УДК 512.6

Буринский М.И., студент

4 курс, направления «Информационная безопасность»

Балтийский Федеральный Университет им. И. Канта

Россия, г. Калининград

Аширов А.М., студент

4 курс, направления «Инфокоммуникационные сети и системы связи»

Балтийский Федеральный Университет им. И. Канта

Россия, г. Калининград

Джураева Д.Х., студент

4 курс, направления «Информационная безопасность»

Балтийский Федеральный Университет им. И. Канта

Россия, г. Калининград

Велиев Р.И., студент

4 курс, направления «Информационная безопасность»

Балтийский Федеральный Университет им. И. Канта

Россия, г. Калининград

ПОВЫШЕНИЕ ЗНАНИЙ СОТРУДНИКОВ РАЗРАБОТКИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ: «ЯВНЫЕ ВЫЧИСЛЕНИЯ В ЯКОБИАНЕ НЕГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ РОДА 3 С БОЛЬШИМ ЧИСЛОМ ТОЧЕК.»

Аннотация: *Кривые рода 1, 2, и 3 пригодны для использования в криптографии и теории кодирования, например, протокол Д-Х на эл. кривых. В своей работе я буду рассматривать НЕгиперэллиптические кривые рода 3 – про такие кривые мало что известно, малое кол-во алгоритмов используют такие кривые, а если и используют, то, скорее всего, кривые Пикара. Также* *хотелось бы отметить, что для криптографических приложений важно, чтобы арифметика в якобиане кривой была эффективной, иначе создание такой криптосистемы не имеет смысла. Ну и такой полуоткрытый вопрос – а что нам вообще известно о негиперэллиптических кривых.*

Ключевые слова: *Негиперэллиптические кривые, кривые Пикара, криптография, алгоритм Мамфорда, случай гиперизгиба, девизор, граница Хассе-Вейля-Серра, защита информации, ранг матрицы.*

Annotation: *Curves of genus 1, 2, and 3 are suitable for use in cryptography and coding theory, for example, the D-X protocol on electronic curves. In my work, I will consider non–hyperelliptic curves of genus 3 - little is known about such curves, a small number of algorithms use such curves, and if they do, then most likely Picard curves. I would also like to note that for cryptographic applications it is important that the arithmetic in the Jacobian curve is effective, otherwise the creation of such a cryptosystem does not make sense. Well, such a semi–open question - what do we know about non-hyperelliptic curves at all.*

Key words: *Non-hyperelliptic curves, Picard curves, cryptography, Mumford algorithm, hyper-bending case, devisor, Hasse-Weyl-Serre boundary, information security, matrix rank.*

Предварительная информация:

К. Лаутер: $\left|\#C(F_q) - (q+1)\right| \geq 3\lfloor 2\sqrt{q} \rfloor - 3$; $(*)$

Кривая C/F_q рода 3 называется оптимальной, если

$$\#C(F_q) = q + 1 \pm 3\lfloor 2\sqrt{q} \rfloor$$

$C_{a,b}: x^3z + y^3z + x^2y^2 + axyz^2 + bz^4 = 0$, где $a; b \in F_q$;

Примеры:

Для q = 31; 73 кривые $C_{4,2}$; $C_{2,48}$ достигают границы $(*)$;

Для q = 61; 79; 97 кривые $C_{29,34}$; $C_{4,8}$; $C_{56,79}$ являются оптимальными максимальными кривыми.

Пусть C – кривая рода g над полем k, которая не имеет особых точек. Пусть D^{∞} – эффективный k-рациональный дивизор степени g. Следствием теоремы Римана-Роха является следующее представление дивизоров:

Факт: (Представление дивизоров). Пусть D – дивизор степени 0 кривой C над k (то есть элемент $Div_k^0(C)$). Тогда существует эффективный дивизор E над k степени g такой, что $E - D^{\infty} \sim D$. Как правило, дивизор E единствен.

Теперь мы ограничимся случаем, когда C – негиперэллиптическая кривая рода 3. Благодаря каноническому вложению, можно считать, что C – гладкая плоская квартика (пример 5.2.1 из [15]). Обозначим через x, y, z (или иногда x_1, x_2, x_3) координаты в P^2.

