УДК 681.3.06

А.В. БЕССАЛОВ, д-р техн. наук, А.А. ДИХТЕНКО

ИЗОМОРФНЫЕ КАНОНИЧЕСКОЙ ФОРМЕ ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ ЭДВАРДСА НАД РАСШИРЕННЫМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Введение

При построении криптосистем на эллиптических кривых широко используются кривые над простыми полями F_p и кривые над расширенными полями F_{2^m} характеристики 2. Сравнивая их производительность, нельзя гарантировать преимущества какой-либо из них [4], так как быстродействие криптосистемы зависит от множества факторов, и выбор между кривыми исходит из требований к параметрам и возможностей реализации. Кривые над полями F_{2^m} в форме Вейерштрасса рекомендуются действующими стандартами и успешно применяются в протоколах шифрования [11, 12]. Известно большое число усовершенствованных алгоритмов вычислений в этих полях.

Перспективным классом эллиптических кривых сегодня является форма Эдвардса [1 - 10]. В продолжение ряда работ [5 - 10] здесь кратко описываем кривые Эдвардса, заданные над расширенными полями F_{2^m}. По форме уравнения кривой Эдвардса над полями четных и нечетных характеристик существенно отличаются, но есть ряд свойств, сходных для кривых этих двух типов. Главные преимущества кривых Эдвардса – высокая производительность и удобство реализации благодаря полноте закона сложения и наличия аффинных координат нуля группы точек кривой [1 - 10]. В данной работе приведены формулы изоморфного преобразования канонической кривой и кривой Эдвардса для случая полей характеристики 2. На основе действующих стандартов (ДСТУ 4145 – 2002 и FIPS 186-2 – 2000) [11, 12] вычислены параметры изоморфных кривых Эдвардса и координаты генераторов криптосистем над различными расширениями полей характеристики 2. Их перечень дан в разд. 3. Простой порядок генераторов криптосистем в предложенных кривых сравним с величиной соответствующего поля и удовлетворяет стандартным требованиям. Полученные кривые Эдвардса могут быть рекомендованы к реализации в проектируемых криптосистемах.

1. Кривые Эдвардса над расширенными полями характеристики 2

Рассмотрим F_{2^m} – конечное поле четной характеристики и d_1, d_2 – пару элементов этого поля, для которых справедливо $d_1 \neq 0$ и $d_2 \neq {d_1}^2 + d_1$. Тогда кривая Эдвардса над полем F_{2^m} в аффинных будет задаваться уравнением [3, 4]

$$E_{d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2 \qquad (1)$$

Подобно кривым Эдвардса над полями нечетных характеристик [2, 5 - 10], у каждой кривой Эдвардса вида (1) существуют обязательные точки. В данном случае таких точек две: $(1,1)$ – точка второго порядка кривой (1) и $O = (0,0)$ – нейтральный элемент относительно сложения. Отсюда следует, что минимальный сомножитель в порядке кривой Эдвардса над полем F_{2^m} равен 2. Кроме того, для таких кривых справедливо свойство покоординатной симметрии и, при заданных ограничениях на параметры d_1, d_2, кривая вида (1) не имеет точек сингулярности [3, 4]. Авторы [3] также рассматривают альтернативную форму записи кривой Эдвардса над расширенным полем характеристики 2. Переход к этой форме может быть осуществлен посредством изоморфного преобразования кривой (1) по правилу:

$$(x, y) \to (x, y+1).$$

Правило сложения точек (x_1, y_1), (x_2, y_2) кривой вида (1) задается формулами [3]:

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1 y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)},$$

$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1 x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}. \quad (2)$$

Из (1) и (2) следует, что точка (y_1, x_1) будет обратной к точке (x_1, y_1) [3]. С помощью (2) можно также убедиться в том, что $(x_1, y_1) + (0,0) = (x_1, y_1)$ для произвольной точки (x_1, y_1). Более сильное ограничение на параметр $d_2 \neq t^2 + t$, при $t \in F_{2^m}$ обеспечивает полноту закона сложения (2). Это означает, что приведенные формулы справедливы для всех пар точек (x_1, y_1), (x_2, y_2), включая равные, обратные точки и нуль группы О. Полнота закона сложения – главное преимущество кривых вида (1) перед другими формами представления эллиптических кривых с точки зрения практических приложений. Далее будем рассматривать кривые, для которых выполняется условие $d_2 \neq t^2 + t$.

