



# Math-Net.Ru

All Russian mathematical portal

A. A. Illarionov, Asymmetric cryptography and hyperelliptic sequences, *Dal'nevost. Mat. Zh.*, 2019, Volume 19, Number 2, 185–196

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 18.97.9.169

February 18, 2025, 03:44:10



УДК 519.719.2+517.965  
MSC2010 94A60+11Bxx

© А. А. Илларионов<sup>1</sup>

## Асимметричные криптосистемы и гиперэллиптические последовательности

Исследуются последовательности  $\{A_n\}_{n=-\infty}^{+\infty}$  элементов произвольного поля  $\mathbb{F}$ , удовлетворяющие разложениям вида

$$A_{m+n}A_{m-n} = a_1(m)b_1(n) + a_2(m)b_2(n),$$

где  $a_1, a_2, b_1, b_2 : \mathbb{Z} \rightarrow \mathbb{F}$ . Полученные результаты используются для построения аналогов алгоритмов Диффи – Хеллмана и Эль-Гамала, в которых задача дискретного логарифмирования ставится в группе  $(S, +)$ , где множество  $S$  состоит из четверок вида  $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$ ,  $n \in \mathbb{Z}$ , а  $S(n) + S(m) = S(n + m)$ .

Ключевые слова: гиперэллиптические последовательности, нелинейные рекуррентные последовательности, криптосистемы.

### 1. Введение

Быковский<sup>2</sup> предложил следующую конструкцию.

**Определение.** Пусть не равные тождественно нулю последовательности комплексных чисел

$$A = \{A_n\}_{n=-\infty}^{+\infty}, \quad B = \{B_n\}_{n=-\infty}^{+\infty}$$

удовлетворяют (для любых целых  $m, n$ ) разложениям

$$A_{m+n}B_{m-n} = \sum_{j=1}^{N_0} a_j(m)b_j(n), \quad (1)$$

$$A_{m+n+1}B_{m-n} = \sum_{j=1}^{N_1} \tilde{a}_j(m)\tilde{b}_j(n) \quad (2)$$

<sup>1</sup>Хабаровское отделение Института прикладной математики ДВО РАН, 680000, г. Хабаровск, ул. Дзержинского, 54; Тихоокеанский государственный университет, 600042, г. Хабаровск, ул. Тихоокеанская, 136. Электронная почта: illar\_a@list.ru

<sup>2</sup>V. Bykovskii, Elliptic systems of sequences and functions, Torus Actions in Geometry, Topology, and Applications February (16–21, 2015, Skolkovo institute of science and technology, Moscow, Russia)

с некоторыми  $a_j, b_j, \tilde{a}_j, \tilde{b}_j: \mathbb{Z} \rightarrow \mathbb{C}$  и минимально возможными  $N_0, N_1 \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ . Тогда пару  $(A, B)$  будем называть *гиперэллиптической системой последовательностей*, величину  $R_0(A, B) = N_0$  — ее 0-рангом, а величину  $R_1(A, B) = N_1$  — ее 1-рангом.

Эту конструкцию несложно распространить на случай, когда поле  $\mathbb{C}$  заменяется на произвольное поле  $\mathbb{F}$ . Ограничимся случаем, когда  $A = B$  и выполняется только уравнение (1).

**Определение.** Пусть не равная тождественно нулю последовательность  $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$  удовлетворяет (для любых целых  $m, n$ ) разложению

$$A_{m+n}A_{m-n} = \sum_{j=1}^N a_j(m)b_j(n) \quad (3)$$

с некоторыми  $a_j, b_j: \mathbb{Z} \rightarrow \mathbb{F}$  и минимально возможным  $N \in \mathbb{Z}_+$ . Тогда последовательность  $A$  будем называть *полугиперэллиптической последовательностью*, а величину  $R_0(A) = N$  — ее 0-рангом.

В настоящей работе рассматривается вопрос о построении асимметричных криптосистем с помощью полугиперэллиптических последовательностей в конечном поле. По сути речь идет об алгоритмах Диффи – Хеллмана и Эль-Гамала, в которых задача дискретного логарифмирования ставится в группе  $(S, +)$ , где множество  $S$  состоит из четверок вида

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2}), \quad n \in \mathbb{Z},$$

а  $S(n) + S(m) = S(n+m)$ . Подобные идеи впервые появились в докладе [1], в котором вместо гиперэллиптических последовательностей рассматривалась последовательность Сомос-4 в поле вычетов по простому модулю  $p$ . Применение последовательностей Сомоса наталкивается на некоторые препятствия (см. замечание 2 ниже), которые можно обойти, используя (полу)гиперэллиптические последовательности.

