УДК 681.3.06

Кривые Эдвардса почти простого порядка над расширениями малых простых полей

Бессалов А.В., Гурьянов А.И., Дихтенко А.А.

В задаче поиска приемлемых для криптографии кривых Эдвардса предложен подход, состоящий в построении кривой минимального порядка 4 над малыми полями F_5 и F_7 с последующим простым расширением этих полей. Найдены 5 кривых, которые можно рекомендовать в проектируемых криптосистемах.

Введение

Традиционные асимметричные криптосистемы на эллиптических кривых свыше десятилетия успешно применяются на основе действующих национальных и международных стандартов [5]. Вечные поиски более совершенных алгоритмов привели в последние годы к замечательной альтернативе канонической формы кривых – кривым в форме Эдвардса [1 – 4]. Главные их достоинства: рекордная производительность и простота программирования. Вместе с тем кривые Эдвардса пока не стандартизированы, для них необходимо инициировать поиск кривых с почти простым порядком $N_E = 4n$, где n – простое число. Минимальный кофактор 4 в порядке кривой связан с наличием в любой такой кривой двух точек 4-го порядка. Нетрудно ограничением на параметр d кривой исключить точки 8-го порядка [3], но в общем случае для поиска подходящих кривых Эдвардса придется адаптировать известные алгоритмы SEA или Satoh [5].

В настоящей работе предлагается наиболее простой путь нахождения кривой Эдвардса почти простого порядка $4n$. Наподобие с кривыми Коблитца над полями характеристики 2, мы предлагаем найти две кривые Эдвардса минимального порядка $N_{E1} = 4$ над малыми простыми полями F_5 и F_7 , после чего найти порядки этих кривых над расширениями степени m этих полей с последующим отбором при простых m подходящего почти простого порядка $4n$. В результате нами были определены несколько кривых в области криптографических приложений.

Поиск кривых Эдвардса почти простого порядка и результаты

Форма кривых Эдвардса над конечными полями характеристики $p > 3$ имеет вид

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

Здесь все множество различных значений параметра c дает изоморфные кривые, поэтому можно принять с = 1, $\tilde{d} = d$, тогда различные кривые Эдвардса определяются лишь одним параметром d в уравнении

$$x^2 + y^2 = (1 + dx^2y^2), \qquad d(1 - d) \neq 0, \;\; d \neq A^2. \tag{1}$$

Пусть кривая определена над полем F_5, здесь допустимыми значениями параметра d являются квадратичные невычеты 2 и 3. Они являются мультипликативно обратными, поэтому образуют пару кривых кручения. Границы Хассе $p + 1 \pm 2\sqrt{p}$ при p = 5 лежат в интервале 2…10, в пределах которого для кривых Эдвардса допустимы лишь 2 значения порядка N_E кривой, равные 4 и 8. Согласно утверждению 1 в [3] точка 8-го порядка существует, если $1 - d$ – квадратичный вычет, и не существует в противном случае. При d = 2 значение $(1 - d)$ = 4mod5 – квадратичный вычет, и соответствующая кривая имеет порядок 8. При d = 3 значение $(1 - d)$ = 3mod5 – квадратичный невычет, и соответствующая кривая имеет порядок 4. Она содержит обязательные 4 точки всех кривых Эдвардса $(0, \pm 1)$, $(\pm 1, 0)$ при c = 1.

Итак, мы принимаем d = 3, тогда из $N_{E1} = p + 1 - t_1 = 4$ след уравнения Фробениуса t_1 = 2. Рассчитаем порядки кривых над расширениями $F_p{}^m$ по известной формуле [5]

$$N_{Em} = p^m + 1 - t_m, \tag{2}$$

где для определения параметра t_m воспользуемся рекуррентной зависимостью

$$t_m = t_1\, t_{m-1} - pt_{m-2}\,, \;\; m = 2, 3, \ldots, \;\; t_0 = 2. \tag{3}$$

Результаты расчетов по формулам (2), (3) с отбором простых значений $n = N_{Em}/4$ приведены в таблице 1. Во второй колонке таблицы даны округленные значения для длины модуля поля m_b = $m$logp/log2 в битах. Тестирование числа n на простоту с помощью алгоритма Миллера-Рабина осуществлялось специальной прикладной программой.

В границах Хассе имеется еще одна кривая с минимальным порядком $N_{E1} = p + 1 - t_1 = 4$ при p = 7 и t_1 = 4. Она также имеет параметр d = 3, который является квадратичным невычетом в поле F_7, причем $1 - d$ = 5 – тоже невычет. Почти простые порядки этой кривой над расширениями $F_7{}^m$, рассчитанные с помощью (2), (3), даны в таблице (2).

p = 5 Таблица 1

m	m_b	$n = N_{Em}/4$
3	7	37
5	11	761
17	39	190734426721
47	109	177635683940025049111870902558317
53	123	27755575615628913519432138978855094 01
181	420	81566305849981556583878676365706844446264553225862081846982955622470058935583394181280598166864036391710622583401627348551324 1
227	527	11591269220898191830411672692336373479273639933618096882665747059117441687798840670250687806029382008026655960498496355087266800506918498606995903214468432291 7
353	819	13625471488026082303712171891991388314389109549794181122960160293908508251985766836112118027927542086233890704552817681219819158519647915156383473783742883700653042365583720331179910890621621002009304697009015594466023580409118149203179025776784 01

$p = 7$ Таблица 2

m	m_b	$n = N_{Em}/4$
5	14	4261
7	19	205759
17	47	58157621574673
43	120	5459535939979491492246532674488972 83
47	132	1310834579189075908634545043798558782183
127	356	5313627311420041771108259577647405608329845418409996270259916002240165733248795639934133379678813039875435 9
223	626	7158185222694162293329973741165919793298110441517376345166152707319559892792401780383939607571148856774258554873765716518606020812820444545621959754591269503845751314733544709671638352603 9

Приходится констатировать, что наши априорные ожидания достаточно большого числа приемлемых для криптографии кривых Эдвардса над расширениями малых простых полей характеристики p > 3 не подтвердились. Как следует из таблиц 1 и 2, в границах стандартных требований к порядку генератора криптосистемы и близким к нему расширением $2^{mb}(m_b \cong 180 \ldots 600)$ мы нашли всего 3 кривые Эдвардса: 2 кривые над полем $F_5{}^m$ со степенями $m = 181$ и $m = 227$, и одну кривую над полем $F_7{}^m$ со степенью $m = 127$. К ним, правда, можно добавить еще 2 кривые с завышенным уровнем стойкости и значением $m_b > 600$ (со временем он перестанет быть завышенным).

Следует заключить, что найденные кривые с минимальным и простым значением параметра $d = 3$ обеспечат при заданной стойкости наивысшую скорость вычислений групповых операций. В операции сложения разных точек мы экономим на одной полевой операции умножения 1U на параметр кривой [4], так как умножение на 3 заменяется трехкратным сложением в поле, т.е.

практически бесплатной операцией. Арифметика вычислений в расширениях малых полей часто эффективней арифметики в простых полях большой характеристики. Полагаем, что найденные кривые можно рекомендовать как для проектов будущих стандартов, так, возможно, и для использования в криптопротоколах уже сегодня.

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. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника №167, 2011. С.203-208.
4. 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.
5. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

Опубликовано: Прикладная радиоэлектроника, том 11, №2, 2012. С.225-227