ФИНИТНЫЕ ФУНКЦИИ В АЛГОРИТМАХ СИММЕТРИЧНОГО ШИФРОВАНИЯ

В статье дается алгоритм симметричного шифрования с использованием функций ОФФ-базиса, приводится пример его использования в решении криптографической задачи. Идея использования в алгоритмах криптографии ОФФ без свойства их ортогональности создана Леонтьевым В.Л.. Реализация алгоритма криптографии с использованием подобных финитных функций проведена Щуренко А.В. с участием Леонтьева В.Л., в рамках диссертационной работы Щуренко А.В.

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], [4].

Алгоритм основан на идее аппроксимации многочлена с использованием функций ОФФ-базиса. После представления блока информации в виде многочлена проводится его аппроксимация с помощью выбранного ОФФ-базиса в заданных узлах сетки, после чего результат шифрования представляется в виде значений определенной функции ОФФ-базиса в точке между узлами сетки. Зная вид базисных ОФФ-функций и точки, в которых проводилась аппроксимация, можно восстановить исходный вид многочлена.

Использование алгоритма шифрования на основе ортогональных финитных функций существенно повышает стойкость шифрования по сравнению с шифром гаммирования и многими другими алгоритмами симметричной криптографии.

Все операции проводятся в кольце многочленов степени, не превосходящей n, над кольцом вычетов $\mathbb{Z}_N$, где n – длина сообщения, а N простое. Все элементы $\mathbb{Z}_N$ являются целыми неотрицательными числами. Сообщение длины, большей n, при шифровании следует разбить на блоки длиной n.

Количество функций в используемой части ОФФ-базиса должно быть не меньше n. Для этого на равномерной сетке $x_1 < x_2 < \cdots < x_l$ с целыми неотрицательными x_i и шагом h задается набор $t = (t_1, t_2, \dots, t_n)$, состоящий из n точек $t_i = (x_i, y_i)$ с попарно различными x_i, причем все t_i совпадают с узлами сетки. Далее задается соответствующий набор ортогональных финитных функций $f = (f_1, f_2, \dots, f_n)$. В данном случае взяты ОФФ, являющиеся частным случаем [1, с.11]. При использовании равномерной сетки с шагом h каждому узлу сетки x_i ставится в соответствие сеточная функция вида

$$f_i(x) = \begin{cases} (x - x_{i-1})/h, \ x \in [x_{i-1}, x_{i-1} + h_1] \cup [x_{i-1} + h_2, x_i], \\ -\alpha + 2(\alpha h + h_1)(x_{i-1} + d_n - x)/(h(h_2 - h_1)), \ x \in [x_{i-1} + h_1, x_{i-1} + d_n], \\ -\alpha + 2(\alpha h + h_2)(x - x_{i-1} - d_n)/(h(h_2 - h_1)), \ x \in [x_{i-1} + d_n, x_{i-1} + h_2], \\ (x_{i+1} - x)/h, \ x \in [x_i + h_2, x_{i+1}], \\ \beta + 2(\beta h + h_1 - h)(x - x_i - d_n)/(h(h_2 - h_1)), \ x \in [x_i + h_1, x_i + d_n], \\ \beta + 2(\beta h + h_2 - h)(x_i + d_n - x)/(h(h_2 - h_1)), \ x \in [x_i + d_n, x_i + h_2], \\ 0, \ x \notin [x_{i-1}, x_{i+1}], \end{cases} \quad (1)$$

где $d_n = (h_1 + h_2)/2, h_1 = H_1 h, h_2 = H_2 h$ $(0 \le h_1 < h_2 \le h)$. H_1, H_2, α, β - некоторые константы, $\alpha > 0, \beta > 0$.

Основная идея алгоритма состоит в том, чтобы отбросить условие ортогональности $4\alpha\beta + \alpha - \beta = 0$ и подбирать набор $f(x)$, исходя только из условия $\alpha = \beta - 1$. При этом числовое значение параметра может быть любым действительным числом, что значительно повышает стойкость алгоритма к атакам, основанным на подборе верного ключа. Функции (1) при этом принимают следующий вид:

$$f_i(x) = \begin{cases} 2\alpha(x_{i-1} - x)/h, & x \in [x_{i-1}, x_{i-1} + h/2], \\ 2(\alpha + 1)(x - x_i)/h + 1, & x \in [x_{i-1} + h/2, x_i], \\ 2(\beta - 1)(x - x_i)/h + 1, & x \in [x_i, x_i + h/2], \\ 2\beta(x_{i+1} - x)/h, & x \in [x_i + h/2, x_{i+1}], \\ 0, & x \notin [x_{i-1}, x_{i+1}]. \end{cases}$$

Пусть A - множество всех открытых текстов, K - множество ключей, а B - множество всех шифртекстов. Алфавитом A является множество неотрицательных целых чисел от 0 до $L - 1$ $(1 < L \le N)$, алфавиты K и B – множества неотрицательных целых чисел от 0 до $N - 1$. Запишем исходное сообщение $a \in A$ в векторном виде:

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

Пусть также выбран ключ $k \in K$:

$$k = (k_1, k_2, \dots, k_n),$$

при этом $\forall i = \overline{1,n}, j = \overline{1,n}: i \ne j \to k_i \ne k_j$. Кроме того, $\forall i = \overline{1,n}$: $k_i \in [x_{j_i} + x_{j_i+1})$, где x_{j_i} и x_{j_i+1} $(j_i \in \mathbb{Z}_l)$ - узлы сетки, между которыми лежит k_i. Другими словами, каждый k_i является координатой на оси Ox точки, лежащей между двумя соседними узлами сетки x_{j_i} и x_{j_i+1}. Каждый участок сетки между двумя соседними узлами должен содержать не более одного k_i. Другими словами, пусть $K_i' = \{k \mid k \in [x_i, x_{i+1})\}$. Тогда $\forall i = \overline{1, l-1}: |K_i'| = 1$.