В следующем разделе приводится детерминантное уравнение, эквивалентное (3). В § 3 строятся примеры полугиперэллиптических последовательностей в различных полях. В § 4 изучаются некоторые свойства последовательностей с  $R_0(A) = 2$ , а в § 5 формулируются аналоги алгоритмов Диффи – Хеллмана и Эль-Гамала для таких последовательностей. В последнем разделе обсуждаются нерешенные задачи и возможные обобщения.

## 2. Детерминантное уравнение

Пусть  $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ . Для любых целых  $m_0, \dots, m_k, n_0, \dots, n_k$  определим

$$D_A \begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = \det \begin{pmatrix} A_{m_0+n_0} A_{m_0-n_0} & \dots & A_{m_0+n_k} A_{m_0-n_k} \\ \vdots & & \vdots \\ A_{m_k+n_0} A_{m_k-n_0} & \dots & A_{m_k+n_k} A_{m_k-n_k} \end{pmatrix}.$$

**Лемма 1.** Неравенство  $R_0(A) \leq k$  равносильно тому, что

$$D_A \begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = 0 \tag{4}$$

для всех  $m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}$ .

**Доказательство.** Пусть  $R_0(A) = N \leq k$ . Тогда выполняется разложение (3). Из него вытекает линейная зависимость строк (столбцов) определителя из левой части равенства (4). Значит, справедливо соотношение (4).

Пусть выполняется (4). Если  $A_{m+n}A_{m-n} = 0$  при всех  $m, n \in \mathbb{Z}$ , то  $A \equiv 0$ . Поэтому существуют  $N \in \mathbb{N}$  и целые  $m_1, \dots, m_N, n_1, \dots, n_N$  такие, что

$$D_A \begin{pmatrix} m_1 & \dots & m_N \\ n_1 & \dots & n_N \end{pmatrix} \neq 0.$$

Пусть  $N$  — наибольшее натуральное, удовлетворяющее этому условию. Тогда  $N \leq k$  в силу (4). Кроме того, для любых  $m, n \in \mathbb{Z}$

$$D_A \begin{pmatrix} m_1 & \dots & m_N & m \\ n_1 & \dots & n_N & n \end{pmatrix} = 0.$$

Раскладывая этот определитель по последнему столбцу (или последней строке), получаем разложение вида (3). Значит,  $R_0(A, B) \leq N \leq k$ . □

*Замечание 1.* Утверждение, аналогичное лемме 1, приведено в [2, § 3] (см. также [3, 4]) для случая, когда  $A$  — функция  $\mathbb{C} \rightarrow \mathbb{C}$ .

### 3. Примеры полугиперэллиптических последовательностей

1. Пусть  $\mathbb{F}$  — произвольное поле. Положим

$$A_n = P_1(n)a_1^n + \dots + P_s(n)a_s^n,$$

где  $P_j$  — многочлены из  $\mathbb{F}[X]$ , а  $a_j \in \mathbb{F}$ . Нетрудно заметить, что тогда выполняется разложение вида (3). Такое же утверждение справедливо для последовательности

$$A_n = \begin{cases} P_1(n)a_1^n + \dots + P_s(n)a_s^n & \text{при четном } n \\ Q_1(n)b_1^n + \dots + Q_t(n)b_t^n & \text{при нечетном } n \end{cases},$$

где  $P_j, Q_j \in \mathbb{F}[X]$ ,  $a_j, b_j \in \mathbb{F}$ .

2. Пусть  $\mathbb{F} = \mathbb{C}$ . Все известные на сегодняшний день гиперэллиптические системы последовательностей в поле  $\mathbb{C}$  приведены в [3, § 9]. Все неэлементарные (отличные от указанных в п. 1) случаи описываются с помощью сужений производных многомерных тета-функций на пространство  $\mathbb{C}$ . Существуют и другие варианты *полугиперэллиптических* последовательностей. Например, пусть  $u_1, u_2, v_1, v_2 \in \mathbb{C}$ , а  $\sigma_1, \sigma_2$  — сигма-функции Вейерштрасса, ассоциированные с разными решетками. Положим

$$A_n = \begin{cases} \sigma_1(nu_1 + v_1) & \text{при четном } n \\ \sigma_2(nu_2 + v_2) & \text{при нечетном } n \end{cases}.$$

Тогда  $R_0(A) \leq 4$ . Для доказательства достаточно использовать формулу сложения (для сигма-функции) и учесть, что числа  $m+n$  и  $m-n$  имеют одинаковую четность.

**3.** Пусть  $\mathbb{F} = \mathbb{Z}_p$  — поле вычетов по простому модулю  $p$ . Пусть  $A$  — полугиперэллиптическая последовательность в поле  $\mathbb{C}$ ,  $R_0(A) = N$ . Предположим, что последовательность  $A$  — целочисленная. Так как  $A$  удовлетворяет равенству (4) (в кольце  $\mathbb{Z}$ ), то последовательность

$$\tilde{A}(n) = A(n) \pmod{p}$$

удовлетворяет этому же уравнению в поле  $\mathbb{Z}_p$ . Следовательно,  $R_0(A) \leq N$ . Целочисленные полугиперэллиптические последовательности небольшого ранга можно строить следующим образом.

