Scientific-technical journal

Volume 1 | Issue 2 Article 20

6-7-2018

CHOICE OF AN ELLIPTIC CURVE AND DEVELOPMENT OF AN ALGORITHM OF ADDITION OF ITS POINTS WITH RATIONAL COORDINATES ON A FINITE FIELD

D E. Akbarov
Kokand state pedagogical institute

U Y. Akbarov
Kokand state pedagogical institute

A A. Xashimov
Regional center for retraining and professional public education staff under the Fergana State University

M M. Nurullaev
Bukhara Engineering and Technology Institute

УДК 681.3

CHOICE OF AN ELLIPTIC CURVE AND DEVELOPMENT OF AN ALGORITHM OF ADDITION OF ITS POINTS WITH RATIONAL COORDINATES ON A FINITE FIELD

[1]D.E. Akbarov, [1]U.Y.Akbarov, [2]A.A. Xashimov, [3]M.M. Nurullaev

[1]Kokand state pedagogical institute,
[2]Regional center for retraining and professional public education staff under the Fergana State University,
[3]Bukhara Engineering and Technology Institute

ВЫБОР ЭЛЛИПТИЧЕКСКОЙ КРИВОЙ И БАЗОВОЙ ТОЧКИ В РАЗРАБОТКЕ АЛГОРИТМА СЛОЖЕНИЯ ЕЁ ТОЧЕК С РАЦИОНАЛЬНЫМИ КООРДИНАТАМИ НА КОНЕЧНОМ ПОЛЕ

[1]Д.Е. Акбаров, [1]У.Й. Акбаров , [2]А. А. Хашимов , [3]М.М. Нуриллаев

[1]Кокандский государственный педагогический институт,
[2]Ферганский филиал Ташкентского университета информационных технологий,
[3]Бухарский инженерно-технологический институт,

ЧЕКЛИ МАЙДОНДА ЭЛЛИПТИК ЭГРИ ЧИЗИҚНИ ТАНЛАШ ВА УНИНГ РАЦИОНАЛ КООРДИНАТАЛИ НУҚТАЛАРИНИ ҚЎШИШ АЛГОРИТМИНИ ИШЛАБ ЧИҚИШ

[1]Д.Е. Акбаров, [1] У.Й. Акбаров, [2] А.А. Хашимов, [3]М.М. Нуриллаев

[1]Қўқон давлат педагогика институти.
[2]Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали
[3]Бухора муҳандислик- технология институти

Abstract. *The article deals with the problems of solving problems of determining and calculating EC parameters for the correct implementation of asymmetric cryptoalgorithms. Using the Vieta formulas, for the roots of polynomials, the method of choosing the coefficients is given. The interval for selecting the base point is indicated. The formulas of the tangent to the base point and finding the coordinates of the point of intersection of the tangent with the EC are determined. A recurrence formula is obtained for the addition of a base point with other points of EC with rational coordinates.*

Keywords: elliptic curve, asymmetrical crypto algorithm, discriminant, cubic equation, Vieta formulas, basic point, order of a basic point.

Аннотация. *В статье исследованы вопросы решения задач определение и вычисление параметры ЭК для корректной реализации асимметричных крипто алгоритмов. Используясь формулами Виета, для корней многочленов, приведено способ выбора коэффициентов. Указан интервал выбора базовой точки. Определены формулы касательной к базовой точке и нахождения координаты точки пересечения касательной с ЭК. Получена рекуррентная формула сложения базовой точки с другими точками ЭК с рациональными координатами.*

Ключевые слова: эллиптическая кривая, асимметричный крипто алгоритм, дискриминант, кубическое уравнение, формулы Виета, базовая точка, порядок базовой точки.

Аннотация. *Мақолада асимметрик криптоалгоритмларни бенуқсон тадбиқлари учун эллиптик эгри чизиқ параметрларини аниқлаш ва ҳисоблаш масалалари ечимлари таҳлил этилган. Кўпҳад илдизлари учун Виет теоремасидан фойдалани, коэффициентларни танлаш услуби берилган. Базавий нуқтани танлаш оралиғи кўрсатилган. Базавий нуқтага ўтказилган уринма тенгламаси ва уринманинг эллиптик эгри чизиқ билан кесишиш нуқтаси формулалари аниқланган. Базавий нуқтани бошқа рационал координатали нуқталар билан қўшишнинг рекуррент формуласи олинган.*

Таянч сўзлар: эллиптик эгри чизиқ, асимметрик криптоалгоритм, дискриминант, кубик тенглама, Виет формуласи, базавий нуқта, базавий нуқтанинг тартиби.

