Щуренко А.В.
Ульяновский государственный университет

В данной статье предлагается алгоритм симметричного шифрования, основанный на применении ортогональных финитных функций (ОФФ). Теория ОФФ-базисов и ее применение в алгоритмах численных методов изложены в [1], [2], [3].

Основная идея предлагаемого алгоритма заключается в аппроксимации многочлена, содержащего в себе исходное сообщение, с использованием функций ОФФ-базиса. После представления блока информации в виде многочлена проводится его аппроксимация с помощью ОФФ-базиса в выбранных узлах сетки, затем вычисляются значения ОФФ-аппроксимации, после чего результат шифрования представляется в виде блока ОФФ-аппроксимации. Информация о координатах точек, в которых проводилась аппроксимация, позволяет восстановить исходный многочлен и содержащееся в нем сообщение.

Операции по получению коэффициентов аппроксимации проводятся в кольце многочленов степени, не превосходящей n, над кольцом вычетов $\mathbb{Z}_N$, элементы которого образуют полную систему вычетов по модулю N. При этом n – четное число, равное длине сообщения, а N – простое число. Сообщение длины, большей n, при шифровании следует разбить на блоки длины n.

Количество функций в используемой части ОФФ-базиса должно быть не меньше n. Для выполнения этого требования на равномерной сетке $x_1 < x_2 < \cdots < x_l$ $(l \geq 2n)$ с целыми неотрицательными x_i и шагом h задается набор $t = (t_1, t_2, \dots, t_n)$, состоящий из n точек $t_i = (x_i, y_i)$, где все x_i $(i = \overline{1,n})$ попарно различны. При этом все y_i принадлежат $\mathbb{Z}_N$, но их точные значения вычисляются уже в процессе шифрования. Далее задается соответствующий набор ОФФ $f = (f_1, f_2, \dots, f_n)$. В качестве примера берутся ОФФ, являющиеся частным случаем [1, с.11].

Пусть A - множество всех открытых текстов, K - множество выбранных случайным образом векторов k, а B - множество всех шифртекстов.

Запишем исходное сообщение $a \in A$ в векторном виде:

$$a = (a_1, a_2, \dots, a_n).$$

Пусть также выбран вектор $k \in K$, $k = (k_1, k_2, \dots, k_n)$ и значения β, h и x_1, определяющие используемую сетку. При этом все компоненты k попарно различны, а также $\forall i = \overline{1, n/2}$:

$$\begin{cases} k_m \in [x_{j_i};\ x_{j_i+1}], & m = 2i-1, 2i \\ k_m \notin [x_{j_i-1};\ x_{j_i+2}], & m \neq 2i-1, 2i' \end{cases}$$

где x_{j_i} и x_{j_i+1} $(j_i \in \mathbb{Z}_l,\ j_{i+1} \in \mathbb{Z}_l)$ - узлы сетки, между которыми лежат k_{2i-1} и k_{2i}.

Для большей определенности в предлагаемом алгоритме пусть $k_{2i-1} \in [x_{j_i};\ x_{j_i} + h/2]$, $k_{2i} \in [x_{j_i} + h/2;\ x_{j_i+1}]$.

При $k_{2i-1} \in [x_{j_i};\ x_{j_i} + h/2]$, $k_{2i} \in [x_{j_i} + h/2;\ x_{j_i+1}]$, для исключения многозначности результатов расшифрования, пусть

$$(\beta - 1)(k_{2i-1} - x'_{2i-1}) > \beta(x'_{2i} - k_{2i}).$$

Обозначим x' вектор узлов сетки, используемых при аппроксимации многочлена. При этом $x'_{2i-1} = x_{j_i}$, $x'_{2i} = x_{j_i+1}$ $(i = \overline{1, n/2})$. В качестве f возьмем набор $f = (f_1, f_2, \dots, f_n)$, где каждая f_i – ОФФ-функция, соответствующая узлу x'_i. Вектор (k, β, h, x_1) является ключом. Вектор $b \in B$, $b = (b_1, b_2, \dots, b_n)$ является шифртекстом.

