи // Динамика сложных систем — XXI век. 2016. Т. 10, № 4. С. 71—77.

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

9. *Мурин Д. М.* Модификация метода Лагариаса—Одлыжко для решения обобщенной задачи о рюкзаке и систем задач о рюкзаках // Прикладная дискретная математика. 2013. № 2(20). С. 91—100.

10. *Marden M.* Geometry of Polynomials. Providence, RI: American Mathematical Society. 1966. 243 p.

11. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.

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

13. *Метлинов А. Д.* Модификация протокола TLS на основе разреженной криптосистемы с общей памятью // Изв. вузов. Приборостроение. 2018. Т. 6, № 11. С. 60—64.

Сведения об авторах

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

Илья Игоревич Сорокин — магистрант; ВлГУ, кафедра информатики и защиты информации; E-mail: night7117@gmail.com

Поступила в редакцию
26.11.18 г.

Ссылка для цитирования: *Александров А. В., Сорокин И. И.* Симметричная криптографическая система с общей памятью, основанная на рекуррентных базисах в задаче укладки рюкзака // Изв. вузов. Приборостроение. 2019. Т. 62, № 4. С. 320—330.

SYMMETRICAL CRYPTOGRAPHIC SYSTEM WITH A SHARED MEMORY BASED ON RECURRENT BASES IN THE TASK OF KNAPSACK PACKING

A. V. Aleksandrov, I. I. Sorokin

Vladimir State University, 600000, Vladimir, Russia
E-mail: alex_izi@mail.ru

In terms of the bases of return sequences and their corresponding signatures for the backpacking problem, a class of binary return bases characterized by a slower growth compared to the binary ones is distinguished. The inclusion of bases in this class provides a departure from attack of reduction of the basis of Koester—Lagarias—Odlyzko and gives a packing density outside the interval (0,1). The constructions of such bases are employed to develope a symmetric block encryption algorithm that uses shared memory of sender and recipient in Shannon model of secret communication. The algorithm also uses the chaining mode of the ciphertext blocks and generates the corresponding hash function. An additive protocol for creating a symmetric key is given.

Keywords: shared memory, knapsack packing problem, sparse knapsacks, Koester—Lagarias—Odlyzko packing density, block cipher with block engagement mode, hash function, cryptographic protocol

REFERENCES

1. Aleksandrov A.V., Metlinov A.D. *Journal of Instrument Engineering*, 2015, no. 5(58), pp. 344–350. (in Russ.)
2. Hamlin N., Krishnamoorthy B., and Webb W. *Fibonacci Quarterly*, 2015, no. 1(53), pp. 24–33.
3. Markushevich A.I. *Vozvratnyye posledovatel'nosti* (Return Sequences), Moscow, 1983, 48 p. (in Russ.)
4. Merkle D.R., Hellman M. *Information Theory, IEEE Transactions*, 1978, pp. 525–530.
5. Hamlin N. *Open Journal of Discrete Mathematics*, 2017, no. 7, pp. 13–31.
6. Aleksandrov A.V., Metlinov A.D. *Journal of Instrument Engineering*, 2017, no. 1(60), pp. 5-9.
7. Aleksandrov A.V. *Dynamics of Complex Systems – XXI century*, 2016, no. 4(10), pp. 71–77. (in Russ.)
8. Coster M.J., Joux A., LaMacchia B.A. et al. *Computational Complexity*, 1992, no. 2, pp. 111–128.
9. Murin D.M. *Prikladnaya Diskretnaya Matematika*, 2013, no. 2(20), pp. 91–100. (in Russ.)
10. Marden M. *Geometry of Polynomials*. Providence, RI: American Mathematical Society, 1966, 243 p.
11. Cheremushkin A.V. *Kriptograficheskiye protokoly. Osnovnyye svoystva i uyazvimosti* (Cryptographic Protocols. Key Features and Vulnerabilities), Moscow, 2009, 272 p. (in Russ.)
12. Dolev D., Yao A. *IEEE Transact on Information Theory*, 1983, no. 2(29), pp. 198–208.
13. Metlinov A.D. *Journal of Instrument Engineering*, 2018, no. 1(61), pp. 60–64. (in Russ.)

Data on authors

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

Ilya I. Sorokin — Master Student; Vladimir State University, Department of Informatics and Information Security; E-mail: night7117@gmail.com

For citation: Aleksandrov A. V., Sorokin I. I. Symmetrical cryptographic system with a shared memory based on recurrent bases in the task of knapsack packing. *Journal of Instrument Engineering*. 2019. Vol. 62, N 4. P. 320—330 (in Russian).

DOI: 10.17586/0021-3454-2019-62-4-320-330