Введение. Асимметричные криптографические алгоритмы конструируются на основе вычислительных сложностей: разложения достаточно большого натурального числа на простые множители, дискретного логарифмирования на конечном поле с достаточно большой характеристикой, сложения точек с рациональными координатами эллиптической кривой (ЭК) на конечном поле. Напоминается, что алгоритмы шифрования RSA и Эль-Гамал, также стандарт алгоритмы электронной цифровой подписи DSA и ГОСТ Р 34.10-94, их модификации на ЭК ЕС DSA-2000 и ГОСТ Р 34.10-2001 являются широко используемыми [1-4].

Постановка задачи. Приложения асимметричных алгоритмов требуют предварительного выбора (установки) параметров для корректной работы и обеспечения гарантируемой стойкости. Установить параметров открытых и закрытых параметров требует не простые вычисления исходя из особенности сложности, на которой основан алгоритм. Для обеспечения гарантируемой стойкости в применении алгоритма RSA требуется найти желательно достаточно больших простых чисел, которые хранится в секрете. Как известно, задача: определение достаточного большого данного натурального числа простое или непростое не имеет своё полное решение [4-7]. В приложениях алгоритма Эль-Гамал выбор параметров проще, генерация открытых y и закрытых x ключей по равенству $y = a^x \bmod n$,где n – достаточно большое натуральное число, не порождает большой вычислительной сложности. Алгоритмы на ЭК требуют: определение коэффициенты самой ЭК, осуществление операции на конечном поле характеристикой желательно простым числом, нахождение базовую точку рациональными координатами порядком простого числа, сложные вычисления, связанные со спецификой модели алгоритма. В предлагаемой статье исследуется вопросы решения задач определением и вычислением параметров ЭК для корректной реализации асимметричных алгоритмов.

Решение задачи. В приложениях криптографическим алгоритмам ЭК используется её вид $y^2 = x^3 + px + q$ на конечном поле характеристикой, например m, т.е.

$$y^2 = x^3 + px + q(\bmod m),\ m > 3. \quad (1)$$

Если коэффициенты удовлетворяют неравенству $\frac{q^2}{4} + \frac{p^3}{27} = \frac{4p^3 + 27q^2}{108} < 0$, то уравнение

$$x^3 + px + q = 0 \quad (2)$$

имеет три разных действительных решений x_1, x_2, x_3, следовательно, ЭК пересекает ось OX на точках $(x_1,0)$, $(x_2,0)$, $(x_3,0)$. Именно это случае является эффективным в приложении [3, 4].

Если кубическое уравнение имеет вид $x^3 + ax^2 + bx + c = 0$,

то его решение x_1, x_2, x_3 находится по следующим формулам:

$x_1 = -2sqrt(Q)\cos(t) - a/3;\quad x_2 = -2sqrt(Q)\cos(t + (2pi/3)) - a/3;$

$x_3 = -2sqrt(Q)\cos(t - (2pi/3)) - a/3$ где $t = a\cos(R/sqrt(Q^3))/3$, $Q = (a^2 - 3b)/9$,

$R = (2a^3 - 9ab + 27c)/54$.

Предлагается подход использования теоремой Виета, ЭК можно выбрать со способом, удобным в приложениях. Для этого выбираются точки с рациональными координатами:

$(x_1,0)$, $(x_2,0)$, $(x_3,0)$ с условиями $x_1+x_2+x_3=0$, $x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3=p$, $x_1\cdot x_2\cdot x_3=-q$. Далее, фиксируются: x_1 и x_2, находится, $x_3=-(x_1+x_2)$, вычисляются $p=x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3$, $q=-(x_1\cdot x_2\cdot x_3)$.