Алгоритм шифрования состоит из следующих четырех шагов.

Шаг 1. Вектору a сопоставляется многочлен:

$$a(x) = a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1}.$$

Шаг 2. Проводится аппроксимация многочлена $a(x)$ с помощью функций f_i. При этом аппроксимирующая функция $F(x)$ будет являться суммой произведений ОФФ-функций f_i и соответствующих коэффициентов аппроксимации r_i:

$$F(x) = \sum_{i=1}^{n} r_i f_i(x).$$

Коэффициент каждой i-й ОФФ-функции равен значению многочлена в точке с координатой x'_i. Таким образом, значения вектора коэффициентов аппроксимации $r = (r_1, r_2, \dots, r_n)$ находятся по формуле

$$r_i = a(x'_i) \ (mod\ N).$$

Шаг 3. Формируется вектор $b = (b_1, b_2, \dots, b_n)$, где каждая компонента рассчитывается по формуле $b_i = F(k_i), i = \overline{1, n}$.

Поскольку для всех $i = \overline{1, n/2}$ точки k_{2i-1} и k_{2i} лежат между узлами x'_{2i-1} и x'_{2i}, то значения аппроксимирующей функции в данных точках равны линейным комбинациям соответствующих значений f_{2i-1} и f_{2i}:

$$F(k_{2i-1}) = r_{2i-1} * f_{2i-1}(k_{2i-1}) + r_{2i} * f_{2i}(k_{2i-1}),$$
$$F(k_{2i}) = r_{2i-1} * f_{2i-1}(k_{2i}) + r_{2i} * f_{2i}(k_{2i}).$$

Отсюда

$$f_{2i-1}(k_{2i-1}) = 2(\beta - 1)(k_{2i-1} - x'_{2i-1})/h + 1,$$
$$f_{2i}(k_{2i-1}) = 2\alpha(x'_{2i-1} - k_{2i-1})/h,$$
$$f_{2i-1}(k_{2i}) = 2\beta(x'_{2i} - k_{2i})/h,$$
$$f_{2i}(k_{2i}) = 2(\alpha + 1)(k_{2i} - x'_{2i})/h + 1.$$

Таким образом,

$$F(k_{2i-1}) = r_{2i-1} * \left(\frac{2(\beta - 1)(k_{2i-1} - x'_{2i-1})}{h} + 1\right) + r_{2i} * \left(\frac{2(\beta - 1)(x'_{2i-1} - k_{2i-1})}{h}\right)$$
$$= \frac{2(\beta - 1)(k_{2i-1} - x'_{2i-1})}{h} * (r_{2i-1} - r_{2i}) + r_{2i-1},$$

(1)

$$F(k_{2i}) = r_{2i-1} * \left(\frac{2\beta(x'_{2i} - k_{2i})}{h}\right) + r_{2i} * \left(\frac{2\beta(k_{2i} - x'_{2i})}{h} + 1\right)$$
$$= \frac{2\beta(x'_{2i} - k_{2i})}{h} * (r_{2i-1} - r_{2i}) + r_{2i}.$$

Шаг 4. Вектор b, являющийся шифртекстом, записывается в виде:

$$b = (\lfloor F(k_1) \rceil, \lfloor F(k_2) \rceil, \dots, \lfloor F(k_n) \rceil).$$

Алгоритм расшифрования заключается в нахождении коэффициентов исходного многочлена $a(x)$ на основе вектора шифртекста b, известных значений k β и, а также параметров сетки h и x_1. Запишем шифртекст $b \in B$ в векторном виде:

$$b = (b_1, b_2, \dots, b_n),$$

где n – четное натуральное число. Пусть известен вектор $k \in K$, $k = (k_1, k_2, \dots, k_n)$, использованный при шифровании, а также значения β, h и x_1.

