S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 16, стр. 144–144 (2019) УДК 004.75
DOI 10.33048/semi.2019.16.xxx MSC 68M14

ИНТЕРПОЛЯЦИЯ ФУНКЦИИ СРАВНЕНИЯ ЧИСЕЛ НАД КОНЕЧНЫМИ ПОЛЯМИ

М.Г. Бабенко, Н.Н. Кучеров, AND Н.В. Хунг

Abstract. The computational complexity of the algorithm for comparing encrypted numbers using homomorphic integer ciphers depends on the number of arithmetic addition operations that must be multiplied to calculate the interpolation polynomial. When implementing the scheme of homomorphic comparison of numbers, the multiplicative depth of the algorithm for comparison of numbers is necessary, since integer homomorphic ciphers support a limited number of multiplications. The paper estimates the degree of the interpolation polynomial of the function for comparing encrypted numbers from the work [2].

Keywords: interpolation, finite fields, comparison of numbers.

1. Введение

В данной статье нами производится оценка степени интерполяционного многочлена функции сравнения зашифрованных чисел представленного в работе [2].

Пусть $\mathbb{Z}_{m^d} = \mathbb{Z}_m[x]/(f(x))$, где $f(x)$ неприводимый многочлен над $\mathbf{Z}_m$ и $\deg f(x) = d$. Зададим отображение $\mathbb{Z}_{m^d}$ в $\mathbb{Z}_m$ используя абсолютный след α:

$$\mathrm{Tr}_{\mathbb{Z}_{m^d}/\mathbb{Z}_m}(\beta\alpha) = \alpha + \alpha^m + \cdot + \alpha^{m^{d-1}} \tag{1}$$

где $\alpha \in \mathbb{Z}_{m^d}$

Тогда используя теорему 2.24 из работы [1][стр. 75] определим линейное отображение $L_\beta(\alpha)$:

Babenko M.G., Kucherov N.N., Hung N.V., Comparison function interpolation over finite fields.

Работа выполнена при поддержки гранта Министерства науки и высшего образования Российской Федерации 075-15-2021-1010 (13.2251.21.0064).

Поступила 1 января 2015 г., опубликована 31 декабря 2015 г.

Теорема 1. [1]*[стр. 75, теорема 2.24] Пусть* $\mathbf{Z}_{m^d}$ *– конечное расширение конечного поля* $\mathbb{Z}_m$*. Тогда линейными отображениями из* $\mathbb{Z}_{m^d}$ *в* $\mathbb{Z}_m$ *являются отображения* $L_\beta, \beta \in \mathbb{Z}_{m^d}$*, определяемые условием* $L_\beta(\alpha) = Tr_{\mathbb{Z}_{m^d}/\mathbb{Z}_m}(\beta\alpha)$ *для всех* $\alpha \in \mathbb{Z}_{m^d}$*, и только они. При этом если* β *и* γ *– различные элементы поля* $\mathbb{Z}_{m^d}$*, то* $L_\beta \neq L_\alpha$*.*

Из теоремы 1, можно сделать вывод о том, что отображения L_α является инъективным и может быть использования для сравнения чисел. Таким образом задача сравнения чисел в целочисленных гомоморфных шифрах сводиться к задаче сравнения чисел заданных над простым полем.

Функцию сравнения чисел над простым полем $\mathbb{Z}_m$ определим следующим образом:

$$\operatorname{comp}_m(x,y) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = y \\ -1 & \text{if } x < 0 \end{cases} \tag{2}$$

где m – простое число и $x, y \in \mathbb{Z}_m$. Еесли m–составное число, то не существует многочлена от двух переменных над $\mathbb{Z}_m$ определяющего функцию сравнения чисел. В работе [2] используется интерполяционные многочлен Лагранжа от двух переменных построил функцию для сравнения чисел над $\mathbb{Z}_m$.

Метод [2] позволяет сравнивать целые числа в зашифрованном виде. Вычислительная сложность метода зависит от степени многочлена $c(x,y)$. Учитывая, что степень многочлена $c(x,y)$ меньше либо равна $2m-2$. В работе, мы проведем уточнение оценки для степени интерполяционного многочлена $c(x,y)$ из [2] и покажем, что $\deg c(x,y) = m$.

2. Матрица и их свойство

Рассмотрим матрицы D_x вида $D_x = x \cdot E$ над $\mathbf{Z}_m$, где E – единичная матрица порядка $m-1$ и m–простое число. Обратим внимание, что матрицы обладают следующими свойствами:

Свойство 1.

(1) $D_{x\cdot y} = x \cdot y \cdot E = x \cdot E \cdot y \cdot E = D_x \cdot D_y$.
(2) $D_{x+y} = (x+y) \cdot E = x \cdot E + y \cdot E = D_x + D_y$.
(3) $\forall x \in \mathbb{Z}_m^* : D_x^{-1} = D_{\frac{1}{x}} = \frac{1}{x} \cdot E$.
(4) $\forall x \in \mathbb{Z}_m^* : \det D_x = x^{m-1} \equiv 1 \pmod m$

Лемма 1. *Если* m *– простое число, то* $\det \bar{D} \in \{-1, 0, 1\}$ *над* $\mathbb{Z}_m$*, где*

$$\bar{D} = \begin{pmatrix} D_{d_{1,1}} & D_{d_{1,2}} & \cdots & D_{d_{1,n}} \\ D_{d_{2,1}} & D_{d_{2,2}} & \cdot & D_{d_{2,n}} \\ \vdots & \vdots & \ddots & \vdots \\ D_{d_{n,1}} & D_{d_{n,2}} & \cdots & D_{d_{n,n}} \end{pmatrix} \tag{3}$$

