Math-Net.Ru

Общероссийский математический портал

А. С. Кузьмин, Г. Б. Маршалко, А. А. Нечаев, Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению, *Матем. вопр. криптогр.*, 2010, том 1, выпуск 2, 31–56

DOI: <https://doi.org/10.4213/mvk9>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.253.173

26 апреля 2023 г., 16:34:40

УДК: 511.216, 519.113.6

Восстановление линейной рекуррентной последовательности над примарным кольцом вычетов по ее усложнению

А. С. Кузьмин¹, Г. Б. Маршалко², А. А. Нечаев³

^{1,3} Академия криптографии Российской Федерации, Москва

² Лаборатория ТВП, Москва

Получено 22.IV.2010

Рассматриваются псевдослучайные последовательности v над полем $\mathbb{Z}_p$, $p \geq 3$, которые получаются усложнением знаков ЛРП u максимального периода над кольцом $\mathbb{Z}_{p^n}$. Изучаются возможность и способы однозначного восстановления u по v . Приводится обзор предшествующих результатов.

Ключевые слова: Линейная рекуррентная последовательность, кольцо вычетов, примитивный многочлен

Reconstruction of linear recurrent sequence over prime residue ring from its image

A. S. Kuzmin¹, G. B. Marshalko², A. A. Nechaev³

^{1,3} Academy of Cryptography of Russian Federation, Moscow

² TVP Laboratory, Moscow

Abstract. We consider pseudorandom sequences v over $\mathbb{Z}_p$, $p \geq 3$, obtained from a primitive sequence u over integer residue ring $\mathbb{Z}_{p^n}$ by means of some compressing map. We study sufficient conditions for the reconstruction of u from known v and suggest some methods of such reconstruction. The review of known results is presented also.

Key words: Compressing map, integer residue ring, linear recurrent sequence, primitive sequence

Citation: *Mathematical Aspects of Cryptography*, 2010, vol. 1, no. 2, pp. 31–56 (Russian).

Введение

Одной из актуальных проблем современной криптографии является разработка различных способов получения псевдослучайных последовательностей (ПСП). К настоящему моменту достаточно глубоко исследованы и широко применяются способы построения ПСП, основанные на усложнении линейных рекуррентных последовательностей над полем.

В последние десятилетия в отечественной литературе в работах А. А. Нечаева, А. С. Кузьмина, В. Л. Куракина и их учеников были опубликованы способы получения ПСП из координатных последовательностей линейных рекуррентных последовательностей (ЛРП) над кольцами вычетов и кольцами Галуа по следующей схеме.

Пусть p — простое число, $n \in \mathbb{N}$ и $R = (\mathbb{Z}_M, +, \cdot)$ — кольцо вычетов кольца $\mathbb{Z}$ целых чисел по модулю $M = p^n$ с единицей e . Пусть $G(x) \in R[x]$ — унитарный многочлен степени m вида $G(x) = x^m - \sum_{j=0}^{m-1} g_j \cdot x^j$, $g_j \in R$. Последовательность $u: \mathbb{N}_0 \rightarrow R$ над кольцом R называют линейной рекуррентной последовательностью (ЛРП) порядка m с характеристическим многочленом $G(x)$, если ее знаки удовлетворяют соотношениям

$$u(i+m) = \sum_{j=0}^{m-1} g_j \cdot u(i+j), \quad i = 0, 1, 2, \dots$$

В этом случае унитарный многочлен $G(x) = x^m - \sum_{j=0}^{m-1} g_j \cdot x^j$ называют характеристическим многочленом последовательности u .

Характеристический многочлен ЛРП u наименьшей возможной степени называют ее минимальным многочленом, а его степень $\text{гк } u$ — рангом (линейной сложностью) этой последовательности. Если последовательность u не является линейной рекуррентой, то полагаем $\text{гк } u = \infty$.

Каждый элемент $a \in R$ имеет однозначное p -ичное представление вида:

$$a = \sum_{s=0}^{n-1} a_s \cdot p^s, \quad a_s \in \mathbb{Z}_p = \{0, \dots, p-1\}, \quad s \in \{0, \dots, n-1\}.$$

Будем называть коэффициент a_s в последней сумме s -й (p -ичной) координатой элемента a и использовать обозначение $a_s = \delta_s(a)$. В соответствии с этим каждой последовательности $u \in R^\infty$ соответствуют n последовательностей $u_s = \delta_s(u) \in \mathbb{Z}_p^\infty$, $s \in \{0, \dots, n-1\}$, члены которых определяются соотношением

$$u(i) = \sum_{s=0}^{n-1} u_s(i) \cdot p^s, \quad u_s(i) = \delta_s(u(i)), \quad s \in \{0, \dots, n-1\}. \quad (1)$$

Назовем $u_0, \dots, u_{n-1}$ *координатными последовательностями последовательности u* . Очевидно, каждая из этих последовательностей есть ЛРП над полем $\mathbb{Z}_p$.

Основным объектом изучения в качестве ПСП являются последовательность u_{n-1} и последовательности $v \in \mathbb{Z}_p^\infty$ более общего вида:

$$v(i) = \Psi(u(i)), \quad (2)$$

где $\Psi: R^k \rightarrow \mathbb{Z}_p$, $k \in \{0, \dots, n-1\}$ — некоторая функция. Будем кратко писать в этом случае $v = \Psi(u)$. Заметим, что, пользуясь разложением (1), функцию $\Psi(x)$ над R можно рассматривать как многочлен $\Psi(x) = \psi(x_0, \dots, x_{n-1})$ над полем $\mathbb{Z}_p$ от переменных $x_s = \delta_s(x)$. При этом последовательности $z = u_{n-1}$ соответствует функция $\Psi(x) = \psi(x_{n-1}) = x_{n-1}$.

Требуется сформулировать условия на многочлен G и функцию усложнения Ψ , при которых возможно восстановление исходной рекурренты u по последовательности z , т. е. однозначное определение элементов исходной последовательности по элементам усложненной последовательности.

Унитарный многочлен $G(x) \in R[x]$ назовем *реверсивным*, если существуют числа $t \in \mathbb{N}$ такие, что $G(x) \mid x^t - e$. Наименьшее из таких t называется *периодом многочлена $G(x)$* и обозначается $T(G)$. Критерий реверсивности многочлена $G(x)$: $G(0) \in R^*$, т. е. $G(0) \not\equiv 0 \pmod{p}$.

Известно, что для любого реверсивного многочлена $G(x) \in R[x]$ степени m выполняется неравенство

$$T(G) \leq p^{n-1}(p^m - 1).$$

Если $T(G) = p^{n-1}(p^m - 1)$, то многочлен G называется *многочленом максимального периода (МП-многочленом)* или *примитивным многочленом над кольцом R* .

Для любого реверсивного многочлена $G(x) \in R[x]$ ЛРП $u \in L_R(G)$, будем называть *реверсивной (чисто периодической) последовательностью*, ее период удовлетворяет условию $T(u) \mid T(G)$. При этом существуют последовательности $u \in L_R(G)$ со свойством $T(u) = T(G)$.

Таким образом, любая реверсивная ЛРП над R ранга m имеет период $T(u) \leq p^{n-1}(p^m - 1)$. Последовательность u над R будем называть *линейной рекуррентой максимального периода (ЛРП МП)*, если

$$\text{rk } u = m, \quad T(u) = p^{n-1}(p^m - 1). \quad (3)$$

Назовем поле $\overline{R} = R/pR = \mathbb{Z}_p$ полем вычетов кольца R и для любой последовательности $u \in R^\infty$ и любого многочлена $G(x) \in R[x]$ через $\overline{u}$, $\overline{G}$

обозначим соответствующие образы при естественном эпиморфизме $R \rightarrow \bar{R}$. Для любого унитарного многочлена $G(x) \in R[x]$ положим

$$L_R(G)^* = \{u \in L_R(G) : \bar{u} \neq \bar{0}\}.$$

Тогда (3) равносильно тому, что для некоторого унитарного многочлена $G(x) \in R[x]$ степени m выполняются условия

$$u \in L_R(G)^*, \quad T(G) = p^{n-1}(p^m - 1). \quad (4)$$

Заметим, что условие (4) влечет за собой условие $T(\bar{G}(x)) = p^m - 1$, т. е. $\bar{G}(x)$ — неприводимый и, более того, примитивный многочлен над $\bar{R}$.

В [5–14] были получены результаты, подтверждающие хорошие статистические свойства и сложное аналитическое строение (большую линейную сложность) ПСП вида (2) при условии (4). Были разработаны алгоритмы определения начального вектора ЛРП МП по ее старшей координатной последовательности.

Параллельно появилась серия зарубежных публикаций [19–28], в которых также рассматривались усложнения (2) последовательности (4), названные *сжимающими отображениями* (compressing maps). Исследовались классы таких отображений, которые «не приводят к потере информации», т. е. позволяют однозначно восстановить исходную ЛРП по ее усложнению. Последние названы *инъективными* (injective compressing maps). Однако результаты этих работ получены при существенных, не всегда оправданных ограничениях как на соответствующий характеристический многочлен ЛРП, так и на параметры функции усложнения. Кроме того, в этих работах доказывалась лишь принципиальная возможность восстановления последовательности u по последовательности z и не указываются алгоритмы восстановления.