Шаг 1. Вектору a исходного сообщения при шифровании был сопоставлен многочлен

$$a(x) = a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1}.$$

При проведении аппроксимации $a(x)$ с помощью ОФФ-функций f в точках x' получился вектор коэффициентов аппроксимации $r = (r_1, r_2, \dots, r_n)$, где все компоненты находятся по формуле

$$r_i = a(x_i)\ (mod\ N).$$

Для нахождения значений вектора r при расшифровании значения вектора b берутся парами, и первый элемент в паре складывается с элементом, обратным второму, то есть находятся значения $b'_i = b_{2i-1} - b_{2i}$ $(i = \overline{1, n/2})$**:**

$$b'_i = \left(\frac{2(\beta - 1)(k_{2i-1} - x'_{2i-1})}{h} - \frac{2\beta(x'_{2i} - k_{2i})}{h} + 1 \right) * (r_{2i-1} - r_{2i});$$

Далее находятся значения $(r_{2i-1} - r_{2i})$ по формуле

$$(r_{2i-1} - r_{2i}) = \left\lfloor \frac{b'_i}{2(\beta - 1)(k_{2i-1} - x'_{2i-1}) \,/\, h \; - 2\beta(x'_{2i} - k_{2i}) \,/\, h + 1} \right\rfloor$$

.

Шаг 2. Находятся значения вектора r. Для этого используется известная формула (1)

$$b_{2i} = \lfloor F(k_{2i}) \rceil = \left\lfloor \frac{2\beta(x'_{2i} - k_{2i})}{h} * (r_{2i-1} - r_{2i}) \right\rfloor + r_{2i},$$

где $i = \overline{1, n/2}$.

$$r_{2i} = \left(b_{2i} - \left\lfloor \frac{2\beta(x'_{2i} - k_{2i})}{h} * (r_{2i-1} - r_{2i}) \right\rfloor \right);$$

$$r_{2i-1} = (b_i + r_{2i}).$$

Шаг 3. По значениям вектора k определяются все x_i' ($k_{2i} \in [x'_{2i-1}; x'_{2i}], i = \overline{1, n/2}$). Решение системы уравнений

$$\begin{cases} a(x_1') = r_1 \\ a(x_2') = r_2 \\ \dots \\ a(x_n') = r_n \end{cases} \quad (2)$$

дает коэффициенты многочлена $a(x)$.

Решить данную систему можно, применив сеточные полиномы Лагранжа для набора точек $t = ((x_1', r_1), (x_2', r_2), \dots, (x_n', r_n))$. Тогда $a(x)$ будет иметь вид:

$$a(x) = \sum_{i=1}^{n} r_i l_i(x),$$

где

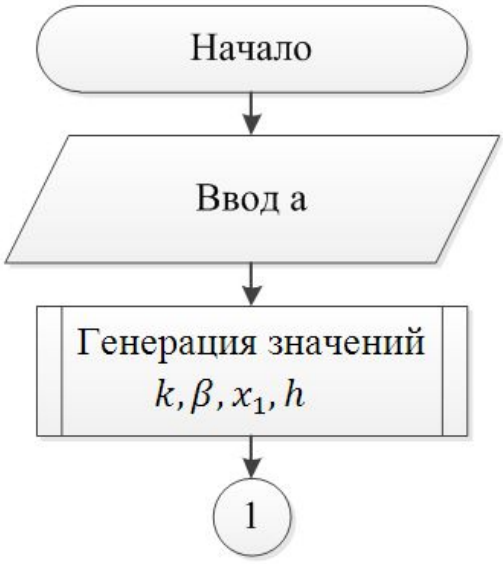
$$l_i(x) = \prod_{j=1, \forall j \neq i}^{n} \frac{x - x_j'}{x_i' - x_j'}$$