Доказательство. Используя преобразования строк матрицы 1–го типа, сохраняющих значение определителя [3][стр. 80, Предложение 2] и свойства 1 матрицы D_x, приведем матрицу $\bar{D}$ к квазитреугольному виду:

$$\bar{D}'_{\oplus} = \begin{pmatrix} D_{d'_{1,1}} & D_{d'_{1,2}} & \cdots & D_{d'_{1,n}} \\ D_{d'_{2,1}} & D_{d'_{2,2}} & \cdots & D_{d'_{2,n}} \\ \vdots & \vdots & \ddots & \vdots \\ D_{d'_{n,1}} & D_{d'_{n,2}} & \cdot & D_{d'_{n,n}} \end{pmatrix} \tag{4}$$

или

$$\bar{D}'_{\ominus} = - \begin{pmatrix} D_{d'_{1,1}} & D_{d'_{1,2}} & \cdots & D_{d'_{1,n}} \\ D_{d'_{2,1}} & D_{d'_{2,2}} & \cdots & D_{d'_{2,n}} \\ \vdots & \vdots & \ddots & \vdots \\ D_{d'_{n,1}} & D_{d'_{n,2}} & \cdot & D_{d'_{n,n}} \end{pmatrix} \tag{5}$$

Используя теорему 4 [3][стр. 82] вычислим значения определителя квазитреугольных матриц $\bar{D}'_{\oplus}$ и $\bar{D}_{\ominus}$, получим:

$$\det \bar{D}'_{\oplus} = -\det \bar{D}'_{\ominus} = \prod_{i=1}^{n} \det D_{d'_{i,i}} \tag{6}$$

Учитывая, что

$$\forall i \in \overline{1,n} : \det D_{d'_{i,i}} = \begin{cases} 1 & \text{if } d'_{i,i} \mathbf{Z}_m^*, \\ 0 & \text{if } d'_{i,i} \equiv 0 \pmod m, \end{cases} \tag{7}$$

следовательно, $\prod_{i=1}^{n} \det D_{d'_{i,i}}$ может принимать два значения $\prod_{i=1}^{n} \det D_{d'_{i,i}} = 1$ если $\forall i \in \overline{1,n} : d'_{i,i} \in \mathbf{Z}_m^*$ и $\prod_{i=1}^{n} \det D_{d'_{i,i}} = 0$ если $\exists i \in \overline{1,n} : d'_{i,i} = 0$, значит, $\det \bar{D} \in \{-1, 0, 1\}$. □

Лемма 2. *Если m – простое число, то $\det \bar{D}$ над $\mathbb{Z}_m$ равно нулю тогда и только тогда, когда $\det \tilde{D}$ над $\mathbb{Z}_m$, где $\tilde{D} = (d_{i,j})_{n \times n}$.*

Доказательство. Покажем, что если $\det \tilde{D} = 0$, то $\det \bar{D} = 0$. Для этого предположим, что $\det \tilde{D} = 0$ то строки матрицы $\tilde{D}$ линейно зависимы, следовательно существуют такие числа α_i не все равные нулю одновременно удовлетворяющие условию: $\sum_{i=1}^{n} \alpha_i \cdot \vec{d_i} = 0$, значит будет существовать такой номер $j \in \overline{1,n} : \alpha_j \neq 0$ и удовлетворяющий $\vec{d_j} = \sum_{i=1, i \neq j}^{n} \alpha'_i \vec{d_i}$, где $\forall i \in \overline{1,n} : \alpha'_i = -\frac{\alpha_i}{\alpha_j}$ и $\forall i \in \overline{1,n} : \vec{d_i} = (d_{i,1}, d_{i,2}, \cdots, d_{i,n})$. Обозначим через $\vec{D}_i$ вектор элементами которого являются блочные матрицы $D_{d_{i,j}}$: $\vec{D}_i = \left(D_{d_{i,1}}, D_{d_{i,2}}, \cdots, D_{d_{i,n}}\right)$.

Вычислим значение $\sum_{i=1,i\neq j}^{n}\alpha'_i\vec{D}_i$ используя свойства 1, получим:

$$\begin{aligned}\sum_{i=1,i\neq j}^{n}\alpha'_i\vec{D}_i &= \left(\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,1}},\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,2}},\cdots,\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,n}},\right)= \\ &= \left(\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,1}},\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,2}},\cdots,\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,n}},\right)= \\ &= \left(D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,1}},D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,2}},\cdots,D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,n}},\right)= \\ &= \vec{D}_j\end{aligned} \tag{8}$$

Из (8), следует, что линейные строки матриц $\bar{D}$ линейно зависимы следовательно, $\det\bar{D}=0$.

Покажем, что если $\det\bar{D}=0$, то $\det\tilde{D}=0$. Предположим: что $\det\bar{D}=0$ равен нулю, тогда строки матрицы линейно зависимы и существуют такие числа α_i не все равные нулю одновременно удовлетворяющие условию: $\sum_{i=1}^{n}\alpha_i\vec{D}_i=0$, значит существует такое $j\neq 0$ удовлетворяющая условию: $\vec{D}_j=\sum_{i=1,i\neq j}^{n}\alpha'_i\vec{D}_i$.

