УДК 681.3.06

ДЕЛЕНИЕ ТОЧКИ НА ДВА ДЛЯ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

А.В. БЕССАЛОВ

Дано решение обратной удвоению задачи деления точки на два для эллиптических кривых, представленных в форме Эдвардса. Получены оценки сложности операции деления на два в сравнении с удвоением точки. Рассмотрено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме.

Ключевые слова: эллиптическая кривая, форма Эдвардса, удвоение точки, деление точки на два.

ВВЕДЕНИЕ

Наряду с классической групповой операцией удвоения точки эллиптической кривой в задачах криптоанализа и экспоненцирования точек может бать полезным решение обратной задачи: при известных координатах точки 2P найти координаты точки P. Для несуперсингулярных кривых над полями характеристики 2 такая задача рассматривалась в [1]. Замечательным свойством операции деления здесь оказалась предельная простота групповой операции, сводящаяся в одном из приложений к одной операции умножения в поле. Последовательное выполнение операции деления на два практически на порядок ускоряет вычисления.

В данной статье приведено решение обратной удвоению задачи для перспективного класса кривых Эдвардса [2, 3] над простым полем $\mathbf{F}_p$ порядка $p > 2$. Определены условия существования и координаты двух точек деления на два, даны оценки сложности групповой операции в сравнении с операцией удвоения. Рассмотрены приложения операции деления для нахождения порядка случайной точки кривой.

1. ВЫЧИСЛЕНИЕ КООРДИНАТ ТОЧЕК ДЕЛЕНИЯ НА ДВА

Пусть $P = (x_1, y_1)$ и $2P = (a,b)$. Согласно закону удвоения точки кривой Эдвардса

$$E_{ED}: x^2 + y^2 = 1 + dx^2y^2 \tag{1}$$

с параметром $d \neq c^2$ [2, 3] имеем

$$2P = 2(x_1, y_1) = \left(\frac{2x_1y_1}{1+\tilde{d}x_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1-\tilde{d}x_1^2y_1^2}\right) = (a,b). \tag{2}$$

Обозначим $X = x_1^2$, $Y = y_1^2$, $Z = X + Y$. Заменим знаменатели в (2) на $X + Y$ и $2 - X - Y$ соответственно. Возводя первую координату в (2) в квадрат и умножая результат на d, можно получить квадратное уравнение

$$z^2 - \frac{4}{da^2}z + \frac{4}{da^2} = 0$$

с двумя решениями

$$z_{1,2} = \frac{2}{da^2}\left(1 \pm \sqrt{1-da^2}\right). \tag{3}$$

Необходимым условием существования точек деления на 2 является то, что дискриминант $1\text{-}da^2 = A^2$ является квадратичным вычетом поля F_p. В противном случае для некоторой случайной точки точек деления на 2 не существует.

Из равенства для второй координаты в (2) с учетом введенных обозначений получим систему уравнений

$$\begin{gathered}(b\text{-}1)X + (b+1)Y = 2b, \\ X + Y = z_{1,2}.\end{gathered} \tag{4}$$

Отсюда

$$\begin{gathered}X(b) = \frac{1+b}{2}z_{1,2} - b, \\ Y(b) = \frac{1-b}{2}z_{1,2} + b = X(-b).\end{gathered} \tag{5}$$

Здесь выбор одного из решений z_1 или z_2 определяется тем, что значения (5) должны быть квадратами в поле F_p. Значения координат точек деления на два вычисляются извлечением квадратных корней из (5).

При выполнении условия существования точек деления получим две точки $P = (x_1, y_1)$ и $P^* = (-x_1, -y_1)$, которые связаны как $P^* = P + D$, где $D = (0, -1)$ – точка 2-го порядка. При этом, очевидно, $2P = 2P^*$, т. к. $2D = O = (0, 1)$ – нуль группы точек кривой Эдвардса. Заметим также, что порядки точек P^* и P отличаются в 2 раза.

В качестве примера рассмотрим кривую $x^2 + y^2 = 1 + 8x^2y^2 \bmod 13$, которая имеет порядок $N_E = 12$. Пусть $P = (3, 6)$, тогда согласно (2) $2P = (6, 3)$, т.е. $a = 6$, $b = 3$. Ясно, что дискриминант в (3) $1 - da^2 = 12 = 25 \bmod 13$, является квадратичным вычетом, так что $z_{1,2} = 1 \pm 5 = \{6, 9\}$. Из (5) при выборе $z_1 = 6$ получим квадратичные вычеты $X = 9$, $Y = 10$ (выбор $z_2 = 9$ дает невычеты). Извлекая квадратные корни, получаем две точки деления на 2: $P = (3, 6)$ и $P^* = (-3, -6) = P + D$. Другие две точки $(-3, 6)$ и $(3, -6)$, обратные точкам P и P^*, не проходят проверку удвоением, которая дает точку $-2P$. Для этого достаточно вычислить лишь первую координату точки $-2P$, равную $-a$.