В данной работе для случая $p \geq 3$ на основе полученных ранее методов изучения свойств координатных последовательностей ЛРП МП u над $\mathbb{Z}_{p^n}$ получены более общие условия возможности восстановления u по ее полиномиальному усложнению z , а также построены конкретные алгоритмы восстановления начального вектора рекурренты в этой ситуации.

Структура настоящей работы такова.

В первом параграфе приводится краткий обзор полученных к настоящему моменту результатов в исследуемой области.

Во втором параграфе излагается математический аппарат. Основным инструментом, используемым при доказательстве возможности восстановления рекурренты и построения самого алгоритма восстановления, является метод сечений. Под *сечением координатной последовательности* в данном случае понимается результат ее умножения на подходящий многочлен, являющийся существенно более простой последовательностью.

В третьем параграфе описаны методы восстановления для различных типов функций усложнения. В частности, приводятся алгоритм восстановления рекуррент по старшей координатной последовательности, оценки его сложности и количества необходимого материала.

В четвертом параграфе исследуются вопросы принципиальной возможности восстановления исходной рекуррентной последовательности в случае, когда функция усложнения, зависящая только от старшей координатной последовательности, имеет произвольный вид.

Случай $p = 2$ планируется рассмотреть в следующей статье.

1. Обзор результатов

Принципиально важной является теорема 1.

Теорема 1. Пусть $G(x)$ — МП-многочлен над R . Тогда сжимающее отображение Ψ вида $\Psi(x) = \delta_{n-1}(x) = x_{n-1}$ инъективно, т. е. для любых $u, u' \in L_R(G)^*$

$$u = u' \iff u_{n-1} = u'_{n-1}.$$

Этот результат получен в 1982 г. А. А. Нечаевым для $p = 2$ и в 1985 г. А. С. Кузьминым для $p > 2$. При этом были построены алгоритмы восстановления u по u_{n-1} и оценена их сложность. Теорема 1 в эквивалентной формулировке (в терминах теории кодов) была опубликована в [2].

Эта теорема показывает, что ЛРП МП над кольцом $\mathbb{Z}_{p^n}$ однозначно определяется своей старшей координатной последовательностью. В работах [5, 12, 14] показано, что последняя имеет большую линейную сложность.

Независимо, в более слабой форме, этот результат был получен в [19].

Всюду далее $R = \mathbb{Z}_{p^n}$, $p \geq 3$, $n > 1$, $G(x) \in R[x]$ — МП-многочлен степени m . Положим $\tau = p^m - 1$. Тогда существует (см. [2, 3, 12]) единственный многочлен $\Phi_1(x) \in R[x]$ такой, что

$$x^\tau \equiv e + p\Phi_1(x) \pmod{G(x)}, \quad \deg \Phi_1(x) < m, \quad \overline{\Phi}_1(x) \neq \overline{0}. \quad (5)$$

Для любой ЛРП $u \in L_R(G)^*$ назовем последовательность

$$u^{(s)} = \Phi_s(x)u$$

s -й производной (от) последовательности u . Заметим, что так как по предположению $\overline{G}(x)$ — неприводимый многочлен над полем $\overline{R}$, то $(\overline{\Phi}_s(x), \overline{G}(x)) = \overline{e}$, и потому $u^{(s)} \in L_R(G)^*$. Кроме того, в силу (11) справедливы равенства:

$$u_0^{(s)} = u_0^{(1)}, \quad s \in \{2, \dots, n-1\}. \quad (6)$$

В работе [21] для случая $p > 2$ была доказана теорема о возможности восстановления ЛРП МП по расположению нулей на определенных местах старшей координатной последовательности.

Теорема 2. Пусть $u, v \in L_R(G)^*$ и $u^{(1)} = \Phi_1(x)u$. Тогда если

$$\forall i \in \mathbb{N}_0: (u_0^{(1)}(i) \neq 0) \Rightarrow (u_{n-1}(i) = 0 \iff v_{n-1}(i) = 0),$$

то $u = v$.

Следующие результаты доказывают возможность восстановления ЛРП МП u по последовательности z вида (2) в случае усложнения более общего вида, чем в теореме 1.

Теорема 3. Последовательность $u \in L_R(G)^*$ однозначно восстанавливается по последовательности (2) в следующих ситуациях:

(а) $p \geq 5$, $\Psi(x) = x_{n-1}^k \oplus \eta(x_0, \dots, x_{n-2})$, $k \in \{2, \dots, p-1\}$ (см. [22]);

(б) $p \geq 3$, $\deg \bar{\Phi}_1(x) \geq 1$;

$$\Psi(x) = g(x_{n-1}) \oplus \eta(x_0, \dots, x_{n-2}), \quad 1 \leq \deg g(x_{n-1}) \leq p-1 \quad (\text{см. [24]}).$$

Ниже результат теоремы 3 (а) распространяется теоремой 7 на случай $k = 1$, $p \geq 3$, $\deg \eta_{x_{n-1}}(x_0, \dots, x_{n-1}) \leq p-2$ с указанием алгоритма восстановления ЛРП u и оценкой его сложности.

Отметим, что в [22, 24] МП-многочлен G с условием $\deg \bar{\Phi}_1(x) \geq 1$ называется *сильно примитивным*.

Случай (б) теоремы 3 обобщается теоремой 8, которая позволяет избавиться от ограничения $\deg \bar{\Phi}_1(x) \geq 1$ и рассматривать более широкий класс многочленов $\Psi(x)$.

Теорема 4. (См. [23]). Пусть $\deg \Phi_1(x) \geq 1$ и $\mathcal{G}$ — множество всех многочленов вида

$$\Psi(x) = g(x_{n-1}) \oplus \eta(x_0, \dots, x_{n-2}) \in \mathbb{Z}_p[x_0, \dots, x_{n-1}], \quad 2 \leq \deg g(x_{n-1}) \leq p-1.$$

Тогда

$$\forall \Psi_1, \Psi_2 \in \mathcal{G}, u, v \in L_R(G)^*: \Psi_1(u) = \Psi_2(v) \iff (\Psi_1 = \Psi_2, u = v).$$

2. Математический аппарат

2.1. Свойства функции переноса в кольце $\mathbb{Z}_{p^n}$

Очевидно, для любых $x, y \in \{0, \dots, p-1\}$ справедливо равенство $x + y = \delta_0(x + y) + p\delta_1(x + y)$. В дальнейшем важна функция $\Delta(x, y)$, которую можно определить следующим образом:

$$\Delta: \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p,$$

$$\Delta(x, y) = \begin{cases} 0, & \text{если в кольце } \mathbb{Z} \quad x + y < p; \\ 1, & \text{если в кольце } \mathbb{Z} \quad x + y \geq p. \end{cases} \quad (7)$$

Мы назовем Δ функцией переноса в кольце $\mathbb{Z}_{p^n}$. Она может быть задана полиномом над полем $\mathbb{Z}_p$ вида

$$\Delta(x, y) = \sum_{\alpha, \beta \in \overline{0, p-1}} c_{\alpha, \beta} x^\alpha y^\beta.$$

Более того, так как $\Delta(0, y) = \Delta(x, 0) = 0$, то в этом представлении все коэффициенты $c_{0, \beta}, c_{\alpha, 0}$ равны нулю, т. е.

$$\Delta(x, y) = \sum_{\alpha, \beta \in \overline{1, p-1}} c_{\alpha, \beta} x^\alpha y^\beta. \quad (8)$$

Вид данной функции более точно описывает следующая лемма.

Лемма 1. (См. [7, 15]). Пусть функция $\Delta(x, y)$ определена условиями (7), тогда коэффициенты из представления (8) функции $\Delta(x, y)$ в виде полинома над $\mathbb{Z}_p$ удовлетворяют соотношениям:

1. $c_{\alpha, \beta} = c_{\beta, \alpha}, \alpha, \beta \in \{0, \dots, p-1\};$
2. $c_{\alpha, \beta} = 0$, если $\alpha + \beta > p;$
3. $c_{\alpha, \beta} = (-1)^{\alpha+\beta} \frac{(\alpha + \beta - 1)!}{\alpha! \beta!} q_{p-\alpha-\beta}, \alpha + \beta \leq p, \alpha > 0, \beta > 0, \quad (9)$

где последовательность $q_0, q_1, \dots$ задается рекуррентным соотношением

$$\sum_{s=0}^r q_s \binom{r}{s} \frac{1}{r+1-s} = 1, \quad q_0 = 1, \quad q_1 = \frac{1}{2}.$$

Непосредственным вычислением с помощью формулы (9) доказывається следующая теорема.

Теорема 5. В условиях леммы 1 при $p \geq 3$ коэффициенты функции $\Delta(x, y)$ удовлетворяют равенствам:

1. $c_{\alpha, \beta} = \frac{(-1)^\alpha}{\alpha}$, если $\alpha + \beta = p$;
2. $c_{\alpha, \beta} = \frac{(-1)^{\alpha+1}}{2}$, если $\alpha + \beta = p - 1$;
3. $c_{\alpha, \beta} = 0$, если $\alpha + \beta < p - 1$, $\alpha + \beta \not\equiv 0 \pmod{2}$.