Вычислим значение $\vec{D}_j=\sum_{i=1,i\neq j}^{n}\alpha'_i\vec{D}_i$ используя свойства 1, получим:

$$\begin{aligned}\vec{D}_j &= \sum_{i=1,i\neq j}^{n}\alpha'_i\vec{D}_i= \\ &= \left(\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,1}},\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,2}},\cdots,\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot D_{d_{i,n}},\right)= \\ &= \left(\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,1}},\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,2}},\cdots,\sum_{i=1,i\neq j}^{n}D_{\alpha'_i\cdot d_{i,n}},\right)= \\ &= \left(D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,1}},D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,2}},\cdots,D_{\sum_{i=1,i\neq j}^{n}\alpha'_i\cdot d_{i,n}},\right)\end{aligned} \tag{9}$$

Из 9, следует, что $\vec{d_j}=\sum_{i=1,i\neq j}^{n}\alpha'_i\vec{d_i}$, значит строки матрицы $\tilde{D}$ линейно зависимы и $\det\tilde{D}=0$. Так как равенство выполняется в обе стороны, то лемма доказана. □

Лемма 3. *Если m – простое число, то $\det D_V\neq 0$ над $\mathbb{Z}_m$, где*

$$D_V=\begin{pmatrix}D_1 & D_{1^2} & \cdots & D_{1^{m-1}}\\ D_2 & D_{2^2} & \cdots & D_{2^{m-1}}\\ \vdots & \vdots & \ddots & \vdots\\ D_{m-1} & D_{(m-1)^2} & \cdots & D_{(m-1)^{m-1}}\end{pmatrix} \tag{10}$$

Доказательство. Рассмотрим матрицу Вандермонда V равную:

$$V=\begin{pmatrix}1 & 1^2 & \cdots & 1^{m-1}\\ 2 & 2^2 & \cdots & 2^{m-1}\\ \vdots & \vdots & \ddots & \vdots\\ m-1 & (m-1)^2 & \cdots & (m-1)^{m-1}\end{pmatrix} \tag{11}$$

Определитель матрицы V равен

$$\det V = \prod_{i \leq j < i \leq m-1} (i-j) = \prod_{i=1}^{m-1} i^{m-i} \not\equiv 0 \pmod{m} \tag{12}$$

Из Леммы 2 следует, что $\det D_V \neq 0$. □

3. Полиномиальная интерполяция функции сравнения чисел над простым полем

Теорема 2. *Если m–простое число и $m \geq 3$, то в поле $\mathbb{Z}_m[x]$ существует многочлен $c(x,y) \in \mathbb{Z}_m[x,y]$ для которого многочлен $b(x,y) \in \mathbb{Z}_m[x,y]$ определяется единственным образом, такой что $\forall x, y \in \mathbb{Z}_m : \mathrm{comp}_m(x,y) \equiv c(x,y) \pmod{m}$ и $\deg c(x,y) \leq 2m-2$, где*

$$c(x,y) = x^{m-1} - y^{m-1} + \sum_{t=1}^{m-1} \sum_{k=1}^{m-1} b_{t,k} \cdot x^t \cdot y^k \tag{13}$$

где

$$\begin{aligned} \forall 1 \leqslant t < k \leqslant m-1 : & \\ b_{t,k} &= \sum_{1 \leq i < j \leq m-1} \left(i^{m-1-k} \cdot j^{m-1-t} - i^{m-1-t} \cdot j^{m-1-k} \right) \\ b_{k,t} &= -b_{t,k} \\ b(x,y) &= \sum_{t=1}^{m-1} \sum_{k=1}^{m-1} b_{t,k} \cdot x^t \cdot y^k. \end{aligned} \tag{14}$$

Доказательство. Пусть существует многочлен $c(x,y) \in \mathbb{Z}_m[x,y]$ такой что $\forall x, y \in \mathbb{Z}_m : \mathrm{comp}_m(x,y) = c(x,y)$, тогда его можно представить в виде:

$$c(x,y) = \alpha + \eta(x) + \xi(y) + b(x,y) \tag{15}$$

где $\alpha \in \mathbb{Z}_m$, $\eta(x) \in \mathbb{Z}_m[x]$ и $x | \eta(x)$, $\xi(y) \in \mathbb{Z}_m[y]$ и $y | \xi(y)$, $b(x,y) \in \mathbb{Z}_m[x,y]$ и $(x \cdot y) | b(x,y)$

Так как $\mathrm{comp}_m(0,0) = 0$, то $c(0,0) = \alpha = 0$. Учитывая, что $\forall x \in \mathbb{Z}_m^* : \mathrm{comp}_m(x,0) = 1$, то $c(x,0) = \eta(x) \equiv 1 \pmod{m}$, следовательно, $\forall a \in \mathbb{Z}_m : (x-a) | (\eta(x) - 1)$, значит, $\left(x^{m-1} - 1\right) | (\eta(x) - 1)$. Выбирая в качестве $\eta(x)$ многочлен наименьшей степени, удовлетворяющий условиям $x | \eta(x)$ и $\left(x^{m-1} - 1\right) | (\eta(x) - 1)$, получим $\eta(x) = x^{m-1}$.