Пусть  $b, c$  — рациональные положительные. Рассмотрим последовательность рациональных чисел, удовлетворяющую уравнению (последовательность Сомос-4)

$$A_{n+2}A_{n-2} = bA_{n+1}A_{n-1} + cA_n^2.$$

Так как  $b, c > 0$ , то она не имеет нулевых элементов и однозначно определяется начальными членами  $A_0, A_1, A_2, A_3$ . В этом случае (см., например, [5] и ссылки там)

$$D_A \begin{pmatrix} m_0 & m_1 & m_2 \\ n_0 & n_2 & n_2 \end{pmatrix} = 0$$

Поэтому  $R_0(A) \leq 2$ . При некоторых ограничениях, наложенных на исходные данные  $b, c, A_0, A_1, A_2, A_3$ , последовательность  $A$  является целочисленной (см. [3, 6–9] и ссылки там).

#### 4. Свойства полугиперэллиптических последовательностей при $R_0(A) = 2$

Всюду в этом разделе считаем, что  $\mathbb{F}$  — произвольное поле,  $A: \mathbb{Z} \rightarrow \mathbb{F}$  и  $R_0(A) = 2$ . Мы рассмотрим два вопроса:

- 1) задание последовательности  $A$  конечным набором параметров из  $\mathbb{F}$ ;
- 2) «быстрый» (полиномиальный по  $m$ ) алгоритм вычисления  $A_{n+m}$  по заданным номеру  $m$  и элементу  $A_n$  ( $n$  — неизвестно).

Из леммы 1 вытекает равенство

$$D_A \begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ A_3A_{-1} & A_2A_0 & A_1^2 \\ A_2A_{-2} & A_1A_{-1} & A_0^2 \end{vmatrix} = 0,$$

которое равносильно уравнению

$$aA_{n+2}A_{n-2} + bA_{n+1}A_{n-1} + cA_n^2 = 0, \quad (5)$$

где

$$a = \begin{vmatrix} A_2A_0 & A_1^2 \\ A_1A_{-1} & A_0^2 \end{vmatrix}, \quad b = - \begin{vmatrix} A_3A_{-1} & A_1^2 \\ A_2A_{-2} & A_0^2 \end{vmatrix}, \quad c = \begin{vmatrix} A_3A_{-1} & A_2A_0 \\ A_2A_{-2} & A_1A_{-1} \end{vmatrix}.$$

Для вычисления  $a, b, c$  достаточно знать шесть (начальных) элементов

$$A_{-2}, A_{-1}, A_0, A_1, A_2, A_3. \tag{6}$$

Все остальные могут быть найдены из соотношения (5) при условии, что *последовательность A не имеет нулевых членов*. Если поле  $\mathbb{F}$  конечное, то привести условия на начальные данные, гарантирующие выполнение этого предположения для достаточно широкого класса последовательностей, довольно проблематично. Поэтому нашей ближайшей целью является выяснение того, как могут быть расположены нулевые элементы последовательности  $A$ .

*Замечание 2.* Последовательность  $A$ , удовлетворяющая уравнению вида (5) (в котором  $a \neq 0$ ) называется последовательностью Сомос-4. Если она содержит нулевые члены, то ее нельзя однозначно построить, используя только коэффициенты  $a, b, c$  и некоторый (конечный) набор начальных значений (см. [10]). На взгляд автора, это является основным препятствием на пути использования последовательностей Сомоса в криптографии.

**Расположение нулевых элементов последовательности  $A$ .** Пусть

$$Z_A = \{n \in \mathbb{Z} : A_n = 0\}.$$

**Лемма 2.** Пусть  $abc \neq 0$  и  $Z_A \neq \emptyset$ . Тогда  $Z_A$  — арифметическая прогрессия с разностью  $\geq 4$ .

*Доказательство.* Пусть

$$h = \min\{n_0 - m_0 : A_{n_0} = A_{m_0} = 0, n_0 > m_0\}.$$

Не умаляя общности, считаем, что  $A_0 = A_h = 0$ . В противном случае следует перейти к рассмотрению последовательности  $\hat{A}_n = A_{n+n_0}$ , где номер  $n_0$  удовлетворяет условию  $A_{n_0} = A_{n_0+h} = 0$ , и учесть, что  $R_0(A) = R_0(\hat{A})$ .

1. Пусть  $h = 1$ , т.е.  $A_0 = A_1 = 0$ . Рассматривая (5) при  $n = -1, \pm 2, \pm 3, \dots$ , приходим к выводу, что все элементы последовательности  $A$  равны нулю. Это противоречит условиям.