Выбор базовую точку $P(x_0,y_0)$ на ЭК с координатами рациональных чисел осуществляется следующим образом. Для определённости сначала упорядочат значения x_1, x_2, x_3 по возрастанию: если $x_1<x_2<x_3$, то нумерацию оставить как есть, иначе переномеровать. Из области определения ЭК фиксируется $x=x_0$ по условию $-\sqrt{-\frac{p}{3}}<x_0<x_2$, и далее на этой точке вычисляется ${x_0}^3+px_0+q=z_0$, следовательно $y_0=\pm\sqrt{z_0}$. Как результат умножения и сложения рациональных чисел, значение z_0 будет рациональным. Но y_0 не всегда будет рациональным. Поэтому x_0 выбрать так чтобы y_0 тоже было рациональным числом. Мы предположим, что точка с рациональными координатами $P(x_0,y_0)$ найдена, хотя нахождение такую точку тоже не так просто. На пример ЭК можно выбрать $y^2=x^3+px+q=x^3-26x-40$ и базовую точку на ней $P(x_0,y_0)=(-2;2)$.

Не посредственным вычислением можно убедится, что при $p=-26$ и $q=-40$ инвариант ЭК [3-6] :

$$J(E)\equiv 1728\frac{4p^3}{4p^3+27q^2}(\mathrm{mod}\,m)=16\cdot 108\frac{4p^3}{4p^3+27q^2}(\mathrm{mod}\,m)=16\cdot 27\cdot 4\frac{4p^3}{4p^3+27q^2}(\mathrm{mod}\,m)$$

в соответствующем выборе характеристики $m>3$ конечного поля удовлетворяются условия $J(E)\neq 0$ и $J(E)\neq 1728$.

Определяется уравнение касательной ЭК на точке $P(x_0,y_0)$. Для этого вычисляется производная на точке $P(x_0,y_0)$, т.е. $y_0'=\frac{3{x_0}^2+p}{2y_0}$, которое представляет угловой коэффициент искомой касательной. Тогда уравнение касательной имеет вид

$$y-y_0=\frac{3{x_0}^2+p}{2y_0}(x-x_0) \text{ или } y=\frac{3{x_0}^2+p}{2y_0}x+\left(y_0-\frac{3{x_0}^2+p}{2y_0}x_0\right).$$

Непосредственно решая систему уравнений

$$\begin{cases} y^2=x^3+px+q \\ y=\frac{3{x_0}^2+p}{2y_0}x+\left(y_0-\frac{3{x_0}^2+p}{2y_0}x_0\right) \end{cases}$$

находится точку пересечения (x_1,y_1) касательной с ЭК. Отсюда имеется следующее кубическое уравнение

$$x^3-\left(\frac{3{x_0}^2+p}{2y_0}\right)^2x^2+\left(p-\frac{3{x_0}^2+p}{y_0}\left(y_0-\frac{3{x_0}^2+p}{2y_0}x_0\right)\right)x+\left[q-\left(y_0-\frac{3{x_0}^2+p}{2y_0}x_0\right)^2\right]=0. \quad (3)$$

Обозначив,

$a=-\left(\frac{3x_0{}^2+p}{2y_0}\right)^2$, $b=p-\frac{3x_0{}^2+p}{y_0}\left(y_0-\frac{3x_0{}^2+p}{2y_0}x_0\right)$, $c=q-\left(y_0-\frac{3x_0{}^2+p}{2y_0}x_0\right)^2$ уравнение (3) запишется в виде

$$x^3+ax^2+bx+c=0\,. \qquad (4)$$

Так как рассматривается, нахождения координаты точку пересечения касательной с ЭК естественно полагать, что в решении уравнения (4) $x_1=x_2=x_0$, где x_0-координата базовой точки $P(x_0,y_0)$. Пользуясь теоремой Виета, имеется соотношения $x_1+x_2+x_3=-a$, $x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3=b$, $x_1\cdot x_2\cdot x_3=-c$, отсюда:

$$x_3=-a-2x_0=\frac{b-x_0{}^2}{2x_0}=-\frac{c}{x_0{}^2}\ \text{ и }\ y_3=\frac{3x_0{}^2+p}{2y_0}x_3+\left(y_0-\frac{3x_0{}^2+p}{2y_0}x_0\right)$$