Другими словами, справедливо равенство

$$\begin{aligned} \Delta(x, y) = & \sum_{\alpha=1}^{p-1} \frac{(-1)^\alpha}{\alpha} x^\alpha y^{p-\alpha} + \sum_{\alpha=1}^{(p-2)} \frac{(-1)^{(\alpha+1)}}{2} x^\alpha y^{p-1-\alpha} + \\ & + \sum_{i=1}^{\frac{p-3}{2}} \sum_{\alpha=1}^{2i-1} c_\alpha x^\alpha y^{2i-\alpha}. \end{aligned} \quad (10)$$

2.2. Сечения

Всюду далее $G(x)$ — МП-многочлен степени m над $R = \mathbb{Z}_{p^n}$, $p \geq 3$, $n \geq 2$. Обозначим $\tau_s = p^s(p^m - 1)$, $s = \{0, \dots, n-1\}$. Заметим, что $\tau_0 = \tau$.

Предложение 1. (См. [2, 3, 5, 12]). Пусть $u \in L_R(G)$. Тогда:

(а) если $u_0 \neq 0$, то

$$\begin{aligned} T(u) &= T(G(x)) = \tau_{n-1}, \\ T(u_s) &= \tau_s, \quad s \in \{0, \dots, n-1\}; \end{aligned}$$

(б) если $u_0 = u_1 = \dots = u_{s-1} = 0$, $u_s \neq 0$, $1 \leq s \leq n-1$, то

$$T(u) = p^{-s} T(G(x)) = \tau_{n-s-1}.$$

В работах [2, 3, 5, 12] показано, что для многочлена максимального периода справедливы следующие соотношения, обобщающие (5):

$$\begin{aligned} x^{\tau_s} - e &\equiv p^{s+1} \Phi^{(s+1)}(x) \pmod{G(x)}, \quad \deg \Phi^{(s+1)}(x) < m, \\ \overline{\Phi}^{(s+1)}(x) &= \overline{\Phi}^{(1)}(x) \neq \overline{0}, \quad s = \{0, \dots, n-2\}. \end{aligned} \quad (11)$$

Заметим, что многочлен $\Phi^{(s)}(x)$ определен однозначно только по модулю p^{n-s} .

Определим произведение произвольной последовательности $u \in R^\infty$ на многочлен $A(x) = \sum_{i \in \mathbb{N}_0} a_i x^i \in R[x]$ соотношениями

$$A(x)u = v \in R^\infty, \quad v(j) = \sum_{i \in \mathbb{N}_0} a_i u(i+j).$$

Далее там, где возможно двусмысленное толкование, операции сложения и умножения по модулю p на факторкольце $\bar{R}$ и на координатном множестве $\mathbb{Z}_p$ обозначаются символами $\oplus, \otimes$. В соответствии с этим произведение многочлена $\bar{A}(x) \in \bar{R}[x]$ и многочлена $f(x) \in \mathbb{Z}_p[x]$ на последовательность $u \in \mathbb{Z}_p^\infty$ обозначаются $\bar{A}(x) \otimes u$ и $f(x) \otimes u$ соответственно. Заметим, что $\bar{A}(x) \otimes u = \overline{A(x)u}$.

Стандартным методом, используемым при доказательстве возможности восстановления рекурренты $u \in L_R(G)^*$ по ее усложнению, является метод сечений ее координатных последовательностей u_s . Под сечением в данном случае понимается последовательность вида $f(x) \otimes u_s$, которая при подходящем выборе многочлена $f(x) \in \mathbb{Z}_p[x]$ оказывается устроенной «проще», чем u_s . В этом пункте будут описаны необходимые для дальнейшего изложения сечения.

Для многочленов $f(x, y) \in \mathbb{Z}_p[x, y]$ определим преобразование Λ по правилу:

$$\Lambda(f(x, y)) = f(x + y, y) \ominus f(x, y).$$

Лемма 2. Верно соотношение $\Lambda^{p-2}(\Delta(x, y)) = y^{p-1}x \oplus \frac{y^{p-1} \oplus y}{2}$.

Доказательство. Очевидно, что если $f(x, y) \neq 0$, то $\deg_x \Lambda(f(x, y)) < \deg_x f(x, y)$. Кроме того, легко видеть, что Λ — линейное преобразование $\mathbb{Z}_p[x, y]$ как модуля над кольцом $\mathbb{Z}_p[y]$ и справедливы соотношения:

$$\Lambda^t(x^k) = \Lambda^t(x^k y^0) \begin{cases} 0, & \text{если } t > k; \\ k! y^k, & \text{если } t = k; \\ k! x y^{k-1} \oplus \frac{k-1}{2} k! y^k, & \text{если } t = k-1. \end{cases} \quad (12)$$

Отсюда ввиду (8) следует равенство

$$\Lambda^{p-2}(\Delta(x, y)) = \sum_{\alpha \in \{p-2, p-1\}} \sum_{\beta \in \{1, \dots, p-1\}} c_{\alpha, \beta} \Lambda^{p-2}(x^\alpha) y^\beta,$$

которое с использованием теоремы 5 дает:

$$\begin{aligned}
 \Lambda^{p-2}(\Delta(x, y)) &= \\
 &= c_{p-1,1}\Lambda^{p-2}(x^{p-1})y \oplus c_{p-2,1}\Lambda^{p-2}(x^{p-2})y \oplus c_{p-2,2}\Lambda^{p-2}(x^{p-2})y^2 = \\
 &= \frac{(-1)^{p-1}}{p-1} \left((p-1)!xy^{p-2} \oplus \frac{p-2}{2}(p-1)!y^{p-1} \right) y \oplus \\
 &\quad \oplus \frac{(-1)^{p-1}}{2} \left((p-2)!y^{p-2} \right) y \oplus \\
 &\quad \oplus \frac{(-1)^{p-2}}{p-2} \left((p-2)!y^{p-2} \right) y^2 = \\
 &= \frac{(-1)^{p-1}}{p-1} (p-1)!(xy^{p-1} \oplus \frac{p-2}{2}y^p) \oplus \frac{1}{2} (y^{p-1}) \oplus \frac{1}{2} (y^p) = \\
 &= xy^{p-1} \oplus \frac{1}{2}y^{p-1} \oplus \frac{p-1}{2}y^p = xy^{p-1} \oplus \frac{1}{2}(y^{p-1} \oplus y),
 \end{aligned}$$

что и доказывает лемму.

Лемма 3. Для координатных последовательностей ЛРП $u \in L_R(G)^*$ справедливы следующие соотношения:

$$1. (x^{j\tau_{s-1}} \ominus e) \otimes u_s = ju_0^{(1)} \text{ для } s = \{1, \dots, n-1\}, j = \{1, \dots, p-1\}; \quad (13)$$

$$2. (x^{\tau_{s-2}} \ominus e) \otimes u_s = u_1^{(s-1)} \oplus \Delta(u_{s-1}; u_0^{(1)}) \text{ для } s = \{2, \dots, n-1\}; \quad (14)$$

3. для $0 \leq t < s-1$ последовательность

$$v_{s,t} = (x^{\tau_0} \ominus e)^{p^{s-1}-p^t} u_s \quad (15)$$

имеет вид

$$v_{s,t} = \left((u_0^{(1)})^{p-1} \otimes u_{t+1} \right) \oplus \frac{1}{2} \left((u_0^{(1)})^{p-1} \oplus u_0^{(1)} \right) \oplus \xi(p, s, t), \quad (16)$$

где

$$\xi(p, s, t) = \begin{cases} (u_0^{(1)})^{p-1} \otimes (\overline{\Phi}^{(1)}(x)^2 \otimes u_0), & \text{если } p = 3, t = 0, s > 2; \\ \overline{\Phi}^{(1)}(x)^2 \otimes u_0, & \text{если } p = 3, t = 0, s = 2; \\ 0 - \text{в остальных случаях;} \end{cases}$$

$$4. (x^{\tau_{s-1}} \ominus e)^k \otimes u_s^k = k! \left(u_0^{(1)} \right)^k \text{ для } s = \{1, \dots, n-1\}, k \in \{1, \dots, p-1\}; \quad (17)$$

$$\begin{aligned}
& 5. (x^{\tau_{s-1}} \ominus e)^{k-1} \otimes u_s^k = \\
& = k! \left(u_0^{(1)}\right)^{k-1} u_s \oplus \frac{k-1}{2} k! \left(u_0^{(1)}\right)^k \text{ для } s \in \{2, \dots, n-1\}, k \in \{1, \dots, p-1\}.
\end{aligned} \tag{18}$$

Доказательство.