2. Пусть  $h = 2$ , т.е.  $A_0 = A_2 = 0$ . Полагая в (5)  $n = 0$ , получаем, что  $A_1A_{-1} = 0$ . Но тогда  $h = 1$ . Получили противоречие.

3. Пусть  $h = 3$ , т.е.  $A_0 = A_3 = 0$ . Полагая в (5)  $n = 1$ , получаем, что  $A_1^2 = 0$ . Но тогда  $h = 1$ . Получили противоречие.

4. Пусть  $h \geq 4$ . Докажем, что  $A_{jh} = 0$  при  $j = 1, 2, \dots$ . Используем метод математической индукции по  $j = 1, 2, \dots$ . При  $j = 1$  утверждение выполнено. Пусть  $A_{jh} = 0$  при  $j = 1, 2, \dots, n - 1$ , где  $n \geq 2$ . Согласно лемме 1

$$D_A \begin{pmatrix} h & nh & 1 \\ 0 & h & 1 \end{pmatrix} = \begin{vmatrix} 0 & 0 & A_{h+1}A_{h-1} \\ A_{nh}^2 & 0 & * \\ * & A_{1+h}A_{1-h} & * \end{vmatrix} = A_{nh}^2 A_{h+1} A_{h-1} A_{1+h} A_{1-h} = 0.$$

Здесь и далее символом \* обозначены элементы, значения которых не влияют на определитель. Так как  $A_0 = A_h = 0$ , то  $A_{h+1}A_{h-1}A_{1-h} \neq 0$  по определению  $h$ . Значит,  $A_{nh} = 0$ . Поэтому  $A_{jh} = 0$  при  $j = 1, 2, \dots$

Аналогичным образом доказывается, что  $A_{jh} = 0$  при  $j = -1, -2, \dots$ . Значит,  $Z_A = \{0, \pm h, \pm 2h, \dots\}$  согласно определению  $h$ .  $\square$

**Лемма 3.** Пусть  $a \neq 0$ ,  $bc = 0$ , причем

$$\text{не более чем один элемент из } A_{-2}, A_{-1}, A_0, A_1, A_2, A_3 \text{ равен нулю.} \quad (7)$$

Тогда  $Z_A = \emptyset$ .

*Доказательство.* Согласно (5)

$$\begin{aligned} aA_{n+2}A_{n-2} &= -bA_{n+1}A_{n-1} && \text{при } c = 0, b \neq 0, \\ aA_{n+2}A_{n-2} &= -cA_n^2 && \text{при } c \neq 0, b = 0, \\ A_{n+2}A_{n-2} &= 0 && \text{при } c = b = 0. \end{aligned} \quad (8)$$

Последний случай невозможен из-за условия (7). Если только один коэффициент из  $b, c$  равен нулю, то согласно (8) и условию (7) среди элементов  $A_{-2}, A_{-1}, A_0, A_1, A_2, A_3$  нет нулей. Тогда все другие члены последовательности находятся по соответствующей формуле из (8) и также являются ненулевыми.  $\square$

**Восстановление последовательности  $A$  по начальным данным.**

**Определение.** Набор из восьми элементов  $A_{-3}, \dots, A_4$  будем называть *расширенными начальными данными*.

Из леммы 1 вытекает равенство

$$D_A \begin{pmatrix} n & 1 & 0 \\ 3 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+3}A_{n-3} & A_{n+1}A_{n-1} & A_n^2 \\ A_4A_{-2} & A_2A_0 & A_1^2 \\ A_3A_{-3} & A_1A_{-1} & A_0^2 \end{vmatrix} = 0.$$

Поэтому

$$aA_{n+3}A_{n-3} + \tilde{b}A_{n+1}A_{n-1} + \tilde{c}A_n^2 = 0, \quad (9)$$

где

$$\tilde{b} = - \begin{vmatrix} A_4A_{-2} & A_1^2 \\ A_3A_{-3} & A_0^2 \end{vmatrix}, \quad \tilde{c} = \begin{vmatrix} A_4A_{-2} & A_2A_0 \\ A_3A_{-3} & A_1A_{-1} \end{vmatrix}.$$

Для вычисления  $\tilde{b}, \tilde{c}$ ,  $a, b, c$  достаточно знать расширенные начальные данные.

**Лемма 4.** Пусть  $a \neq 0$  и выполняется условие (7). Тогда последовательность  $A$  однозначно находится по расширенным начальным данным с помощью формул

$$A_{n+4} = \begin{cases} -\frac{bA_{n+3}A_{n+1} + cA_{n+2}^2}{aA_n} & \text{при } A_n \neq 0 \\ \frac{\tilde{c}A_{n+2}A_{n+1}}{bA_{n-1}} & \text{при } A_n = 0 \end{cases}, \quad (10)$$

$$A_{n-1} = \begin{cases} -\frac{bA_nA_{n+2} + cA_{n+1}^2}{aA_{n+3}} & \text{при } A_{n+3} \neq 0, \\ \frac{\tilde{c}A_{n+2}A_{n+1}}{bA_{n+4}} & \text{при } A_{n+3} = 0. \end{cases} \quad (11)$$

**Доказательство.** Если  $A_n = 0$  ( $A_{n+3} = 0$ ), то  $A_{n-1} \neq 0$  ( $A_{n+4} \neq 0$ ) согласно леммам 2, 3. Кроме того,  $b \neq 0$ , если последовательность  $A$  имеет нулевые члены. Поэтому в формулах (10), (11) деления на ноль не происходит.

