the infrared region of the spectrum are applied, as well as methods and methods for processing such images. The work related to the tasks of face recognition, the determination of temperature in the infrared range, has been going on for the last 10 years and is being solved with the help of high-sensitivity video cameras operating in the reflected IR range. The possibility of using thermal imaging cameras for this type of research has recently appeared. Information signs in thermography are subcutaneous drawings of arteries and veins, which are unique and unchanged for each person, since the vascular pattern does not depend on face temperature, plastic surgery and the aging factor of a person, like a fingerprint. A study was made of the physiological features of a person's face with a view to isolating a universal and stable temperature region, which can be used as a binding area in the allocation of the face area. The approach to the study of thermographic images, human recognition for the tasks of intellectual video surveillance, medical, security, cartographic purposes is presented. An algorithm for automatic facial recognition and determination of the human body temperature in the infrared (IR) radiation range is proposed, the results of its work are presented and the efficiency analysis is performed. The optimal place for determining the human temperature - the internal angles of the eyes was determined experimentally, since this region has the most reflection in the infrared range. The algorithm is developed in the MatLab environment and can be ported to other programming languages. A study was made of the method of applying one image to another, and the optimal method was chosen. The analysis showed high efficiency of the algorithm – 90 % of successfully recognized images. Possible use in ready-made thermal imagers and security systems.
Keywords: pattern recognition; image analysis; video surveillance systems; thermography; Face detection, combination of images.

Надійшла до редакції
23 березня 2018 року

Рецензовано
16 квітня 2018 року

УДК 681.3

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

Акбаров Д. Е. , Умаров Ш. А.
Ферганский филиал Ташкентского университета информационных технологий имени Мухаммад аль-Харезми, Фергана, Республика Узбекистан
E-mail: sht00357@gmail.com

В статье исследованы вопросы решения задач определения и вычисления параметров эллиптической кривой (ЭК) для корректной реализации асимметричных криптоалгоритмов. Использованы формулы Виета для корней многочленов, приведен 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.*

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.

Напомним, что алгоритмы шифрования RSA и Эль-Гамал, также стандарт алгоритмов 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, как показано в работах [1 – 4].

Постановка задачи

Приложения асимметричных алгоритмов требуют предварительного выбора (установки) параметров для корректной работы и обеспечения гарантируемой стойкости. Установка параметров открытых и закрытых параметров требует прове-

дения непростых вычислений, исходя из особенности сложности, на которой основан алгоритм. Для обеспечения гарантируемой стойкости в применении алгоритма RSA требуется найти достаточно больших простых чисел, которые хранятся в секрете. Как известно, задача: определение достаточного большого данного натурального числа простое или непростое не имеет своего полного решения [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: определения коэффициентов самой ЭК, осуществления операции на конечном поле характеристикой желательно простым числом, нахождения базовой точки рациональными координатами порядком простого числа, сложных вычислений, связанных 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.

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

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

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

имеет три разных действительных решения x_1, x_2, x_3, следовательно, ЭК пересекает ось OX в точках $(x_1, 0)$, $(x_2, 0)$, $(x_3, 0)$. Именно этот случай 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:

$$x_1 = -2sqrt(Q)\cos(t) - a/3;$$
$$x_2 = -2sqrt(Q)\cos(t + (2pi/3)) - a/3;$$
$$x_3 = -2sqrt(Q)\cos(t - (2pi/3)) - a/3$$

где $t = a\cos(R/sqrt(Q^3))/3$, $Q = (a^2 - 3b)/9$, $R = (2a^3 - 9ab + 27c)/54$.

Предлагается подход использования 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 базовой точки $P(x_0, y_0)$ на ЭК с координатами рациональных чисел осуществляется следующим образом. Для определённости сначала необходимо упорядочить 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 $-\sqrt{-\frac{p}{3}} < x_0 < x_2$, 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 стоит выбрать так, чтобы y_0 тоже было рациональным числом. Мы предположим, что точка с рациональными координатами $P(x_0, y_0)$ найдена, хотя нахождение такой точки тоже не так просто. Например, ЭК можно выбрать $y^2 = x^3 + px + q = x^3 - 26x - 40$ и базовую точку на ней $P(x_0, y_0) = (-2; 2)$.