1) Равенство (13) при $j = 1$ следует из соотношений $(x^{\tau_{s-1}} - e)u = p^s \Phi^{(s)}(x)u = p^s u^{(s)} \equiv p^s u^{(1)} \pmod{p^{s+1}}$ и свойств производных последовательностей ЛРП u . При $j > 1$ получаем:

$$\begin{aligned}
u_s(i + j\tau_{s-1}) - u_s(i) &= u_s(i + j\tau_{s-1}) - u_s(i + (j-1)\tau_{s-1}) + \\
&+ \dots + u_s(i + \tau_{s-1}) - u_s(i) = ju_0^{(1)}(i).
\end{aligned}$$

2) Заметим, что ввиду (13), (6)

$$u_{s-1}(i + \tau_{s-2}) = u_{s-1}(i) \oplus u_0^{(s-1)}(i) = u_{s-1}(i) \oplus u_0^{(1)}(i), \quad i \in \mathbb{N}_0.$$

Отсюда, пользуясь тем, что для любых $a, b \in \mathbb{Z}_p$ справедливо равенство $(a \oplus b) - a = b - p\Delta(a; b)$, получаем

$$u_{s-1}(i + \tau_{s-2}) - u_{s-1}(i) \equiv u_0^{(1)}(i) - p\Delta(u_{s-1}(i); u_0^{(1)}(i)) \pmod{p^2},$$

и равенство (14) вытекает из сравнений

$$(x^{\tau_{s-2}} - e)u \equiv p^{s-1}u^{(s-1)} \pmod{p^{s+1}},$$

$$(x^{\tau_{s-2}} - e)u \equiv p^{s-1}((x^{\tau_{s-2}} - e)u_{s-1} + p(x^{\tau_{s-2}} \ominus e)u_s) \pmod{p^{s+1}}.$$

3) Докажем (16) индукцией по параметру $s - 2 - t \in \{0, \dots, s - 2\}$. Пусть $s - 2 - t = 0$, т. е. $t = s - 2$. Так как $v_{s,s-2} = (x^{\tau_{s-2}} \ominus e)^{p-1} \otimes u_s$, то из (14) следует равенство

$$v_{s,s-2} = (x^{\tau_{s-2}} \ominus e)^{p-2} \otimes \left(u_1^{(s-1)} \oplus \Delta(u_{s-1}; u_0^{(1)})\right). \tag{19}$$

Поскольку $T(u_0^{(1)}) = \tau_0 | \tau_{s-2}$, ввиду (14) имеем:

$$(x^{\tau_{s-2}} \ominus e)^{p-2} \otimes \Delta(u_{s-1}; u_0^{(1)}) = \Lambda^{p-2} \left(\Delta(u_{s-1}; u_0^{(1)}) \right).$$

Отсюда согласно лемме 2 получаем:

$$(x^{\tau_{s-2}} \ominus e)^{p-2} \otimes \Delta(u_{s-1}; u_0^{(1)}) = \left(u_0^{(1)}\right)^{p-1} \otimes u_{s-1} \oplus \frac{\left(u_0^{(1)}\right)^{p-1} \oplus u_0^{(1)}}{2}. \tag{20}$$

Кроме того, справедливы равенства

$$(x^{\tau_{s-2}} - e)^{p-2} \otimes u_1^{(s-1)} = \begin{cases} \overline{\Phi}^{(1)}(x)^2 \otimes u_0, & \text{если } p = 3, s = 2; \\ 0 & \text{— в остальных случаях.} \end{cases} \quad (21)$$

Подставляя (21), (20) в (19), получаем соотношение (16) для случая $t = s - 2$.

Для проведения индуктивного шага достаточно заметить, что если для $t = \{1, \dots, s - 2\}$ выполняется соотношение вида (16), то

$$\begin{aligned} v_{s,t-1} &= (x^{\tau_0} - e)^{p^t - p^{t-1}} \otimes v_{s,t} = \left(u_0^{(1)}\right)^{p-1} \otimes \left((x^{\tau_{t-1}} - e)^{p-1} \otimes u_{t+1}\right) = \\ &= \left(u_0^{(1)}\right)^{p-1} \otimes u_t \oplus \frac{\left(u_0^{(1)}\right)^{p-1} \oplus u_0^{(1)}}{2} \oplus \left(u_0^{(1)}\right)^{p-1} \otimes \left((x^{\tau_{t-1}} - e)^{p-2} \otimes u_1^{(t)}\right) \end{aligned}$$

и справедливы соотношения

$$\begin{aligned} &\left(u_0^{(1)}\right)^{p-1} \otimes \left((x^{\tau_{t-1}} - e)^{p-2} \otimes u_1^{(t)}\right) = \\ &= \begin{cases} \left(u_0^{(1)}\right)^{p-1} \otimes \left(\overline{\Phi}^{(1)}(x)^2 \otimes u_0\right), & \text{если } p = 3, t = 1; \\ 0 & \text{— в остальных случаях.} \end{cases} \end{aligned} \quad (22)$$

Отсюда следует (16) для $v_{s,t-1}$.

4–5) Докажем (17) и (18). В силу (13) для $i = 0, 1, 2, \dots$

$$u_s(i + \tau_{s-1})^k - u_s(i)^k = \sum_{j=0}^{k-1} \binom{k}{j} u_s(i)^j u_0^{(1)}(i)^{k-j}.$$

Так как $T(u_0^{(1)}) = \tau_0 | \tau_{s-1}$, то для $r > k$ справедливо равенство

$$(x^{\tau_{s-1}} - e)^r u_s^k = 0. \quad (23)$$

Теперь соотношения (17) и (18) доказываются непосредственно последовательным домножением ЛРП u_s^k на многочлены $(x^{\tau_{s-1}} - e)^r$, $r = \{1, \dots, k\}$, и применением полученных выше соотношений.

Лемма доказана.

Определим норму произвольного элемента $x \in R$ равенством

$$\|x\| = \max\{l \in \{0, \dots, n\} : x \in p^l R\}.$$

Лемма 4. Для координатных последовательностей ЛРП $u \in L_R(G)^*$ справедливы следующие соотношения:

$$u_s \left(i + \frac{\tau_s}{2} \right) = \begin{cases} \ominus u_s(i), & \text{если } \|u(i)\| \geq s, \\ \ominus 1 \ominus u_s(i), & \text{если } \|u(i)\| < s, \end{cases} \quad (24)$$

$$i \in \mathbb{N}_0, \quad s \in \{1, \dots, n-1\}.$$

Доказательство. Воспользуемся представлением ЛРП u через функцию «след» (см. [4, 9, 12]). Существует расширение Галуа S степени $m = \deg G(x)$ кольца $\mathbb{Z}_{p^n}$. Это расширение есть кольцо Галуа $S = \text{GR}(q^n, p^n)$ мощности q^n , $q = p^m$, и характеристики p^n . Кольцо S содержит корень α многочлена $G(x)$, и для любой ЛРП $u \in L_R(G)$ существует такой элемент $\beta \in S$, что

$$u(i) = \text{Tr}_R^S(\beta \alpha^i), \quad i \in \mathbb{N}_0, \quad (25)$$

где $\text{Tr}_R^S: S \rightarrow R$ — функция «след». При этом $\text{ord } \alpha = T(G) = \tau_{n-1}$. Следовательно, $\alpha^{\frac{\tau_{n-1}}{2}} = -e$ и

$$u \left(i + \frac{\tau_{n-1}}{2} \right) = -u(i), \quad i \in \mathbb{N}_0. \quad (26)$$

Заметим, что для любого элемента $x \in R$ с p -ичным разложением $x = \sum_{s=0}^{n-1} x_s p^s$, $0 \leq x_s < p$, справедливо равенство

$$-x = (p - x_k) p^k + \sum_{s>k}^{n-1} (p - e - x_s) p^s, \quad \text{где } k = \|x\|. \quad (27)$$

Отсюда вытекает, что s -й разряд p -ичного разложения элемента $-x$ равен $p - 1 - x_s = \ominus 1 \ominus x_s$, если $\|x\| < s$, и равен $p - x_s = \ominus x_s$, если $\|x\| \geq s$. Теперь (24) для $s = n-1$, т. е. для старшей координатной последовательности ЛРП МП u , следует из (26).

Для $s < n-1$ рассмотрим естественный эпиморфизм $R \rightarrow \bar{R} = R/p^{s+1} = \mathbb{Z}_{p^{s+1}}$ и соответствующие образы $\tilde{G}(x) \in \bar{R}[x]$, $\tilde{u} \in \bar{R}^\infty$ многочлена $G(x)$ и последовательности u соответственно. Тогда $\tilde{G}(x)$ — МП-многочлен над $\bar{R}$ периода τ_s , $\tilde{u} \in L_R(\tilde{G})^*$ и координатные последовательности $\tilde{u}$ суть $\tilde{u}_t = u_t$, $t \in \{0, \dots, s\}$.

Теперь соотношение (24) есть уже доказанное соотношение для старшей координатной последовательности ЛРП МП.

3. Восстановление ЛРП МП по ее усложнениям

3.1. Восстановление ЛРП по старшей координатной последовательности (базовый алгоритм)

Теорема 6. Начальный вектор ЛРП $u \in L_R(G)^*$ однозначно восстанавливается со сложностью $O\left(p^{\frac{m}{2}} + mp^n\right)$ по $O(mp^n)$ знакам последовательности u_{n-1} , расположенным на ее отрезке длины $(p^m - 1)p^{n-2} + m$.