Если  $A_n \neq 0$  ( $A_{n+3} \neq 0$ ), то формула (10) (формула (11)) получается из (5) путем замены  $n$  на  $n + 2$  ( $n$  на  $n + 1$ ).

Докажем (10) при  $A_n = 0$ . В этом случае  $A_{n+2} \neq 0$ . Кроме того, согласно (5), (9)

$$aA_{n+2}A_{n-2} + bA_{n+1}A_{n-1} = 0, \quad aA_{n+4}A_{n-2} + \tilde{c}A_{n+1}^2 = 0.$$

Выражая из предпоследнего соотношения  $A_{n-2}$  и подставляя полученное значение в последнее соотношение, получаем

$$A_{n-2} = -\frac{bA_{n+1}A_{n-1}}{aA_{n+2}}, \quad -b\frac{A_{n+4}A_{n+1}A_{n-1}}{A_{n+2}} + \tilde{c}A_{n+1}^2 = 0.$$

Из последней формулы вытекает (10).

Докажем (11) при  $A_{n+3} = 0$ . В этом случае  $A_{n+1} \neq 0$ . Кроме того, согласно (5), (9)

$$aA_{n+5}A_{n+1} + bA_{n+4}A_{n+2} = 0, \quad aA_{n+5}A_{n-1} + \tilde{c}A_{n+2}^2 = 0.$$

Выражая из предпоследнего соотношения  $A_{n+5}$  и подставляя полученное значение в последнее соотношение, получаем

$$A_{n+5} = -\frac{bA_{n+4}A_{n+2}}{aA_{n+1}}, \quad -b\frac{A_{n+4}A_{n+2}A_{n-1}}{A_{n+1}} + \tilde{c}A_{n+2}^2 = 0.$$

Из последней формулы вытекает (11). □

*Замечание 3.* Пусть нам известен набор из шести элементов (6). Тогда мы можем найти  $a, b, c$  и вычислить  $A_4$  при  $A_0 \neq 0$ , а также  $A_{-3}$  при  $A_1 \neq 0$ , используя формулу (5). Таким образом, при  $A_0A_1 \neq 0$  для нахождения всей последовательности достаточно знать начальные данные (6). Однако если  $A_0A_1 = 0$ , то начальных данных (6) может быть недостаточно для однозначного восстановления всей последовательности (см. [10]).

**Следствие 1.** Пусть поле  $\mathbb{F}$  — конечное и состоит из  $r$  элементов. Пусть  $a \neq 0$  и выполняется условие (7). Тогда последовательность  $A$  имеет период  $\leq r^5$ .

**Доказательство.** Согласно (10) существует функция  $f : \mathbb{F}^5 \rightarrow \mathbb{F}$  такая, что

$$A_{n+4} = f(A_{n-1}, A_n, A_{n+1}, A_{n+2}, A_{n+3}).$$

Требуемое утверждение вытекает из элементарных свойств рекуррентных последовательностей с элементами из конечного множества. □

*Замечание 4.* По-видимому, период последовательности  $A$  не больше, чем  $r^4$ . Если, например,  $A_n$  не содержит нулевых членов, то это следует из формулы (10).



**Алгоритм «быстрого» вычисления элементов последовательности  $A$ .** Из леммы 1 вытекает равенство

$$D_A \begin{pmatrix} n+m & 1 & 0 \\ m & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2m}A_n & A_{n+m+1}A_{n+m-1} & A_{n+m}^2 \\ A_{1+m}A_{1-m} & A_2A_0 & A_1^2 \\ A_mA_{-m} & A_1A_{-1} & A_0^2 \end{vmatrix} = 0.$$

Раскладывая определитель из этого равенства по первой строке, получаем формулу

$$A_{n+2m} = \frac{1}{aA_n} P(-m, -m+1, m, m+1, n+m-1, n+m, n+m+1), \quad (12)$$

где

$$\begin{aligned} P(-m, -m+1, m, m+1, n+m-1, n+m, n+m+1) &= \\ &= A_{n+m+1}A_{n+m-1} \begin{vmatrix} A_{1+m}A_{1-m} & A_1^2 \\ A_mA_{-m} & A_0^2 \end{vmatrix} - A_{n+m}^2 \begin{vmatrix} A_{1+m}A_{1-m} & A_2A_0 \\ A_mA_{-m} & A_1A_{-1} \end{vmatrix}. \end{aligned}$$

Заменяя в (12)  $n$  на  $n+1$ , получаем еще одну формулу

$$A_{n+2m+1} = \frac{1}{aA_{n+1}} P(-m, -m+1, m, m+1, n+m, n+m+1, n+m+2). \quad (13)$$

**Определение.** Для любого целого  $n$  набор  $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$  будем называть *состоянием*.