2. ОЦЕНКА СЛОЖНОСТИ УДВОЕНИЯ И ДЕЛЕНИЯ ТОЧКИ НА ДВА В АФФИННЫХ КООРДИНАТАХ

Пусть M, S, I, R – полевые операции умножения, возведения в квадрат, инверсии и извлечения квадратного корня. Игнорируя простые операции сложения и вычитания, из (2) после замены знаменателей на $x_1^2 + y_1^2$ и $2 - x_1^2 - y_1^2$ соответственно получим оценку сложности удвоения точки

$$\mathrm{DUBBL} = 2I + M + 2S.$$

Процедура вычисления двух точек деления на 2 согласно (3) – (5) имеет трудоемкость не менее

$$\mathrm{DIV} = I + 4M + S + 3R.$$

Если принять I = 10M, S = 0.7M, R = 4M, DUBBL = 22.4M, DIV = 26.7M, т.е следует ожидать более высоких вычислительных затрат при делении точки на два по сравнению с удвоением. При вычислении скалярного произведения точки эта операция, скорее всего, не дает положительного эффекта (как это имеет место для полей характеристики 2). Вместе с тем эта операция может оказаться полезной при нахождении порядка случайной точки и генератора криптосистемы. Это обсуждается в следующем параграфе.

3. УСЛОВИЕ ДЕЛЕНИЯ ТОЧКИ НА ДВА ДЛЯ ОПРЕДЕЛЕНИЯ ПОРЯДКА СЛУЧАЙНОЙ ТОЧКИ КРИВОЙ ЭДВАРДСА

В криптографических приложениях наиболее приемлемыми являются кривые Эдвардса с минимальным кофактором 4 порядка кривой N_E=4n, где n – достаточно большое простое число. Если порядок генератора P кривой E_{ED} равен Ord$P$ = 4n, то генератор криптосистемы G = 4P имеет порядок Ord$G$ = n. Любая кривая содержит нуль группы O = (0, 1), точку D = (0, –1) второго порядка и точки $\pm Q$ = ($\pm$ 1,0) четвертого порядка. Точки 8-го порядка отсутствуют, поэтому (1 – d) – квадратичный невычет [3].

Утверждение 1. На кривой Эдвардса порядка 4n не существует точек деления на 2 для точек $< P >$ максимального порядка и точек Q четвертого порядка, и существуют – для всех других точек кривой.

Доказательство. Каждой точке kP кривой отвечает скалярный множитель k как элемент кольца целых чисел Z_N операциями по модулю N_E = 4n. Все нечетные элементы кольца, которым соответствуют точки кривой максимального порядка 4n и порядка 4, не делятся на 2 в кольце Z_N. С другой стороны, все четные элементы k = 2s при делении на два по модулю N_E дают два значения s и $s + N_E/2$, удвоение которых дает вновь k = 2s. Возвращаясь к точкам kP кривой, заключаем, что утверждение 1 доказано.

На кривой E_{ED} приблизительно половина всех точек имеет максимальный порядок 4n, четверть точек – порядок 2n, и четверть точек – порядок n. При выборе случайной точки как точки T = (a, b) максимального порядка получим в результате тестирования, что (1 – da^2) является невычетом в поле $\mathbf{F}_p$, после чего генератор криптосистемы определяется как G = 4T. Если же (1 – da^2) является квадратичным вычетом в поле $\mathbf{F}_p$, то порядок точки T равен 2n или n. Удвоение любой из таких точек даст точку G порядка n.

Литература

[1] Бессалов А.В. Метод решения проблемы дискретного логарифмирования на эллиптических кривых путем деления точек на два // Кибернетика и системный анализ, №6, 2001. – С. 50–53.

[2] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007. – PP. 1–20.

[3] Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. – С. 203–208.

Поступила в редколлегию 09.04.2013

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на стр. 277.

УДК 681.3.06

Ділення точки на два для кривої Едвардса над простим полем / Бессалов А.В. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 278–279.

Дано розв'язок оберненої до здвоєння задачі ділення точки на два для еліптичних кривих, які подані у формі Едвардса. Отримано оцінки складності операції ділення на два в порівнянні зі здвоєнням точки. Розглянуто один з додатків властивостей ділення точки на два для визначення порядку точки у криптосистемі.

Ключові слова: еліптична крива, форма Едвардса, здвоєння точки, ділення точки на два.

Бібліогр.: 3 найм.

UDC 681.3.06

Dividing a point by two for the Edwards curve over a simple field / Bessalov A.V. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 278–279.

The solution of an inverse to doubling point-halving problem for elliptic Edwards curves is given. Estimations of complexity of a point-halving operation in comparison with point-doubling are obtained. One of the applications of properties of a point-halving divisibility to define a point order in a cryptosystem is considered.

Keywords: elliptic curve, Edwards form, point doubling, point halving.

Ref.: 3 items.