Непосредственным вычислением можно убедиться, что при $p = -26$ и $q = -40$ инвариант ЭК [3 – 6]:

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

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

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

$$y - y_0 = \frac{3x_0^2 + p}{2y_0}(x - x_0)$$

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 точка пересечения (x_1, y_1) касательной

с ЭК. Отсюда имеем следующее кубическое уравнение

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

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

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 нахождение координаты точки пересечения касательной с ЭК, естественно полагать, что решение уравнения (4) $x_1=x_2=x_0$, где x_0 – координата базовой точки $P(x_0,y_0)$. Пользуясь теоремой Виета, имеем соотношения

$x_1+x_2+x_3=-a,\qquad x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3=b,$

$x_1\cdot x_2\cdot x_3=-c$, отсюда

$$x_3=-a-2x_0=\frac{b-x_0{}^2}{2x_0}=-\frac{c}{x_0{}^2}$$

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

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

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

Координаты точки

$(x_3,y_3)=[3]P(x_0,y_0)=P(x_0,y_0)+[2]P(x_0,y_0)$

находятся симметричным отображением точки 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

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

Вычисляем это выражение и подставляем в уравнение ЭК, тогда

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

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

Поскольку $a=-\left(\frac{y_2-y_0}{x_2-x_0}\right)^2$,

$$b=p-2\frac{y_2-y_0}{x_2-x_0}\left(y_0-\frac{x_0(y_2-y_0)}{x_2-x_0}\right),$$

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

то, 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 точки 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 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 находятся координаты точки

$[i+1]P(x_0,y_0)=P(x_0,y_0)+$

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

формулами:

$$x_{i+1}=\frac{\left\{\left[y_0-\frac{x_0(y_i-y_0)}{x_i-x_0}\right]^2-q\right\}}{x_0\cdot x_i}$$ 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 остановится 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 $(4p^3 + 27q^2) \bmod m \neq 0$;

– 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 определения и вычисления параметров 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. Используя формулы Виета для корней многочленов, приведен 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.

Литература

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд. Москва: Гелиос АРВ, 2002. – 480 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва: ТРИУМФ, 2003. – 816 с.
3. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. Г. Математические и комьютерные основы криптологии. ООО «Новое знание» 2003. 381 с.
4. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. Тошкент: «Ўзбекистон маркаси», 2009. 434 бет.
5. Коблиц Н. Курс теории чисел и криптографии. Москва: Научное изд-во ТВП, 2001. 261 с.
6. Умаров Ш. А., Акбаров Д. Е. Разработка нового алгоритма шифрования данных с симметричным ключом // Журнал Сибирского федерального университета. Серия: Техника и технологии. 2016. Т. 9, № 2. С. 214 – 224.
7. Акбаров Д. Е., Умаров Ш. А. Алгоритм хеш-функции с новыми базовыми преобразованиями // Вісник Національного технічного університету України "Київський політехнічний інститут". Серія: Приладобудування. 2016. № 51 (1). С. 100 – 108.
DOI: https://doi.org/10.20535/1970.51(1).2016.78112
8. Акбаров Д.Е., Умаров Ш.А. Новый алгоритм блочного шифрования данных с симметричным ключом // Вісник Національного технічного університету України "Київський політехнічний інститут". Серія: Приладобудування. 2016. № 52 (2). С. 82 – 91.
DOI: https://doi.org/10.20535/1970.52(2).2016.92963
9. Молдавян А. А., Молдавян Н. А. Введение в криптосистемы с открытым ключом. Санкт – Петербург, БХВ-Петербург, 2005. – 288 с.
10. Венбо Мао. Современная криптография. Теория и практика. Москва – Санкт-Петербург – Киев: Лори Вильямс, 2005. 768 с.