Вычислим $\forall a \in \mathbb{Z}_m^* : \mathrm{comp}_m(0,y) = -1$, получим: $\forall a \in \mathbb{Z}_m^* : c(0,a) = \xi(y) \equiv -1 \pmod{m}$, рассуждая аналогично $\eta(x)$, получим $\xi(y) = -y^{m-1}$. Таким образом (x,y) примет следующий вид:

$$c(x,y) = x^{m-1} - y^{m-1} + b(x,y) = x^{m-1} - y^{m-1} + \sum_{i=1}^{m-1} \sum_{j=1}^{m-1} b_{i,j} x^i \cdot y^j \tag{16}$$

Покажем, что $\forall x, y \in \mathbb{Z}_m^*$ существует единственный многочлен $b(x,y) = \sum_{i=1}^{m-1}\sum_{j=1}^{m-1} b_{i,j}x^i \cdot y^j$, удовлетворяющий условию: $b(x,y) = c(x,y)$.

$$H \times \begin{pmatrix} b_{1,1} \\ b_{1,2} \\ \vdots \\ b_{m-1,m-1} \end{pmatrix} = \begin{pmatrix} \mathrm{comp}_m(1,1) \\ \mathrm{comp}_m(1,2) \\ \vdots \\ \mathrm{comp}_m(m-1,m-1) \end{pmatrix} \tag{17}$$

где

$$H = \begin{pmatrix} 1^1 \cdot 1^1 & \cdots & 1^{m-1} \cdot 1^{m-1} \\ 1^1 \cdot 2^1 & \cdots & 1^{m-1} \cdot 2^{m-1} \\ \vdots & \ddots & \vdots \\ (m-1)^1 \cdot (m-1)^1 & \cdots & (m-1)^{m-1} \cdot (m-1)^{m-1} \end{pmatrix} \tag{18}$$

Матрицу H можно представить в следующем виде:

$$H = D_V \times \begin{pmatrix} V & D_0 & \cdots & D_0 \\ D_0 & V & \cdots & D_0 \\ \vdots & \vdots & \ddots & \vdots \\ D_0 & D_0 & \cdots & V \end{pmatrix} \tag{19}$$

Используя теорему 6 из работы [3][стр. 85] вычислим значение определителя матрицы H, получим

$$\begin{aligned} \det H &= \det D_V \cdot \det \begin{pmatrix} V & D_0 & \cdots & D_0 \\ D_0 & V & \cdots & D_0 \\ \vdots & \vdots & \ddots & \vdots \\ D_0 & D_0 & \cdots & V \end{pmatrix} \\ &= \det D_V \cdot (\det V)^{m-1} \\ &\equiv \det D_V \pmod m \end{aligned} \tag{20}$$

Из леммы 3, следует $\det H \not\equiv 0 \pmod m$, значит существует единственное решение матричного уравнения и многочлен $b(x,y) \in \mathbb{Z}_m^*[x,y]$ определяется единственным образом.

Вычислим, многочлен $b(x,y)$ используя интерполяционный многочлен Лагранжа от двух переменных. Вычислим базисные многочлены.

$$L_{i,j}(x,y) = \frac{g_i(x)}{g_i(i)} \cdot \frac{g_j(y)}{g_j(j)} \tag{21}$$

где $g_i(x) = \sum_{t=1}^{m-1} i^{m-1-t} \cdot x^t$. Вычислим значение $g_i(i)$, получим:

$$g_i(i) = \sum_{t=1}^{m-1} i^{m-1-t} \cdot i^t = \sum_{t=1}^{m-1} i^{m-1} \equiv m-1 \pmod m \tag{22}$$

Следовательно,

$$\begin{aligned} L_{i,j}(x,y) &\equiv g_i(x) \cdot g_j(y) \\ &\equiv \left(\sum_{t=1}^{m-1} i^{m-1-t} \cdot x^t\right)\left(\sum_{k=1}^{m-1} i^{m-1-k} \cdot y^k\right) \pmod m \end{aligned} \tag{23}$$

Используя [4][стр. 57, формула 2.34]

$$\left(\sum_{k=1}^{m-1} a_k\right)\left(\sum_{t=1}^{m-1} b_t\right) = \tag{24}$$
$$= (m-1)\sum_{k=1}^{m-1} a_k \cdot b_k - \sum_{i\le t<k\le m-1} (a_k - a_t)(b_k - b_t)$$

вычислим значение $L_{i,j}(x,y)$, учитывая, что $a_k = i^{m-1-k}\cdot x^k$ и $b_k = j^{m-1-k}\cdot y^k$, получим:

$$L_{i,j}(x,y) = (m-1)\sum_{k=1}^{m-1} i^{m-1-k}\cdot x^k \cdot j^{m-1-k}\cdot y^k - \tag{25}$$
$$- \sum_{1\le t<k\le m-1} \left(i^{m-1-k}\cdot x^k - i^{m-1-t}\cdot x^t\right)\left(j^{m-1-k}\cdot y^k - j^{m-1-t}\cdot y^t\right)$$

Так как $\forall i,j,x,y \in \mathbb{Z}_m^*$:

$$i^{m-1-k}\cdot x^k \cdot j^{m-1-k}\cdot y^k = \left(\frac{x\cdot y}{i\cdot j}\right)^k, \tag{26}$$
$$i^{m-1-k}\cdot x^k - i^{m-1-t}\cdot x^t = x^t\cdot i^{-k}\left(x^{k-t} - i^{k-t}\right) \tag{27}$$
$$j^{m-1-k}\cdot y^k - j^{m-1-t}\cdot y^t = y^t\cdot j^{-k}\left(y^{k-t} - j^{k-t}\right) \tag{28}$$