Доказательство.

1 этап. Восстановление последовательностей $u_0^{(1)}$ и u_0 .

Из соотношений (13)

$$u_{n-1}(i + \tau_{n-2}) \ominus u_{n-1}(i) = u_0^{(1)}(i), \quad i \in \{0, \dots, m-1\},$$

определяем начальный вектор $u_0^{(1)}[0, \dots, m-1] = (u_0^{(1)}(0), \dots, u_0^{(1)}(m-1))$ последовательности $u_0^{(1)}$. Так как $u_0^{(1)} \in L_{\mathbb{Z}_p}(\bar{G})$, то этим вектором последовательность $u_0^{(1)}$ определена однозначно.

Для определения последовательности u_0 заметим, что многочлен $\Phi_1(x)$ из (5) удовлетворяет условию $(\bar{\Phi}_1(x), \bar{G}(x)) = \bar{e}$, и потому существует такой многочлен $\Phi_1(x)^{-1} \in \mathbb{Z}_p[x]$, что

$$\bar{\Phi}_1(x) \otimes \Phi_1(x)^{-1} \equiv \bar{e} \pmod{\bar{G}(x)}, \quad \deg \Phi_1(x)^{-1} < m.$$

Тогда

$$u_0 = \Phi_1(x)^{-1} \otimes u_0^{(1)}. \quad (28)$$

Так как $u_0 \in L_{\mathbb{Z}_p}(\bar{G})$, то эта последовательность однозначно определяется начальным вектором $u_0[0, \dots, m-1]$, который определяется из (28) по отрезку $u_0^{(1)}[0, \dots, 2m-1]$.

2 этап. Вычисление опорной точки i_0 . Так как $u_0^{(1)}$ — ненулевая ЛРП МП из $L_{\mathbb{Z}_p}(\bar{G})$, то существует такое значение $i_0 \in \{0, \dots, \tau_0 - 1\}$, что отрезок $u_0^{(1)}[i_0, \dots, i_0 + m - 1]$ не содержит нулей.

3 этап. Вычисление векторов $u_t[i_0, \dots, i_0 + m - 1]$, $t \in \{1, \dots, n-2\}$. Из соотношений (16) получаем, что для любых $0 \leq t+1 < s \leq n-1$ справедливы соотношения

$$\begin{aligned} \left(u_0^{(1)}\right)^{p^{-1}} \otimes u_{t+1} &= \left((x^{\tau_0} \ominus e)^{p^{s-1}-p^t} \otimes u_s\right) \ominus \\ &\ominus \frac{1}{2} \left((u_0^{(1)})^{p^{-1}} \ominus u_0^{(1)}\right) \ominus \xi(p, s, t), \end{aligned} \quad (29)$$

где

$$\xi(p, s, t) = \begin{cases} \left(u_0^{(1)}\right)^{p-1} \otimes \left(\overline{\Phi}^{(1)}(x)^2 \otimes u_0\right), & \text{если } p = 3, t = 0, s > 2; \\ \overline{\Phi}^{(1)}(x)^2 \otimes u_0, & \text{если } p = 3, t = 0, s = 2; \\ 0 & \text{— в остальных случаях.} \end{cases}$$

Так как для $j \in \{i_0, \dots, i_0 + m - 1\}$ $\left(u_0^{(1)}(j)\right)^{p-1} = 1$, то при данных значениях параметра j левая часть выражения (29) равна $u_{t+1}(j)$.

Перебирая в (29) значения (s, t) в последовательности $(n-1, n-3), (n-2, n-4), \dots, (2, 0)$, однозначно определяем значения

$$u_{n-2}[i_0, \dots, i_0 + m - 1], u_{n-3}[i_0, \dots, i_0 + m - 1], \dots, u_1[i_0, \dots, i_0 + m - 1]. \quad (30)$$

При этом знаки последовательности $\xi(p, s, t)$ вычисляются по известным последовательностям u_0 и $u_0^{(1)}$.

4 этап. Вычисление начального вектора ЛРП u . Имея векторы $u_s[i_0, \dots, i_0 + m - 1]$, $s \in \{0, \dots, m-1\}$, вычисляем отрезок ЛРП u :

$$u[i_0, \dots, i_0 + m - 1] = \sum_{s=0}^{n-1} p^s u_s[i_0, \dots, i_0 + m - 1].$$

Пусть

$$x^i \equiv c_{i,0} + c_{i,1}x + \dots + c_{i,m-1}x^{m-1} \pmod{G(x)}$$

и

$$\lambda_i(x_0, \dots, x_{m-1}) = c_{i,0}x_0 + c_{i,1}x_1 + \dots + c_{i,m-1}x_{m-1}, \quad i \in \mathbb{N}_0.$$

Тогда начальный вектор ЛРП u вычисляется по вектору $u[i_0, \dots, i_0 + m - 1]$ как решение системы линейных уравнений:

$$\begin{aligned} \lambda_{i_0}(u[0, \dots, m-1]) &= u(i_0), \\ \lambda_{i_0+1}(u[0, \dots, m-1]) &= u(i_0 + 1), \\ &\dots \\ \lambda_{i_0+m-1}(u[0, \dots, m-1]) &= u(i_0 + m - 1). \end{aligned} \quad (31)$$

Оценим сложность базового алгоритма. Основной вклад в трудоемкость вносят этапы 2 и 3.

Номер такта i_0 на этапе 2 можно найти, например, решив «задачу о расстоянии» между вектором $u_0^{(1)}[0, \dots, m-1]$ и, допустим, вектором $(1, \dots, 1)$, принадлежащим циклу ЛРП МП $u_0^{(1)}$ периода τ_0 над полем $\mathbb{Z}_p$. Средняя сложность решения этой задачи, эквивалентной задаче дискретного логарифмирования в конечном поле, можно оценить величиной $O(\sqrt{\tau_0}) = O(p^{\frac{m}{2}})$.

Основной вклад в трудоемкость 3 и 4 этапов алгоритма вносит нахождение p -ичных разрядов $u_t(i_0 + j)$, $t = 1, \dots, n-2$, $j = 0, \dots, m-1$ знаков $u(i_0 + j)$, $j = 0, \dots, m-1$ линейной рекурренты u , причем наибольшая сложность связана с нахождением значений $u_1(i_0 + j)$, $j = \{0, \dots, m-1\}$. Действительно, сложность нахождения знаков $u_{t+1}(i_0 + j)$, $j = \{0, \dots, m-1\}$ определяется сложностью вычисления левой части в равенстве (17), и наибольшая трудоемкость вычислений при этом достигается при $t = 0$. Нетрудно видеть, что в качестве оценки трудоемкости определения знака $u_t(i_0 + j)$, $t = 1, \dots, n-2$, $j = 0, \dots, m-1$ можно взять трудоемкость умножения ЛРП u_{n-1} на многочлен $(x^{\tau_0} - e)^{p^{s-1}-p^t}$, которая, в свою очередь, определяется числом ненулевых коэффициентов многочлена. Из равенств

$$(x^{\tau_0} \ominus e)^{p^{n-2}-p^t} = \sum_{j=0}^{p^{n-t-2}-1} \left(x^{\tau_0 p^t}\right)^j (-1)^{p^{n-t-2}-j} \binom{p^{n-t-2}-1}{j},$$

$$\binom{p^{n-t-2}-1}{j} \not\equiv 0 \pmod{p}, \quad 0 \leq j \leq p^{n-t-2}-1,$$

следует, что сложность описанного алгоритма в операциях поля $GF(p)$ оценивается величиной $O(p^{m/2} + mp^n)$.

Проследивая этапы алгоритма, нетрудно увидеть, что для его реализации требуется порядка $O(mp^n)$ знаков последовательности u , которые расположены отрезками по m знаков на отрезке $u[0, \dots, \tau_{n-2} + m - 1]$.

3.2. Восстановление ЛРП по последовательности, полученной из исходной с помощью функции усложнения

$$\Psi(x) = x_{n-1} \oplus \eta(x_0, \dots, x_{n-2}), \deg_{x_{n-2}} \eta \leq p-2$$

Теорема 7. Пусть $u \in L_R(G)^*$ и $v \in \mathbb{Z}_p^\infty$ — последовательность вида $v = \psi(u)$, где

$$\Psi(x) = x_{n-1} \oplus \eta(x_0, \dots, x_{n-2}), \quad \eta \in R[x_0, \dots, x_{n-2}], \quad \deg_{x_{n-2}} \eta \leq p-2.$$

Тогда начальный вектор ЛРП и однозначно восстанавливается со сложностью $O\left(\frac{m}{p^2} + mp^n\right)$ по $O(mp^n)$ знакам последовательности v , расположенным на ее отрезке длины $(p^m - 1)p^{n-2} + m$.

