2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/3

УДК 512.548.2

ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ В КОНЕЧНОМЕРНОЙ АЛГЕБРЕ НАД ПОЛЕМ[1]

С. Ю. Катышев

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: sairos87@mail.ru

Описывается алгоритм, сводящий с полиномиальной сложностью задачу дискретного логарифмирования в конечномерной алгебре к задаче дискретного логарифмирования над конечным полем.

Ключевые слова: *открытое распределение ключей, неассоциативные группоиды, конечномерные алгебры, дискретное логарифмирование.*

Введение

В работе [1] предложены варианты обобщения хорошо известного алгоритма Диффи — Хеллмана [2], использующего циклические группы для реализации протокола открытого распределения ключей, на случай, когда вместо группы используется неассоциативный группоид. Опишем один из вариантов предложенных обобщений.

Для элемента g конечного группоида $(\Omega, *)$ и заданного $r \in \mathbb{N}$ определим *правую r-ю степень* равенством

$$g^{[r]} = \underbrace{(\ldots((g * g) * g)\ldots)}_{r \text{ сомножителей}}.$$

Назовём g *элементом с перестановочными правыми степенями*, или *ППС-элементом*, если

$$\forall m, n \in \mathbb{N} \quad \left(g^{[m][n]} = g^{[n][m]}\right).$$

Если это тождество выполняется для всех элементов $g \in \Omega$, то будем называть $(\Omega, *)$ *ППС-группоидом.*

Алгоритм открытого распределения ключей. Выбрав (несекретный) ППС-элемент g группоида Ω, абоненты A и B независимо друг от друга выбирают произвольные числа $r_A, r_B \in \mathbb{N}$ соответственно и обмениваются элементами $g^{[r_A]}$ и $g^{[r_B]}$. Затем формируют общий секретный ключ $g^{[r_A][r_B]} = g^{[r_B][r_A]}$.

Сложность восстановления наблюдателем секретного ключа по открытой информации g, $g^{[r_A]}$, $g^{[r_B]}$ не превосходит сложности *задачи правого дискретного логарифмирования в группоиде*, т. е. сложности решения уравнения

$$g^{[x]} = h.$$

В качестве ППС-группоида могут быть выбраны конечномерные алгебры над конечным полем, обладающие свойством перестановочности степеней.

В связи с этим представляется интересным решение задачи правого дискретного логарифмирования в неассоциативной конечномерной алгебре над полем.

В работе описывается алгоритм, с полиномиальной сложностью сводящий задачу дискретного логарифмирования в конечномерной алгебре к задаче дискретного логарифмирования над конечным полем.

[1]Работа выполнена при поддержке гранта Президента РФ НШ-6260.2012.10 и Академии криптографии РФ.

1. Основные определения и предварительные результаты

Пусть $(P,+,\cdot)$ — поле из q элементов с единицей e.

P-алгеброй, или алгеброй над полем P, называют P-модуль Ω с билинейным отображением $*:\Omega\times\Omega\to\Omega$, называемым *операцией умножения* [3]. Условие билинейности операции $*$ означает выполнение законов дистрибутивности справа и слева и условия

$$\forall u,v\in\Omega, a\in P\ \ ((u*v)a=u*(va)=(ua)*v=a(u*v)).$$

Размерностью P-алгебры называют размерность $\dim\Omega=\dim_P\Omega$ пространства ${}_P\Omega$.

