УДК 681.3.06

Бессалов А.В., Дихтенко А.А., Третьяков Д.Б.

Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем

Введение

В работе профессора университета Нью-Йорка Г. Эдвардса [1] предложена нормальная форма представления эллиптических кривых, которая изучалась еще Абелем в 1828 году. Эта форма, получившая в научном мире название формы Эдвардса, обладает рядом замечательных свойств для криптографических приложений. Одной из первых публикаций в развитие этого направления следует отметить работу [2]. Оказалось, что наряду с симметрией, свойствами полноты и универсальности закона сложения, заменой точки на бесконечности аффинной точкой (нуль группы), кривые Эдвардса среди известных являются наиболее производительными: в проективных координатах групповая операция выполняется минимальным числом 10M + 1S + 1U операций в поле (M - умножение, S – возведение в квадрат, U – умножение на параметр кривой). В настоящей работе мы даем детальный сравнительный анализ вычислительной сложности групповой операции в проективных координатах для кривых в форме Эдвардса и канонической эллиптической кривой над полем характеристики, не равной 2 и 3.

1. Сложность групповой операции для кривой Эдвардса

В наиболее общем виде кривая Эдвардса над конечным полем F_q ($q = p^m$) характеристики $p > 3$ может быть выражена как [2]

$$E_{ED}: \quad x^2 + y^2 = c^2\left(1 + \tilde{d}\, x^2 y^2\right), \quad \tilde{d} = c^{-4}d,\ \tilde{d}(1 - \tilde{d}c^4) \neq 0,\ \tilde{d} \neq A^2. \quad (1)$$

Закон сложения двух точек этой кривой имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{c(1 + \tilde{d} x_1 x_2 y_1 y_2)},\ \frac{y_1 y_2 - x_1 x_2}{c(1 - \tilde{d} x_1 x_2 y_1 y_2)}\right). \quad (2)$$

Варьирование параметра c дает изоморфные кривые, поэтому с точностью до изоморфизма можно полагать $c = 1$, $\tilde{d} = d$. Наличие 2-х инверсий в (2) заставляет обращаться к проективным координатам [4]. Введем третью координату Z как общий знаменатель в (2). Полагаем $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, тогда гомогениосное уравнение кривой (1) в проективных координатах имеет вид

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2 .$$

Сумма двух точек теперь записывается как $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$. С учетом подстановок выразим координаты суммарной точки согласно (2)

$$x_3 = \frac{X_3}{Z_3} = \frac{\left(\frac{X_1Y_2}{Z_1Z_2} + \frac{X_2Y_1}{Z_1Z_2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{{Z_1}^2{Z_2}^2}\right)}{\left(1 + d\frac{X_1X_2Y_1Y_2}{{Z_1}^2{Z_2}^2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{{Z_1}^2{Z_2}^2}\right)} =$$

$$= \frac{Z_1Z_2\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)(X_1Y_2 + X_2Y_1)}{\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right)\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)}$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}$$

Обозначим:

$$A = Z_1Z_2;\ B = A^2;\ C = X_1X_2;\ D = Y_1Y_2;\ E = dCD;\ F = B - E;\ G = B + E$$

Тогда

$X_3 = A{\cdot}F{\cdot}\ ((X_1 + Y_1){\cdot}(X_2 + Y_2) - C - D)$,

$Y_3 = A{\cdot}G{\cdot}(D - C)$,

$Z_3 = F{\cdot}G$.

Игнорируя простую операцию сложения (вычитания) в поле, находим сложность вычисления суммы различных точек V_{ED} = 10M + 1S + 1U. Заметим, что сложность возведения в квадрат оценивается приблизительно как $1S \cong \frac{2}{3}M$ [2].

Нетрудно подобным же образом определить сложность удвоения точки как W_{ED} = 3M + 4S. Экономия в вычислениях здесь достигается заменой согласно (1) знаменателей в (2) $(1 + dx_1^2y_1^2)$ на $(x_1^2 + y_1^2)$, а $(1 - dx_1^2y_1^2)$ – на $(2 - (x_1^2 + y_1^2))$.