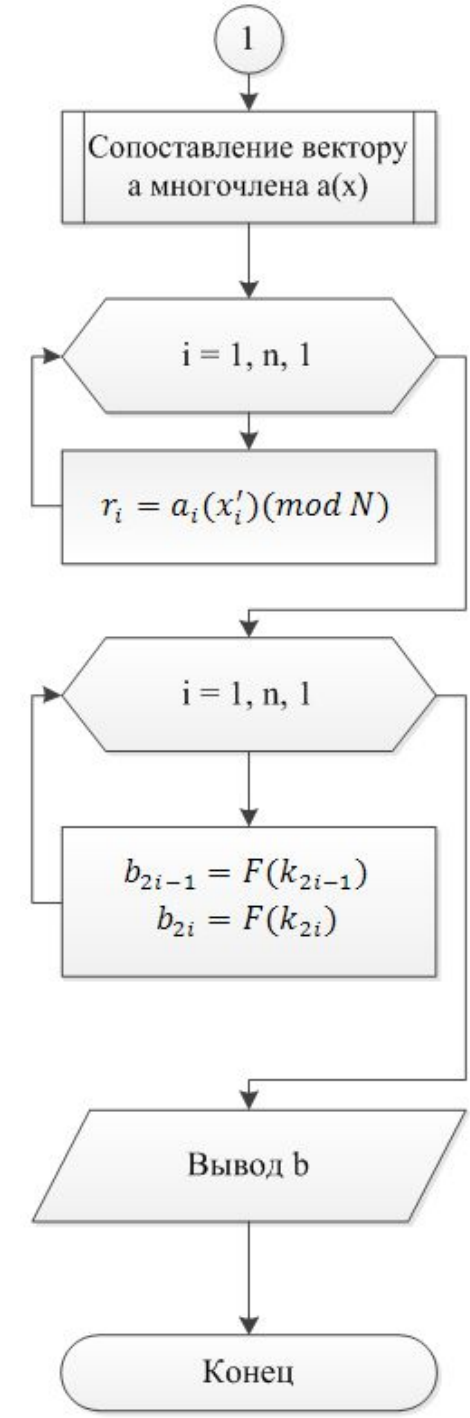
есть многочлены Лагранжа, связанные с узлами x_i' сетки.

Шаг 4. По значениям коэффициентов многочлена $a(x)$ строится вектор a, являющийся исходным сообщением.

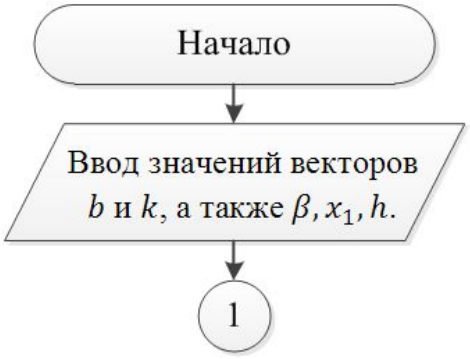
Представим предложенный алгоритм в виде блок-схемы.