то $L_{i,j}(x,y)$ преобразуется к следующему виду:

$$L_{i,j}(x,y) = (m-1)\sum_{k=1}^{m-1}\left(\frac{x\cdot y}{i\cdot j}\right)^k - \tag{29}$$
$$- \sum_{1\le t<k\le m-1} (x\cdot y)^t\cdot(i\cdot j)^{-k}\left(x^{k-t} - i^{k-t}\right)\left(y^{k-t} - j^{k-t}\right)$$

Вычислим разность $L_{i,j}(x,y) - L_{j,i}(x,y)$:

$$L_{i,j}(x,y) - L_{j,i}(x,y) =$$
$$= \sum_{1\le t<k\le m-1} (x\cdot y)^t\cdot(i\cdot j)^{-k}\left(x^{k-t} - j^{k-t}\right)\left(y^{k-t} - i^{k-t}\right) -$$
$$- \sum_{1\le t<k\le m-1} (x\cdot y)^t\cdot(i\cdot j)^{-k}\left(x^{k-t} - i^{k-t}\right)\left(y^{k-t} - j^{k-t}\right)$$

Используя сочетательный закон [4][стр. 48, формула 2.16] преобразуем $L_{i,j}(x,y) - L_{j,i}(x,y)$ к следующему виду:

$$L_{i,j}(x,y) - L_{j,i}(x,y) = \sum_{1\le t<k\le m-1} (x\cdot y)^t\cdot(i\cdot j)^k \times$$
$$\times\left(\left(x^{k-t} - j^{k-t}\right)\left(y^{k-t} - i^{k-t}\right) - \left(x^{k-t} - i^{k-t}\right)\left(y^{k-t} - j^{k-t}\right)\right)$$

Учитывая, что

$$\left(x^{k-t} - j^{k-t}\right)\left(y^{k-t} - i^{k-t}\right) - \left(x^{k-t} - i^{k-t}\right)\left(y^{k-t} - j^{k-t}\right) =$$
$$= \left(x^{k-t} - y^{k-t}\right)\cdot\left(j^{k-t} - i^{k-t}\right)$$

то

$$L_{i,j}(x,y) - L_{j,i}(x,y) = \sum_{1\le t<k\le m-1} (x\cdot y)^t \cdot (i\cdot j)^{-k} \left(x^{k-t} - y^{k-t}\right)\cdot\left(j^{k-t} - i^{k-t}\right)$$

Таким образом используя интерполяционную функцию Лагранжа, вычислим многочлен $b(x,y)$:

$$\begin{aligned} b(x,y) &= -\sum_{1\le i<j\le m-1} \left(L_{i,j}(x,y) - L_{j,i}(x,y)\right) \\ &= -\sum_{1\le i<j\le m-1}\ \sum_{1\le t<k\le m-1} (x\cdot y)^t \cdot (i\cdot j)^{-k} \left(x^{k-t} - y^{k-t}\right)\cdot\left(j^{k-t} - i^{k-t}\right) \end{aligned}$$

Используя правило изменения порядка суммирования и обобщающий сочетательный закон [4][стр. 53, формула 2.27], получим:

$$b(x,y) = -\sum_{1\le t<k\le m-1} (x\cdot y)^t \cdot \left(x^{k-t} - y^{k-t}\right) \sum_{1\le i<j\le m-1} (i\cdot j)^{-k} \cdot \left(j^{k-t} - i^{k-t}\right)$$

Таким образом, мы можем сделать вывод о том, что, если $1 \le t < k \le m-1$: $b_{t,k} = \sum_{1\le i<j\le m-1} (i\cdot j)^{-k} \cdot \left(j^{k-t} - i^{k-t}\right)$ и $b_{k,t} = -b_{t,k}$.

Вычислим $\forall 1 \le t < k \le m-1$ значение $b_{t,k}$, получим:

$$\begin{aligned} b_{t,k} &= \sum_{1\le i<j\le m-1} (i\cdot j)^{-k} \cdot \left(j^{k-t} - i^{k-t}\right) \\ &= \sum_{1\le i<j\le m-1} \left(i^{m-1-k}\cdot j^{m-1-t} - i^{m-1-t}\cdot j^{m-1-k}\right) \end{aligned} \tag{30}$$

□

4. Свойства

В предыдущем разделе мы определили формулу для интерполяции функции сравнения чисел с помощью интерполяционной формулы Лагранжа. В этом разделе мы рассмотрим свойства коэффициентов многочлена $b(x,y)$.

Свойство 2.

(1) Если $t+k$ – четное число, то $b_{t,k} = 0$.

(2) Если t–четное и k–нечетное, то

$$b_{t,k} = 2\cdot \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-} j^{m-1-t} \tag{31}$$

(3) Если t–нечетное и k–четное, то

$$b_{t,k} = -2\cdot \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{32}$$

Доказательство. Используя теореме 2 вычислим значения коэффициента $b_{t,k}$

$$b_{t,k} = \sum_{1\le i<j\le m-1} \left(i^{m-1-k}\cdot j^{m-1-t} - i^{m-1-t}\cdot j^{m-1-k}\right) \tag{33}$$

$$= \sum_{i=1}^{m-2}\sum_{j=i+1}^{m-1} \left(i^{m-1-k}\cdot j^{m-1-t} - i^{m-1-t}\cdot j^{m-1-k}\right) \tag{34}$$

Используя сочетательный закон [4][стр. 48, формула 2.16], получим:

$$b_{t,k} = \sum_{i=1}^{m-2} \sum_{j=i+1}^{m-1} i^{m-1-k} \cdot j^{m-1-t} - \sum_{i=1}^{m-2} \sum_{j=i+1}^{m-1} i^{m-1-t} \cdot j^{m-1-k} \tag{35}$$

