Об использовании одного свойства ортогональных финитных функций в алгоритмах криптографии

Леонтьев В.Л., Щуренко А.В.
Ульяновский государственный университет

В статье впервые предлагается применять ортогональные финитные функции (ОФФ) [1] в алгоритме криптографии в том случае, в котором ***ОФФ не обладают свойством ортогональности****. При этом последовательность сеточных наборов ОФФ, утративших свойство ортогональности, по-прежнему* ***является базисом*** *в пространстве Соболева, что доказано в соответствующих теоремах [1]. Потеря ОФФ свойства ортогональности придает ОФФ* ***новое свойство – множественность вариантов задания параметра ОФФ****, что позволяет создавать* ***дополнительные ключи*** *в криптографическом алгоритме шифрования. Такая идея использования ОФФ, не имеющих свойства ортогональности, в алгоритме криптографии 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. Идея введения в алгоритме двух наборов участков сетки, на которых шифрование проводится различным образом, принадлежит 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].

Основная идея предлагаемого алгоритма заключается в аппроксимации многочлена 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 с учетом произвольно заданного значения ключа, после чего результат шифрования представляется в виде блока ОФФ-аппроксимации. Зная координаты точек, в которых проводилась аппроксимация, можно восстановить исходный вид многочлена.

Использование алгоритма шифрования на основе ортогональных финитных функций, утративших свойство ортогональности, существенно повышает стойкость шифрования по сравнению с шифром гаммирования.

Все операции проводятся в кольце многочленов степени, не превосходящей n, над кольцом вычетов $\mathbb{Z}_N$, где n – четное число, равное длине сообщения, а N – простое число. 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 выполнения этого требования 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

$t_i = (x_i, y_i)$, где $\forall i = \overline{1,n}, j = \overline{1,n}: i \neq j \rightarrow x_i \neq x_j$, а все x_i $(i = \overline{1,n})$ совпадают с узлами сетки. При этом все y_i – целые неотрицательные числа от 0 до $N-1$, но их точные значения вычисляются уже в процессе шифрования. Далее задается соответствующий набор ОФФ $f = (f_1, f_2, \dots, f_n)$. В нашем случае в качестве примера 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 $d_n = (h_1 + h_2)/2, h_1 = H_1 h, h_2 = H_2 h$ $(0 \leq h_1 < h_2 \leq h)$. H_1, H_2, α, β - некоторые константы, $\alpha > 0, \beta > 0$. Каждая f_i представляет собой сумму B-сплайна первой степени с конечным носителем $[-1, 1]$ и двух B-сплайнов первой степени, взятых с разными знаками, с более компактными по сравнению с $[-1, 1]$ конечными носителями. За счет двух дополнительных B-сплайнов и с помощью выбора значений α, β, h_1, h_2 достигается выполнение условий ортогональности $\forall\, i \neq j: (f_i, f_j) = 0$. Функции $f_i(x), i = \overline{1,n}$ линейно независимы, а их аппроксимирующие свойства представлены следующей теоремой:

Теорема 1 [1]. Если $u(x) \in W_2^1(\mathbb{R})$ и $H_1 + H_2 = 1$ $(h_1 + h_2 = h)$, а $\alpha = \beta - 1$, то существует функция $u^h = \sum_{i-1}^{n} \alpha_i f_i \in M_n$ (α_i- некоторые постоянные):

$$||u - u^h||_{\mathbb{L}_2(\mathbb{R})} \leq ch\big||u|\big|_{W_2^1(\mathbb{R})}, \sum_{i=1}^{n} |\alpha_i|^2 \leq c_1\big||u|\big|^2_{\mathbb{L}_2(\mathbb{R})}, \quad (2)$$

где M_n - линейная оболочка $f_i(x)$, а постоянные c и c_1 не зависят от u и h. W_2^l - функциональное пространство Соболева, $\mathbb{L}_2 = W_2^0$.

