8. *Стоян Ю. Г.* Математические модели и оптимизационные методы геометрического проектирования / Стоян Ю. Г., Яковлев С. В. – К. : Наук. думка, 1986. – 268 с.
9. *Яковлев С. В.* Теория выпуклых продолжений функции на вершинах выпуклых многогранников... / Яковлев С. В. // ЖВМ и МФ. – 1994. – Т. 34, № 7. – С. 1112–1119.
10. *Стоян Ю. Г.* Построение выпуклых и вогнутых функций на перестановочном многограннике / Стоян Ю. Г., Яковлев С. В. // ДАН УССР, Сер А. – 1988. – № 5. – С. 68–70.
11. *Яковлев С. В.* О минимизации линейной функции на вершинах перестановочного многогранника с учетом линейных ограничений / Яковлев С. В., Валуйская О. А. // Доп. НАНУ. – 1999. – № 11. – С. 103–107.
12. *Гребенник И. В.* Решение некоторых задач условной оптимизации линейных функций на перестановочном многограннике / Гребенник И. В. // Радиоэлектроника и информатика. – 1999. – № 1. – С. 55–59.
13. *Гребенник И. В.* Экстремальные свойства функций на классах композиционных образов комбинаторных множеств / Гребенник И. В., Баранов А. В. // Бионика интеллекта. – 2007. – № 1(66). – С. 99–102.
14. *Гребенник И. В.* Оптимизация линейных функций с линейными ограничениями на комбинаторных множествах на основе случайного поиска / Гребенник И. В., Баранов А. В. // Искусственный интеллект. – 2007. – № 1. – С. 132–137.

Надійшла 16.09.2008

Досліджуються задачі оптимізації опуклих функцій на комбінаторних множинах. Будуються оцінки мінімумів опуклих функцій для класів комбінаторних множин перестановок, з урахуванням та без урахування лінійних обмежень на змінні. Побудова оцінок включає в себе додаткову процедуру оптимізації. Наводяться приклади, аналізуються результати обчислювальних експериментів.

The paper is devoted to the problem of convex functions optimization on combinatorial sets. Estimates of convex function minimum are constructed for different classes of combinatorial sets of permutations, with or without linear constraints on the variables. Estimates construction includes an addi-tional procedure of optimization. Examples are given; results of numerical experiments are analyzed.

УДК 681.3.06

В. И. Долгов, А. В. Неласая

МЕТОД ВЫЧИСЛЕНИЯ МАТРИЦЫ ХАССЕ – ВИТТА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ СПЕЦИАЛЬНОГО ВИДА

В статье предложен метод вычисления элементов матрицы Хассе – Витта гиперэллиптических кривых специального вида, основанный на использовании формулы бинома Ньютона.

ВВЕДЕНИЕ

Двухключевая криптография основана на трудности решения определенных математических задач. На первых порах развития этого направления такими задачами рассматривались разложения большого числа на простые множители и дискретное логарифмирование в простом поле Галуа. Современные стандарты цифровой подписи и направленного шифрования основаны на использовании операций в группах точек эллиптических кривых. Они обеспечивают меньшие длины параметров и, соответственно, более высокое быстродействие при сохранении заданного уровня стойкости. В частности, ныне действующий в Украине стандарт электронной цифровой подписи ДСТУ 4145-2002 основан на преобразованиях в группе точек эллиптических кривых, определенных над расширенными конечными полями $GF(2^m)$.

Естественным теоретическим и практическим обобщением эллиптических кривых являются гиперэллиптические кривые. Источником абелевой группы в этом случае выступает группа классов дивизоров (якобиан) гиперэллиптической кривой. Теория дивизоров гиперэллиптических кривых сегодня играет важную роль и при конструировании систем, основанных на спариваниях Вейля и Тейта, а также при решении задач дискретного логарифмирования на эллиптических кривых (метод спуска Вейля).

Основное преимущество при использовании гиперэллиптических кривых состоит в том, что размер основного поля, над которым определена кривая, уменьшается пропорционально роду кривой без потери стойкости, хотя сама формула группового сложения выглядит более громоздко.

Среди важных направлений совершенствования современных технологий применения гиперэллиптических кривых в криптографии можно выделить задачи, связанные с определением порядков якобианов кривых, которые и сегодня считаются вычислительно сложными [1, 2].