Отсюда, находится координаты точку

$$[2]P(x_0,y_0)=P(x_0,y_0)+P(x_0,y_0)=(x_3,-y_3)$$

на ЭК с симметричным отображением точку пересечения относительно оси *OX*. Теперь переопределяя, что $(x_2,y_2)=[2]P(x_0,y_0)=(x_3,-y_3)$ имеем:

$$x_2=-\frac{c}{x_0{}^2}=\frac{(y_0-\frac{3x_0+p}{2y_0}x_0)^2-q}{x_0{}^2}\ \text{ и }\ y_2=-\frac{3x_0{}^2+p}{2y_0}x_2-(y_0-\frac{3x_0+p}{2y_0}x_0).$$

Координаты точки $(x_3,y_3)=[3]P(x_0,y_0)=P(x_0,y_0)+[2]P(x_0,y_0)$ находится симметричным отображением точку пересечения ЭК с прямой, проходящей через точки $P(x_0,y_0)$ и $[2]P(x_0,y_0)$. Уравнение прямой, проходящей через эти точки определяется формулой: $\frac{y-y_0}{y_2-y_0}=\frac{x-x_0}{x_2-x_0}$ или отсюда

$$y=y_0+\frac{x-x_0}{x_2-x_0}(y_2-y_0)=\frac{y_2-y_0}{x_2-x_0}x+y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\,.$$

Вычисляется: $y^2=\left(\frac{y_2-y_0}{x_2-x_0}\right)^2x^2+2\left[\frac{y_2-y_0}{x_2-x_0}\left(y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right)\right]x+\left[y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right]^2$ и это выражение вставится на уравнение ЭК, тогда

$$\left(\frac{y_2-y_0}{x_2-x_0}\right)^2x^2+2\left[\frac{y_2-y_0}{x_2-x_0}\left(y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right)\right]x+\left[y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right]^2=x^3+px+q$$

или

$$x^3-\left(\frac{y_2-y_0}{x_2-x_0}\right)^2x^2+\left[p-2\frac{y_2-y_0}{x_2-x_0}\left(y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right)\right]x+q-\left[y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right]^2=0\ .$$

Опять обозначив, что $a=-\left(\frac{y_2-y_0}{x_2-x_0}\right)^2$, $b=p-2\frac{y_2-y_0}{x_2-x_0}\left(y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right)$,

$$c=q-\left[y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right]^2,$$

учитывая, что его решения $x_1=x_0$ и x_2 известны, находится

$$x_3=\left\{\left[y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right]^2-q\right\}\Big/(x_0\cdot x_2)\ .$$

отсюда, $y_3 = \frac{y_2 - y_0}{x_2 - x_0} x_3 + y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0}$.

Координаты симметричного отображения точку пересечения относительно оси OX следующие: $x_3 = \frac{\left\{\left[y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0}\right]^2 - q\right\}}{x_0 \cdot x_2}$ и пологая $y_3 = -y_3 = -\left(\frac{y_2 - y_0}{x_2 - x_0} x_3 + y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0}\right)$

Аналогично находится координаты точку

$$[i+1]P(x_0, y_0) = P(x_0, y_0) + [i]P(x_0, y_0) = (x_{i+1}, y_{i+1}),\ (i = 2,3,..., n;)$$

формулами:

$$x_{i+1} = \frac{\left\{\left[y_0 - \frac{x_0(y_i - y_0)}{x_i - x_0}\right]^2 - q\right\}}{x_0 \cdot x_i} \quad \text{и} \quad y_{i+1} = -\left(\frac{y_i - y_0}{x_i - x_0} x_{i+1} + y_0 - \frac{x_0(y_i - y_0)}{x_i - x_0}\right).$$

Возникает вопрос, когда остановиться этот процесс сложения точек ЭК.

Если при некотором значении $n = i + 1$ имеет место $(x_n, y_n) = (x_0, -y_0)$, процесс остановиться и число n называется порядком базовой точки $P(x_0, y_0)$ [3-10].

В приложениях желательно чтобы было значение числа n достаточно большое и простое.

