УДК 681.3.06

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

Оценка реальной стойкости криптосистемы на кривой Эдвардса над расширениями малых полей

Рассмотрены элементы арифметики кривых Эдвардса над расширениями степени m малых полей характеристики $p > 3$, с возможностью формирования 4-х законов сложения точек. Предложена модификация метода расчета квадратного корня в поле F_p^m. Дана оценка незначительных потерь сложности порядка $\sqrt{2m}$ проблемы дискретного логарифмирования на кривой, связанных с классами эквивалентности кривой.

Введение

В перспективе значительная часть эллиптической криптографии может быть успешно переведена с классической канонической формы кривых к изоморфным кривым в форме Эдвардса [1, 2]. Эта бисимметричная форма кривой (с двойной симметрией точек относительно осей x и y), кроме универсальности закона сложения точек, простоты программирования и наличием координат нулевой точки группы, обладает рекордной на сегодня производительностью [2, 5] и выигрышем в скорости вычислений приблизительно в полтора раза. Не очень весомым ограничением этого класса кривых является обязательное наличие одной точки 2-го порядка и двух точек 4-го порядка, при этом порядок наилучшей кривой $N_E = 4n$ содержит минимальный кофактор 4 (при простом n).

В известных стандартах эллиптических криптосистем кривые с порядком $4n$ встречаются лишь среди кривых над расширенными полями F_2^m. Для кривых Эдвардса над полями F_p^m при $p > 3$ приходится заново решать задачу поиска кривых приемлемого порядка. В авторской работе [3] предложен простой путь нахождения кривой Эдвардса почти простого порядка $4n$. По аналогии с кривыми Коблица над полями характеристики 2, в работе найдены две кривые Эдвардса минимального порядка $N_{E1} = 4$ над малыми простыми полями F_5 и F_7, после чего рассчитаны порядки этих кривых над расширениями степени m этих полей с последующей селекцией при простых степенях m подходящего почти простого порядка $4n$. В результате были определены и табулированы порядки нескольких кривых в области криптографических приложений.

Применение эндоморфизма Фробениуса к точкам кривой над расширениями простых полей порождает классы эквивалентности [6], ведущие к незначительному снижению стойкости криптосистемы. В настоящей работе

дана оценка потерь стойкости предложенных в [3] кривых с учетом атаки на классы эквивалентности, пропорциональная $\sqrt{m}$.

Арифметика кривых Эдвардса

С точностью до изоморфизма кривая Эдвардса с одним параметром d над конечным полем характеристики $p \neq 2$ задается аффинным уравнением

$$x^2 + y^2 = (1 + dx^2y^2),\ d(1-d) \neq 0,\ d \neq A^2,\ \ x, y, d \in \mathrm{F}_p{}^m \qquad (1)$$

Все точки (x, y) кривой как решения уравнения (1) всегда содержат следующие 4 точки: O = (0, 1), D = (0,–1), $F1$ = (–1, 0), $F2$ = (1, 0). Других точек на осях x, y не существует. Число всех точек N_E кривой называют ее порядком. Координаты x, y точек как элементы поля $\mathrm{F}_p{}^m$ в общем случае являются m-мерными векторами (или полиномами) с компонентами из основного поля F_p (они могут быть также элементами подполей поля $\mathrm{F}_p{}^m$).

Если закон сложения точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ задать как $R = P + Q = (x_3, y_3)$, где

$$(x_3, y_3) = \left(\frac{x_1y_2 + x_2y_1}{1+dx_1x_2y_1y_2},\ \frac{y_1y_2 - x_1x_2}{1-dx_1x_2y_1y_2}\right), \qquad (2)$$

то точка O является нулем абелевой группы точек, точка D – точкой 2-го порядка, а точки $F1$ и $F2$ – точками 4-го порядка. В силу двойной симметрии можно изменить расположение этих 4-х точек поворотом на углы, кратные $\frac{\pi}{4}$, для чего следует трансформировать закон сложения (2). Например, принимая вместо (1)

$$(x_3, y_3) = \left(\frac{x_1x_2 - y_1y_2}{1-dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1+dx_1x_2y_1y_2}\right),$$

и нуль группы как O = (1,0), получим $(x_1, y_1) + (1, 0) = (x_1, y_1)$. Соответственно разворачиваются на угол $\frac{\pi}{4}$ и точки 2-го и 4-го порядков. Подобным образом можно представить 4 формы для закона сложения точек с различными определениями точки O. Важно то, что вместо не имеющей аффинных координат точки на бесконечности для канонических эллиптических кривых мы здесь имеем точку O с координатами в простом поле.