В этой работе предлагается метод вычисления элементов матрицы Хассе – Витта гиперэллиптической кривой, с использованием которой можно решить задачу определения порядка якобиана гиперэллиптической кривой [1, 2]. Этот метод требует для реализации существенно меньших вычислительных затрат по сравнению с известными. Он основан на использовании формулы бинома Ньютона и применим для кривых специального вида.

1 КРАТКАЯ ХАРАКТЕРИСТИКА МЕТОДОВ ОПРЕДЕЛЕНИЯ ПОРЯДКА ЯКОБИАНОВ ГЭК

Пусть F_q – конечное поле и пусть $\overline{F}_q$ – алгебраическое замыкание поля F_q. Гиперэллиптическая кривая C рода $g \geq 1$ над полем F_q представляет собой [3] набор решений $(x, y) \in F_q \times F_q$ уравнения

$$C: y^2 + h(x)y = f(x), \qquad (1)$$

где $h(x) \in F_q[x]$ – полином степени не более g, $f(x) \in \in F_q[x]$ – нормированный полином степени $2g+1$ и не существует решений (особых точек) $(x, y) \in \overline{F}_q \times \overline{F}_q$, которые бы одновременно удовлетворяли уравнению (1) и уравнениям $2y + h(x) = 0$ и $h'(x)y - f'(x) = 0$. Считается, что бесконечно удаленная точка P_∞ также принадлежит кривой.

Оператор Картера – Манина кривой, определенной над конечным полем, вместе с матрицей Хассе – Витта [4, 5] удобно использовать для изучения арифметических свойств якобиана кривой. Эта матрица используется как часть процедуры определения порядка якобиана, который является наиболее важным параметром для обеспечения стойкости криптосистемы на гиперэллиптических кривых [6].

Как известно, порядок якобиана гиперэллиптической кривой ограничен интервалом Хассе – Вейля.

$$\left\lceil (\sqrt{q-1})^{2g} \right\rceil \leq \#J(C/F_q) \leq \left\lfloor (\sqrt{q}+1)^{2g} \right\rfloor, \qquad (2)$$

где q – характеристика основного поля, над которым определена кривая, g – род кривой.

В нашей работе [2] приведен общий анализ существующих методов определения порядка якобианов ГЭК. Отмечено, что порядок якобиана напрямую зависит от количества точек кривой над основным полем и его расширениями q^2, ..., q^g [1]. В общем случае операция определения количества точек кривой является вычислительно сложной. Исследователями были выделены частные виды кривых (кривые Коблица, кривые Фурукавы), для которых разработаны эффективные методы определения порядка якобиана.

Основная идея большинства методов определения порядка заключается в использовании эндоморфизма Фробениуса.

Для $K = F_q$, $q = p^m$ это отображение вида

$$\phi_q = \phi_{p^m} : x \to x^{p^m}. \qquad (3)$$

Характеристическим полиномом эндоморфизма Фробениуса называется нормированный полином степени $2g$ с коэффициентами из кольца Z:

$$\chi_q(T) = T^{2g} + a_1 T^{2g-1} + \ldots + a_g T^g + \\ + a_{g-1} q T^{g-1} + \ldots + a_1 q^{g-1} T + q^g. \qquad (4)$$

При этом

$$\#J(C/F_q) = \chi_q(1). \qquad (5)$$

Следовательно, для определения порядка якобиана достаточно найти коэффициенты характеристического полинома эндоморфизма Фробениуса.

Другие методы определения порядка якобиана, например такие, как p-адические методы, использующие алгоритм Kedlaya, эффективны в полях малой характеристики.

Для кривых над большими простыми полями наиболее перспективно использование метода, использующего оператор Картера – Манина и матрицу Хассе – Витта [4, 5]. Применение этого метода дает возможность определить коэффициенты характеристического полинома эндоморфизма Фробениуса по модулю характеристики основного поля, что позволяет ограничить интервал их поиска значениями, кратными характеристике основного поля.

Матрица Хассе – Витта является обобщением инварианта Хассе эллиптической кривой и определяется следующим образом.