2. Изоморфизм между несуперсингулярной канонической кривой и кривой Эдвардса над полем F_{2^m}

Эллиптическая кривая в канонической форме над расширенным полем характеристики 2 имеет вид [3, 11]

$$v^2 + uv = u^3 + a_2 u^2 + a_6, \quad (3)$$

где $a_6 \neq 0$.

Нулем группы точек эллиптической кривой относительно сложения является точка О на бесконечности.

В отличие от случая кривых над полями нечетной характеристики, где класс канонических эллиптических кривых шире соответствующего класса кривых Эдвардса, каждая каноническая кривая вида (3) изоморфна некоторой кривой Эдвардса вида (1). Посредством следующих формул осуществляется изоморфное преобразование от формы кривой (1) к форме (3) [3]:

$$u = d_1(d_1^2 + d_1 + d_2)\frac{(x + y)}{(xy + d_1(x + y))},\ v = d_1(d_1^2 + d_1 + d_2)\left(\frac{x}{(xy + d_1(x + y))} + d_1 + 1\right),$$

$$a_2 = (d_1^2 + d_2),\ a_6 = {d_1}^4({d_1}^4 + {d_1}^2 + {d_2}^2). \quad (4)$$

Обратное преобразоване задается формулами

$$x = \frac{d_1(u + d_1^2 + d_1 + d_2)}{(u + v + ({d_1}^2 + d_1)(d_1^2 + d_1 + d_2))},\ y = \frac{d_1(u + d_1^2 + d_1 + d_2)}{(v + ({d_1}^2 + d_1)(d_1^2 + d_1 + d_2))}. \quad (5)$$

Используя приведенные выше формулы можно осуществить изоморфный переход от известных канонических эллиптических кривых (которые уже применяются на практике и рекомендованы действующими стандартами [11, 12]) к кривым в форме Эдвардса. В следующем пункте мы приводим перечень таких кривых и кратко описываем механизм соответствующего перехода.

3. Нахождение криптостойких кривых Эдвардса над расширенными полями характеристики 2

Для поиска кривых Эдвардса над расширенными полями характеристики 2 были взяты за основу канонические эллиптические кривые действующего украинского стандарта ДСТУ 4145 – 2002 и кривые стандарта FIPS 186-2 – 2000. Зная значения коэффициентов a_2, a_6 канонической эллиптической кривой над заданным полем, вычисляем параметры d_1, d_2 следующим образом [3]:

1. Выбираем некоторый случайный параметр d_1 так, чтобы выполнялись условия

$$Tr(d_1) = Tr(a_2) + 1 \qquad \text{и} \qquad Tr\left(\frac{\sqrt{a_6}}{{d_1}^2}\right) = 1.$$

2. Рассчитываем значение второго параметра по формуле $d_2 = {d_1}^2 + d_1 + \frac{\sqrt{a_6}}{{d_1}^2}$.

В итоге получим параметры кривой в форме Эдвардса, изоморфной данной над исходным полем. Результаты расчетов приведены в табл. 1 и 2 в шестнадцатеричной системе. Здесь также приведены координаты генератора (x_G, y_G) для каждой из полученных кривых Эдвардса. Поиск генератора осуществлялся алогично работам [8 - 9]. В табл. 1 содержатся кривые для случая американского национального стандарта FIPS 186-2 – 2000 [11], в табл. 2 – кривые для случая украинского стандарта ДСТУ 4145 – 2002 [11, 12].

Таблица 1

Кривые Эдвардса для случая стандарта FIPS 186-2 – 2000

B-163:	$P(x) = x^{163} + x^7 + x^6 + x^3 + 1$, **n=400000000000000000000292FE7E70C12A4234C33**
d_1 =	4
d_2 =	6AC25B85BADF8927593D21C366DA89C03969F3494
x_G =	687540D72D2908FD3841129BCA7958858B6C5C2BE
y_G =	699BB09A27DAD0407498C71F6F64BC9209430B2F0
B-233:	$P(x) = x^{233} + x^{74} + 1$, **n=1000000000000000000000000000013E974E72F8A6922031D2603CFE0D7**
d_1 =	2
d_2 =	61FE1589EE5E1D39D1FB8C781B5C72ABBA94BC8494F97E51B41876A448
x_G =	107D76A232756C62932C89C879CDD4A452072D06663DDE1714CB8B5B09F
y_G =	11A4B8C4C816DE81462BD446A6BE32B22750BB2FA6AF5183A4B509F93D2
B-283:	$P(x) = x^{283} + x^{12} + x^7 + x^5 + 1$, **n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEF90399660FC938A90165B042A7CEFADB307**
d_1 =	8
d_2 =	6DCAF32715E4AC7AFA0660C227EDBE0D68BF48828C11093285F020AB85D10ABB7A6EB70
x_G =	6AD770485BE05F6282F2C9702B8B6EEF71CDB66E3B47BCEB988045F1CB8DE8F82A5CC31
y_G =	148E3745CBC60604095D85F56B6E41328A91E7341D954AC04AE63BF3B1AD12CCD68B76E
B-409:	$P(x) = x^{409} + x^{87} + 1$, **n=1000000000000000000000000000000000000000000000000001E2AAD6A612F33307BE5FA47C3C9E052F838164CD37D9A21173**
d_1 =	2