Пусть $\mathbf{e}=(e_1,\dots,e_n)$ — базис конечномерной алгебры ${}_P\Omega$. Тогда операция $*$ определяется заданием произведений

$$e_i*e_j=\sum_{k=1}^{n}e_k a_{ij}^{(k)}, \tag{1}$$

поскольку из (1) и условия билинейности $*$ имеем

$$\left(\sum_{i=1}^{n}e_iu_i\right)*\left(\sum_{j=1}^{n}e_jv_j\right)=\sum_{k=1}^{n}e_k\left(\sum_{i,j=1}^{n}u_ia_{ij}^{(k)}v_j\right).$$

Элементы $a_{ij}^{(k)}$ из (1) называют *структурными константами* P-алгебры, набор матриц $A_k=(a_{ij}^k)_{n\times n}$, $k=1,\dots,n$, — *матрицами структурных констант.*

Рассмотрим представление P-алгебры в базисе $\mathbf{e}$. Пусть $\vec{u},\vec{v}\in P^n$ — строки координат элементов $u,v\in\Omega$ в базисе $\mathbf{e}$; тогда строка координат произведения $u*v$ удовлетворяет равенству

$$\overrightarrow{u*v}=(\vec{u}\,A_1v^{\downarrow},\dots,\vec{u}\,A_nv^{\downarrow}). \tag{2}$$

Для удобства изложения будем рассматривать P-алгебру Ω как её представление P^n в некотором базисе $\mathbf{e}$ с операцией (2). P-алгебру P^n с матрицами структурных констант $A_1,\dots,A_n$ и умножением, определённым равенством (2), будем обозначать $\mathscr{G}(A_1,\dots,A_n)$.

Рассмотрим свойства операции умножения в P-алгебре $\mathscr{G}(A_1,\dots,A_n)$, где $A_k=$ $=(a_{ij}^{(k)})_{n\times n}$, $k=1,\dots,n$.

Равенство (2) можно записать также следующим образом:

$$\begin{aligned}&\vec{u}*\vec{v}=\vec{u}\cdot R(\vec{v}),\quad R(\vec{v})=\left(A_1v^{\downarrow}\dots A_nv^{\downarrow}\right),\\&\vec{u}*\vec{v}=\vec{v}\cdot L(\vec{u}),\quad L(\vec{u})=\left(A_1^Tu^{\downarrow}\dots A_n^Tu^{\downarrow}\right).\end{aligned} \tag{3}$$

Тогда справедливо

Утверждение 1. Для произвольного элемента $\vec{u}$ P-алгебры $\mathscr{G}(A_1,\dots,A_n)$, для любого натурального k верны равенства

$$\vec{u}^{[k+1]}=\vec{u}\,R(\vec{u})^k,\quad {}^{[k+1]}\vec{u}=\vec{u}\,L(\vec{u})^k. \tag{4}$$

На основании равенств (4) можно предложить алгоритм вычисления степени $\vec{u}^{[k]}$, аналогичный бинарному алгоритму вычисления степени элемента абелевой группы [4], имеющий сложность, полиномиально зависящую от $\log k$.

P-алгебры $(\Omega, *, +)$ и $(\Omega, \star, +)$ называют *изоморфными*, если существует невырожденное линейное преобразование ψ пространства ${}_P\Omega$ со свойством

$$\forall u, v \in \Omega \quad (\psi(u) \star \psi(v) = \psi(u * v)).$$

Будем называть элемент u *реверсивным* (справа), если для некоторого натурального t выполнено $u^{[t+1]} = u$.

Утверждение 2. Если элемент $\vec{u} = (u_1, \dots u_n)$ P-алгебры $\mathscr{G}(A_1, \dots, A_n)$ реверсивен и существует набор $c_1, \dots, c_n$ элементов поля P, такой, что

$$c_1 A_1 + \ldots + c_n A_n = 0, \tag{5}$$

то выполнено соотношение $c_1 u_1 + \ldots + c_n u_n = 0$.