Доказательство. По условию последовательность $\eta = \eta(u_0, \dots, u_{n-2})$ имеет вид

$$\eta = \sum_{k \in \{0, \dots, p-2\}} u_{n-2}^k \eta_k(u_0, \dots, u_{n-3}), \quad (32)$$

и $T(\eta)|_{\tau_{n-2}}$ согласно предложению 1. Тогда, применяя оператор $x^{\tau_{n-2}} \ominus e$ к последовательности $v = u_{n-1} + \eta$, получаем согласно п. 1 леммы 3:

$$(x^{\tau_{n-2}} \ominus e) \otimes v = (x^{\tau_{n-2}} \ominus e) \otimes u_{n-1} = \Phi(x) \otimes u_0 = u_0^{(1)}.$$

Ввиду условия $\deg_{x_{n-2}} \eta(x_0, \dots, x_{n-2}) \leq p - 2$ из (23) следует, что

$$(x^{\tau_0} \ominus e)^{p^{n-2}-p^{n-3}} \otimes v = (x^{\tau_{n-3}} \ominus e)^{p-1} \otimes u_{n-1}.$$

Таким образом, имеем равенство

$$(x^{\tau_0} \ominus e)^{p^{n-2}-p^{n-3}} \otimes v = u_{n-2} + \xi_{n-2},$$

из которого, зная последовательность u_0 , находим ξ_{n-2} , и получаем:

$$u_{n-2} = (x^{\tau_0} \ominus e)^{p^{n-2}-p^{n-3}} \otimes v \ominus \xi_{n-2}.$$

Последовательно домножая это равенство на многочлены

$$(x^{\tau_0} \ominus e)^{p^{n-3}-p^{n-4}}, \dots, (x^{\tau_0} \ominus e)^{p^2-p}$$

и пользуясь тем, что каждая из последовательностей ξ_i нам известна, причем их периоды делят τ_0 , получаем систему соотношений:

$$\begin{aligned} u_{n-2} &= (x^{\tau_0} \ominus e)^{p^{n-2}-p^{n-3}} \otimes v \ominus \xi_{n-2}, \\ u_{n-3} &= (x^{\tau_0} \ominus e)^{p^{n-2}-p^{n-4}} \otimes v \ominus \xi_{n-3}, \\ \dots &\dots \dots \\ u_1 &= (x^{\tau_0} \ominus e)^{p^{n-2}-1} \otimes v \ominus \xi_1. \end{aligned} \quad (33)$$

Теперь по равенству $v = u_{n-1} \oplus \eta(u_0, \dots, u_{n-2})$ восстанавливается последовательность u_{n-1} . Нетрудно видеть, что сложность и количество материала, необходимого для данного метода восстановления начального вектора ЛРП, совпадает со сложностью и количеством материала в случае базового алгоритма.

3.3. Восстановление ЛРП по последовательности, полученной из исходной с помощью функции усложнения

$$\Psi(x) = x_{n-1}^k \oplus \oplus c_{k-1} x_{n-1}^{k-1} \oplus \eta(x_0, \dots, x_{n-1}), \deg_{x_{n-1}} \eta \leq k-2$$

Теорема 8. Пусть $u \in L_R(G)^*$ и $v \in \mathbb{Z}_p^\infty$ — последовательность вида $v = \Psi(u)$, где

$$\Psi(x) = c_k x_{n-1}^k \oplus c_{k-1} x_{n-1}^{k-1} \oplus \eta(x_0, \dots, x_{n-1}), \eta \in \mathbb{Z}_p[x_0, \dots, x_{n-1}],$$

$$\deg_{x_{n-1}} \eta(x_0, \dots, x_{n-1}) \leq k-2, 2 \leq k \leq p-1,$$

и пусть выполнено хотя бы одно из условий:

(a) $(k, p-1) = 1$,

(b) $c_{k-1} \neq \frac{k}{2}$,

(c) k нечетно, $n \geq 4$.

Тогда начальный вектор ЛРП и однозначно восстанавливается со сложностью $O\left(p^{\frac{m}{2}} + t k p^n\right)$ по $O(t k p^n)$ знакам последовательности v , расположенным на ее отрезке длины $(p^m - 1)p^{n-2} + t$.

Доказательство. Из соотношения (23) и условия

$$\deg_{x_{n-1}} \eta(x_0, \dots, x_{n-1}) \leq k-2$$

следует, что последовательность $\eta = \eta(u_0, \dots, u_{n-1})$ аннулируется многочленом $(x^{\tau_{n-2}} - e)^{k-1}$. Отсюда и из леммы 3 получаем:

$$(x^{\tau_{n-2}} \ominus e)^k \otimes v = k! \left(u_0^{(1)}\right)^k, \quad (34)$$

$$\begin{aligned} (x^{\tau_{n-2}} \ominus e)^{k-1} \otimes v &= k! \left(u_0^{(1)}\right)^{k-1} \otimes u_{n-1} \oplus \\ &\oplus k! \frac{k-1}{2} \left(u_0^{(1)}\right)^k \oplus c_{k-1} (k-1)! \left(u_0^{(1)}\right)^{k-1} \end{aligned} \quad (35)$$

Из соотношения (34) определяем последовательность $\left(u_0^{(1)}\right)^k$; так же, как в базовом алгоритме, находим m подряд идущих знаков со свойством $u_0^{(1)}(i_0 + j) \neq 0$, $j = 0, \dots, m-1$.

(a) Если $(p-1, k) = 1$, то последовательность $u_0^{(1)}$ однозначно определяется по последовательности $\left(u_0^{(1)}\right)^k$, а далее из соотношения (35) определяются знаки ЛРП u_{n-1} , и для восстановления ЛРП u используется базовый алгоритм.

(b) Если $(p-1, k) > 1$, то по $\left(u_0^{(1)}\right)^k$ однозначно найти ЛРП $u_0^{(1)}$ нельзя. В этом случае, используя соотношения (17), (18), (34), (35), мы можем построить вспомогательную последовательность v' :

$$v' = \frac{1}{(k-1)!} \left((x^{\tau_{n-2}} \ominus e)^{k-1} \otimes v \ominus \frac{k(k-1)}{2} (x^{\tau_{n-2}} \ominus e)^k \otimes v \right),$$

которая после приведения подобных членов приобретает вид

$$v' = k \left(u_0^{(1)}\right)^{k-1} \otimes u_{n-1} \oplus c_{k-1} \left(u_0^{(1)}\right)^{k-1}. \quad (36)$$

Выбирая такие значения i , что $u_0(i) \neq 0$, и пользуясь соотношениями (24), получаем:

$$\begin{aligned} v' \left(i + \frac{\tau_{n-1}}{2} \right) &= k (-1)^k \left(u_0^{(1)}(i)\right)^{k-1} (e \oplus u_{n-1}(i)) \oplus c_{k-1} (-1)^{k-1} \left(u_0^{(1)}\right)^{k-1} = \\ &= (-1)^k k \left(u_0^{(1)}\right)^{k-1} u_{n-1}(i) \oplus \left(k (-1)^k \oplus c_{k-1} (-1)^{k-1} \right) \left(u_0^{(1)}\right)^{k-1}. \end{aligned}$$

Отсюда

$$v' \left(i + \frac{\tau_{n-1}}{2} \right) \oplus (-1)^{k-1} v'(i) = (-1)^{k-1} \left(u_0^{(1)}(i)\right)^{k-1} (-k \oplus c_{k-1} \oplus c_{k-1}).$$

Следовательно, если $c_{k-1} \neq \frac{k}{2}$, то по последовательности v' можно однозначно найти последовательность $\left(u_0^{(1)}\right)^{k-1}$, а по ней и по последовательности $\left(u_0^{(1)}\right)^k$ определить все ненулевые элементы ЛРП $u_0^{(1)}$. Далее знаки последовательности u_{n-1} находятся из (35).

(c) Рассмотрим случай, когда k – нечетное число и $n \geq 4$. Как и выше, получаем последовательность v' , умножая ее на многочлен $(x^{\tau_{n-3}} - e)$, получаем последовательность $v'' = (x^{\tau_{n-3}} - e) v'$ и строим вектор

$$(v''(i), v''(i + \tau_{n-3}), \dots, v''(i + (p-1)\tau_{n-3})). \quad (37)$$

Согласно п. 2 леммы 3, из (36) и условия $\tau_1 | \tau_{n-3}$ следует, что

$$v'' = (x^{\tau_{n-3}} - e) v' = k \left(u_0^{(1)}\right)^{k-1} \left(u_1^{(n-2)} \oplus \Delta \left(u_0^{(1)}, u_{n-2}\right)\right).$$

Поскольку функция $\Delta(x, y)$ может принимать только два значения, то в векторе (37) компоненты могут принимать только два значения:

$$v''_0 = k \left(u_0^{(1)}\right)^{k-1} u_1^{(n-2)} \quad \text{и} \quad v''_1 = k \left(u_0^{(1)}\right)^{k-1} \left(u_1^{(n-2)} \oplus e\right).$$

При этом так как по п. 1 леммы 3

$$v''(i + j\tau_{n-3}) = k \left(u_0^{(1)} \right)^{k-1} \left(u_1^{(n-2)}(i) \oplus \Delta \left(u_0^{(1)}(i), u_{n-2}(i) \oplus ju_0^{(1)}(i) \right) \right),$$

то при условии $u_0^{(1)}(i) = 0$ все координаты вектора (37) равны v_0'' , а при условии $u_0^{(1)}(i) \neq 0$ совокупность координат этого вектора есть совокупность элементов

$$k \left(u_0^{(1)} \right)^{k-1} \left(u_1^{(n-2)}(i) \oplus \Delta \left(u_0^{(1)}(i), t \right) \right), \quad t \in \{0, \dots, p-1\},$$

в которой значение v_1'' встречается лишь при $t \in \{p - u_0^{(1)}(i), \dots, p-1\}$, т.е. ровно $u_0^{(1)}(i)$ раз. Таким образом, проведя маркировку значений компонент вектора (37), мы получим пару значений $\{u_0^{(1)}, p - u_0^{(1)}\}$. Так как k нечетно, то

$$\left(u_0^{(1)} \right)^k \neq \left(p \ominus u_0^{(1)} \right)^k = - \left(u_0^{(1)} \right)^k,$$

и по известному из (34) значению $\left(u_0^{(1)} \right)^k$ из пары значений $\{u_0^{(1)}, p - u_0^{(1)}\}$ однозначно выделяется значение $u_0^{(1)}$, после чего из (35) находится значение $u_{n-1}(i)$ для тех значений i , при которых $u_0^{(1)}(i) \neq 0$.