Основная идея алгоритма состоит в том, чтобы, отказавшись от выполнения условия ортогональности финитных функций

$$4\alpha\beta + \alpha - \beta = 0,$$

подбирать ОФФ, исходя только из условия

$$\alpha = \beta - 1.$$

При этом числовое значение параметра β может быть любым, что является основой дополнительного шага шифрования исходного сообщения, связанного не только с

деталями алгоритма шифрования, но и с дополнительным произвольно задаваемым ключом β. В общем случае значения параметра β могут быть разными на различных участках выбранной сетки с узлами x_i. Отказ от ортогональности ОФФ значительно расширяет область применения ОФФ, которые, не обладая уже свойством ортогональности, представляют собой особую часть исходного множества ОФФ. Функции (1) при этом, если $h_1 = h_2 = 0$, 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 $L-1$ $(1 < L \leq N)$, 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 $k \in K$:

$$k = \left(k_1, k_2, \dots, k_{n/2}\right),$$

при этом $\forall i = \overline{1, n/2}, j = \overline{1, n/2}: i \neq j \rightarrow k_i \neq k_j$. Кроме того, $\forall i = \overline{1, n/2}$: $k_i = (x_{j_i} + x_{j_i+1})/2$, где x_{j_i} и x_{j_i+1} $(j_i \in \mathbb{Z}_l)$ - узлы сетки, между которыми лежит k_i. Другими словами, каждая компонента ключа k_i является координатой на оси Ox точки, лежащей между двумя соседними узлами сетки x_{j_i} и x_{j_i+1}

Обозначим x' вектор узлов сетки, используемых при аппроксимации многочлена: $x' = (x'_1, x'_2, \dots, x'_n)$. При этом $\forall i = \overline{1, n/2}: x'_{2i-1} = x_{j_i}, \; x'_{2i} = x_{j_i+1}$. 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:

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

Шаг 2. Проводится аппроксимация $a(x)$ с помощью функций f в точках x'. При этом значение аппроксимирующей функции $F(x)$ будет являться суммой произведений ОФФ-функций f_i и соответствующих коэффициентов аппроксимации r_i:

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

поскольку $\forall i = \overline{1,n},\ j = \overline{1,n}: f_j(x_i') = \delta_{ij}$, где δ_{ij} – символ Кронекера, и следовательно, коэффициент каждой i-й ОФФ-функции равен значению многочлена в точке с координатой x_i'. Значения этих коэффициентов – неотрицательные целые числа.

Таким образом находятся значения вектора коэффициентов аппроксимации $r = (r_1, r_2, \dots, r_n)$, где $\forall i = \overline{1,n}:\ r_i = a(x_i')\ (mod\ N)$.

Шаг 3. Строится вектор $b' = (b_1', b_2', \dots, b_{n/2}')$, где каждый b_i' равен значению аппроксимирующей функции по модулю N в точке с координатами по оси Ox, равными k_i. Иными словами, $\forall i = \overline{1,n/2}: b_i' = F(k_i)$. Поскольку k_i лежит между узлами x_{2i-1}' и x_{2i}', значение аппроксимирующей функции в данной точке равно сумме соответствующих f_{2i-1} и f_{2i}:

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

Поскольку $f_{2i-1}(k_i) = 2(\beta - 1)(k_i - x_i)/h + 1$, а $k_i = x_i + h/2$, получаем

$$f_{2i-1}(k_i) = \frac{2(\beta - 1) * h/2}{h} + 1 = \beta.$$

Аналогично, поскольку $f_{2i}(k_i) = 2(\alpha + 1)(k_i - x_i)/h + 1$, а $k_i = x_i - h/2$, получаем