Определение [3]. Пусть γ_k – коэффициент полинома $\gamma(x) = f(x)^{(p-1)/2}$ при переменной степени k. Матрица Хассе – Витта – это матрица размера $g \times g$ с коэффициентами из поля F_q, заданная как

$$H = (\gamma_{ip-j})_{1 \leq i, j \leq g} = \begin{bmatrix} \gamma_{p-1} & \gamma_{p-2} & \cdots & \gamma_{p-g} \\ \gamma_{2p-1} & \gamma_{2p-2} & \cdots & \gamma_{2p-g} \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{gp-1} & \gamma_{gp-2} & \cdots & \gamma_{gp-g} \end{bmatrix}. \qquad (6)$$

Порядок вычисления оператора Картера – Манина $\chi_q(T) = (-1)^g T^g k(T) (\mathrm{mod} p)$ определяется следующей теоремой.

Теорема 1 [4]. Пусть C – ГЭК рода g, определенная над полем F_q и $q = p^m$. Пусть H – матрица Хассе – Витта кривой C и пусть $M = H \times H^{(p)} \times \ldots \times \times H^{(p^{m-1})}$, где $H^{(t)}$ – это матрица, состоящая из элементов H, возведенных в степень t. Пусть $k(T) = \det(T \times I_g - M)$ – характеристический полином матрицы M, тогда $\chi_q(T) = (-1)^g T^g k(T) (\mathrm{mod} p)$.

Основная сложность применения оператора Картера – Манина заключается в построении матрицы Хассе – Витта, а именно, в возведении полинома в большую степень

$$\gamma(x) = f(x)^{(p-1)/2}. \qquad (7)$$

Тривиальный способ вычисления необходимых коэффициентов состоит в полном возведении полинома в большую степень и выборе нужных коэффициентов их полученного результата. В этом случае для достаточно большого p, что является необходимым условием для построения стойкой криптосистемы, требуется

слишком много системных ресурсов и вычисления являются слишком медленным даже для кривых второго рода.

В работе [3] приводится оптимизированный метод определения элементов матрицы Хассе – Витта как термов линейных рекуррентных последовательностей, используя свойство формулы $\gamma(x) = f(x)^{(p-1)/2}$:

$$f(x)\cdot\gamma'(x) - \frac{p-1}{2}\cdot f(x)'\cdot\gamma(x) = 0.$$

Его сложность определяется как

$$O((R_M(g)g\sqrt{p} + g^3R_P(\sqrt{p}))(d\lg(p)^{\mu}),$$

где $R_M(s)$ – число операций кольца при умножении двух $s\times s$ матриц над кольцом; $R_P(s)$ – число операций кольца при умножении двух полиномов степени s над кольцом; μ – константа такая, что два B-битовых целых могут быть умножены за время B^{μ}.

Изложим теперь сущность предлагаемого метода.

2 МЕТОД ОПРЕДЕЛЕНИЯ ЭЛЕМЕНТОВ МАТРИЦЫ ХАССЕ – ВИТТА

За основу берется метод определения характеристического полинома эндоморфизма Фробениуса, основанный на теореме 1. Самой трудоемкой операцией в этом методе является возведение полинома $f(x)$ в степень $(p-1)/2$.

Заметим, однако, что для формирования матрицы Хассе – Витта необходимо лишь $g\times g$ коэффициентов полученного полинома $\gamma(x)$.

Как показано в [3], для значений $p>3$ уравнение любой гиперэллиптической кривой несложными преобразованиями можно привести к виду

$$y^2 = f(x). \qquad (8)$$

Будем рассматривать кривые специального вида, в которых многочлен $f(x)$ представлен в виде суммы двух одночленов, то есть

$$f(x) = x^{2g+1} + ax^k, \qquad (9)$$

где k может принимать любое целое значение из интервала $[2\ldots 2g]$.

При представлении (9) определению гиперэллиптической кривой (1) будут удовлетворять только кривые, для которых параметр k равен 0 или 1. Остальные кривые имеют особую точку (0, 0) и требуют более тщательного анализа. Возможность использования таких рациональных кривых рода 1 в криптографических приложениях рассматривалась в работе [7].