Оценим сложность и количество материала, достаточного для восстановления начального заполнения. Прежде чем применять базовый алгоритм восстановления рекурренты, необходимо определить порядка $O(mp^n)$ знаков координатной ЛРП u_{n-1} . Для вычисления одного знака ЛРП u_{n-1} требуется: $2k$ операций в поле $\mathbb{Z}_p$ — для нахождения значения $\left(u_0^{(1)} \right)^k$, $2k$ операций — для нахождения значения $v'(i)$ из (36). Если $(k, p-1) = 1$, то отсюда сразу находим значение $u_{n-1}(i)$.

Если k нечетно, то в последовательности $v'(i)$ требуется знать уже $p+1$ знаков, по которым за $O(p)$ операций строится вектор (37) и находятся значения $u_0^{(1)}$ и $u_{n-1}(i)$.

Если $c_{k-1} \neq \frac{k}{2}$, то в последовательности v' необходимо знать два знака, по которым сразу определяется значение $\left(u_0^{(1)} \right)^{k-1}$, после чего находятся искомые значения $u_0^{(1)}$ и $u_{n-1}(i)$. Следовательно, начальный вектор ЛРП u однозначно восстанавливается со сложностью $O\left(p^{\frac{m}{2}} + mkp^n\right)$ по $O(mkp^n)$ знакам последовательности v , расположенным на ее отрезке длины $(p^m - 1)p^{n-2} + m$.

4. Инъективные отображения вида $\Psi(x) = \psi(x_{n-1})$

Полученные в предыдущих параграфах результаты показывают, что для линейных рекуррент максимального периода над примарным кольцом вычетов $\mathbb{Z}_{p^n}$, $p \geq 3$, можно (при определенных ограничениях на вид функции усложнения) строить алгоритмы восстановления начального заполнения исходной рекурренты. В данном параграфе мы сначала указываем признаки неинъективных отображений

$$\Psi: L_R(G)^* \rightarrow \mathbb{Z}_p^\infty \quad (38)$$

вида

$$\begin{aligned} \Psi(x) &= \psi(x_{n-1}), \\ \psi: \mathbb{Z}_p &\rightarrow \mathbb{Z}_p, \\ \psi(x_{n-1}) &= \sum_{j=0}^k c_j x_{n-1}^j, \quad 0 < k < p, c_k \neq 0. \end{aligned} \quad (39)$$

Теорема 9. Если функция (38) вида (39) не инъективна, то выполняются следующие условия:

- (a) $(k, p-1) > 1$;
- (b) $\deg \overline{\Phi_1}(x) = 0$;
- (c) $c_k k = 2c_{k-1}$.

Доказательство. Предположим, что существуют две различные ЛРП $u, v \in L_R(G)^*$ такие, что

$$\Psi(v) = \Psi(u). \quad (40)$$

Умножая обе части равенства (40) на многочлен $(x^{\tau_{n-2}} - e)^k$, в силу (17) получаем:

$$c_k k! \left(u_0^{(1)}\right)^k = c_k k! \left(v_0^{(1)}\right)^k. \quad (41)$$

Следовательно, существует ненулевая константа $\alpha \in \mathbb{Z}_p \setminus \{0\}$, удовлетворяющая условию

$$v_0^{(1)} = \alpha u_0^{(1)}, \quad \alpha^k = e. \quad (42)$$

Умножая обе части равенства (40) на многочлен $(x^{\tau_{n-2}} - e)^{k-1}$, в силу (17) и (18) для $i \geq 0$ получаем:

$$\begin{aligned} c_k k! \left(u_0^{(1)}(i)\right)^{k-1} u_{n-1}(i) \oplus c_k k! \frac{k-1}{2} \left(u_0^{(1)}(i)\right)^k \oplus c_{k-1}(k-1)! \left(u_0^{(1)}(i)\right)^{k-1} = \\ = c_k k! \left(v_0^{(1)}(i)\right)^{k-1} v_{n-1}(i) \oplus c_k k! \frac{k-1}{2} \left(v_0^{(1)}(i)\right)^k \oplus c_{k-1}(k-1)! \left(v_0^{(1)}(i)\right)^{k-1}. \end{aligned}$$

Отсюда с учетом (42) следует:

$$\begin{aligned} c_k k u_{n-1} \left(u_0^{(1)}(i)\right)^{k-1} \oplus c_{k-1} \left(u_0^{(1)}(i)\right)^{k-1} = \\ = c_k k v_{n-1} \left(v_0^{(1)}(i)\right)^{k-1} \oplus c_{k-1} \left(v_0^{(1)}(i)\right)^{k-1}. \end{aligned} \quad (43)$$

(а) Если $(k, p-1) = 1$, то из (41) имеем: $u_0^{(1)} = v_0^{(1)}$, и из (43) следует, что $u_{n-1}(i) = v_{n-1}(i)$ для всех $i \in \mathbb{N}_0$ таких, что $u_0^{(1)} \neq 0$. Тогда ввиду базового алгоритма восстановления ЛРП МП по старшей координатной последовательности, изложенного в разделе 3, имеет место равенство $u = v$. Таким образом, в случае $(k, p-1) = 1$ рассматриваемое отображение Ψ инъективно. Следовательно, $(k, p-1) > 1$.

(б) Покажем, что $\deg \overline{\Phi_1}(x) = 0$.

Пусть $n > 2$. Домножив обе части равенства (43) на многочлен $(x^{\tau_0} - e)^{p^{n-2}-1}$, из (16) получаем соотношение

$$\begin{aligned} c_k k \left(\left(u_0^{(1)}\right)^{k-1} \otimes u_1 \oplus \frac{\left(u_0^{(1)}\right)^{k-1} \ominus \left(u_0^{(1)}\right)^k}{2} \oplus \left(u_0^{(1)}\right)^{k-1} \otimes \xi_u(p, n-1, 0) \right) = \\ = c_k k \left(\left(v_0^{(1)}\right)^{k-1} \otimes v_1 \oplus \frac{\left(v_0^{(1)}\right)^{k-1} \ominus \left(v_0^{(1)}\right)^k}{2} \oplus \left(v_0^{(1)}\right)^{k-1} \otimes \xi_v(p, n-1, 0) \right), \end{aligned} \quad (44)$$

причем из определения последовательности ξ (см. лемму 3) следует равенство

$$\xi_v(p, n-1, 0) = \alpha \xi_u(p, n-1, 0).$$

Подставляя (42) в (44), получаем

$$\alpha \left(u_0^{(1)}\right)^{k-1} \otimes u_1 \oplus \alpha \frac{\left(u_0^{(1)}\right)^{k-1}}{2} = \left(v_0^{(1)}\right)^{k-1} \otimes u_1 \oplus \frac{\left(v_0^{(1)}\right)^{k-1}}{2}. \quad (45)$$

Нетрудно проверить, что для первой координатной последовательности соотношение (24) можно представить в виде

$$\left(x^{\frac{\tau_1}{2}} + e\right) \otimes u_1 = -u_0^{p-1}.$$

Домножая (45) на многочлен $(-1)^{k-1}x^{\frac{\tau_1}{2}} + e$, получаем равенство

$$-\alpha \left(u_0^{(1)}\right)^{k-1} \otimes u_0^{p-1} \oplus \alpha \left(u_0^{(1)}\right)^{k-1} = -\left(v_0^{(1)}\right)^{k-1} \otimes u_0^{p-1} \oplus \left(v_0^{(1)}\right)^{k-1}. \quad (46)$$

В силу (42) имеем $v_0 = \alpha u_0$. Поэтому из (46) следует, что

$$\left(u_0^{(1)}\right)^{k-1} (\alpha \ominus e) \left(v_0^{p-1} \ominus e\right) = 0. \quad (47)$$

Так как $v_0^{(1)}$ и v_0 являются линейными рекуррентными последовательностями максимального периода над полем $\mathbb{Z}_p$ с минимальным многочленом $\bar{G}(x)$, то равенство (47) означает, что члены этих последовательностей с одинаковыми номерами либо равны нулю, либо одновременно отличны от нуля. Это возможно в силу соотношения (6) только в случае, когда $\deg \bar{\Phi}^{(1)}(x) = 0$.