Обозначим через $(*)$ следующее условие: существует рациональная прямая l^{∞}, которая пересекает C в четырех (не обязательно различных, но тогда с кратностью) k-рациональных точках $P_1^{\infty}, P_2^{\infty}, P_3^{\infty}, P_4^{\infty}$.

Далее мы выберем $D^{\infty} = P_1^{\infty} + P_2^{\infty} + P_3^{\infty}$. Этот частный случай позволит геометрически описать групповой закон в якобиане кривой C (см. Теорему 3.2.1). Более того, через k мы будем обозначать конечное поле F_q, где $q = p^n$ для некоторого простого числа p.

Напомним, что для квартики существует 5 вариантов для дивизора пересечения $(l^{\infty} \cdot C) = P_1^{\infty} + P_2^{\infty} + P_3^{\infty} + P_4^{\infty}$:

1. Четыре точки попарно различны. Это общий случай.
2. $P_1^{\infty} = P_2^{\infty}$, тогда l^{∞} касается C в P_1^{∞}.
3. $P_1^{\infty} = P_2^{\infty} = P_4^{\infty}$. Точка P_1^{∞} тогда называется изгибом.
4. $P_1^{\infty} = P_2^{\infty}$ и $P_3^{\infty} = P_4^{\infty}$. Прямая l^{∞} называется бикасательной для кривой C. Хорошо известно (см., например, [22]), что если $char(k) \neq 2$, то C имеет ровно 28 бикасательных. Если $char(k) = 2$, то C имеет соответственно 7, 4, 2 или 1 бикасательных согласно 2-рангу своего якобиана (соотв. 3, 2, 1, 0).
5. $P_1^{\infty} = P_2^{\infty} = P_3^{\infty} = P_4^{\infty}$. Точка P_1^{∞} называется гиперизгибом. Как правило, такая точка не существует (т. е. множество квартик с хотя бы с одним гиперизгибом имеет коразмерность 1 в пространстве квартик).

Эффективность алгебраической версии алгоритма будет зависеть от выбора l^{∞}. Теперь рассмотрим ситуации, когда условие $(*)$ выполнено:

Предложение: Условие $(*)$ выполняется в следующих случаях:

Таблица 1. «Условия ограничения для числа точек кривой.»

Условие для p	Условие для n	Условие для q	Условие для $\|C(k)\|$
$p > 2$		$q \geq 10^6$	
$p > 2$		$q > 8$	$\|C(k)\| \geq q - \sqrt{q}/4 + 7/4$
$p = 2$	$n > 3$	$q > 8$	$\|C(k)\| \geq q + 3$

В частности, для больших нечетных q на невырожденной квартике всегда существуют четыре коллинеарных точки.

Геометрическое описание алгоритма

С этого момента мы предполагаем, что условие $(*)$ выполнено.

Напомним, что тогда мы выбираем $D^{\infty} = P_1^{\infty} + P_2^{\infty} + P_3^{\infty}$. Для элемента D в $Div_k^0(C)$ пусть $D^{+}-$ эффективный дивизор (в общем случае уникальный) такой, что $D^{+} - D^{\infty} \sim D$. В этом случае будем говорить, что кривая C' проходит через nP, если $i\,(C, C'; P) = n$, где $i(C, C'; P)$ обозначает кратность пересечения C и C' в точке P.

Теорема: Пусть $D_1, D_2 \in Div_k^0(C)$. Тогда $D_1 + D_2$ эквивалентен дивизору $D = D^{+} - D^{\infty}$, где точки из носителя дивизора D^{+} задаются следующим алгоритмом:

1. Возьмем уникальную кубику E, которая проходит (с учетом кратности) через носители дивизоров D_1^{+}, D_2^{+} и $P_1^{\infty}, P_2^{\infty}, P_4^{\infty}$. Эта кубика также пересекает C в вычетном эффективном дивизоре D_3.
2. Возьмем уникальную конику Q, которая проходит через носители D_3 и $P_1^{\infty}, P_2^{\infty}$. Эта коника также пересекает C в вычетном эффективном дивизоре D^{+}.

