МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра компьютерной алгебры и теории чисел

Криптосистемы на гиперэллиптических кривых

Автореферат магистерской работы

студента 2 курса 227 группы

направление 02.04.01 — Математика и компьютерные науки

механико-математического факультета

Магомедшерифова Бекера Гюлеметовича

Научный руководитель
доцент, к.ф.-м.н., доцент В. В. Кривобок

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент А.М. Водолазов

Саратов 2019

Содержание

ВВЕДЕНИЕ

Вместе с неограниченными возможностями компьютерные технологии приносят новые проблемы, главной из них стала проблема защиты информации. Поэтому параллельно с усовершенствованием технологий стали быстро развиваться методы защиты информации. Одновременно с улучшениями систем защиты совершенствуются и алгоритмы взлома. А это в свою очередь требует немедленного усовершенствования и повышения надежности защиты персональных данных. Для этого был создан раздел науки под название криптология, чьим основным направлением является криптография.

Криптография в основном базируется на методах предлагаемых алгебраической геометрией, абстрактной алгеброй, теорией чисел. Один из таких перспективных методов криптографии основан на теории эллиптических кривых, а эллиптические кривые в свою очередь являются важным частым случаем гиперэллиптических кривых.

Цель данной работы - изучить гиперэллиптические кривые и как важный частный случай эллиптические кривые, их особенности, разобрать несколько криптосистем.

В данной работе представлено четыре раздела. В первом собраны необходимые определения и теоремы из теории эллиптических кривых. Во втором разделе дается оценка количества точек эллиптической кривой, описываются алгоритмы подсчета точек. В третьем рассмотрены основные криптосистемы на эллиптических кривых. В четвертом разделе рассмотрены гиперэллиптические кривые, особенности построения криптосистем на них.. В приложении представлен код реализации сложения точек эллиптической кривой, умножения на число.

1 Криптосистемы на гиперэллиптических кривых

1.1 Гиперэллиптические кривые

1.1.1 Функции на кривых

Гиперэллиптической кривой C над полем K называется аффинная кривая заданная уравнением

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

и не имеющая особых точек на аффинной плоскости над $\overline{K}$, где h, f - полиномы с коэффициентами из K, $deg(f) = 2g + 1, deg(h) \leq g$.

Натуральное число число g называется *родом кривой*. Эллиптическую кривую можно рассматривать как гиперэллиптическую кривую рода 1.

Теорема 1. Если характеристика поля равна 2, то $h \neq 0$. Если характеристика поля отлична от 2, то с помощью обратимой аффинной замены переменных можно задать гиперэллиптическую кривую уравнением

$$y^2 = f(x) \qquad (1')$$

Над полем комплексных чисел гиперэллиптическая кривая изоморфна замкнутой поверхности без краев (у которой есть наружная и внутренняя стороны) с g «отверстиями» аналогично тому, как тор является замкнутой поверхностью без краев с одним «отверстием»

Гиперэллиптическая кривая во многом аналогична эллиптической кривой. Пересечение соответствующей проективной гиперэллиптической кривой с бесконечно удаленной прямой $Z = 0$ задается условием $X = 0$. Таким образом, гиперэллиптическая кривая имеет единственную бесконечно удаленную точку $P_\infty = (0, 1, 0)$. Если $g > 1$, то точка P_∞ является особой.

Если род g гиперэллиптической кривой отличен от 1 (то есть $deg(f) \geq 5$), то бесконечно удаленная точка всегда является особой. Однако это не накладывает ограничений на использование такой кривой, поскольку на практике можно рассматривать только аффинную часть кривой.

В общем случае прямая пересекается с гиперэллиптической кривой над алгебраически замкнутым полем более чем в трех точках. Например, прямая $y = 0$ пересекается с кривой (1') в $2g+1$ точках (это следует из того, что правая часть уравнения кривой имеет $2g + 1$ корень над $\overline{K}$). Поэтому арифметика на гиперэллиптической кривой задается с помощью функций на кривой.