Пусть $n = 2$. Тогда из (43) следует:

$$c_k k u_1 \left(u_0^{(1)}(i)\right)^{k-1} \oplus c_{k-1} \left(u_0^{(1)}(i)\right)^{k-1} = c_k k v_1 \left(v_0^{(1)}(i)\right)^{k-1} \oplus c_{k-1} \left(v_0^{(1)}(i)\right)^{k-1}.$$

Домножая это равенство на многочлен $(-1)^{k-1}x^{\frac{\tau_1}{2}} + e$ и учитывая (42), получаем

$$\left(u_0^{(1)}\right)^{k-1} (\alpha \ominus e) \left(v_0^{p-1} \ominus \frac{2c_{k-1}}{c_k k}\right) = 0. \quad (48)$$

Если $\frac{2c_{k-1}}{c_k k} = e$, то (48) совпадает с (47), и равенство (48) возможно только в случае, когда $\deg \bar{\Phi}^{(1)}(x) = 0$.

Если $\frac{2c_{k-1}}{c_k k} = 0$, то (48) невозможно, так как в силу свойств производных последовательностей существует значение i такое, что $v_0^{(1)}(i) \neq 0$ и $v(i) \neq 0$. Если $\frac{2c_{k-1}}{c_k k} \in \{2, 3, \dots, p-1\}$, то $v_0^{p-1} \ominus \frac{2c_{k-1}}{c_k k} \neq 0$, и равенство (48) нарушается для всех значений i , для которых $v_0^{(1)}(i) \neq 0$. Таким образом, если $\deg \bar{\Phi}^{(1)}(x) > 0$, то отображение Ψ инъективно.

Пусть многочлен $G(x)$ не является сильно примитивным. В этом случае существует ненулевая константа $\beta \in \mathbb{Z}_p$, удовлетворяющая условиям

$v_0^{(1)} = \beta v_0$ и $u_0^{(1)} = \beta u_0$. Поскольку в силу (42) знаки $v_0^{(1)}(i)$ и $u_0^{(1)}(i)$ либо одновременно равны нулю, либо одновременно отличны от нуля, поскольку из леммы 4 следует, что если $v_0^{(1)}(i) \neq 0$, то

$$\begin{aligned} v_{n-1}\left(i + \frac{\tau_{n-2}}{2}\right) &= -v_{n-1} \ominus e, \\ u_{n-1}\left(i + \frac{\tau_{n-2}}{2}\right) &= -u_{n-1} \ominus e. \end{aligned} \quad (49)$$

Домножим соотношение (43) на многочлен $(-1)^{k-1}x^{\frac{\tau_{n-1}}{2}} + e$. Тогда с учетом (49) получаем

$$\left(u_0^{(1)}\right)^{k-1} (2c_{k-1} \ominus c_k k) = \left(v_0^{(1)}\right)^{k-1} (2c_{k-1} \ominus c_k k).$$

Отсюда в случае $2c_{k-1} \ominus c_k k \neq 0$ вытекает равенство

$$\left(u_0^{(1)}\right)^{k-1} = \left(v_0^{(1)}\right)^{k-1}.$$

Подставляя (42) в получившееся равенство, получаем $\alpha = e$ и $u_0^{(1)} = v_0^{(1)}$. Тогда, как отмечалось выше, из (43) следует, что члены последовательностей u_{n-1} и v_{n-1} совпадают для всех значений i , для которых $v_0^{(1)} \neq 0$, и в силу алгоритма восстановления ЛРП МП по старшей координатной последовательности, изложенного в разделе 3 данной работы, имеет место равенство $u = v$. Таким образом, если многочлен $G(x)$ не является сильно примитивным и $2c_{k-1} \ominus c_k k \neq 0$, то отображение ψ инъективно.

Следствие 1. Если либо $(k, p-1) = 1$, либо $\deg \overline{\Phi_1}(x) > 0$, либо $c_k k \neq 2c_{k-1}$, то отображение (38) вида (39) инъективно.

Заключение

В работе исследована возможность восстановления ЛРП МП над примарным кольцом вычетов по ее усложнению. Результаты работы, в отличие от последних работ зарубежных авторов, показывают не только возможность подобного восстановления, но и предлагают для некоторых классов функций усложнения алгоритмы восстановления начального вектора ЛРП МП с оценкой трудоемкости и объемом необходимого для работы алгоритма материала. В максимально общем (в рамках предложенного метода сечений) случае описаны условия инъективности функции усложнения, зависящей от старшей координатной последовательности.

Список литературы

1. Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1979 г.
2. Кузьмин А. С., Нечаев А. А. Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа. — М.: УМН, 1992, т. 47, в. 5, с. 183–184.
3. Kuzmin A. S., Nechaev A. A. Linear recurrent sequences over Galois rings. — In: Proceedings 2-nd International Conference on Algebra. — Barnaul, 1991, p. 174.
4. Нечаев А. А. Код Кердока в циклической форме. — Дискрет. матем., 1989, т. 1, в. 4, 1989, с. 123–139.
5. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа. — Алгебра и логика, 1995, т. 3, в. 2, с. 169–189.
6. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 139–202.
7. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Свойства линейных и полилинейных рекуррент над кольцами Галуа. — В сб.: Труды по дискретной математике. Т. 2. — М.: ТВП, 1997, с. 191–222.
8. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Свойства линейных и полилинейных рекуррент над кольцами Галуа (II). — Обозрение прикл. и промышл. матем. Сер. дискрет. матем., 2000, т. 7, в. 1, с. 5–59.
9. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент. — В сб.: Труды по дискретной математике. Т. 3. — М.: ТВП, 2000, с. 155–194.
10. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Вполне равномерные линейные рекурренты. — В сб.: Труды по дискретной математике. Т. 5. — М.: ФИЗМАТЛИТ, 2002, с. 103–158.
11. Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами. — Дискрет. матем., 1991, т. 3, в. 4, с. 107–121.
12. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules. — J. Math. Sci., 1995, v. 76, № 6, p. 2793–2915.
13. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа. — УМН, 1993, т. 48, в. 1, с. 167–168.
14. Кузьмин А. С. Нижние оценки рангов координатных последовательностей линейных рекуррентных последовательностей над примарными кольцами вычетов. — УМН, 1993, т. 48, в. 3, с. 193–194.
15. Куракин В. Л. Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа. — Дискрет. матем., 1994, т. 6, в. 2, с. 88–100.
16. Куракин В. Л. Представления над полем линейных рекуррент максимального периода над кольцом вычетов. — Успехи матем. наук, 1994, т. 49, в. 2, с. 157–158.

17. Куракин В.Л. Полиномиальные преобразования линейных рекуррентных последовательностей над кольцом $\mathbb{Z}_{p^2}$. — Дискрет. матем., 1999, т. 11, в. 2, с. 40–65.
18. Куракин В.Л. Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами. — Дискрет. матем., 2000, т. 12, в. 3, с. 3–36.
19. Min-Qiang Huang, Zong-Duo Dai Projective maps of linear recurring sequences with maximal p -adic periods. — Fibonacci Quart., 1992, v. 30(2), p. 139–143.
20. Min-Qiang Huang Analysis and cryptologic evaluation for primitive sequences over an integer residue ring. — Ph.D. Thesis. — Graduate School of USTC, Beijing, China: Academia Sinica, 1988.
21. Xuan-Yong Zhu, Weng-Feng Qi Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}_{p^n}$. — Finite Fields Appl., 2005, v. 11(1), p. 30–44.
22. Xuan-Yong Zhu, Weng-Feng Qi Compression mappings on primitive sequences over $\mathbb{Z}_{p^n}$. — IEEE Trans. Inform. Theory, 2004, v. 50(10), p. 2442–2448.
23. Xuan-Yong Zhu, Wen-Feng Qi Further result of compressing maps on primitive sequences modulo odd prime powers. — IEEE Trans. Inf. Theory, 2007, v. 53(8), p. 2985.
24. Tian Tian, Wen-Feng Qi Injectivity of compressing maps on primitive sequences over $\mathbb{Z}/(p^e)$. — IEEE Trans. Inf. Theory, 2007, v. 53(8), p. 2960.
25. Zong-Duo Dai Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. — Cryptology, 1992, v. 5(4), p. 193–207.
26. Weng-Feng Qi, Xuan-Yong Zhu Compressing maps on primitive sequences over $\mathbb{Z}_{2^n}$ and its Galois extension. — Finite Fields Appl., 2002, v. 8(4), p. 570–588.
27. Weng-Feng Qi Compressing maps on primitive sequences over $\mathbb{Z}_{2^n}$ and analysis of their derivate sequences. — Ph.D. Thesis. — Zhengzhou, China: Zhengzhou Inform. Eng. Univ., 1997.
28. Weng-Feng Qi, Jun-Hui Yang, Jin-Jun Zhou ML-sequences over rings $\mathbb{Z}_{2^n}$. — Lect. Notes Comput. Sci., 1998, v. 1514, p. 315–325.