

## КРИВЫЕ ЭДВАРДСА ПОЧТИ ПРОСТОГО ПОРЯДКА НАД РАСШИРЕНИЯМИ МАЛЫХ ПРОСТЫХ ПОЛЕЙ

А.В. БЕССАЛОВ, А.И. ГУРЬЯНОВ, А.А. ДИХТЕНКО

В задаче поиска криптостойких 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 порядки 5 кривых, которые можно рекомендовать в будущих стандартах и проектируемых криптосистемах.

*Ключевые слова:* эллиптические кривые, кривые Эдвардса, порядок кривой, порядок точки, простое поле, расширенное поле.

### 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 Коблицца 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

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

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

$$x^2 + y^2 = (1 + dx^2y^2), \\ d(1 - d) \neq 0, d \neq A^2. \quad (1)$$

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  $(1-d) = 4 \pmod{5}$  — квадратичный вычет, и соответствующая кривая имеет порядок 8. При  $d=3$  значение  $(1-d) = 3 \pmod{5}$  — 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]

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

где для определения параметра  $t_m$  воспользуемся рекуррентной зависимостью

$$t_m = t_1 t_{m-1} - p t_{m-2}, \\ m = 2, 3, \dots, t_0 = 2. \quad (3)$$

Результаты расчетов по формулам (2), (3) с отбором простых значений  $n = N_{Em}/4$  приведены в табл. 1. Во второй колонке таблицы даны округленные значения для длины модуля поля  $m_b = m \log p / \log 2$  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 табл. 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	2775557561562891351943213897885509401
181	420	815663058499815565838786763657068444462645532258620818469829556224700589355833941812805981668640363917106225834016273485513241
227	527	115912692208981918304116726923363734792736399336180968826657470591174416877988406702506878060293820080266559604984963550872668005069184986069959032144684322917
353	819	1362547148802608230371217189199138831438910954979418112296016029390850825198576683611211802792754208623389070455281768121981915851964791515638347378374288370065304236558372033117991089062162100200930469700901559446602358040911814920317902577678401

$p = 7$

Таблица 2

$m$	$m_b$	$n = N_{Em}/4$
5	14	4261
7	19	205759
17	47	58157621574673
43	120	545953593997949149224653267448897283
47	132	1310834579189075908634545043798558782183
127	356	53136273114200417711082595776474056083298454184099962702599160022401657332487956399341333796788130398754359
223	626	71581852226941622933299737411659197932981104415173763451661527073195598927924017803839396075711488567742585548737657165186060208128204445456219597545912695038457513147335447096716383526039

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  $2^{m_b}$  ( $m_b \cong 180...600$ ) 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, вып. 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. – 224 с.

Поступила в редколлегия 30.03.2012



**Бессалов Анатолий Владимирович**, доктор технических наук, профессор, профессор кафедры ММЗИ ФТИ НТУУ «КПИ». Область научных интересов: криптография, теория корректирующего кодирования.



**Гурьянов Александр Игоревич**, выпускник лицея №38 им. В.М. Молчанова гор. Киева. Область научных интересов: асимметричная криптография.



**Дихтенко Алиса Анатольевна**, аспирант кафедры теории упругости и вычислительной математики Донецкого национального университета. Область научных интересов: асимметричная криптография.

УДК 681.3.06

**Криві Едвардса майже простого порядку над розширеннями малих простих полів / А.В. Бессалов, О.І. Гурьянов, А.А. Діхтенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 225–227.**

У задачі пошука криптостійких кривих Едвардса запропоновано підхід, що полягає в побудові кривої мінімального порядку 4 над малими полями  $F_5$  і  $F_7$  з наступним простим розширенням цих полів. Знайдені порядки 5 кривих, які можна рекомендувати в майбутніх стандартах і проектуємих криптосистемах.

*Ключеві слова:* еліптичні криві, криві Едвардса, порядок кривої, порядок точки, просте поле, розширене поле.

Табл. 02. Бібліогр.: 5 найм.

UDC 681.3.06

**Edwards curves of almost prime order over extensions of small prime fields / A.V. Bessalov, A.I. Gur'yanov, A.A. Dikhtenko // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 225–227.**

The paper suggests an approach to the problem of searching for Edwards curves acceptable to cryptography which consists in constructing a curve of minimum order 4 over the small fields  $F_5$  and  $F_7$  with a consequent prime extension of the said fields. The orders of five curves are found which can be recommended for use in future standards and cryptosystems under design.

*Keywords:* elliptic curves, Edwards curves, curve order, point order, prime field, extension field.

Tab. 02. Ref.: 5 items.