Лемма 1. Если вектор $\vec{\omega} = (\omega_1, \dots, \omega_n)$ равен произведению векторов $\vec{\alpha} * \vec{\beta}$, то при условии (5) для его координат выполнено соотношение

$$c_1\omega_1 + \ldots + c_n\omega_n = 0. \tag{6}$$

Доказательство. Верна цепочка равенств
$c_1\omega_1 + \ldots + c_n\omega_n = c_1\ \vec{\alpha}\ A_1\beta^{\downarrow} + \ldots + c_n\ \vec{\alpha}\ A_n\beta^{\downarrow} = \vec{\alpha}\ (c_1A_1 + \ldots + c_nA_n)\beta^{\downarrow} = 0$. ■

Доказательство утверждения 2. Для реверсивного элемента $\vec{u}$ существует $k > 1$, такое, что $\vec{u} = \vec{u}^{[k]} = \vec{u}^{[k-1]} * \vec{u}$. Теперь утверждение 2 следует из леммы 1. ■

Пусть $\mathscr{G}' = \{\vec{w} = (w_1, \dots, w_n) \in P^n : c_1w_1 + \ldots + c_nw_n = 0\}$. Заметим, что $\mathscr{G}'$ — подалгебра алгебры $\mathscr{G}(A_1, \dots, A_n)$, причём ввиду утверждения 2 $\mathscr{G}'$ содержит все реверсивные элементы. Будем называть $\mathscr{G}'$ *подалгеброй, определённой тождеством* (6).

Утверждение 3. Пусть $\mathscr{G}(A_1, \dots, A_n)$ — алгебра над полем P и существует ненулевой набор $c_1, \dots, c_{n-1}$ элементов поля P, такой, что $A_n = c_1A_1 + \ldots + c_{n-1}A_{n-1}$. Тогда подалгебра $\mathscr{G}'$ алгебры $\mathscr{G}$, определённая тождеством $\omega_n = c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$, изоморфна P-алгебре $\mathscr{G}(B_1, \dots, B_{n-1})$, где матрицы $B_k = (b_{ij}^k)_{(n-1)\times(n-1)}$ для $k = 1$, $\dots, n-1$ определены соотношениями

$$b_{ij}^k = a_{ij}^k + c_j a_{in}^k + c_i a_{nj}^k + c_i c_j a_{nn}^k, \quad i, j = 1, \dots, n-1. \tag{7}$$

Доказательство. Зададим отображение $\varphi : \mathscr{G}' \to \mathscr{G}(B_1, \dots, B_{n-1})$ следующим образом: $\varphi((\omega_1, \dots, \omega_n)) = (\omega_1, \dots, \omega_{n-1})$. Очевидно, φ биективно. Покажем, что φ — гомоморфизм. По определению φ

$$\forall\ \vec{u}, \vec{v} \in \mathscr{G}'\ \left(\varphi(\vec{u} * \vec{v}) = (\vec{u}\ A_1v^{\downarrow}, \dots, \vec{u}\ A_{n-1}v^{\downarrow})\right).$$

Для $k = 1, \dots, n-1$ рассмотрим k-ю координату:

$$\vec{u}\ A_kv^{\downarrow} = \left((u_1, \dots u_{n-1}, \sum_{i=1}^{n-1} c_iu_i)A_k(v_1, \dots v_{n-1}, \sum_{i=1}^{n-1} c_iv_i)^T\right) =$$

$$= \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} u_iv_ja_{ij}^k + \sum_{i=1}^{n-1} u_i\left(\sum_{j=1}^{n-1} c_jv_j\right)a_{in}^k + \sum_{j=1}^{n-1}\left(\sum_{i=1}^{n-1} c_iu_i\right)v_ja_{nj}^k + \left(\sum_{i=1}^{n-1} c_iu_i\right)\left(\sum_{j=1}^{n-1} c_jv_j\right)a_{nn}^k.$$

Сгруппировав суммы, получаем равенство

$$\vec{u}\ A_kv^{\downarrow} = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} u_iv_j(a_{ij}^k + c_ja_{in}^k + c_ia_{nj}^k + c_ic_ja_{nn}^k) = \varphi(\vec{u})B_k\varphi(\vec{v})^T.$$

Таким образом, $\varphi(\vec{u} * \vec{v}) = \left(\varphi(\vec{u})B_1\varphi(\vec{v})^T, \ldots, \varphi(\vec{u})B_{n-1}\varphi(\vec{v})^T\right) = \varphi(\vec{u}) \star \varphi(\vec{v})$, где $\star$ — операция в $\mathscr{G}(B_1, \ldots, B_{n-1})$. ■

Следующий результат иногда позволяет решить задачу проверки перестановочности степеней и дискретного логарифмирования в алгебре меньшей размерности.