Любой полином $q(x, y) \in \overline{K}[C]$ можно записать в виде

$$q(x, y) = a(x) - b(x)y \qquad (2)$$

где $a, b \in \overline{K}[x]$, поскольку на кривой C полином y^2 рекурсивно заменяется полиномом $f - hy$.

Любая функция из поля функций с точностью до константы задается списком нулей и полюсов, то есть дивизором.

Функция $q(x, y) \in K(C)$ определена в аффинной точке $(x_p, y_p) \in C(K)$, если ее знаменатель отличен от 0. Значение функции вычисляется как $q(x_p, y_p)$.

Теорема 2. Пусть $q(x, y) \in K(C)$, $P \in C(K)$ - аффинная точка такая, что $2y_p + h(x_p) \neq 0$ и $q(x_p, y_p) = 0$. Тогда существует представление $q(x, y) = (x - x_p)^m r(x, y)$ и $r(x_p, y_p) \notin \{0, \infty\}$.

Теорема 3. Пусть $P \in C(K)$ - аффинная точка такая, что $P = P'$. Тогда существует представление функции $x - x_p = (y - y_p)^2 r(x, y)$, где функция $r \in K(C)$ не имеет ни нулей, ни полюсов в точке P.

1.1.2 Якобиан

Дивизор на гиперэллиптической кривой $C(K)$ представляет собой формальную сумму конечного числа слагаемых $D = \sum_{P_i \in C(K)} m_i P_i$.

Теорема 4. Число нулей полинома $q \in \overline{K}[C]$ равно числу полюсов с учетом кратности.

Поскольку рациональная функция из $\overline{K}(C)$ является отношением двух полиномов, число ее нулей равно числу полюсов с учетом кратности. Следовательно, дивизор функции имеет нулевую степень.

Функции на кривой образуют группу по умножению, поэтому и их гомоморфные образы - дивизоры функций - образуют группу главных дивизоров и имеют степень 0. Следовательно, определен и существует *якобиан* $J(C)$ *гиперэллиптической кривой* C - фактор группа дивизоров степени 0 по подгруппе главных дивизоров. Элементы якобиана определены с точностью до главного дивизора, так же как классы идеалов квадратичных порядков определены с точностью до главного идеала. Поэтому группа классов квадратичного порядка аналогична якобиану гиперэллиптической кривой.

Теорема 5. Каждый дивизор $D \in J(C)$ может быть представлен в виде

$$D = \sum_{i=1}^{m}(P_i) - m(P_\infty) \qquad (4)$$

где точки P_i не обязательно различны, причем в носитель дивизора входит не более чем одна из точек P, P'.

Сложение двух приведенных дивизоров $D_1 = div(a_1, b_1)$ и $D_2 = div(a_2, b_2)$ представленных полиномами, выполняется в два этапа: сначала вычисляется полуприведенный дивизор, затем выполняется его приведение.

Обозначим $J(m)$ якобиан порядка m гиперэллиптической кривой $C(K)$, где поле K конечно. На кривой $C(K)$ можно определить спаривание Вейля e_m, устанавливающее вложение якобиана в мультипликативную группу расширения L поля K, порядок которой делит порядок якобиана.

Можно записать $J[m] = Div^0[m]/Pr(C(L))$, где $Div^0[m]$ - группа дивизоров степени 0 таких, что для любого $D \in Div^0[m]$ дивизор mD является главным. Пусть $\{\mu_m\}$ -группа корней степени m из 1 в L^*. Если $D_1, D_2 \in Div^0[m]$ - дивизоры с не пересекающимися носителями, $f_{D_1}, F_{D_2} \in L(C)$ - функции с дивизорами $div(f_{D_1}) = mD_1, div(f_{D_2}) = mD_2$, то можно определить функцию

$$w_m : \ Div^0[m] \oplus Div^0[m] \to \{\mu_m\},$$
$$w_m(D_1, D_2) = \frac{f_{D_1}(D_2)}{f_{D_2}(D_1)}.$$

С помощью функции w_m определяется спаривание Вейля

$$e_m : J[m] \oplus J[m] \to \{\mu_m\}$$

следующим образом. Пусть $A, B \in J[m]$ и носители дивизоров $D_1, D_2 \in Div^0[m]$ не пересекаются, при этом $D_1 \in A, D_2 \in B$. Тогда

$$e_m(A, B) = w_m(D_1, D_2).$$

Спаривание Вейля на гиперэллиптических кривых является важным инструментом при анализе криптографических алгоритмов с открытым ключом.