Доказательство. Обозначим $\omega = \frac{dx}{df/dy}$ – дифференциал, где f – уравнение нашей кривой C. Поскольку C – гладкая кривая, то $supp(div(\omega)) =$

l^∞. С помощью замены координат $X = \frac{y}{z}$; $Y = \frac{x}{z}$ получаем $\frac{dx}{df/_{dy}} = -\frac{dy}{df/_{dx}} = \frac{Y}{\tilde{f}(X;Y)}dY$, где $\tilde{f}(X;Y) = f\left(\frac{X}{Y};\frac{1}{Y}\right) \cdot Y$. Точка в бесконечности имеет порядок $degC - 3 = 1$, следовательно, дивизор $K = (C \cdot l^\infty)$ – канонический. Таким образом, $(E \cdot C) \sim 3K$ и $(Q \cdot C) \sim 2K$. Имеем:

1. $D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_E \sim 3K$, где D_E – некоторый дивизор и кривой C, и кубики E.
2. $E + P_1^\infty + P_2^\infty + D_E' \sim 2K$, где D_E' – некоторый дивизор и кривой C, и коники Q.
3. $P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty \sim K$.

Объединяя эти результаты, получаем:

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_E \sim 3K \sim$$
$$\sim D_E + P_1^\infty + P_2^\infty + D_E' + P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty,$$

откуда $D_1^+ + D_2^+ \sim D_E' + P_1^\infty + P_2^\infty + P_3^\infty$ или, что равносильно,

$$(D_1^+ - (P_1^\infty + P_2^\infty + P_3^\infty)) + (D_2^+ - (P_1^\infty + P_2^\infty + P_3^\infty)) \sim$$
$$\sim D_E' - (P_1^\infty + P_2^\infty + P_3^\infty),$$

где $P_1^\infty + P_2^\infty + P_3^\infty = D^\infty$.

Окончательно получаем, $D_1 + D_2 \sim D_E' - D^\infty$. Пологая, что $D_E' = D^+$, имеем $D_1 + D_2 \sim D$.

Алгебраическое описание алгоритма

В этом разделе мы дадим алгебраическое описание алгоритма. Оно зависит от прямой l^∞. Сначала мы ищем простые представления кривой и ее дивизоров: мы можем предположить (после k-линейного преобразования), что P_1^∞– точка на бесконечности (т.е. такая, что ее z-координата равна 0), и что l^∞ есть прямая $z = 0$. Пусть $f(x,y) = 0$ – аффинное уравнение кривой C.

Предложение: Теперь рассмотрим представление Мамфорда, когда дивизор $D \in Div_k^0(C)$ задается парой полиномов (u, v). Оно уникально при следующих общих допущениях относительно D (при таких допущениях будем называть дивизор типичным):

1. Три точки в носителе дивизора D не коллинеарны. В этом случае D^+ единственный. Фактически, если $P_1 + P_2 + P_3 + (f) = Q_1 + Q_2 + Q_3$, то функция $f \in L(P_1 + P_2 + P_3)$ и f должна быть постоянной по теореме Римана-Роха.
2. В носителе дивизора D^+ не присутствует бесконечной точки. Пусть $P_i = (x_i: y_i: 1)(i = 1, 2, 3)$ – три точки в носителе D^+и $u = \prod(x - x_i)$. Поскольку D^+– рациональный дивизор, то $u \in k[x]$.
3. $(x_i)_{i=1,2,3}$ – различны. В этом случае существует единственный многочлен $v \in k[x]$ степени 2 такой, что $y_i = v(x_i)$ для i = 1, 2, 3 (интерполяционный многочлен).

И наоборот, зная пару (u, v), такую, что:

- $u, v \in k[x]$,

- $u = \prod(x - x_i)$ является унитарным многочленом степени 3 и имеет простые корни,

- $\deg(v) = 2$,

- $u \mid f(x, v(x))$,

мы можем определить рациональный дивизор кривой C как $P_1 + P_2 + P_3 - D^\infty$, где для $i \in \{1, 2, 3\}$ имеем $P_i = (x_i: v(x_i): 1)$.

Наконец, очевидно, что сложение двух типичных дивизоров в общем случае является типичным дивизором. Поскольку нам интересны криптографические приложения, то стоит реализовывать алгоритм только в этом случае.

Касательный случай. После линейного преобразования уравнения исходной кривой можно считать, что l^∞ – касательная в точке $P_1^\infty = (0: 1: 0)$ и проходит через точку $P_4^\infty = (1: 0: 0)$. Тогда уравнение для C имеет вид

$$y^3 + h_1 y^2 + h_2 y = f_4,$$

где $h_1, h_2, f_4 \in F_q[x]$ и $\deg(h_1) \leq 2, \deg(h_2) \leq 3, \deg(f_4) \leq 4$. Если $\deg(f_4) = = 4$, можно дополнительно предположить, что f_4 является унитарным.