Теорема 1. В алгебре $\mathscr{G}(A_1, \ldots, A_n)$ существует подалгебра $\mathscr{G}'$, содержащая все реверсивные элементы и изоморфная некоторой алгебре $\mathscr{G}(B_1, \ldots, B_t)$, $t \leqslant n$, такой, что система матриц $B_1, \ldots, B_t$ линейно независима.

Доказательство. Индукция по $k = n - \operatorname{rank}\{A_1, \ldots, A_n\}$ с применением утверждения 3. ■

Алгебру $\mathscr{G}(B_1, \ldots, B_t)$ из теоремы 1 будем называть *приведённым видом алгебры* $\mathscr{G}(A_1, \ldots, A_n)$.

Пусть $\vec{u}$ — произвольный элемент алгебры $\mathscr{G}(A_1, \ldots, A_n)$. Для произвольного $k \in \mathbb{N}$ положим $\vec{u}^{[k]} = (u_1^r(k), \ldots, u_n^r(k))$. Тогда последовательность векторов

$$\vec{u}^{\mathbb{N}} = (\vec{u}, \vec{u}^{[2]}, \ldots, \vec{u}^{[k]}, \ldots) \tag{8}$$

можно рассматривать как вектор $\vec{u}^{\mathbb{N}} = (u_1^r, \ldots, u_n^r)$ из n координатных последовательностей

$$u_i^r = (u_i^r(1) = u_i, u_i^r(2), \ldots, u_i^r(k), \ldots), \quad i = 1, \ldots, n. \tag{9}$$

Через $\vec{u}^{[\mathbb{N}]}$ обозначим множество всех различных элементов вида $\vec{u}^{[r]}$, $r \in \mathbb{N}$.

Следующее утверждение показывает, что задачи логарифмирования и определения потенциала элемента алгебры иногда могут быть перенесены в алгебру ещё меньшей размерности.

Утверждение 4. Пусть $\vec{u}$ — элемент P-алгебры $\mathscr{G}(A_1, \ldots, A_n)$. Тогда для некоторой P-алгебры $\mathscr{G}(B_1, \ldots, B_t)$, $t \leqslant n$, существует инъективное отображение $\varphi : \vec{u}^{[\mathbb{N}]} \to \to \mathscr{G}(B_1, \ldots, B_t)$, обладающее следующими свойствами:

1) система координатных последовательностей $\{\varphi(\vec{u})_i^r : i = 1, \ldots, t\}$ линейно независима;
2) для любого натурального k верно равенство $\varphi(u^{[k]}) = (\varphi(u))^{[k]}$.

Лемма 2. Пусть $\vec{u} \in \mathscr{G}(A_1, \ldots, A_n)$ и существует ненулевой набор $c_1, \ldots, c_{n-1}$ элементов поля P, такой, что система последовательностей $\{u_1^r, \ldots, u_n^r\}$ удовлетворяет соотношению

$$u_n^r = c_1u_1^r + \ldots + c_{n-1}u_{n-1}^r. \tag{10}$$

Рассмотрим алгебру $\mathscr{G}(B_1, \ldots, B_{n-1})$ с операцией $\star$, где матрицы структурных констант B_i определены соотношением (7). Тогда отображение $\psi : \vec{u}^{[\mathbb{N}]} \to \mathscr{G}(B_1, \ldots, B_{n-1})$, $\psi((v_1, \ldots, v_n)) = (v_1, \ldots, v_{n-1})$ есть инъективное отображение со свойством

$$\psi(u^{[*r]}) = (\psi(u))^{[\star r]}. \tag{11}$$

Доказательство. В силу соотношения (10) ψ инъективно. Докажем равенство (11) методом математической индукции. При $r = 1$ равенство очевидно. Пусть при $r = m$ утверждение верно, докажем его при $r = m + 1$. Пусть $v = u^{[*m]}$, тогда по определению ψ

$$\psi(\vec{u}^{[*m+1]}) = \psi(\vec{v} * \vec{u}) = (\vec{v}\ A_1u^{\downarrow}, \ldots, \vec{v}\ A_{n-1}u^{\downarrow}).$$