Заменим j на $m-j$,

$$b_{t,k} = \sum_{i=1}^{m-2} \sum_{j=1}^{m-i-1} i^{m-1-k} \cdot (m-j)^{m-1-t} - \sum_{i=1}^{m-2} \sum_{j=1}^{m-i-1} i^{m-1-t} \cdot (m-j)^{m-1-k} \tag{36}$$

Так как

$$(m-j)^{m-1-t} \equiv (-1)^{m-1-t} j^{m-1-t} \pmod{m}$$

и

$$(m-j)^{m-1-k} \equiv (-1)^{m-1-k} j^{m-1-k} \pmod{m},$$

то

$$b_{t,k} = (-1)^{m-1-t} \sum_{i=1}^{m-2} \sum_{j=1}^{m-i-1} i^{m-1-k} \cdot j^{m-1-t} - (-1)^{m-1-k} \sum_{i=1}^{m-2} \sum_{j=1}^{m-i-1} i^{m-1-t} \cdot j^{m-1-k}$$

Используя распределительный закон [4][стр. 48, формула 2.16] преобразуем сумм к следующему виду:

$$b_{t,k} = (-1)^{m-1-t} \sum_{i=1}^{m-2} i^{m-1-k} \times \times \sum_{j=1}^{m-i-1} j^{m-1-t} - (-1)^{m-1-k} \sum_{i=1}^{m-2} i^{m-1-t} \times \sum_{j=1}^{m-i-1} j^{m-1-k} \tag{37}$$

Учитывая, что:

$$\sum_{i=1}^{m-2} i^{m-1-t} \sum_{j=1}^{m-i-1} j^{m-1-k} = \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{38}$$

то

$$b_{t,k} = \left((-1)^{m-1-t} - (-1)^{m-1-k} \right) \cdot \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{39}$$

Рассмотрим четыре случая:

Случай 1. Если t–четное и k–четное, то $m-1-t$ – четное и $(m-1-k)$ – четное, следовательно:

$$b_{t,k} = 0 \tag{40}$$

Случай 2. Если t–четное и k–нечетное, то $(m-1-t)$ – четное и $(m-1-k)$ – нечетное, следовательно:

$$b_{t,k} = 2 \cdot \sum_{i=1}^{m-2} i^{m-1-k} \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{41}$$

Случай 3. Если t–нечетное и k–нечетное, то $(m-1-t)$ – нечетное и $(m-1-k)$ – нечетное, следовательно:

$$b_{t,k} = 0 \tag{42}$$

Случай 4. Если t–нечетное и k–четное, то $(m-1-t)$ – нечетное и $(m-1-k)$ – четное, следовательно:

$$b_{t,k} = -2 \cdot \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{43}$$

Из Случая 1 и 3 можно сделать вывод о том, что если $t+k$ – четное число, то $b_{t,k} = 0$. □

Свойство 3.

$$b_{m-1,2\cdot k+1} = \begin{cases} 2 & \text{если } k = 0, \\ 0 & \text{иначе} \end{cases} \tag{44}$$

Доказательство. Так как по условию теоремы 2 m – простое число и $m \geq 3$, то m – нечетное число, следовательно, $m-1$ – четное число. Число вида $2 \cdot k + 1$ всегда нечётное число, значит значение $b_{m-1,2\cdot k+1}$ вычисляется свойству 2 случай 2:

$$b_{m-1,2\cdot k+1} = 2 \cdot \sum_{i=1}^{m-2} i^{m-2-2\cdot k} \cdot \sum_{j=1}^{m-i-1} j^0 \tag{45}$$

Учитывая, что $\sum_{j=1}^{m-i-1} j^0 = \sum_{j=1}^{m-i-1} 1 = m-i-1$, то

$$\begin{aligned} b_{m-1,2\cdot k+1} &= 2 \cdot \sum_{i=1}^{m-2} i^{m-2-2\cdot k} \cdot (m-i-1) \equiv \\ &\equiv -2 \sum_{i=1}^{m-2} i^{m-1-2\cdot k} - 2 \cdot \sum_{i=1}^{m-2} i^{m-2-2\cdot k} \pmod{m} \end{aligned} \tag{46}$$

Представим

$$\begin{aligned} \sum_{i=1}^{m-2} i^{m-1-2\cdot k} &= -(m-1)^{m-1-2\cdot k} + \sum_{i=1}^{m-1} i^{m-1-2\cdot k} \equiv \\ &\equiv -(-1)^{m-1-2\cdot k} + \sum_{i=1}^{m-1} i^{m-1-2\cdot k} \pmod{m} \end{aligned} \tag{47}$$

$$\begin{aligned} \sum_{i=1}^{m-2} i^{m-2-2\cdot k} &= -(m-1)^{m-2-2\cdot k} + \sum_{i=1}^{m-1} i^{m-2-2\cdot k} \equiv \\ &\equiv -(-1)^{m-2-2\cdot k} + \sum_{i=1}^{m-1} i^{m-2-2\cdot k} \pmod{m} \end{aligned} \tag{48}$$