2.Сложность групповой операции для канонической кривой

Обратимся теперь к канонической эллиптической кривой над полем F_q

E: $y^2 = x^3 + ax + b$,

с законом сложения различных точек [4]

$$(x_1, y_1) + (x_2, y_2) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\ , - y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_1)\ \right)$$

В проективных координатах с заменой $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ имеем

$$\frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}} = \frac{u}{v}. \quad u = Y_2Z_1 - Y_1Z_2, \qquad v = X_2Z_1 - X_1Z_2.$$

Тогда

$$\frac{X_3}{Z_3} = \left(\frac{u}{v}\right)^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2} = \frac{Z_1Z_2u^2 - v^2(X_1Z_2 + X_2Z_1)}{Z_1Z_2v^2} = \frac{vg}{Z_3},$$

где

$$Z_3 = Z_1Z_2v^3, \qquad g = Z_1Z_2u^2 - v^3 - 2v^2X_1Z_2.$$

Далее

$$\frac{Y_3}{Z_3} = -\frac{Y_1}{Z_1} + \left(\frac{u}{v}\right)\left(\frac{X_1}{Z_1} - \frac{vg}{Z_1Z_2v^3}\right) = \frac{-Y_1Z_2v^3 + u(X_1Z_2v^2 - g)}{Z_1Z_2v^3}$$

Итак, имеем

$$X_3 = vg,$$
$$Y_3 = -Y_1Z_2v^3 + u(X_1Z_2v^2 - g),$$
$$Z_3 = Z_1Z_2v^3.$$

Расчет числа операций дает сложность вычисления суммы точек канонической кривой E V_E = 12M + 2S. Аналогичный расчет для удвоения точек приводит к результату [4] W_E = 7M + 5S.

2. Сравнение сложности вычислений для кривых E_{ED} и E

Принимая вычислительную сложность возведения в квадрат 1S = 0.67M, а умножения на параметр кривой 1U = 0.5M, получим оценки сложности сложения и удвоения на кривой Эдвардса V_{ED} = 11.17M, W_{ED} = 3M + 4S= 5.68M. Удвоение, как видим, практически вдвое быстрее сложения. Для канонической эллиптической кривой имеем V_E = 13.33M, W_E = 10.35M. В среднем кривые Эдвардса обеспечивают выигрыш в производительности в $\gamma = (V_E + W_E)/(V_{ED} + W_{ED}) = 1.41$ раза.

При вычислении скалярного произведения rQ точки Q число r представляется в двоичной форме, тогда работает алгоритм последовательного сложения-удвоения, а приведенный результат для γ справедлив при равновероятных 0 и 1 в числе r. Пусть ν_0 – относительная частота знаков 0 в

двоичной последовательности r, $(1 - \nu_0)$ – относительная частота знаков 1, тогда в более общей форме выигрыш

$$\gamma = \frac{v_0 W_E + (1-v_0)V_E}{v_0 W_{ED} + (1-v_0)V_{ED}} = \frac{10.35v_0 + 13.33(1-v_0)}{5.68v_0 + 11.17(1-v_0)}.$$

При преобладании знаков 0 в числе r, например, со значением $\nu_0 = 0.75$, получаем выигрыш $\gamma = 1.573$. В пределе для числа $r = 2^m$ максимальный выигрыш достигает значения $\gamma_{max} = 1.82$. Это ясно, так как удвоение выполняется гораздо быстрее сложения точек. При преобладании единиц в последовательности r результат будет обратным. В частности, при $r = 2^m - 1$ минимальный выигрыш равен $\gamma_{min} = 1.193$. Заметим, что приведенные результаты относительно нижней границы γ в некоторой степени условны, так как мы приняли 1U = 0.5M. В частных случаях параметр d, использующийся при вычислении сложения точек, может принимать малые значения, тогда величиной 1U вообще можно пренебречь (при этом $\gamma_{min} = 1.249$).

В заключение резюмируем, что кривые Эдвардса имеют неоспоримые преимущества как перед каноническими эллиптическими кривыми, так и перед другими известными изоморфными формами кривых [5]. Главные из них – быстродействие и удобство программирования. Хотя класс этих кривых приблизительно в 4 раза уже класса всех кривых, их применение в криптосистемах перспективно.

Поправка к расчетам

В формуле для γ ошибка: удвоение на каждом шаге вычисления осуществляется всегда, а сложение – только при знаках 1 двоичного представления числа k точки kP. Если ν_1 – относительная частота знаков 1, то получим

$$\gamma = \frac{W_E + v_1 V_E}{W_{ED} + v_1 V_{ED}} = \frac{10.35 + 13.33v_1}{5.68 + 11.17v_1}$$

Отсюда максимальный выигрыш при $\nu_1 \to 0$ равен $\gamma_{max} = 1.82$, а минимальный при $\nu_1 \to 1$ равен $\gamma_{min} = 1.41$. Тогда средний выигрыш при $\nu_1 = 0.5$ равен 1.51

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. 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. Bernstein Daniel J., Lange Tanja, Farashahi R.R. Binary Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2008, PP.1..23.

4. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

5. Daniel J. Bernstein, Tanja Lange, Explicit-formulas database (2007). hyperelliptic.org/EFD.

Опубликовано: Сучасний захист інформації. №4, 2011. – с.33 – 36.