Обозначим $n = (p-1)/2$, тогда выражение (7) можно записать в виде

$$\gamma(x) = f(x)^n = (x^{2g+1} + ax^k)^n. \qquad (10)$$

В этом случае для формирования матрицы Хассе – Витта нет необходимости полностью возводить $f(x)$ в степень n, а можно лишь вычислить коэффициенты при необходимых членах с помощью формулы бинома Ньютона [8].

$$(a+b)^n = \sum_{m=0}^{n} C_n^m a^{n-m}b^m, \qquad (11)$$

где

$$C_n^m = \frac{n!}{m!(n-m)!} = \frac{n(n-1)\ldots(n-m+1)}{m!}. \qquad (12)$$

Для кривых (10) при $k = 0$ запишем формулу (11) в виде

$$\gamma(x) = (x^{2g+1}+a)^n = \sum_{m=0}^{n} C_n^m (x^{2g+1})^{n-m}\cdot a^m = \sum_{d_0=0}^{(2g+1)n} C_n^{\frac{(2g+1)n-d_0}{(2g+1)}} a^{\frac{(2g+1)n-d_0}{(2g+1)}} x^{d_0}. \qquad (13)$$

В (13) введена новая переменная $d_0 = (2g+1)(n-m)$ и, следовательно, показатели степени переменной d_0: $2g+1$ и

$$m = \frac{(2g+1)n-d_0}{(2g+1)} = n - \frac{d_0}{2g+1}. \qquad (14)$$

При $k = 1$ представим $\gamma(x)$ как

$$\gamma(x) = (x^{2g+1}+ax)^n = [x(x^{2g}+a)]^n.$$

$$\gamma(x) = (x^{2g+1}+ax)^n = \sum_{m=0}^{n} C_n^m (x^{2g})^{n-m}\cdot a^m\cdot x^n = \sum_{d_1=n}^{(2g+1)n} C_n^{\frac{(2g+1)n-d_1}{2g}} a^{\frac{(2g+1)n-d_1}{2g}} x^d,$$

где введена новая переменная $d_1 = 2g(n-m)+n = (2g+1)n-2gm$ и, следовательно, для показателей степени переменной многочлена $\gamma(x)$ справедливо соотношение $d_1 - \frac{p-1}{1}$: $2g$ и для показателя степени m справедливо соотношение

$$m = \frac{(2g+1)n-d_1}{2g} = n + \frac{n-d_1}{2g}. \qquad (15)$$

Тогда в первом случае при $k = 0$ для значений показателя степени d_0, принимающем значения $d_0 \in \{p-1, \ldots, p-g, 2p-1, \ldots, 2p-g, \ldots, gp-1, \ldots, gp-g\}$ имеем

$$m_1 = \frac{p-1}{2} - \frac{p-1}{2g+1},\quad m_2 = \frac{p-1}{2} - \frac{p-2}{2g+1},$$

. . . . . .

$$m_{g(p-1)} = \frac{p-1}{2} - \frac{g(p-1)}{2g+1}.$$

Из этих результатов нас устраивают только те, которые дают целые значения.

Для случая $k = 1$ по аналогии с предыдущим получаем

$$m_2 = \frac{p-1}{2} + \frac{\frac{p-1}{2} - (p-1)}{2g} = \frac{p-1}{2} - \frac{p-1}{4g},$$

$$m_2 = \frac{p-1}{2} + \frac{\frac{p-1}{2} - (p-2)}{2g} = \frac{p-1}{2} + \frac{p-1-2(p-2)}{4g},$$

$$m_{p-g} = \frac{p-1}{2} + \frac{\frac{p-1}{2} - (p-g)}{2g} = \frac{p-1}{2} + \frac{p-1-2(p-g)}{4g},$$

. . . . . .

$$m_{g(p-1)} = \frac{p-1}{2} + \frac{\frac{p-1}{2} - g(p-1)}{2g} = \frac{p-1}{2} + \frac{p-1-2g(p-1)}{4g}.$$

И здесь, очевидно, берутся только целые значения.

Далее можно уже можно определять интересующие нас коэффициенты многочлена $\gamma(x)$, для чего необходимо вычислить соответствующие коэффициенты бинома Ньютона C_n^m. При этом соответствующий элемент матрицы Хассе – Витта определяется по формуле:

$$\gamma_i = C_n^{m_i} \cdot a^{m_i} (\mathrm{mod} p). \qquad (16)$$

Дальнейшие вычисления состоят в применении оператора Картера – Манина к полученной матрице.