В силу (10) $u_n = \sum\limits_{i=1}^{n-1} c_i u_i$ и $v_n = \sum\limits_{i=1}^{n-1} c_i v_i$. Для $k = 1, \ldots, n-1$ рассмотрим k-ю координату вектора $\vec{u}^{[*(m+1)]}$:

$$\vec{v}\ A_k u^{\downarrow} = \left((v_1, \ldots v_{n-1}, \sum_{i=1}^{n-1} c_i v_i) A_k (u_1, \ldots u_{n-1}, \sum_{i=1}^{n-1} c_i u_i)^T \right) =$$

$$= \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} v_i u_j a_{ij}^k + \sum_{i=1}^{n-1} v_i \left(\sum_{j=1}^{n-1} c_j u_j \right) a_{in}^k + \sum_{j=1}^{n-1} \left(\sum_{i=1}^{n-1} c_i v_i \right) u_j a_{nj}^k + \left(\sum_{i=1}^{n-1} c_i v_i \right) \left(\sum_{j=1}^{n-1} c_j u_j \right) a_{nn}^k.$$

Сгруппировав суммы, получаем равенство

$$\vec{v}\ A_k u^{\downarrow} = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} v_i u_j (a_{ij}^k + c_j a_{in}^k + c_i a_{nj}^k + c_i c_j a_{nn}^k) = \psi(\vec{v}) B_k \psi(\vec{u})^T.$$

Тогда $\psi\left(\vec{u}^{[*(m+1)]}\right) = \left(\psi(\vec{v})B_1\psi(\vec{u})^T, \ldots, \psi(\vec{v})B_{n-1}\psi(\vec{u})^T\right) = \psi(\vec{v}) \star \psi(\vec{u}) =$
$= (\psi(u))^{[\star(m+1)]}$. ■

Доказательство утверждения 4. Индукция с применением леммы 2 по параметру $k = n - \operatorname{rank}\{\varphi(\vec{u})_i^r : i = 1, \ldots, n\}$. ■

Алгебру $\mathscr{G}(B_1, \ldots, B_t)$ из утверждения 4 будем называть *приведённой алгеброй для элемента* $\vec{u}$.

Замечание 1. Для нахождения линейной зависимости между координатными последовательностями степеней элемента $\vec{u}$ достаточно найти линейную зависимость между столбцами матрицы, составленной из строк $\vec{u}$, $\vec{u}^{[2]}$, …, $\vec{u}^{[n]}$.

2. Дискретное логарифмирование

Для любого унитарного многочлена $F(x) \in P[x]$ и любого $n \in \mathbb{N}$ обозначим через $L_{P^n}(F)$ семейство всех линейных рекуррентных последовательностей (ЛРП) над пространством ${}_P P^n$ с характеристическим многочленом $F(x)$ [5, 6].

Утверждение 5. Последовательности $\vec{u}^{\mathbb{N}}$ из (8) и u_i^r, $i = 1, \ldots, n$, из (9) суть ЛРП с характеристическим многочленом, равным характеристическому многочлену $\chi_{R(\vec{u})}(x)$ матрицы $R(\vec{u})$ из (3): $u^{\mathbb{N}} \in L_{P^n}(\chi_{R(\vec{u})})$; $u_i^r \in L_P(\chi_{R(\vec{u})})$, $i = 1, \ldots, n$.