$$f_{2i}(k_i) = \frac{2(\alpha + 1) * (-h/2)}{h} + 1 = -\alpha.$$

Таким образом, $F(k_i) = \beta r_{2i-1} - \alpha r_{2i}$. Поскольку $\alpha = \beta - 1$, получаем $F(k_i) = \beta r_{2i-1} - (\beta - 1) r_{2i} = \beta(r_{2i-1} - r_{2i}) + r_{2i}$. Соответственно,

$$b_i' = \beta(r_{2i-1} - r_{2i}) + r_{2i}\ \ (mod\ N).$$

Шаг 4. Строится вектор $b'' = (b_1'', b_2'', \dots, b_{n/2}'')$, где $\forall i = \overline{1,n/2}$: $b_i'' = (r_{2i-1} - r_{2i})\ (mod\ N)$.

Шаг 5. Строится вектор b, являющийся объединением векторов b' и b'': $b = (b_1', b_2', \dots, b_{n/2}', b_1'', b_2'', \dots\ , b_{n/2}'')$. 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. Запишем шифртекст $b \in B$ в векторном виде:

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

где n – четное натуральное число. Пусть также известен ключ $k \in K$, использованный при шифровании:

$$k = \left(k_1, k_2, \dots, k_{n/2}\right),$$

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_{2i-1} и x_{2i}:
$\forall i = \overline{1,n/2}: k_i = (x_{2i-1} + x_{2i})/2$. Вектором $a \in A, a = (a_1, a_2, \dots, a_n)$ обозначается исходное сообщение.

Шаг 1. Вектор b разбивается на векторы $b' = (b'_1, b'_2, \dots, b'_{n/2})$ и $b'' = (b''_1, b''_2, \dots, b''_{n/2})$, где $\forall i = \overline{1,n/2}: b'_i = b_i, \quad b''_i = b_{i+n/2}$.

Шаг 2. 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 $\forall i = \overline{1,n}: r_i = a(x_i)\ (mod\ N)$. Для нахождения значений r_i $(i = \overline{1,n})$ при расшифровании по значениям b'_i используются известные формулы

$$b'_i = (\beta(r_{2i-1} - r_{2i}) + r_{2i})(mod\ N), \qquad b''_i = (r_{2i-1} - r_{2i})\ (mod\ N),$$

содержащие известный ключ β.

Исключение $(r_{2i-1} - r_{2i})$ в первой формуле дает $b'_i = (\beta b''_i + r_{2i})\ (mod\ N)$. Поскольку значения β, b'_i и b''_i $(i = \overline{1,n/2})$ известны, r_{2i} находятся по формуле

$$r_{2i} = (b'_i - \beta b''_i)(mod\ N).$$

Подстановка значения r_{2i} в уравнение $b''_i = (r_{2i-1} - r_{2i})\ (mod\ N)$ дает значение r_{2i-1}:

$$r_{2i-1} = (b''_i + r_{2i})\ (mod\ N).$$

Шаг 4. Вектор коэффициентов аппроксимации r известен, по значениям вектора K определяются все x'_i $(\forall i = \overline{1,n/2}: x'_{2i-1} = k_i - h/2, \quad x'_{2i} = k_i + h/2)$. Следовательно, можно построить полином $a(x)$, 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 5. По значениям коэффициентов многочлена $a(x)$ строится вектор a, являющийся исходным сообщением.

Пример. Пусть дана равномерная сетка, определяемая значениями $h = 4$, $x_1 = 0$ и задано значение параметра ОФФ $\beta = 3$. При этом ОФФ-функции $f_i(x)$ имеют следующий вид:

$$f_i(x) = \begin{cases} (x_{i-1} - x), \ x \in [x_{i-1}, x_{i-1} + 2], \\ 3(x - x_i)/2 + 1, \ x \in [x_{i-1} + 2, x_i], \\ (x - x_i) + 1, \ x \in [x_i, x_i + 2], \\ 3(x_{i+1} - x)/2, \ x \in [x_i + 2, x_{i+1}], \\ 0, \ x \notin [x_{i-1}, x_{i+1}]. \end{cases}.$$

Пусть также $N = 257, L = 256$.