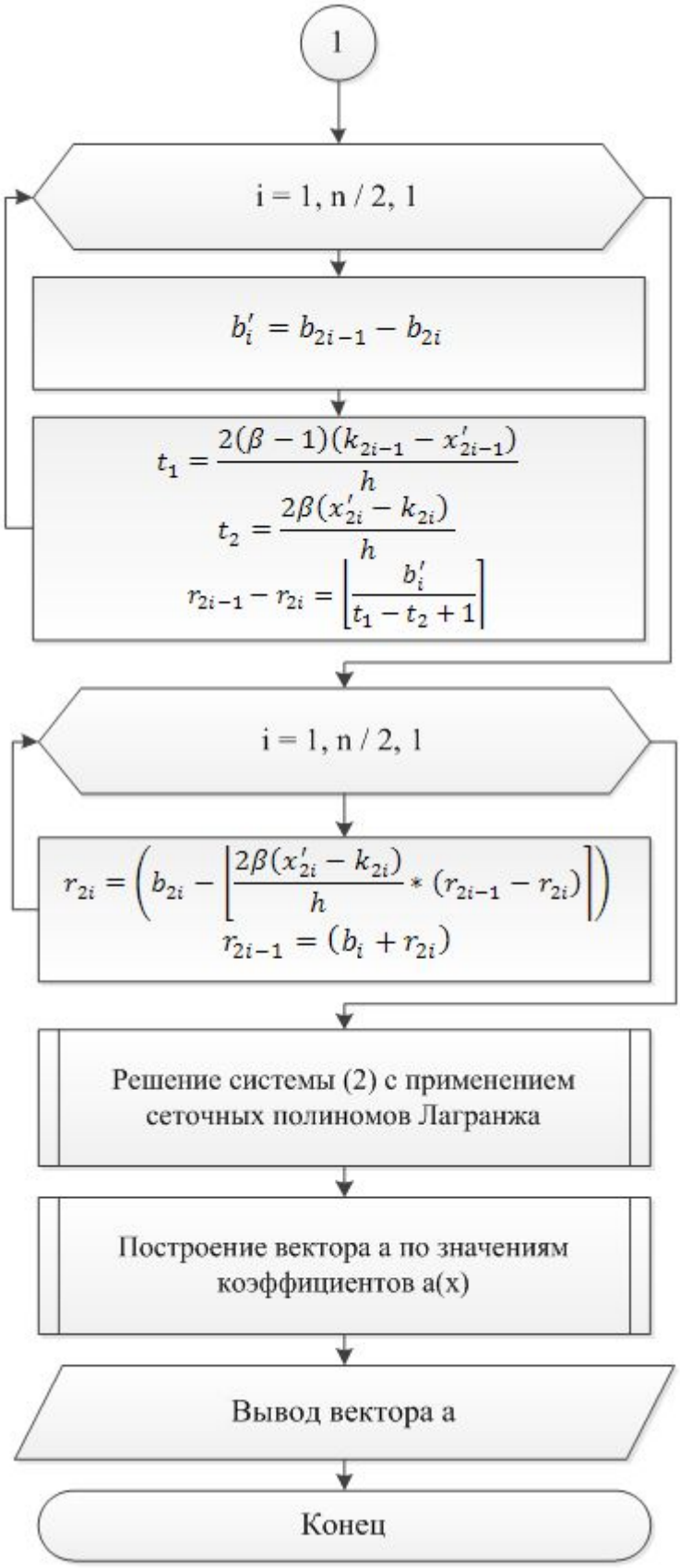
Алгоритм шифрования выглядит следующим образом:





Алгоритм расшифрования в форме блок-схемы выглядит следующим образом:




1
i = 1, n / 2, 1
$b_i' = b_{2i-1} - b_{2i}$
$t_1 = \frac{2(\beta-1)(k_{2i-1} - x'_{2i-1})}{h}$
$t_2 = \frac{2\beta(x'_{2i} - k_{2i})}{h}$
$r_{2i-1} - r_{2i} = \left\lfloor \frac{b_i'}{t_1 - t_2 + 1} \right\rfloor$
i = 1, n / 2, 1
$r_{2i} = \left(b_{2i} - \left\lfloor \frac{2\beta(x'_{2i} - k_{2i})}{h} * (r_{2i-1} - r_{2i}) \right\rfloor \right)$
$r_{2i-1} = (b_i + r_{2i})$
Решение системы (2) с применением сеточных полиномов Лагранжа
Построение вектора a по значениям коэффициентов a(x)
Вывод вектора a
Конец

Список литературы

1. *Леонтьев В.Л.* Ортогональные финитные функции и численные методы — Ульяновск: УлГУ, 2003. — 178 с.

2. *Леонтьев В.Л., Лукашанец Н.Ч.* Сеточные базисы ортогональных финитных функций // Журнал вычислительной математики и математической физики. — 1999. — т.39, №7. — с. 1158

3. *Леонтьев В.Л.* Ортогональные сплайны и вариационно-сеточный метод // Математическое моделирование. — 2002. — т.14, №3. — с. 117.