Обозначим x' вектор узлов сетки, используемых при аппроксимации многочлена: $x' = (x_1', x_2', \dots, x_n')$. При этом $\forall i = \overline{1,n}: x_i' = x_{j_i}$. В качестве f возьмем набор $f = (f_1, f_2, \dots, f_n)$, где каждая f_i – ОФФ-функция, соответствующая узлу x_i'. Вектором $b \in B, b = (b_1, b_2, \dots, b_n)$ обозначается шифртекст.

Алгоритм шифрования выглядит следующим образом:

Шаг 1. Вектору a сопоставляется многочлен:

$$a(x) = a_1 + a_2x + a_3x^2 + \cdots + a_nx^{n-1}.$$

Шаг 2. Проводится аппроксимация $a(x)$ в узлах x'. При этом значение аппроксимирующей функции $F(x)$ будет являться совокупностью сумм ОФФ-функций f_i и соответствующих коэффициентов аппроксимации r_i:

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

Поскольку $\forall i = \overline{1,n}\ f_i(x_i') = 1$, коэффициент каждой i-й ОФФ-функции на единицу меньше значения многочлена в точке с координатой x_i'. Значения этих коэффициентов – неотрицательные целые числа. Зная все $a(x_i')$, можно найти все значения вектора $r = (r_1, r_2, \dots, r_n)$ по формуле

$$r_i = a(x_i') - 1\ (mod\ N).$$

При этом все r_i – неотрицательные целые числа.

Шаг 3. Зная все значения вектора коэффициентов аппроксимации r, можно найти значения f_i в точках k_i, находящихся между узлами сетки. Поскольку $\forall i = \overline{1,n}$: $k_i \in [x_{j_i}, x_{j_i+1})$, значения f_i в точке k_i вычисляются по формуле

$$f_i = \begin{cases} 2(\beta - 1)(x - x_{j_i})/h + 1, & x \in [x_{j_i}, x_{j_i} + h/2], \\ 2\beta(x_{j_i+1} - x)/h, & x \in [x_{j_i} + h/2, x_{j_i+1}]. \end{cases}$$

Шаг 4. Вычисляются значения вектора b по формуле

$$b_i = \lfloor r_i + f_i(k_i) \rceil\ (mod\ N).$$

Вектор b является шифртекстом.

Алгоритм расшифрования заключается в нахождении коэффициентов исходного многочлена $a(x)$ на основе вектора шифртекста b, известного ключа k, а также β. Шифртекст $b \in B$ записывается в векторном виде:

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

Пусть также известен ключ $k \in K$, использованный при шифровании:

$$k = (k_1, k_2, \dots, k_n),$$

при этом $\forall i = \overline{1,n}, j = \overline{1,n}: i \neq j \rightarrow k_i \neq k_j$. Каждый k_i является координатой на оси Ox точки, лежащей между двумя соседними узлами сетки x_{j_i} и x_{j_i+1}:
$\forall i = \overline{1,n}: k_i \in [x_{j_i} + x_{j_i+1})$. Вектором $a \in A, a = (a_1, a_2, \dots, a_n)$ обозначается исходное сообщение.

Шаг 1. Известно, что $b_i = \lfloor r_i + f_i(k_i) \rceil \, (mod\ N)$. Следовательно, $b_i \in [r_i + f_i(k_i) - 0.5, r_i + f_i(k_i) + 0.5)$. Поскольку все r_i - неотрицательные целые числа, дробная часть b_i равна дробной части $f_i(k_i)$. Вычислив все $f_i(k_i)$, можно вычислить точные значения $\big(r_i + f_i(k_i)\big)(mod\ N)$. Обозначим через $b' = (b'_1, b'_2, \dots, b'_n)$, где $b'_i = \big(r_i + f_i(k_i)\big)(mod\ N)$.

Шаг 2. Поскольку известны все значения вектора b', элементы r_i находятся по формуле

$$r_i = b'_i - f_i(k_i)(mod\ N).$$

Шаг 3. Известно, что $\forall i = \overline{1,n}: a(k_i) = r_i + f_i(k_i)$. Поскольку все r_i, k_i и $f_i(k_i)$ известны, получается система из n линейных уравнений:

$$\begin{cases} a(k_1) = r_1 + f_1(k_1)(mod\ N) \\ a(k_2) = r_2 + f_2(k_2)(mod\ N) \\ \dots \\ a(k_n) = r_n + f_n(k_n)(mod\ N) \end{cases} \quad (2)$$

Коэффициенты многочлена $a(x)$, сопоставленному вектору a, можно найти двумя способами. Первый - решить систему (2) в матричной форме. Второй – найти коэффициенты $a(x)$ с помощью сеточных полиномов Лагранжа. Поскольку вектор коэффициентов аппроксимации r и вектор координат k известны, можно построить полином $a(x)$, применив сеточные полиномы Лагранжа для набора точек $t = ((k_1, r_1), (k_2, r_2), \dots, (k_n, r_n))$. Тогда $a(x)$ будет иметь вид:

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

где $p_i = a(x_{j_i})$, а

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

есть многочлены Лагранжа, связанные с узлами k_i сетки.

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

Список литературы

1. *Леонтьев В.Л.* Ортогональные финитные функции и численные методы — Ульяновск: УлГУ, 2003. — 181с.

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.* Об ортогональных финитных функциях и о численных методах, связанных с их применением // Обозрение прикладной и промышленной математики. — 2002. — т.9, №3. — с. 497

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