3 ЭФФЕКТИВНЫЙ МЕТОД ВЫЧИСЛЕНИЯ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ

Основное время вычислений в предлагаемом авторами методе занимают вычисления биномиальных коэффициентов, а именно операция вычисления факториала длинного числа. В работе [9] приводится эффективный метод вычисления факториала. Его суть состоит в следующем.

Факториал любого неотрицательного числа n может быть эффективно вычислен по формуле

$$n! = 2^{n_2 + n_3 + \ldots + n^{k-1} + n^k} \times n_k! \times n_{k-1}!!! \times \times \underbrace{[n_{k-1}!!! \times \ldots \times n_{k-2}]}_{n_{k-2}!!!} \times \underbrace{[n_{k-2}!!! \times \ldots \times n_{k-3}]}_{n_{k-3}!!!} \times \ldots \times \underbrace{[n_2!!! \times \ldots \times n_1]}_{n_1!!!}, \qquad (17)$$

где $n_1 = n$, $n_i = \left\lfloor \frac{n_{i-1}}{2} \right\rfloor$, $n_k = 1$, символом $n!!!$ обозначено произведение всех нечетных чисел в интервале $[1 \ldots n]$, а обозначение $[a_j \times \ldots \times a_k]$ соответствует произведению всех нечетных чисел, лежащих в интервале от a_j до a_k.

Использование этой формулы позволило авторам усовершенствовать формулу для вычисления биномиальных коэффициентов.

Представим формулу (17) в виде

$$n! = 2^s \cdot t,$$

где

$$s = n_2 + n_3 + \ldots + n^{k-1} + n^k,$$

$$t = n_k! \times n_{k-1}!!! \times \underbrace{[n_{k-1}!!! \times \ldots \times n_{k-2}]}_{n_{k-2}!!!} \times \underbrace{[n_{k-2}!!! \times \ldots \times n_{k-3}]}_{n_{k-3}!!!} \times \ldots \times \underbrace{[n_2!!! \times \ldots \times n_1]}_{n_1!!!}.$$

Тогда формулу для вычисления биномиальных коэффициентов можно переписать в виде

$$C_n^m = \frac{n!}{m!(n-m)!} = \frac{2^{s_n} \cdot t_n}{(2^{s_m} \cdot t_m) \cdot (2^{s_{(n-m)}} \cdot t_{(n-m)})} = 2^{s_n - (s_m + s_{(n-m)})} \cdot \frac{t_n}{t_m \cdot t_{(n-m)}}. \qquad (18)$$

В табл. 1 представлено сравнение скорости вычисления биномиальных коэффициентов в специализированном математическом пакете с помощью стандартной и усовершенствованной процедур.

Таким образом, экспериментально доказана эффективность усовершенствованной формулы вычисления биномиальных коэффициентов.

Таблица 1 – Сравнение скорости процедур вычисления биномиальных коэффициентов

Длина p, бит	p	$n = (p-1)/2$	m	Время mbinomial (n, m, p) (предложение авторов), с	Время binomial (n, m) mod p (стандартная процедура), с
10	997	498	249	меньше 0,1	меньше 0,1
14	9973	4986	2493	меньше 0,1	0,2
17	99991	49995	24997	0,1	11,6
20	999979	499989	249994	1,4	1132,4

4 ВЫЧИСЛИТЕЛЬНЫЙ ПРИМЕР ДЛЯ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ ВТОРОГО РОДА

Определим порядок якобиана гиперэллиптической кривой второго рода

$$y^2 = x^5 + 3 (\mathrm{mod}\ 991). \qquad (19)$$

Согласно [6]

$$\chi_q(T) = T^4 - s_1 \cdot T^3 + s_2 \cdot T^2 - s_1 \cdot q \cdot T + q^2, \quad (20)$$

где

$$|s_1| \le 4 \cdot \sqrt{q}, \ \ |s_2| \le 6 \cdot q,$$
$$\left|2\sqrt{q}|s_1| - 2 \cdot q\right| \le s_2 \le \left\lfloor s_1^2/4 + 2 \cdot q \right\rfloor.$$

Поскольку использование оператора Картера – Манина позволяет определить коэффициенты характеристического полинома только по модулю характеристики основного поля, ограничения на s_1 и s_2 помогут значительно сузить интервал поиска их истинных значений.