Доказательство проводится стандартным способом, с использованием соотношений (4) и теоремы Гамильтона — Кэли (см., например, [6, Example 1.6]). ■

Пусть Q — поле разложения многочлена $\chi_{R(\vec{u})}(x)$ над P и

$$\chi_{R(\vec{u})}(x) = (x - \alpha_1)^{k_1} \cdot \ldots \cdot (x - \alpha_t)^{k_t} \tag{12}$$

— каноническое разложение этого многочлена над Q. Тогда существует представление координатных последовательностей u_i^r через соответствующие биномиальные последовательности [5, 6]:

Следствие 1. Для любого $i \in \{1, \ldots, n\}$ существует вектор-столбец $d_i^{r\downarrow} \in Q^{(n)}$, такой, что

$$u_i^r(k) = \left(\alpha_1^{k-1}, C_{k-1}^1 \alpha_1^{k-1}, \ldots, C_{k-1}^{k_1-1}\alpha_1^{k-1},\ \alpha_2^{k-1}, \ldots, C_{k-1}^{k_2-1}\alpha_2^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) d_i^{r\downarrow}. \tag{13}$$

Для краткости будем использовать запись

$$u_i^r(k) = \left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) d_i^{r\downarrow}, \quad i \in \{1, \ldots, n\}.$$

Следствие 2. При условии (12) существует матрица $D \in Q_{n,n}$, такая, что для любого натурального k правая степень элемента $\vec{u}$ представляется в виде

$$\vec{u}^{[k]} = \left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) D. \tag{14}$$

При этом следующие утверждения равносильны:

a) система координатных последовательностей $u_1^r, \ldots, u_n^r$ последовательности $\vec{u}^{\mathbb{N}}$ линейно независима;

b) матрица D обратима.

Доказательство. Ввиду (13) матрица $D = (d_1^{r\downarrow}, \ldots, d_n^{r\downarrow}) \in Q_{n,n}$ удовлетворяет условию (14).

$(a) \Rightarrow (b)$. Если D — вырожденная матрица, то $Dc^\downarrow = 0^\downarrow$ для некоторого $c^\downarrow \in Q^{(n)} \setminus \{0^\downarrow\}$, и ввиду (14) $(u_1^r, \ldots, u_n^r)c^\downarrow = 0$, что противоречит условию (a).

$(b) \Rightarrow (a)$. Если система координатных последовательностей $u_1^r, \ldots, u_n^r$ линейно зависима, то $(u_1^r, \ldots, u_n^r)c^\downarrow = 0$ для некоторого $c^\downarrow \in Q^{(n)} \setminus \{0^\downarrow\}$. Тогда ввиду (14) для вектора $c'^\downarrow = Dc^\downarrow \neq 0^\downarrow$ выполнено равенство $\left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) c'^\downarrow = 0^\downarrow$. Противоречие, так как система биномиальных последовательностей линейно независима. ■

Следствие 3. В условиях следствия 2 если матрица D обратима, то $\chi_{R(\vec{u})}$ есть минимальный многочлен последовательности $u^{\mathbb{N}}$.

Доказательство. Пусть $G(x) \in P[x]$ — минимальный многочлен ЛРП $u^{\mathbb{N}}$. Тогда $G(x)|\chi_{R(\vec{u})}(x)$, и если $G(x) \neq \chi_{R(\vec{u})}(x)$, то $\deg G(x) = m < n$. В таком случае система из n координатных последовательностей $u_1^r, \ldots, u_n^r$ принадлежит подпространству $L_P(G)$ размерности m и является линейно зависимой. Ввиду (14) это означает, что линейно независимая система из n биномиальных последовательностей $\left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right)$ при умножении на матрицу D становится линейно зависимой, что противоречит обратимости матрицы D. ■

На основании равенства (14) можно предложить метод дискретного логарифмирования. Пусть $\mathscr{G}(A_1, \ldots, A_n)$ — произвольная алгебра над некоторым полем P. Для элементов $\vec{u}, \vec{v} \in \mathscr{G}(A_1, \ldots, A_n)$ решается уравнение $\vec{u}^{[n]} = \vec{v}$.