**Лемма 5.** Пусть  $a \neq 0$  и выполняется условие (7). Зная расширенные начальные данные, состояния  $S(n), S(n+k)$  и  $S(\pm k)$ , а также номер  $k \in \mathbb{Z}$  (номер  $n$  неизвестен) можно вычислить состояние  $S(n+2k)$ , используя  $O(1)$  элементарных операций в поле  $\mathbb{F}$ .

**Доказательство.** Если  $k = \pm 1$ , то достаточно использовать одну из формул (10), (11). Пусть  $|k| \geq 2$ . Нам известны элементы последовательности  $A$  с номерами

$$\begin{array}{cccc} n-1, & n, & n+1, & n+2, \\ n+k-1, & n+k, & n+k+1, & n+k+2, \\ \pm k-1, & \pm k, & \pm k+1, & \pm k+2. \end{array}$$

Нужно найти элементы с номерами  $n+2k-1, n+2k, n+2k+1, n+2k+2$ .

1. Пусть  $A_n A_{n+1} \neq 0$ . Тогда, используя (12) при  $m = k, k+1$ , а также (13) при  $m = k-1, k$ , находим требуемые четыре элемента.

2. Пусть  $A_n = 0$ . Тогда  $A_{n+1}A_{n+2} \neq 0$  согласно лемме 3. Элементы  $A_{n+2k-1}$  и  $A_{n+2k+1}$  вычисляются по формуле (13), в которой  $m = k-1$  и  $m = k$  соответственно. Осталось найти  $A_{n+2k}$  и  $A_{n+2k+2}$ . Используя формулу (10) при  $k > 0$  и (11) при  $k < 0$ , вычисляем  $A_{n+k+2}$ . Заменяя в (12)  $n$  на  $n+2$ , получаем соотношение

$$A_{n+2m+2} = \frac{1}{aA_{n+2}} P(-m, -m+1, m, m+1, n+m+1, n+m+1, n+m+2).$$

Из него при  $m = k-1$  и  $m = k$  находим элементы  $A_{n+2k}$  и  $A_{n+2k+2}$ .

3. Случай, когда  $A_{n+1} = 0$  рассматривается аналогично предыдущему.  $\square$

На основании леммы 5 стандартным образом<sup>1</sup> строится алгоритм «быстрого» вычисления  $S(n+m)$  при заданных  $S(n)$  и  $m$  (и неизвестном  $n$ ). Ограничимся случаем положительного  $m$ . Пусть  $m = (\varepsilon_{s-1} \dots \varepsilon_1 \varepsilon_0)_2$  — представление натурального  $m$  в двоичной системе исчисления, то есть

$$m = \varepsilon_0 + 2\varepsilon_1 + \dots + 2^{s-1}\varepsilon_{s-1}, \tag{14}$$

где  $\varepsilon_0, \dots, \varepsilon_{s-2} \in \{0, 1\}$ , а  $\varepsilon_{s-1} = 1$ . Определим  $m_1, m_2, \dots, m_{s-1}$  по формулам

$$m_1 = 1, \quad m_{j+1} = 2m_j + \varepsilon_{s-1-j}, \quad j = 1, \dots, s-1.$$

Тогда  $m_s = m$ .

**Алгоритм 1.**

*Данные:* начальные элементы  $A_{-3}, \dots, A_4$ , номер  $m = (\varepsilon_{s-1} \dots \varepsilon_1 \varepsilon_0)_2 \in \mathbb{N}$  и состояние  $S(n)$  (номер  $n$  неизвестен).

*Найти:* состояние  $S(n+m)$ .

- 1) Полагаем  $j = 1$ ,  $m_1 = 1$  и вычисляем  $S(n \pm 1)$ .
- 2) Вычисляем  $S(\pm 2m_j)$  и  $S(n + 2m_j)$ .
- 3) Если  $\varepsilon_{s-j-1} = 0$ , то полагаем  $m_{j+1} = 2m_j$  и вычисляем

$$S(\pm m_{j+1}) = S(\pm 2m_j), \quad S(n + m_{j+1}) = S(n + 2m_j).$$

- 4) Если  $\varepsilon_{s-j-1} = 1$ , то полагаем  $m_{j+1} = 2m_j + 1$  и вычисляем

$$S(\pm m_{j+1}) = S(\pm(2m_j + 1)), \quad S(n + m_{j+1}) = S((n + 2m_j) + 1).$$

- 5) Если  $j < s - 1$ , то увеличиваем  $j$  на 1 и переходим к шагу 2.
- 6) Полагаем  $S(n+m) = S(n + m_{j+1})$ . Конец.