получим

$$\begin{aligned} b_{m-1,2\cdot k+1} &= 2\left((-1)^{m-1-2\cdot k} + (-1)^{m-2-2\cdot k}\right) - \\ &- 2 \sum_{i=1}^{m-1} i^{m-1-2\cdot k} - 2 \cdot \sum_{i=1}^{m-1} i^{m-2-2\cdot k} = \\ &= -2 \sum_{i=1}^{m-1} i^{m-1-2\cdot k} - 2 \cdot \sum_{i=1}^{m-1} i^{m-2-2\cdot k} \end{aligned} \tag{49}$$

Так как $\forall k = \overline{0, \frac{m-1}{2}} : \gcd m - 2 \cdot k - 1, m = 1$ и $\forall k = \overline{1, \frac{m-1}{2}} : \gcd m - 2 \cdot k, m = 1$, то используя формулу Бернулли из работы [4][стр. 314, формула 6.78] вычислим значение $\left|\sum_{i=1}^{m-1} i^{m-1-2\cdot k}\right|_m$, получим:

$$\left|\sum_{i=1}^{m-1} i^{m-1-2\cdot k}\right|_m = \left|\frac{1}{m-2\cdot k}\sum_{s=0}^{m-1-2k}\binom{m-2\cdot k}{s}B_s \cdot m^{m-2\cdot k-s}\right|_m = \tag{50}$$
$$= \begin{cases}\left|\binom{m}{m-1}B_{m-1}\right|_m & k=0\\ 0 & \text{иначе}\end{cases}$$

где B_s – числа Бернулли. Вычислим, значение $\left|\sum_{i=1}^{m-1} i^{m-1-2\cdot k}\right|_m$ в случае если $k = 0$, получим:

$$\left|\sum_{i=1}^{m-1} i^{m-1}\right|_m \equiv \left|\sum_{i=1}^{m-1} 1\right|_m \equiv -1 \pmod m \tag{51}$$

следовательно:

$$b_{m-1,2\cdot k+1} = \begin{cases}2 & \text{если } k=0\\ 0 & \text{иначе}\end{cases} \tag{52}$$

□

Свойство 4. Если $t + k > m$, то $b_{t,k} = 0$

Доказательство. Воспользуемся формулой Бернулли [4][стр. 314, формула 6.78] и вычислим значение выражения:

$$\sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \tag{53}$$

получим

$$\sum_{j=1}^{m-i-1} j^{m-1-t} = \frac{1}{m-t}\sum_{s=0}^{m-1-t}\binom{m-t}{s}B_s\,(m-i)^{m-t-s} \tag{54}$$

Так как $\forall t \in \mathbf{Z}_m^*$ и $t \neq m-1 : \gcd m - t, m = 1$, то

$$\frac{1}{m-t}\sum_{s=0}^{m-1-t}\binom{m-t}{s}B_s\,(m-i)^{m-t-s} \equiv \tag{55}$$
$$\equiv -\frac{1}{t}\sum_{s=0}^{m-1-t}\binom{m-t}{s}B_s\,(-i)^{m-t-s} \pmod m$$

Следовательно

$$\sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \equiv \tag{56}$$
$$\equiv \sum_{i=1}^{m-2} i^{m-1-k} \cdot \left(-\frac{1}{t}\sum_{s=0}^{m-1-t}\binom{m-t}{s}B_s\,(-i)^{m-t-s}\right)$$

Используя распределительный закон [4][стр. 48, формула 2.15], получим:

$$\sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} = \tag{57}$$

$$= \frac{(-1)^{m-1-t}}{t} \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{s=0}^{m-1-t} (-1)^s \binom{m-t}{s} B_s i^{m-t-s} =$$

$$= \frac{(-1)^{m-1-t}}{t} \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{s=0}^{m-1-t} (-1)^s \binom{m-t}{s} B_s \cdot t^{m-t-s} =$$

$$= \frac{(-1)^{m-1-t}}{t} \sum_{s=0}^{m-1-t} (-1)^s \binom{m-t}{s} B_s \sum_{i=1}^{m-2} i^{2m-t-k-s-1}.$$

Представим $\sum_{i=1}^{m-2} i^{2m-t-k-s-1}$ в следующем виде, получим:

$$\sum_{i=1}^{m-2} i^{2m-t-k-s-1} = -(m-1)^{2m-t-k-s-1} \sum_{i=1}^{m-1} i^{2m-t-k-s-1} \tag{58}$$

Так как по условию $t + k > m$, то $1 \leq 2m - t - k - s < m$, следовательно $\gcd 2m - t - k - s, m = 1$ и

$$\left| \sum_{i=1}^{m-2} i^{2m-t-k-s-1} \right|_m \equiv -(-1)^{2m-t-k-s-1} + \tag{59}$$

$$+ \frac{1}{2m-t-k-s} \sum_{j=0}^{2m-t-k-s-1} \binom{2m-t-k-s}{j} B_j m^{2m-t-k-s-j} \equiv$$

$$\equiv (-1)^{2m-t-k-s} \pmod{m}$$

Следовательно,

$$\sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} \equiv \tag{60}$$

$$\equiv \frac{(-1)^{m-1-t}}{t} \sum_{s=0}^{m-1-t} (-1)^s \binom{m-t}{s} B_s (-1)^{2m-t-k-s} \equiv$$

$$\equiv \frac{(-1)^{m-1-t} (-1)^{2m-t-k}}{t} \sum_{s=0}^{m-1-t} \binom{m-t}{s} B_s$$