Ввиду утверждения 4 можем считать, что рассматриваемая алгебра является приведённой алгеброй для элемента $\vec{u}$, то есть система координатных последовательностей $\{u_1^r, \ldots, u_n^r\}$ линейно независима.

Пусть Q — расширение поля P, являющееся полем разложения характеристического многочлена $\chi_R(x)$ матрицы $R = (A_1u^\downarrow, \ldots, A_nu^\downarrow)$. Элементы $\alpha_1, \ldots, \alpha_t$ — корни многочлена $\chi_R(x)$, k_i — кратность корня α_i, $i = 1, \ldots, t$.

Замечание 2. Задача нахождения корней многочлена, очевидно, сводится к разложению многочлена на неприводимые сомножители (над полем разложения). Разложение многочлена степени n на множители имеет полиномиальную трудоёмкость относительно величины $n \log |P|$, то есть относительно размера задачи $(\log |P^n|)$. Подробный обзор методов разложения многочлена на множители можно найти в [4].

Последовательность степеней элемента P-алгебры представляется в виде (14), причём матрица D обратима, так как система координатных последовательностей $\{u_i(k) : k = 1, \ldots, n\}$ линейно независима.

Для нахождения матрицы D можно решать систему, составленную из равенств (14), для различных степеней $k \in \{1, \ldots, n\}$. Однозначность нахождения матрицы D следует из линейной независимости системы биномиальных последовательностей в правой части равенства (14). Сложность вычисления матрицы D_r полиномиальна относительно размера матрицы, её можно оценить величиной $\mathrm{O}(n^3)$.

При умножении обеих частей равенства (14) на матрицу D^{-1} справа получаем

$$\vec{v}\ D^{-1} = \vec{u}^{[x]}\ D^{-1} = \left(\alpha_1^{x-1}, C_{x-1}^1\alpha_1^{x-1}, \ldots, C_{x-1}^{k_1-1}\alpha_1^{x-1},\ \alpha_2^{x-1}, \ldots, C_{x-1}^{k_2-1}\alpha_2^{x-1}, \ldots, C_{x-1}^{k_t-1}\alpha_t^{x-1}\right).$$

Пусть $\vec{v}\ D^{-1} = (w_1, \ldots, w_n)$, тогда нахождение решения уравнения (14) равносильно решению системы уравнений

$$\begin{cases} \alpha_1^{x-1} = w_1, \\ C_{x-1}^1\alpha_1^{x-1} = w_2, \\ \ldots \\ C_{x-1}^{k_1-1}\alpha_1^{x-1} = w_{k_1}, \\ \alpha_2^{x-1} = w_{k_1+1}, \\ \ldots \\ C_{x-1}^{k_t-1}\alpha_t^{x-1} = w_n. \end{cases}$$

Нетрудно показать, что решение данной системы уравнений не сложнее однократного логарифмирования в поле Q по основанию примитивного элемента.

В качестве вывода сформулируем результат.

Теорема 2. Задача дискретного логарифмирования на P-алгебре Ω размерности n с полиномиальной сложностью сводится к задаче дискретного логарифмирования в поле Q, являющемся расширением степени l поля P, где $l < n$.

Сложность задачи дискретного логарифмирования в конечном поле имеет субэкспоненциальную оценку. Подробный обзор методов дискретного логарифмирования в конечном поле можно найти, например, в [4].

ЛИТЕРАТУРА

1. *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для открытого распределения ключей // Дискретная математика. 2014. Т. 46. № 3. С. 51–59.
2. *Diffie W. and Hellman M. E.* New directories in cryptography // IEEE Trans. Inf. Theory. 1976. V. 22. P. 644–654.
3. *Пирс Р.* Ассоциативные алгебры: пер. с англ. М.: Мир, 1986. 543 с.
4. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. 2-е изд. М.: МЦНМО, 2007. 326 с.
5. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. В 2-х т. М.: Гелиос, 2003. 336 + 416 с.
6. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.