Следуя универсальному закону сложения (2), обратная точка определяется с вертикальной симметрией как $–P = (–x_1, y_1)$, при этом $P + (–P) = (0,1) = O$. Напомним, для канонических кривых обратная точка симметрична точке P относительно горизонтальной оси x. На линиях $|y| = |x|$ могут лежать точки 8-го порядка (если они существуют [4]). Каждая точка не 8-го порядка (x, y) с ненулевыми координатами порождает семейство из 8 точек $(\pm x, \pm y)$, $(\pm y, \pm x)$,

связанные между собой точками O или 2-го или 4-го порядков. К примеру, сумма *взаимных* точек $(x, y) + (y, x) = (1,0) = F2$.

Программное обеспечение операций на кривой содержит арифметику нижнего уровня (полевые операции сложения, умножения, экспоненцирования, инверсии) и верхнего уровня (сумма и удвоение точек, скалярное произведение kG). После нахождения приемлемого порядка $4n$ кривой (см. [3]) нетривиальной задачей является определение точки $G = (x_0, y_0)$ – генератора криптосистемы простого порядка n.

В качестве иллюстрации рассмотрим кривую $x^2 + y^2 = 1 + 3x^2y^2$ в расширении F_5^5 степени $m = 5$ с порядком $N_E = 4n$, $n = 761$ [3]. Примитивный полином в этом случае можно найти в [7], выберем $f(z) = z^5 + 4z + 2$ (его корень α имеет порядок $5^5 - 1$). При случайном выборе x из уравнения (1) находим $y^2 = (1 - x^2) \cdot (1 - 3x^2)^{-1}$, после чего, полагая $a = y^2$, надо найти квадратный корень $y = \sqrt{a}\ mod(5^5 - 1)$. Его можно найти методом экспоненцирования [6]. Имеем $p = 5 \equiv 1 \bmod 4$, $q = 5^5 \equiv 5 \bmod 8$. В мультипликативной группе поля F_q, если $a = y^2$ – квадратичный вычет, элементы подгруппы F_5^* можно выразить

$$a^{\frac{q-1}{2}} = 1, \quad a^{\frac{q-1}{4}} = -1 = \delta, \quad \delta^{\frac{1}{2}} = \pm 2,$$

тогда

$$a = \delta a \cdot a^{\frac{q-1}{4}} = \delta \cdot a^{\frac{q+3}{4}} \quad \Rightarrow \quad y = \delta^{\frac{1}{2}} \cdot a^{\frac{q+3}{8}}.$$

Принимая $x = \alpha^7 = 01300$, получим $y = 03342$ (младший разряд – справа). Подстановка этих координат в (1) дает тождество. Скалярное умножение этой точки $P = (x, y)$ на число $n = 761$ дает точку 4-го порядка, поэтому искомый генератор $G = (x_0, y_0) = 4P$, $x_0 = 11321, y_0 = 22310$. При проверке получаем $nG = O$.

Эндоморфизм Фробениуса точек кривой и оценка стойкости

Известным свойством для операций в поле F_p^m является равенство $(a + b)^p = a^p + b^p$ [7]. Для каждой точки кривой $Q = (x, y)$ отображение $\varphi(Q) = (x^p, y^p)$ определяется как *эндоморфизм Фробениуса*, причем $\varphi(\varphi(Q)) = \varphi^2(Q) = (x^{p^2}, y^{p^2})$, и т.д. Элементы поля x, x^p, $x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$ называют *сопряженными*, их число при простых степенях m расширений поля равно m. Возводя последовательно уравнение (1) в степени p, p^2, p^3 и т.д., с учетом равенства $d^p = d$, мы видим, что эндоморфизм Фробениуса отображает любую точку кривой Эдвардса в различные точки этой же кривой, образующие *класс эквивалентности* объема m.