Количество шагов 2)–4) равно  $s - 1 = O(\log m)$ . Поэтому из леммы 5 вытекает

**Следствие 2.** *Сложность алгоритма 1 не больше, чем сложность выполнения  $O(\log m)$  элементарных операций в поле  $\mathbb{F}$ .*

**5. Построение криптосистем с помощью полугиперэллиптических последовательностей**

В этом параграфе считаем, что  $\mathbb{F}$  — конечное поле,  $\{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ ,  $R_0(A) = 2$ . Предполагаем, что расширенные начальные данные  $A_{-3}, \dots, A_4$  находятся в открытом доступе.

---

<sup>1</sup>по аналогии, например, с алгоритмом быстрого возведения в степень

**Аналог алгоритма Диффи – Хеллмана.** Абоненты  $B_1, B_2$ , вырабатывают общий секретный ключ  $K \in \mathbb{F}^4$ , используя следующий алгоритм.

- 1) Абонент  $B_1$  выбирает  $k_1 \in \mathbb{Z}$ , вычисляет  $S(k_1)$ , используя алгоритм 1, и посылает абоненту  $B_2$  сообщение  $S(k_1)$  (номер  $k_1$  хранится в секрете).
- 2) Абонент  $B_2$  выбирает  $k_2 \in \mathbb{Z}$ , вычисляет  $S(k_2)$  и посылает абоненту  $B_1$  сообщение  $S(k_2)$  (номер  $k_2$  хранится в секрете).
- 3) Абонент  $B_2$  (абонент  $B_1$ ), зная номер  $k_2$  (номер  $k_1$ ) и состояние  $S(k_1)$  (состояние  $S(k_2)$ ), вычисляет  $S(k_1 + k_2)$ , используя алгоритм 1.

Общим секретом является  $K = S(k_1 + k_2)$ .

Пассивный противник знает состояния  $S(k_1)$  и  $S(k_2)$ . Для того чтобы найти секретный ключ  $S(k_1 + k_2)$ , ему достаточно определить номер  $k_1$  (или номер  $k_2$ ). Для этого нужно решить задачу определения номера  $k$  по заданному элементу  $S(k)$ . Она представляет собой задачу дискретного логарифмирования в группе  $(S, +)$ , где множество  $S$  состоит из четверок вида

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2}), \quad n \in \mathbb{Z},$$

а  $S(n) + S(m) = S(n + m)$ .

**Алгоритм шифрования (аналог алгоритма Эль-Гамала на эллиптической кривой).** Пусть целое число  $n$  — это *общий параметр* всех пользователей. *Секретным ключом абонента В* является некоторое целое  $k$ , а *открытым ключом* — состояние  $S(k)$ .

*Алгоритм шифрования* сообщения  $x = x_{-1}x_0x_1x_2 \in \mathbb{F}^4$ , отправляемого абоненту В.

- 1) Выбираем сеансовый ключ  $r \in \mathbb{Z}$ .
- 2) Вычисляем состояния  $S(n + r)$  и  $S(n + k + r)$ . Для этого можно использовать алгоритм 1, так как нам известны номера  $r, n$  и состояние  $S(k)$ .
- 3) Вычисляем  $y = y_{-1}y_0y_1y_2 \in \mathbb{F}^4$  по формулам:

$$y_j = x_j \cdot A_{n+k+r+j}, \quad j = -1, 0, 1, 2.$$

- 4) Высылаем абоненту В шифртекст  $(S(n + r), y)$ .

*Алгоритм расшифрования* шифртекста  $(S(n + r), y)$  абонентом В.

- 1) Абонент В вычисляет  $S(n + k + r)$ , используя алгоритм 1 (напомним, что В знает состояние  $S(n + r)$  и номер  $k$ ).
- 2) Находит открытый текст  $x = x_{-1}x_0x_1x_2$  по формулам

$$x_j = y_j \cdot A_{n+k+r+j}^{-1}, \quad j = -1, 0, 1, 2.$$

Корректность алгоритма расшифровки очевидна.

*Замечание 5.* Аналогичным образом можно построить алгоритм электронный цифровой подписи (наподобие ГОСТ 34.10-2012), использующий полугиперэллиптические последовательности вместо группы точек на эллиптической кривой.

## 6. Заключение

В настоящей работе были рассмотрены только последовательности с  $R_0(A) = 2$ . Можно разработать криптографические алгоритмы, использующие последовательности более высокого 0-ранга, а также последовательности небольших конечных 1-рангов (последовательности, удовлетворяющие разложению вида (2)). Основная (и, возможно, единственная) проблема заключается в выяснении взаимного расположения нулевых элементов. Отметим, что даже в случае  $R_0(A) = 2$  ряд важных вопросов остается нерешенным. Отметим некоторые из них.