1.2 Криптосистемы на гиперэллиптических кривых

Основная трудность, возникающая при разработке криптосистем на гиперэллиптической кривой, - это выбор кривой $C(K)$, где $K = \mathbb{F}_{p^n}$ такой, что задача логарифмирования в якобиане $J(C)$ является сложной. Порядок якобиана должен иметь большой простой делитель $r \neq char(K)$; $char(K)^k \neq 1(mod\ r)$ для небольших значений k; род кривой должен быть небольшим. Для выбора кривой необходимо решить задачу порядка ее якобиана.

Гиперэллиптическая кривая C/K может рассматриваться над различными расширениями L исходного поля K. При этом могут меняться число точек кривой и порядок якобиана. Для того чтобы уточнить, о каком именно поле идет речь, якобиан будем обозначать $J(C(L))$ или, короче, $J(L)$.

Пусть кривая $C/\mathbb{F}_p$ рода g задана уравнением

$$v^2 + h(u)v = f(u). \qquad (1)$$

Рассмотрим метод вычисления порядка якобиана кривой над расширенным конечным полем с помощью последовательности $N_1,\ N_2, \ldots$ (где $N_k = \#J(\mathbb{F}_{p^k})$) - число элементов якобиана), заключающийся в подсчете $\mathbb{F}_{p^k}$-аффинных точек кривой (1) для $k = 1,\ 2, \ldots, g$.

Пусть $M_k = \#C(\mathbb{F}_{p^k}) - p^k$, где $C(\mathbb{F}_{p^k})$ - число аффинных точек (u, v) кривой. Если $p > 2$, то можно считать в (1) $h = 0$, тогда M_k является суммой квадратичных характеров полинома $f(u)$ в поле $\mathbb{F}_{p^k}$.

По аналогии с эллиптическими кривыми можно ввести дзета-функцию $Z(T)$ - полином степени $2g$ с целыми коэффициентами:

$$Z(T) = T^{2g} + a_1 T^{2g-1} + \ldots + a_{g-1} T^{g+1} + a_g T^g + p a_{g-1} T^{g-1} + p^2 a_{g-2} T^{g-2} + \\ + \ldots + p^{g-1} a_1 T + p^g = \prod_{j=1}^{g} (T - \alpha_j)(T - \overline{\alpha}_j)$$

где $a_1, \ldots, a_g \in \mathbb{Z}$ и $\alpha_j \overline{\alpha_j} = p$

Пусть

$$\widetilde{Z}\,(T) = T^{2g} Z\left(\tfrac{1}{T}\right) = 1 + a_1 T + a_2 T^2 + \ldots + p^g T^{2g},$$

тогда коэффициенты полинома $Z(T)$ связаны с числами M_k соотношениями

$$\ln \widetilde{Z}\,(T) = \sum_{k=1}^{\infty} \tfrac{M_k}{k} T^k \qquad (2)$$

Так как $\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$, то, подставляя в (2) $x = a_1 T + \\ + a_2 T^2 + \ldots + p^g T^{2g}$ и приравнивая коэффициенты при одинаковых степенях T, получаем выражения для коэффициентов полинома, $Z(T)$. Заметим, что для этого достаточно первых g величин $M_1, \ldots, M_g$. Отсюда находим

$$N_n = \prod_{j=1}^{g} |1 - \alpha_j^n|^2,$$

где $|\ldots|$ - модуль комплексного числа. Нетрудно видеть, что $N_1 = Z(1)$.