Учитывая, что $\forall t \in \mathbb{Z}_m^*$ и $t \neq m-1 : m-1-t > 0$, то используя [4][стр. 314, формула 2.79]

$$\sum_{s=0}^{m-1-t} \binom{m-t}{s} B_s = 0 \tag{61}$$

Таким образом согласно свойству 2, если $t + k$ – четное число, то $b_{t,k} = 0$. Если t–четное, k–нечетное, $t + k > m$ и $t \neq m - 1$, то

$$b_{t,k} = 2 \cdot \sum_{i=1}^{m-2} i^{m-1-k} \cdot \sum_{j=1}^{m-i-1} j^{m-1-t} = 2 \cdot 0 = 0 \tag{62}$$

Если t–нечетное, k–четное, $t+k>m$ и $t\neq m-1$, то

$$b_{t,k}=-2\cdot\sum_{i=1}^{m-2}i^{m-1-k}\cdot\sum_{j=1}^{m-i-1}j^{m-1-t}=-2\cdot 0=0 \tag{63}$$

Из свойства 3 следует, что если $t=m-1$, $t+k$ – нечетное число и $t+k>m$, то $b_{t,k}=0$ Следовательно, если $t+k>m$, то $b_{t,k}=0$. □

Из свойства 4 следует, что степень многочлена $c\,(x,y)\leq m$, с другой стороны, согласно свойству 3 $b_{m-1,1}=2$, следовательно коэффициент при $x^{m-1}y$ не равен нулю, значит $\deg c\,(x,y)=m$.Таким образом мы уточнили оценку степени многочлена из работы [2] с $2m-2$ до m.

Пример. Вычислить многочлен (x,y) над $\mathbb{Z}_5$.

Используя свойство 3, вычислим, значения коэффициентов $b_{t,k}$, получим:

$$b_{2,1}=\left|2\cdot\sum_{i=1}^{3}i^3\cdot\sum_{j=1}^{4-i}j^2\right|_m=\left|2\cdot(1+4+9+8\cdot 1+8\cdot 4+27\cdot 1)\right|_5=2 \tag{64}$$

$$b_{3,2}=\left|-2\cdot\sum_{i=1}^{3}i^2\cdot\sum_{j=1}^{4-i}j^2\right|_m=\left|-2\cdot(1+2+3+4\cdot 1+4\cdot 2+9\cdot 1)\right|_m=1 \tag{65}$$

Согласно лемме 1, $b_{4,1}=2$. Используя теорему 2, вычислим значения коэффициентов $b_{1,2}$, $b_{2,3}$ и $b_{1,4}$, получим:

$$b_{1,2} = -b_{2,1}=3 \pmod 5 \tag{66}$$

$$b_{2,3} = -b_{3,2}=4 \pmod 5 \tag{67}$$

$$b_{1,4} = -b_{4,1}=3 \pmod 5 \tag{68}$$

Таким образом многочлен (x,y) над $\mathbb{Z}_5$ имеет, следующий вид:

$$c\,(x,y)=x^4-y^4+3\cdot x\cdot y^2+3\cdot x\cdot y^4+4\cdot x^2\cdot y^3+x^3\cdot y^2+2\cdot x^4\cdot y+2\cdot x^2\cdot y \tag{69}$$

Рассмотрим результат вычисления многочлена $c\,(x,y)$ над $\mathbb{Z}_5$. Результаты вычисления приведем в таблице 1:

Таблица 1. Вычисление многочлена $c\,(x,y)$ над $\mathbb{Z}_5$

$c\,(x,y)$		y				
		0	1	2	3	4
x	0	0	-1	-1	-1	-1
	1	1	0	-1	-1	-1
	2	1	1	0	-1	-1
	3	1	1	1	0	-1
	4	1	1	1	1	0

5. Заключение

Вычислительная сложность алгоритма сравнения зашифрованных чисел с использованием целочисленных гомоморфных шифров зависит от количества

арифметических операций сложения, умножения которые необходимо произвести, для вычисления интерполяционного многочлена. При реализации схемы гомоморфного сравнения чисел является мультипликативная глубина алгоритма сравнения чисел, так как целочисленные гомоморфные шифры поддерживают ограниченное число умножений. Как показано в работе [5] мультипликативная глубина вычисления многочлена с помошью алгоритма Paterson–Stockmeyer зависит от степени многочлена. Мы уточнили оценку степени интерполяционного многочлена функции сравнения зашифрованных чисел из работы [2] с $2m-2$ до m.

References

[1] R. Lidl, H. Niederreiter, *Finite fields*, M.: Mir, 1988.
[2] B.H.M. Tan, H.T. Lee, H. Wang, S.Q. Ren, A.M.M. Khin, *Efficient private comparison queries over encrypted databases using fully homomorphic encryption with finite fields*, IEEE Transactions on Dependable and Secure Computing, 2020.
[3] E. Vinberg, *Algebra course*, Litres, 2017.
[4] R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete mathematics: a foundation for computer science*, Addison-Wesley, Reading, MA, 1989.
[5] R. Player, *Parameter selection in lattice-based cryptography*, Doctoral dissertation, Royal Holloway, University of London, 2018.

Babenko Mikhail Grigorievich
North-Caucasus Federal University,
Pushkin Street, 1,
355017, Stavropol, Russia
Email address: mgbabenko@ncfu.ru

Kucherov Nikolay Nikolaevich
North-Caucasus Federal University,
Pushkin Street, 1,
355017, Stavropol, Russia
Email address: nkucherov@ncfu.ru

Nguyen Viet Hung
Le Quy Don Technical University,
236 Hoang Quoc Viet,
Hanoi, Vietnam
Email address: hungnv@lqdtu.edu.vn