Алгоритм сложения дивизоров:

Ввод: $D_1 = (u_1, v_1)$ и $D_2 = (u_2, v_2)$.

Вывод: $D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$.

1. Вычисление кубики E:

1.1 Вычислить обратный t_1 к $v_1 - v_2$ по модулю u_2.

1.2 Вычислить остаток r от деления $(u_1 - u_2)t_1$ на u_2.

1.3 Решить систему линейных уравнений:

$$\begin{cases} deg_x(-v_1(v_1 + s) + u_1\delta_1) = 3 \\ v_1 + v_2 + s \equiv r\delta_1[u_2] \end{cases},$$

где $s_1, \delta_1 \in k[x], \deg(s) = 2$ и $\deg(\delta_1) = 1$.

Тогда

$$E = (y - v_1)(y + v_1 + s) + u_1\delta_1$$

2. Вычисление коники Q:

2.1 Вычислить $u' = Res^*(E, C, y)/(u_1u_2)$.

2.2 Вычислить обратный α_1 к $t - s_2 - h_2 + sh_1$ по модулю u'.

2.3 Вычислить остаток v' от деления $\alpha_1(st - th_1 - f_4)$ на u'.

3. Вычисление $D_1 + D_2$:

3.1 $v_{D_1+D_2} = v'$

3.2 $u_{D_1+D_2} = \left((v^3 + v^2h_1 + vh_2 - f_4)/\,(u')\right)^*$

3.3 $D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$

Алгоритм удвоения дивизоров:

Ввод: $D_1 = (u_1, v_1)$.

Вывод: $2D_1 = (u_{2D_1}, v_{2D_1})$.

1. Вычисление кубики E:

1.1 Вычислить $\omega_1 = (v_1^3 + v_1^2h_1 + v_1h_2 - f_4)/u_1$.

1.2 Вычислить обратный t_1 к ω_1 по модулю u_1.

1.3 Вычислить остаток r от деления $(3v_1^2 + 2v_1h_1 + h_2)t_1$ на u_1.

1.4 Решить систему линейных уравнений:

$$\begin{cases} deg_x(-v_1(v_1+s)+\ u_1\delta_1)=3 \\ 2v_1+s\ \equiv r\delta_1[u_1] \end{cases},$$

где $s_1,\delta_1\in k[x],\deg(s)=2$ и $\deg(\delta_1)=1$.

Тогда

$$E=(y-v_1)(y+v_1+s)+u_1\delta_1$$

2. Вычисление коники Q:

2.1 Вычислить $u'=Res^*(E,C,y)/(u_1u_2)$.

2.2 Вычислить обратный α_1 к $t-s_2-h_2+sh_1$ по модулю u'.

2.3 Вычислить остаток v' от деления $\alpha_1(st-th_1-f_4)$ на u'.

3. Вычисление $2D_1$:

3.1 $v_{2D_1}=v'$

3.2 $u_{2D_1}=\left((v^3+v^2h_1+vh_2-f_4)/\ (u')\right)^*$

3.3 $2D_1=(u_{2D_1},v_{2D_1})$

Обоснование алгоритма.

Корректность работы алгоритма будет сводиться к тому, что точки дивизоров D_1 и D_2 должны удовлетворять уравнению кубики E и уравнению коники Q. Подразумеваем, что v_1,v_2 – многочлены от x_i, где x_i – абсциссы точек из носителей дивизоров D_1 и D_2 соответственно, и принимаем во внимание, что $D_1=(u_1;v_1),D_2=(u_2;v_2)$ – координаты Кантора-Мамфорда.