Представим симметрическую функцию $s_j = t_1^j + \ldots + t_m^j$ в виде полинома от элементарных симметрических функций:

$$s_j = \begin{cases} s_{j-1}\sigma_1 - s_{j-2}\sigma_2 + \ldots + (-1)^{j-1} j \sigma_j, \text{при} j \le m, \\ s_{j-1}\sigma_1 - s_{j-2}\sigma_2 + \ldots + (-1)^{m-1} s_{j-m}\sigma_m, \text{при} j < m. \end{cases}$$

Применительно к задаче вычисления якобиана эта формула означает, что для каждого n число N_n элементов якобиана можно выразить как полином над кольцом $\mathbb{Z}$ от коэффициентов полинома $Z(T)$.

Тогда для любого $n = 1, 2, \ldots$ справедливо

$$N_n = \sum_{k=0}^{g-1} (-1)^k (1 + p^{(g-k)n}) S_k^{(n)} + (-1)^g S_g^{(n)} \qquad (3)$$

где $S_0^{(n)} = 1$,

$$S_k^{(n)} = \frac{1}{k} \left((-1)^{k-1} S_1^{(kn)} + \sum_{j=1}^{k-1} (-1)^{k-j-1} S_j^{(n)} S_1^{((k-j)n)} \right)$$

при $k \geq 2$,

$$S_1^{(j)} = \begin{cases} S_1^{j-1} S_1^{(1)} - S_1^{(j-2)} S_2^{(1)} + \ldots + (-1)^{(j-1)} j S_j^{(1)}, \text{при} j \leq 2g, \\ \sum_{i=1}^{2g} (-1)^{(i-1)} S_1^{(j-1)} S_1^{(1)}, \text{при} j > 2g. \end{cases}$$

Кроме того, $S_i^{(1)} = (-1)^{(i)} a_i$ при $i \leq g$; $S_i^{(1)} = p^{1-g} S_{2g-1}^{(1)}$ при $g < i \leq 2g$.

Например, порядок якобиана кривой рода 2 над кубическим расширением основного поля задается формулой:

$$N_3 = 3p^4 a_1 + p^3(a_1^3 - 3a_1 a_2) + 3p^2(2a_1^2 - a_2) + 3p(a_1 - a_1^2 a_2) + 1 + a_1^3 - 3a_1 a_2 + a_2^3.$$

Для обеспечения стойкости криптосистемы необходимо, чтобы порядок $N_n = \#J(K)$ якобиана $J(K)$ был простым числом либо имел большой простой делитель r и чтобы спаривание Вейля не позволяло легко вычислить логарифм. В этом случае стойкость равна $O(\sqrt{r})$.

Само N_n редко оказывается простым, так как $J(\mathbb{F}_{p^d})$ есть подгруппа группы $J(K)$ для любого делителя d числа n, и, значит, $N_d | N_n$. Поэтому целесообразно использовать только простые расширения поля $\mathbb{F}_p$ и только кривые с неприводимым над полем рациональных чисел полиномом $Z(T)$.

Для некоторых гиперэллиптических кривых, например, $y^2 = x^5 + B$ с $p \neq \pm 1 \ (mod\ 10)$, число точек найти легко: $M_1 = M_2 = 0$. Однако такие кривые не позволяют обеспечить стойкость по отношению к логарифмированию на основе спаривания Вейля.

Для гиперэллиптической кривой справедлив аналог теоремы Хассе:

$$|p^k + 1 - \#C(\mathbb{F}_{p^k})| \leq 2\sqrt{p^k}$$

для всех $k = 1, 2, \ldots$. Поэтому, если поле K велико, то для расчета значений $M_1, \ldots, M_g$ можно воспользоваться аналогом алгоритма Чуфа для гиперэллиптических кривых.

На практике желательно использовать гиперэллиптические кривые небольшого рода, так как, раскладывая на множители пары полиномов, составляющих дивизор, можно снизить, стойкость криптоалгоритма.

В якобиане гиперэллиптической кривой, как и на эллиптических кривых, может существовать комплексное умножение на целое алгебраическое число θ. Это позволяет ускорить умножение дивизора на целое число z, если представить z в виде полинома от θ. Если кривая $C \setminus \mathbb{F}_p$ рассматривается над полем из p^n элементов, то на ней действует отображение Фробениуса: $\phi : (u, v) \to (u^p, v^p)$, соответствующее умножению элемента якобиана на комплексное число.