УДК 681.3

Д. Е. Акбаров, Ш. А. Умаров

Ферганська філія Ташкентського університету інформаційних технологій імені Мухаммад аль-Харезмі, Фергана, Республіка Узбекистан

ВИБІР ЕЛІПТИЧНОЇ КРИВОЇ ТА БАЗОВОЇ ТОЧКИ ПРИ РОЗРОБЦІ АЛГОРИТМУ ДОДАВАННЯ ЇЇ ТОЧОК З РАЦІОНАЛЬНИМИ КООРДИНАТАМИ НА КІНЦЕВОМУ ПОЛІ

У статті досліджено питання розв’язання задач визначення та обчислення параметрів еліптичної кривої (ЕК) для коректної реалізації асиметричних криптоалгоритмів.

Асиметричні криптографічні алгоритми конструюються на підґрунті розкладання достатньо великого натурального числа на прості множники, дискретного логарифмування на кінцевому полі з достатньо великою характеристикою, додавання точок з раціональними координатами ЕК на кінцевому полі.
Алгоритми на ЕК потребують визначення коефіцієнтів самої кривої, здійснення операції на кінцевому полі характеристикою, бажано простим числом, знаходження базової точки раціональними координатами порядком простого числа, складних обчислень, пов'язаних із специфікою моделі алгоритму.
Наведено умову вибору коефіцієнтів за знаком значення дискримінанта кубічного рівняння для забезпечення ефективності застосування алгоритмів на ЕК. З використанням формул Віета для коренів багаточленів наведено спосіб вибору коефіцієнтів. Зазначено інтервал вибору базової точки. Визначено формули дотичної до базової точки і пошуку координати точки перетину дотичної з ЕК. Отримана рекурентна формула додавання базової точки з іншими точками ЕК з раціональними координатами, яка є узагальненою формулою для додавання будь-яких точок ЕК з раціональними координатами.
Ключові слова: еліптична крива, асиметричний криптоалгоритм, дискримінант, кубічне рівняння, формули Вієта, базова точка, порядок базової точки.

D. E. Akbarov, Sh. Umarov
Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Fergana, Republic of Uzbekistan

THE CHOICE OF AN ELLIPTIC CURVE AND THE BASE POINT IN THE DEVELOPMENT OF AN ALGORITHM FOR ADDING ITS POINTS WITH RATIONAL COORDINATES ON A FINITE FIELD

In article the problems of solving the tasks of determination and calculation the parameters of an elliptic curve (EC) for the correct realization of asymmetric cryptoalgorithms are probed.
Asymmetric cryptographic algorithms are constructed on the basis of the decomposition of a sufficiently large natural number into prime factors, of discrete logarithm on a finite field with a sufficiently large characteristic, of addition of points with rational coordinates EC on a finite field.
The algorithms on the EC require the determination of the coefficients of the curve itself, the operation on the finite field by the characteristic, preferably by a prime number, the finding of a base point by rational coordinates by the order of a prime number, complex calculations related to the specific nature of the algorithm model.
A condition is given for the choice of the coefficients by the sign of the discriminant value of the cubic equation to ensure the efficiency of algorithms application on the EC. Being used by Vieta formulas, for roots of polynoms, it is given a method of a choice of coefficients. The interval of a choice of a basic point is specified.
The formulas of the tangent to the base point and the location 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, which is a generalized formula for the addition of any points of EC with rational coordinates.
Keywords: elliptic curve, asymmetrical cryptoalgorithm, discriminant, cubic equation, Vieta formulas, basic point, order of a basic point.

Надійшла до редакції
23 березня 2018 року

Рецензовано
16 квітня 2018 року

УДК 621: 004.89

АНАЛІЗ МЕТОДІВ ЦИФРОВОЇ ОБРОБКИ ТЕРМОГРАМ

Галаган Р. М., Момот А. С.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
E-mail: rgalagan@ukr.net

Розглянуто актуальне питання підвищення інформативності та достовірності теплового методу неруйнівного контролю. Наведені найбільш перспективні алгоритми цифрової обробки послідовностей термограм. Проведено моделювання процесу активного теплового контролю. Отримана штучна послідовність