Шифрование. Пусть $a = (5, 4, 1, 2)$, $k = (2, 10)$. Тогда вектор координат узлов сетки имеет вид $x' = (0, 4, 8, 12)$.

Шаг 1. Вектору a сопоставляется многочлен:

$$a(x) = 5 + 4x + x^2 + 2x^3.$$

Шаг 2. Проводится аппроксимация $a(x)$ с помощью ОФФ-функций f. В результате получается вектор коэффициентов аппроксимации $r = (r_1, r_2, r_3, r_4)$.

$$r_1 = a(0)(mod\ 257) = 5$$
$$r_2 = a(4)(mod\ 257) = 165\ (mod\ 257)$$
$$r_3 = a(8)(mod\ 257) = 1125 \equiv 97\ (mod\ 257)$$
$$r_4 = a(12)(mod\ 257) = 3653 \equiv 55\ (mod\ 257)$$

Получили вектор $r = (5, 165, 97, 55)$.

Шаг 3. Строится вектор b':

$$b'_1 = 3 * (5 - 165) + 165\ (mod\ 257) = 456 \equiv 199\ (mod\ 257)$$
$$b'_2 = 3 * (97 - 55) + 36\ (mod\ 257) = 181(mod\ 257)$$
$$b' = (199, 181).$$

Шаг 4. Строится вектор b''.

$$b''_1 = 5 - 165 = 97\ (mod\ 257)$$
$$b''_2 = 97 - 55 = 42(mod\ 257)$$
$$b'' = (97, 42).$$

Шаг 5. Строится вектор b.

$$b = (b'_1, b'_2, b''_1, b''_2) = (199, 181, 97, 42).$$

Вектор b является шифртекстом.

Расшифрование. Пусть $b = (199, 181, 97, 42),\ k = (2, 10), x' = (0, 4, 8, 12), \beta = 3$.

Шаг 1. Вектор b разделяется на b' и b''.

$$b' = (199, 181)$$
$$b'' = (97, 42)$$

Шаг 2. Все b'_i представляются в виде $b'_i = (\beta(r_{2i-1} - r_{2i}) + r_{2i})(mod\ N)$, а все b''_i - в виде $b''_i = (r_{2i-1} - r_{2i})\ (mod\ N)$.

$$199 = 3 * (r_1 - r_2) + r_2\ (mod\ 257)$$
$$181 = 3 * (r_3 - r_4) + r_4\ (mod\ 257)$$

$$97 = (r_1 - r_2)(mod\ 257)$$
$$42 = (r_3 - r_4)(mod\ 257)$$

Шаг 3. Строится вектор r.

$$r_2 = (b_1' - \beta b_1'')(mod\ 257) = (199 - 3 * 97)(mod\ 257) = 165$$
$$r_1 = (b_1'' + r_2)\ (mod\ 257) = (97 + 165)(mod\ 257) = 262 \equiv 5\ (mod\ 257)$$
$$r_4 = (b_2' - \beta b_2'')(mod\ 257) = (181 - 3 * 42)(mod\ 257) = 55$$
$$r_3 = (b_3'' + r_4)\ (mod\ 257) = (42 + 55)(mod\ 257) = 97$$
$$r = (5, 165, 97, 55).$$

Шаг 4. Решается система уравнений вида (3).

$$\begin{cases} a(0) = 5\ (mod\ 257) \\ a(4) = 165\ (mod\ 257) \\ a(8) = 97\ (mod\ 257) \\ a(12) = 55\ (mod\ 257) \end{cases}$$

В итоге получается многочлен $a(x) = 5 + 4x + x^2 + 2x^3$.

Шаг 5. По значениям коэффициентов $a(x)$ строится вектор a, являющийся исходным сообщением.

$$a = (5, 4, 1, 2)$$

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.* 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