УДК 681.3.06

Бессалов А.В., Третьяков Д.Б.

УДВОЕНИЕ ТОЧКИ И ОБРАТНАЯ ЗАДАЧА ДЛЯ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Получено решение обратной удвоению задачи 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: криптография, изоморфизм, кривая Эдвардса.

Введение

В современной криптографии на эллиптических кривых большой интерес вызвала изоморфная каноническим кривым 3-й степени форма кривых 4-й степени, изучавшаяся еще Абелем в начале 19-го столетия. В научном мире она названа формой Эдвардса, американського професора университета Нью-Йорка, обнаружившего свойство изоморфизма этих кривых классическим эллиптическим кривым и доказавшего ряд теорем [1]. Специалисты-криптографы сразу взялись за исследование свойств кривых Эдвардса [3]. Имея такие несомненные преимущества, как выигрыш в скорости вычислений, универсальность закона сложения точек, наличие аффинной точки, являющейся нейтральным элементом абелевой группы, кривые Эдвардса можно считать достойной альтернативой кубическим эллиптическим кривым.

В задачах криптоанализа и экспоненцирования точек эллиптической кривой может оказаться полезным решение задачи, обратной удвоению точки: при известных координатах точки $2P$ найти координаты точки P, что определяется как деление точки на два. Для несуперсингулярных кривых над полями характеристики 2 такая задача рассматривалась одним из авторов в [2]. 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 точки на два для несуперсингулярных кривых над полем F_2 практически на порядок ускоряет вычисления.

В настоящей статье получено решение обратной удвоению задачи для перспективного класса кривых Эдвардса [3,4] 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. Несмотря на отсутствие выигрыша в производительности операция деления точки на два может найти применение при нахождении общесистемных параметров криптосистемы, вычислении скалярного произведения и решении проблемы дискретного логарифмирования на эллиптической кривой. Рассмотрены приложения операции деления на два для нахождения порядка случайной точки кривой.

1. Вычисление координат точек деления на два для кривой Эдвардса

Будем полагать, что известны координаты точки $2P$. Требуется найти координаты двух точек: P и $P^* = P + D$, удвоение которых дает одинаковый результат $2P$ (здесь D – точка второго порядка, такая, что $2D = O$, где O – нейтральный элемент абелевой группы точек). Важной особенностью кривых Эдвардса является то, что точка на бесконечности O канонической эллиптической кривой здесь заменяется точкой $O = (0,1)$ с аффинными координатами.

Пусть точка $P = (x_1, y_1)$ и $2P = (a,b)$. Согласно универсальному закону сложения-удвоения точки кривой Эдвардса E_{ED}:

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

над полем характеристики $p \neq 2$ [3,4] с параметром $d \neq c^2$ и $d \neq 1$ [3, 4] имеем

$$2P = 2(x_1, y_1) = \left(\frac{2x_1y_1}{1+dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1-dx_1^2y_1^2}\right) = (a, b). \tag{2}$$

Введем обозначения: $X = x_1^2$, $Y = y_1^2$, $Z = X + Y$. Заменим знаменатели в (2) на $X + Y$ и $2 – X – Y$ соответственно. Возводя первую координату в (2) в квадрат и умножая результат на d, с учетом (1) можно получить квадратное уравнение

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

с двумя решениями

$$Z_{1,2} = \frac{2}{da^2}(1 \pm \sqrt{1 - da^2}). \quad (3)$$

Необходимым условием существования точек деления на 2 является то, что дискриминант $1 - da^2 = A^2$ 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

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

Отсюда

$$X(b) = \frac{1+b}{2}Z_{1,2} - b, \quad Y(b) = \frac{1-b}{2}Z_{1,2} + b = X(-b) \quad (5)$$

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, $2P = 2P^*$, так как $2D = O = (0, 1)$ – 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

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

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

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

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 криптоанализе, а также 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 две точки $\pm Q$ = (± 1,0) четвертого порядка. Точки 8-го порядка отсутствуют, поэтому $(1 - d)$ – квадратичный невычет [4].

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. Иными словами, элемент 2 в кольце не имеет мультипликативно обратного. 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. Таким образом, для нахождения генератора G порядка n случайная точка $T = (a, b)$ проходит тест на делимость на два, после чего умножается на 2 (если $(1 - da^2)$ – квадратичный вычет), или на 4(если $(1 - da^2)$ – квадратичный невычет).

Метод деления точки на два может использоваться и для решения DLP [2]. Здесь важно заметить, что последовательное деление на два в группе <G> с отбором точки деления порядка n могло бы привести к краху DLP, если удастся определить четность (нечетность) числа k точки kP. Для этого достаточно при нечетных k вычитать точку P из предыдущего результата, после чего повторять процедуру делений-вычитаний. Пока, однако, эта проблема не решена, и эллиптические кривые остаются безопасными с экспоненциальной сложностью.

ЛИТЕРАТУРА

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
2. 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.
3. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.
4. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

Надійшла: 10.12.2013р Рецензент: д.т.н., проф. Толюпа С.В.