Так как отображение $\varphi(Q)$ порождает точку того же порядка, как у точки Q, можно записать равенство $\varphi(Q) = \lambda Q$ при некотором единственном целом λ. Отсюда следует: $\varphi^2(Q) = \lambda^2 Q$, $\varphi^3(Q) = \lambda^3 Q$, …, $\varphi^{m-1}(Q) = \lambda^{m-1} Q$, причем $\varphi^m(Q) = \lambda^m Q = Q$. Если порядок $\mathrm{Ord}Q = \mathrm{Ord}G = n$, то порядок λ как элемента мультипликативной группы поля F_n равен m , и, таким образом, $m|(n-1)$. Следовательно, можно без труда найти один из элементов поля F_n порядка m (как $a^{\frac{n-1}{m}}$ при примитивном элементе a), тогда при простом m все степени этого элемента дают элементы подгруппы порядка m, которые совпадают с элементами $\{1, \lambda, \lambda^2, \lambda^3, \ldots, \lambda^{m-1}\}$.

Для точек порядка n эндоморфизм Фробениуса удовлетворяет уравнению [6]

$$\varphi^2(Q) - t\varphi(Q) + pQ = nQ = O,$$

которому, в свою очередь, отвечает характеристическое уравнение

$$\lambda^2 - t\lambda + p = 0 \bmod n . \qquad (3)$$

Здесь t – след уравнения Фробениуса точек кривой над основным полем F_p, равный в приведенном выше примере $t = 2$ для кривой Эдвардса над полем F_5. Возвращаясь к этому примеру, при $p = 5$ и $n = 761$ получим решение уравнения (3) $\lambda = 684$. В поле F_{761} $\mathrm{Ord}\lambda = m = 5$, степени λ^i, $i = 0\ldots4$, равны {1, 684, 602, 67, 168}. Подгруппа точек класса эквивалентности для точки G включает точки:

$G = (11321, 22310)$,

$\varphi(G) = \lambda G = (13102, 21441)$,

$\varphi^2(G) = \lambda^2 G = (10203, 20113)$,

$\varphi^3(G) = \lambda^3 G = (12102, 24432)$,

$\varphi^4(G) = \lambda^4 G = (14331, 23312)$.

Число различных классов эквивалентности для подгруппы точек $<G>$ порядка n равно $(n-1)/m$. Так как внутри классов эквивалентности точки связаны легко рассчитываемыми соотношениями, экспоненциальная сложность решения *проблемы дискретного логарифмирования* (DLP) полным перебором снижается с $O(n)$ до $O(n/m)$, а с учетом обратных точек – до $O(n/2m)$. Наиболее эффективный на сегодня ρ-метод Полларда решения DLP понижает сложность от $O(\sqrt{n})$ [6] до $O(\sqrt{n/2m})$. Это сравнительно небольшое снижение стойкости криптосистем. Например, при $p = 5$ и $m = 181$ потеря стойкости составляет величину $\sqrt{362} \cong 19 \cong 4$ бит при $\sqrt{n} \cong \sqrt{5^{181}} \cong 210$ бит.

Вместе с тем заметим, что увеличение характеристики поля p по сравнению с полем характеристики $p = 2$ ведет к сравнительному снижению потерь стойкости за счет классов эквивалентности. Действительно, при равной стойкости и равенстве $5^{181} \cong 2^{420}$ потери стойкости для поля $F_2{}^m$ составят $\sqrt{840} \cong 29 \cong 5$ бит. Ясно, что с ростом p и m разница в этих незначительных потерях нарастает.

Вообще говоря, вопрос о снижении стойкости кривых Эдвардса над расширением малых полей можно считать спорным. Для кривых над большими простыми полями, где нет этой слабости, точно так же можно предвычислениями найти некоторое ограниченное ресурсами памяти число опорных точек-маркеров k_iG, которые будут полезны аналитику для снижения сложности DLP. Это выравнивает условия для криптоанализа кривых над расширениями малых полей и кривых над простыми полями.

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. Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей. Прикладная радиоэлектроника, Том 11, №2, 2012. С.225-227.
4. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника №167, 2011. С.203-208.
5. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. – с.33 – 36.
6. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.
7. Лидл Р., Нидеррайтер Г. Конечные поля. Т.2. – М.: Мир, 1988. – 822с.

Опубликовано: Сучасний захист інформації, №2, 2012. С. 17-20