1. Криптостойкость описанных в предыдущем разделе алгоритмов зависит от периода последовательности  $A$ . Поэтому очень важен вопрос о разработке алгоритмов вычисления искомого периода (аналог задачи о вычислении порядка группы точек эллиптической кривой над конечным полем), а также о способах построения полугиперэллиптических последовательностей, имеющих большой период.

2. Существует довольно мало примеров полугиперэллиптических последовательностей в конечных полях (см. § 3). Этот пробел можно было бы восполнить путем получения результатов следующего вида: для любых  $a_{-2}, a_{-1}, \dots, a_3 \in \mathbb{F}$  существует последовательность  $A_n \in \mathbb{F}$  такая, что

$$R_0(A) \leq 2, \quad A_j = a_j, \quad j = -2, -1, \dots, 3.$$

3. В [3] описаны все последовательности комплексных чисел, удовлетворяющие условию  $R_0(A) + R_1(A) \leq 4$ . Все неэлементарные случаи с точностью до некоторых простых преобразований имеют вид  $A_n = \sigma(nu + v)$ , где  $u, v \in \mathbb{C}$ , а  $\sigma$  — сигма-функция Вейерштрасса. Возникает вопрос об аналогичном описании множества всех (полу)гиперэллиптических систем в произвольном поле или хотя бы в поле вычетов  $\mathbb{Z}_p$  по простому модулю  $p$ .

## Список литературы

- [1] Richard Schroepel, Hilarie Orman, R. Wm. Gosper, “Somos Sequences and Cryptographic Applications”, 2017, <https://www.osti.gov/servlets/purl/1483215>.
- [2] В. А. Быковский, “Гиперквазимногочлены и их приложения”, *Функц. анализ и его приложения*, **50**:3, (2016), 34–46.
- [3] А. А. Илларионов, “Гиперэллиптические системы последовательностей ранга 4”, *Матем. сб.*, **210**:9, (2019), 59–88.
- [4] А. А. Илларионов, “Функциональное уравнение и сигма-функция Вейерштрасса”, *Функц. анализ и его приложения*, **50**:4, (2016), 43–54.
- [5] А. В. Устинов, “Элементарный подход к изучению последовательностей Сомоса”, *Алгебраическая топология, комбинаторика и математическая физика*, Сборник статей. К 75-летию со дня рождения члена-корреспондента РАН Виктора Матвеевича Бухштабера, Тр. МИАН, т. 305, МАИК, М., 2019.
- [6] S. Fomin, A. Zelevinsky, “The Laurent Phenomenon”, *Adv. Appl. Math.*, **28**, (2002), 119–144.
- [7] A. N. Hone, C. Swart, “Integrality and the Laurent phenomenon for Somos 4 and Somos 5 sequences”, *Math. Proc. Camb. Philos. Soc.*, **145**:1, (2008), 65–85.

- [8] A. N. Hone, “Analytic solutions and integrability for bilinear recurrences of order six”, *Applicable Analysis: An International Journal*, **89**:4, (2010), 473–492.
- [9] В. А. Быковский, А. В. Устинов, “О лорановости последовательностей Сомос-4 и Сомос-5”, *Функц. анализ и его прил.*, **53**:3, (2019), 79–83.
- [10] А. А. Илларионов, “О последовательности Сомос-4”, *Дальневост. матем. журн.*, **18**:2, (2018), 183–188.
- [11] А. А. Илларионов, “Решение функциональных уравнений, связанных с эллиптическими функциями”, *Аналитическая теория чисел*, Сборник статей. К 80-летию со дня рождения Анатолия Алексеевича Карацубы, Тр. МИАН, **299**, 2017, 105–117.

Поступила в редакцию  
7 октября 2019 г.

---

*Illarionov A. A.* Asymmetric cryptography and hyperelliptic sequences. *Far Eastern Mathematical Journal*. 2019. V. 19. No 2. P. 185–196.

#### ABSTRACT

We study sequences  $\{A_n\}_{n=-\infty}^{+\infty}$  of elements of a field  $\mathbb{F}$  that satisfy decompositions of the form

$$A_{m+n}A_{m-n} = a_1(m)b_1(n) + a_2(m)b_2(n),$$

where  $a_1, a_2, b_1, b_2 : \mathbb{Z} \rightarrow \mathbb{F}$ . The results are used to build analogues of the Diffie – Hellman and El-Gamal algorithms. The discrete logarithm problem is posed in the group  $(S, +)$ , where the set  $S$  consists of fours  $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$ ,  $n \in \mathbb{Z}$ , and  $S(n) + S(m) = S(n + m)$ .

Key words: *hyperelliptic sequences, nonlinear recurrence sequences, asymmetric cryptography.*