Матрица Хассе – Витта в нашем случае имеет вид:

$$\begin{bmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{bmatrix} = \begin{bmatrix} c_{990} & c_{989} \\ c_{1981} & c_{1980} \end{bmatrix}. \qquad (21)$$

Согласно предложенному методу, определим элементы матрицы путем вычисления коэффициентов бинома Ньютона при соответствующих степенях переменной x полинома

$$\gamma(x) = (x^5 + 3)^{(991-1)/2}. \qquad (22)$$

Для этого сначала надо определить, какие коэффициенты бинома Ньютона C_n^m надо вычислить, а именно необходимо определить значения переменной m для всех элементов матрицы (22), поскольку n всегда равно $(p-1)/2$ и для нашего примера равно 495. Имеем:

$$m_1 = 495 - \frac{990}{5} = 297, \ \ m_2 = 495 - \frac{989}{5} = \frac{1486}{5},$$

$$m_3 = 495 - \frac{1981}{5} = \frac{494}{5}, \ \ m_4 = 495 - \frac{1980}{5} = 99.$$

Получаем два целых значения $m_1 = 297$ и $m_4 = 99$.

Рассчитаем теперь соответствующие элементы матрицы Хассе – Витта из полинома (23) по формуле (16). Используем усовершенствованную авторами формулу расчета биномиальных коэффициентов.

Следовательно,

```
a:=3:
mbinomial(s, m1, p)*a^m1 mod p;
mbinomial(s, m4, p)*a^m4 mod p;
                    286
                    676
```

$$c_{p-1} = c_{990} = C_{495}^{297} \cdot 3^{297} (\mathrm{mod}\ 991) = 286,$$

$$c_{2p-2} = c_{1980} = C_{495}^{99} \cdot 3^{99} (\mathrm{mod}\ 991) = 676,$$

и матрица Хассе – Витта имеет вид

$$\begin{bmatrix} 286 & 0 \\ 0 & 676 \end{bmatrix}.$$

Далее с помощью оператора Картера – Манина определим характеристический полином эндоморфизма Фробениуса по модулю характеристики основного поля:

$$\chi_{991}(T) = T^4 + 29 \cdot T^3 + 91 \cdot T^2 (\mathrm{mod}\ 991).$$

Пользуясь формулой (20), восстановим полные значения коэффициентов характеристического полинома эндоморфизма Фробениуса:

$$\chi_{991}(T) = T^4 + 29 \cdot T^3 + (91 + k \cdot 991) \cdot T^2 + 29 \cdot 991 \cdot T + 991^2.$$

Как видно, в полученной формуле не вполне определенным осталось только значение коэффициента $s_2 = (91 + k \cdot 991)$. Определим границы для s_2, пользуясь формулой (21).

$$b1 = \left|2\sqrt{q}|s_1| - 2 \cdot q\right| = -157 \ \text{ и}$$

$$b2 = \left\lfloor s_1^2/4 + 2 \cdot q \right\rfloor = 2192.$$

Отсюда возможные значения s_2 и соответствующие этим значениям порядки якобиана кривой $\#J$ получаются равными

$$k = 0, \ \ s_2 = 91, \ \ \#J = 1010941,$$

$$k = 1, \ \ s_2 = 1082, \ \ \#J = 1011932,$$

$$k = 2, \ \ s_2 = 2073, \ \ \#J = 1012923.$$

Окончательный выбор из полученных альтернатив путем умножения произвольно выбранного дивизора $<x - 402, 661>$ на предполагаемые порядки якобиана кривой показал, что правильным в данном случае является значение $\#J = 1010941$.

ЗАКЛЮЧЕНИЕ

Представленный в работе метод вычисления элементов матрицы Хассе – Витта гиперэллиптических кривых, позволяет решить задачу определения якобиана гиперэллиптических кривых. Метод требует для реализации существенно меньших вычислительных затрат по сравнению с известными. Дальнейшие исследования в этом направлении заключаются в совершенствовании формул вычисления биномиальных коэффициентов по модулю большого простого числа, а также в исследовании свойств рациональных гиперэллиптических кривых, соответствующих значениям $k > 1$ в формуле (9).