Криптографические протоколы на гиперэллиптических кривых аналогичны протоколам на эллиптических кривых. Общая несекретная информация: кривая $C(K)$ (то есть поле K и пара полиномов f, h) и дивизор D, образующий группу большого простого r. В основу криптографических протоколов положена задача Диффи-Хелмана: для якобиана $J(K)$, дивизора D и дивизоров tD, sD найти дивизор tsD.

В общем случае строение якобиана как абелевой группы может отличаться от строения группы точек эллиптической кривой. Например, группа точек

кривой над конечным полем циклична или является прямой суммой двух циклических групп, большой и малой, при этом порядок большой группы делится на порядок малой группы. Якобиан может иметь более сложное строение. Это обстоятельство следует учитывать при разработке протоколов.

Так, представляются возможными атаки, основанные на посылке "фальшивых"дивизоров, не являющихся элементами якобиана данной кривой. Для защиты от такой атаки желательно ввести проверку того, что полученный дивизор $div(a(u), b(u))$ является приведенным и соответствует кривой $C(K)$, то есть проверять делимость $a|(b^2 + hb - f)$ в кольце $K[u]$.

ЗАКЛЮЧЕНИЕ

В ходе данной работы были изложены основные моменты теории гиперэллиптической и как важного частного случая эллиптической криптографии.

Подводя итог, следует отметить преимущества и недостатки гиперэллиптической криптографии.

Плюсами являются:высокая стойкость к взлому, гораздо меньшая длина ключа по сравнению с классической асимметричной криптографией; скорость работы алгоритмов гораздо выше, чем у классических; также из-за маленькой длины ключа и высокой скорости работы, алгоритмы могут использоваться в устройствах с ограниченными вычислительными ресурсами.

Минусами являются то, что не всякая гиперэллиптическая кривая подходит для построения криптосистемы; также то, что для переноса криптосистем на гиперэллиптические кривые требуется серьезная теоретическая база.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Коблиц, Н. Введение в эллиптические кривые и модулярные формы. – М.: Мир, 1988. – 320 с.

2 Коблиц, Н. Курс теории чисел и криптографии. – М.: ТВП, 2001. – 254 с.

3 Ростовцев, А. Г., Маховенко, Е. Б.Теоретическая криптография. – СПб.: Профессионал, 2005. – 480 с.

4 Ленг, С. Эллиптические функции. – М.: Наука, 1984. – 312 с.

5 Кнэпп, Э. Эллиптические кривые. – М.: Факториал, 2004. – 488 с.

6 Ван дер Варден, Б. Л. Алгебра. – М.: Наука, 1979. – 623 с.

7 Вейль, А. Основы теории чисел. – М.: Мир, 1972. – 408 с.

8 Маховенко, Е. Б. Теоретико-числовые методы в криптографии. – М.: Гелиос АРВ, 2006. – 320 с.

9 Лидл, Р., Нидеррайтер, Х. Конечные поля. – М.: Мир, 1988. – 390 с.

10 Ростовцев, А. Г. Алгебраические основы криптографии. – СПб.: Мир и Семья, 2000. – 354 с.

11 Прасолов, В. В., Соловьев, Ю. П. Эллиптические кривые и алгебраические уравнения. – СПб.: Факториал, 1997. – 288 с.

12 Ростовцев, А.Г., Маховенко, Е.Б. Введение в криптографию с открытым ключом. – СПб.: Мир и Семья, 2001. – 336 с.

13 Нечаев, В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999. – 109 с.

14 Мао, В. Современная криптография теория и практика. – М.: Вильямс, 2005. – 768 с.

15 Ященко, В.В. Введение в криптографию. – М.: МЦНМО, 1999. – 272 с.

16 Болотов, А.А., Гашков, С.Б., Фролов, А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.

17 Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2006. – 335 с.

18 Смарт, Н. Криптография. – М.: Техносфера, 2005. – 528 с.

19 Жельников, В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 335 с.

20 Шнайер, Б. Прикладная криптография. – М.: Диалектика, 2003. – 610 с.