Алгоритм сложения:

Рассмотрим уравнение кубики $E\colon(y-v_1)(y+v_1+s)+u_1\delta_1=0$. Подставляя значение точки дивизора D_2, получаем:

$$(v_2-v_1)(v_2+v_1+s)+u_1\delta_1=0.$$

Согласно шагу 1:

$$t_1=(v_1-v_2)^{-1}\ (mod\ u_2)\rightarrow\ -t_1^{-1}(v_2+v_1+s)+u_1\delta_1=0.$$

Согласно шагу 2:

$$(u_1-u_2)t_1=u_2q+r\rightarrow u_1t_1\equiv r\ (mod\ u_2).$$

Согласно шагу 3:

$$v_1 + v_2 + s = r\delta_1 \ (mod\ u_2).$$

Тогда, из шага 2 и 3 следует:

$$-\frac{u_1}{r} \cdot r\delta_1 + u_1\delta_1 = 0,$$

откуда получаем верное тождество, значит, точки дивизоров лежат на кубике E.

Алгоритм удвоения:

Рассмотрим $D_1 = (u_1; v_1)$ – дивизор кривой C. Тогда $v_1^3 + h_1v_1^2 + h_2v_1 - f_4 = 0$, где h_1, h_2, f_4 – значения $h_1(u_1), h_2(u_1), f_4(u_1)$ соответственно.

Уравнение кубики E принимает вид:

$$(v_1 - v_1)(v_1 + v_1 + s) + u_1\delta_1 = u_1\delta_1 = u_1 \cdot \frac{2v_1 + s}{r} =$$

$$= u_1 \cdot \frac{2v_1 + s}{(3v_1^2 + 2v_1h_1 + h_2)t_1} =$$

$$= u_1 \cdot \frac{2v_1+s}{(3v_1^2+2v_1h_1+h_2)} \cdot \frac{v_1^3+h_1v_1^2+h_2v_1-f_4}{u_1} = 0,$$

откуда получаем верное тождество, значит, точки дивизора лежат на кубике E.

Рассмотрим точку $P = (x_p; y_p)$ – точка пересечения кубики E с нашей кривой C такая, что $u(x_p) = 0$.

Из вычисления коники следует:

$$v'(x_p) = \frac{s(x_p)t(x_p) - t(x_p)h_1(x_p) - f_4(x_p)}{t(x_p) - s^2(x_p) - h_2(x_p) + s(x_p)h_1(x_p)} \left(mod\ u'(x_p)\right).$$

Учитывая уравнения кривой и кубики: $\begin{cases} y_p^2 + sy_p + t = 0 \\ y_p^3 + h_1y_p^2 + h_2y_p = f_4 \end{cases}$ и тот факт, что P – точка пересечения кубики E с кривой C, имеем

$$\frac{s(-y_p^2 - sy_p) - (-y_p^2 - sy_p)h_1 - (y_p^3 + h_1y_p^2 + h_2y_p)}{-y_p^2 - sy_p - s^2 - h_2 + sh_1} =$$

$$= \frac{-y_p^2s - s^2y_p + y_p^2h_1 + sy_ph_1 - y_p^3 - h_1y_p^2 - h_2y_p}{-y_p^2 - sy_p - s^2 - h_2 + sh_1} =$$

$$= \frac{y_p(-y_p s - s^2 + sh_1 - y_p^2 - h_2)}{-y_p^2 - sy_p - s^2 - h_2 + sh_1} = y_p.$$

Таким образом, коника Q проходит через точки дивизора кубики, которые, в свою очередь, лежат на кривой C. □

Для результанта мы использовали обозначение Res^*, чтобы символизировать частное Res с помощью его старшего коэффициента.

Можно задаться вопросом о выборе дивизора D^∞. Он был выбран так, чтобы коника Q имела вид $y - v$, что дает непосредственно вторую часть представления Мамфорда конечного дивизора. Другой выбор дивизора D^∞ подразумевает использование вспомогательной коники для нахождения представления Мамфорда. Отметим, что алгоритмы сложения и удвоения действительны для любого базового поля (даже в случае характеристики 0).

Использованные источники:

1. Алексеенко Е.С. *Явные конструкции оптимальных кривых рода три*. Дисс. на соиск. уч. степ. канд. физ.-мат. наук – М.: ИППИ им А.А. Харкевича РАН, 2014.
2. Abhyankar S. *Remark on Hessians and flexes*. Nieuw Arch. Wisk., 11:110–117, 1963.
3. Adleman L.M., De Marrais J., Huang M-D. *A subexponential algorithm for discrete logarithms in the rational subgroup of the Jacobian of a hyperelliptic curve over a finite field*. In Algorithmic Number Theory Symposium – 1994, volume 877 of LNCS, 28–40. Springer, 1994.