ПЕРЕЧЕНЬ ССЫЛОК

1. *Colm Ó hÉigeartaigh.* A Comparison of Point Counting methods for Hyperelliptic Curves over Prime Fields and Fields of Characteristic 2 [Электронный ресурс] / Colm Ó hÉigeartaigh: Cryptology ePrint Archive: Report 2004/241, 2004 . – P. 1–12. – Режим доступа: http://eprint.iacr.org/ 2004/241.pdf.
2. *Долгов В. И.* Методы определения порядка якобианов гиперэллиптических кривых / Долгов В. И., Неласая А. В. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – ХНУРЭ, 2007. – Том 6, № 3. – С. 366–369.
3. *Menezes A.* An Elementary Introduction to Hyperelliptic Curves [Электронный ре-сурс] : Published as Technical Report CORR 96–19 Department of C&O University of Waterloo: Ontario: Canada / Menezes A., Wu Y., Zuccherato R. – 1996. – P. 1–35. – Режим доступа: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps.
4. *Манин Ю. И.* О матрице Хассе–Витта алгебраической кривой / Манин Ю. И. // Известия АН СССР. Серия: Математика. – 1961. – Том 25, выпуск 1. – С. 153–172.
5. *Bostan A.* Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator / Bostan A., Gaudry P., Schost É. // Proceedings of Fq7, Lecture Notes in Comput. Sci. – Berlin : Springer-Verlag, 2004. – Vol. 2948. – P. 40–58.
6. *Долгов В. И.* Стойкость криптографических алгоритмов на гиперэллиптических кривых / Долгов В. И., Неласая А. В. // Прикладная радиоэлектроника : тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2006. – Том 5, № 1. – С. 30–34.
7. *Чевардин В. Е.* Метод аутентификации данных на основе ключевого хеширования с использованием арифметики эллиптических кривых : дис. канд. техн. наук : 05.13.21 / Чевардин В. Е. – Полтава, 2006. – 202 с.
8. *Бронштейн И. Н.* Справочник по математике / Бронштейн И. Н. Семендяев К. А. – М. : Наука, 1967. – 608 с.
9. *Ладиков А. В.* Улучшенный алгоритм вычисления факториала / Ладиков А. В. // Математические заметки. – 2008. – Т. 83, № 6. – С. 857–863.

Надійшла 16.09.2008

В статті пропонується метод обчислення елементів матриці Хассе – Вітта гіпереліптичних кривих спеціального виду, що базується на застосуванні формули бінома Ньютона.

The method of calculation of Hasse – Witt matrix for special hyperelliptic curves is proposed. This method is based on using binomial theorem.

УДК 004.93.1

В. М. Заяць

ДОЦІЛЬНІСТЬ ВСТАНОВЛЕННЯ ПРИОРІТЕТУ ПЕРВИННИХ ОЗНАК ПРИ ПОБУДОВІ СИСТЕМ РОЗПІЗНАВАННЯ ТА ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ І ПРОЦЕСІВ НА ОСНОВІ ДЕТЕРМІНОВАНИХ ТА ІМОВІРНІСНИХ МЕТОДІВ

Запропоновано підхід до встановлення пріоритетну первинних ознак при побудованої системи розпізнавання користувачів комп'ютера на основі її опису у вигляді дискретної моделі, що рекурентно зв'язує часові затримки при введені інформації з клавіатури комп'ютера у дискретні відліки часу. Доцільність розроблених підходів проілюстровано при реалізації автоматизованої процедуру ідентифікації користувачів комп'ютера на основі детермінованого та імовірнісного методів.

ПОСТАНОВКА ЗАДАЧІ

При створені нових реальних пристроїв, дослідженні невивчених фізичних явищ чи процесів, побудові систем розпізнавання та ідентифікації, що мають бажані характеристики інформаційного сигналу або невідомі характеристики, які підлягають вивченню, доцільно провести комп'ютерне моделювання та аналіз, створивши адекватні математичної моделі об'єкта, що розробляється чи вивчається. Такий підхід вимагає значно менших часових і технічних засобів порівняно з фізичним експериментом, особливо на попередній стадії розробки, за відсутності достовірної апріорної інформації

Останнім часом в нелінійній динаміці широке застосування знаходять дискретні моделі систем [1–6] для яких дискретність закладена в природі самого