Анализ полученных результатов. Отмечено, что в разработке криптографических алгоритмов воспользуется следующий вид эллиптической кривой [3-10]

$$y^2 = (x^3 + px + q) \bmod m,$$

где коэффициенты $p, q \in F_m$ являются ненулевыми элементами простого поля F_m – числового поля характеристикой $m > 3$, кроме того значение выражения $4p^3 + 27q^2$ по модулю m не равно нулю, т.е. $(4p^3 + 27q^2) \bmod m \neq 0.$

Можно отметить**,** что ЭК $y^2 = x^3 + px + q = x^3 - 26x - 40$ и базовая точка на ней $P(x_0, y_0) = (-2; 2)$ удовлетворяют требованиям [3-6] :

–коэффициенты $p, q \in F_m$ являются ненулевыми элементами простого поля;

– значение выражения $4p^3 + 27q^2$ по модулю m не равно нулю,

т.е. $(4p^3 + 27q^2) \bmod m \neq 0;$

–инвариант $J(E) \neq 0$ и $J(E) \neq 1728;$

поэтому эллиптическая кривая удовлетворяет требованиям корректного приложения в алгоритмах ЭЦП.

Заключение. Исследованы вопросы решения задач определение и вычисление параметры ЭК для корректной реализации асимметричных алгоритмов:

1. Для обеспечения эффективности приложения алгоритмов на ЭК по знаку значения дискриминанта кубического уравнения приведено условие выбора коэффициентов, при которых эллиптическая кривая пересекает ось OX в трёх разных точках;

2. Используясь формулами Виета, для корней многочленов, приведено способ выбора коэффициентов, который является удобным и часто целесообразным по научным замыслам разработчика;

3. Указан интервал выбора базовой точки, что является немало важным с точки зрения рационального вычисления сложения точек ЭК;

4. Определены формулы касательной к базовой точке и нахождения координаты точки пересечения касательной с ЭК;

5. Получена рекуррентная формула сложения базовой точки с другими точками ЭК с рациональными координатами, кроме того она является обобщённой формулой для сложения любых точек ЭК с рациональными координатами;

6. Указано условие определяющее порядок базовой точки.

Все эти перечисленные образует основу для разработки и реализации асимметричных алгоритмов на ЭК.

References:

[1]. Alferov A. P., Zubov A. Yu., Kuzmin A. S., CHeremushkin A. V. Osnovi kriptografii: Uchebnoe posobie, 2-e izd. –M.: Gelios ARV, 2002.-480 s.
[2]. SHnayer B. Prikladnaya kriptografiya. Protokoli, algoritmi, isxodnie teksii na yazike Si. –M.: izdatelstvo TRIUMF, 2003 - 816 s.
[3]. Xarin Yu. S., Bernik V.I., Matveev G. V., Agievich S. G. «Matematicheskie i komyuternie osnovi kriptologii» OOO «Novoe znanie» 2003 g. 381 str.
[4]. Akbarov D. Ye. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi – Toshkent, «O'zbekiston markasi», 2009 – 434 bet.
[5]. Koblits N. Kurs teorii chisel i kriptografii. – M. Nauchnoe izd-vo TVP, 2001g. – 261 str.
[6]. Rostovtsev A. G., Maxovenko Ye. B., Teoreticheskaya kriptografiya. NPO «Professional», Sankt-Peterburg. 2004g. - 478 str.
[7]. Vasilenko O. N. Teoretiko-chislovie algoritmi v kriptografii. M., MTSNMO, 2003. – 328 s.
[8]. Bolotov A.A, Gashkov S.B., Frolov A.B., CHasovskix A.A. Algoritmicheskie osnovi ellipticheskoy kriptografii.-Moskva: Mei, 2000.-100 str.
[9]. Moldavyan A. A., Moldavyan N.A. Vvedenie v kriptosistemi s otkritim klyuchom. Sankt – Peterburg «BXV-Peterburg» 2005g. 288s.
[10]. Venbo Mao. Sovremennaya kriptografiya. Teoriya i praktika. –Moskva–Sankt-Peterburg–Kiev: Lori Vilьams, 2005. –768 s.

Web сайтлар

[1]. bardosh9295@mail.ru,
[2]. sht003@umail.uz ,
[3]. sht003@umail.uz