

6-30-2018

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

U Y. Akbarov

Follow this and additional works at: <https://uzjournals.edu.uz/ferpi>

Recommended Citation

Akbarov, D E. and Akbarov, U Y. (2018) "CHOICE OF AN ELLIPTIC CURVE AND DEVELOPMENT OF AN ALGORITHM OF ADDITION OF ITS POINTS WITH RATIONAL COORDINATES ON A FINITE FIELD," *Scientific-technical journal*: Vol. 22 : Iss. 2 , Article 10.

Available at: <https://uzjournals.edu.uz/ferpi/vol22/iss2/10>

This Article is brought to you for free and open access by 2030 Uzbekistan Research Online. It has been accepted for inclusion in Scientific-technical journal by an authorized editor of 2030 Uzbekistan Research Online. For more information, please contact brownman91@mail.ru.

UDC 681.3

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

D.E. Akbarov¹, U.Y. Akbarov¹, A.A. Xashimov², M.M. Nurullaev³¹ Kokand state pedagogical institute. Ferghana, Uzbekistan,² Ferghana branch of the Tashkent University of Information Technologies named after Muhammad al-Kharezmi. Ferghana, Uzbekistan,³ Bukhara Engineering and Technology Institute. Bukhara, Uzbekistan

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

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.

Key words: elliptic curve, asymmetrical cryptoalgorithm, 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 криптоалгоритмов. Используя 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 криптоалгоритм, 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. Кўпқад илдизлари учун Виет теоремасидан фойдалани, коэффициентларни танлаш услуби берилган. Базавий нуқтани танлаш оралиги кўрсатилган. Базавий нуқтага ўтказилган уринма тенгламаси ва уринманинг эллиптик эгри чизиқ билан кесишиши нуқтаси формулалари аниқланган. Базавий нуқтани бошқа рационал координатали нуқталар билан қўшишининг 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 EC 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 хранятся 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 желательным простым числом, нахождение базовую точку рациональными координатами порядком простого числа, сложные вычисления, связанные со спецификой модели алгоритма. В предлагаемой статье исследуются 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.

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

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:

$$\begin{aligned} x_1 &= -2\sqrt[3]{Q}\cos(t) - a/3; & x_2 &= -2\sqrt[3]{Q}\cos(t + (2\pi/3)) - a/3; \\ x_3 &= -2\sqrt[3]{Q}\cos(t - (2\pi/3)) - a/3 & \text{где } t &= a\cos(R/\sqrt[3]{Q^3})/3, \quad Q = (a^2 - 3b)/9, \\ R &= (2a^3 - 9ab + 27c)/54. \end{aligned}$$

Предлагается подход использования теоремы 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 перенумеровать. Из области определения ЭК фиксируется $x = x_0$ по условию

$-\sqrt[3]{\frac{p}{3}} < x_0 < x_2$, 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 убедиться, что при $p = -26$ и $q = -40$ инвариант ЭК [3-6] :

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

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. $y_0' = \frac{3x_0^2 + p}{2y_0}$, которое представляет угловой коэффициент искомой касательной. Тогда уравнение касательной имеет вид

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

Непосредственно решая систему уравнений

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

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

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

Обозначив,

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

(3) запишется в виде

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

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

$$x_1 + x_2 + x_3 = -a, \quad x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 = b, \quad x_1 \cdot x_2 \cdot x_3 = -c, \text{ откуда:}$$

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

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:

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

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:

$$\frac{y - y_0}{y_2 - y_0} = \frac{x - x_0}{x_2 - x_0} \text{ или отсюда}$$

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

$$\text{Вычисляется: } y^2 = \left(\frac{y_2 - y_0}{x_2 - x_0} \right)^2 x^2 + 2 \left[\frac{y_2 - y_0}{x_2 - x_0} \left(y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0} \right) \right] x + \left[y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0} \right]^2 \text{ и это}$$

выражение вставится на уравнение ЭК, тогда

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

или

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

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

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

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

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

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:

$$x_3 = \frac{\left\{ \left[y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0} \right]^2 - q \right\}}{x_0 \cdot x_2} \text{ и полагая } y_3 = -y_3 = - \left(\frac{y_2 - y_0}{x_2 - x_0} x_3 + y_0 - \frac{x_0(y_2 - y_0)}{x_2 - x_0} \right)$$

Аналогично находится координаты точку

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

формулами:

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

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., Черемушкин А. В. Osnovi kriptografii: Uchebnoe posobie, 2-e izd. –M.: Gelios ARV, 2002.-480 s.
- [2]. Шнайер В. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –M.: izdatelstvo TRIUMF, 2003 - 816 s.
- [3]. Харин Ю. С., Берник В.И., Матвеев Г. В., Агиевич С. Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.
- [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 Vilyams, 2005. –768 s

Список литературы

- [1]. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд. –M.: Гелиос АРВ, 2002.-480 с.
- [2]. Шнайер В. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –M.: издательство ТРИУМФ, 2003 - 816 с.

- [3]. Харин Ю. С., Берник В.И., Матвеев Г. В., Агиевич С. Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.
- [4]. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг кўлланилиши – Тошкент, «Ўзбекистон маркаси», 2009 – 434 бет.
- [5]. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 стр.
- [6]. Ростовцев А. Г., Маховенко Е. Б., Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.
- [7]. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. М., МЦНМО, 2003. – 328 с.
- [8]. Болотов А.А, Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии.-Москва: Мэи, 2000.-100 стр.
- [9]. Молдавян А. А., Молдавян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005г. 288с.
- [10]. Венбо Мао. Современная криптография. Теория и практика. –Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 с.