Продолжение табл.1

$d_2 =$	1A64D7DF91DA3B8BBC8BE6D28A7D4F2D764EACBB42B5F395F06C9927F7A2565433D95D9DC CC9B14A2F2389EE1CAB33C2F09757D
$x_G =$	C76FF6F8C191F824D47A1858A8ABD7307288305F929812EC9F9DC117FF39AAC2CA34F8C69BE6 DA8741585D1015254D75B5149C
$y_G =$	1F6AF8ADC131E10CC369DDF66212EF8E3904F35F641EAFBF9A3C907E9B08BB01793C25A7F7F6 A8EEE144824D4DA16B146B24535
B-571:	**$P(x) = x^{571} + x^{10} + x^5 + x^2 + 1$, n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFE661CE18FF55987308059B186823851EC7DD9CA1161DE93D5174D66E8382E9BB2FE84E47**
$d_1 =$	4
$d_2 =$	7F32D556640C20B5DD739A058DFFD58268D41C59135429EB041D7AA1255902E6362C4800A874A B0B60536B58460CD20C06F0340E3594A7F771BEDFC10CE39B64699B08443B7620D
$x_G =$	8452FAF52887F029A9F928ED8D074ADEEBC27AED0C7F082452AA37A72C7E642281893E50AFD9 6AB2B68FAD5E4DC7DD0941AFB06A4B14348C8249CEE72C8DF3A351A2F68A7DB0A0
$y_G =$	7DAFEB6704D7FE96DF3611B29A4FBBC8DE308DABD10C5555901F01A813D5F68C135ECADF87 21900FB4272EE988D88C301C818661EAA5B738F28DFC7CAC7DF9651D709CA1A6A7864

Таблица 2

Кривые Эдвардса для случая стандарта ДСТУ 4145 – 2002

m = 163	**$P(x) = x^{163} + x^7 + x^6 + x^3 + 1$, n=4000000000000000000002BEC12BE2262D39BCF14D**
$d_1 =$	8
$d_2 =$	768F690F32DC034F5DEDB24C8FB319ED8B486B3DA
$x_G =$	559682C8E8BBC689464D0D7E621E98BBCD8DABD2
$y_G =$	B7F0D7B1B708E25CAA1BE95F45837DCAECC5C0F0
m = 167	**$P(x) = x^{167} + x^6 + 1$, n=3FFFFFFFFFFFFFFFFFFFFFB12EBCC7D7F29FF7701F**
$d_1 =$	2
$d_2 =$	7545508021921A6B02567AA6A4417DC34053497001
$x_G =$	4F162059495517E97160CD0F5E9A7479EA77878A34
$y_G =$	22222912562574D05A1F8C5C99521C737C2114BCEE
m = 173	**$P(x) = x^{173} + x^{10} + x^2 + x + 1$, n=800000000000000000000189B4E67606E3825BB2831**
$d_1 =$	1
$d_2 =$	1D182BC81F177A6A25AA0137888AF3E6A3DCFBAF1DDD
$x_G =$	B3F998920A5710E0ADD293A70643A69699E49293F11
$y_G =$	1EABC4D59CB70A65D6C5E3540BF8B28DC5CB07AD585A
m = 179	**$P(x) = x^{179} + x^4 + x^2 + x + 1$, n=3FFFFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF**
$d_1 =$	2
$d_2 =$	34437707C8E046F16D6C49D2815725284CE51C7F993D2
$x_G =$	57A15986F8B562BE752B53CA3BF400CC21368BCA9F693
$y_G =$	369D420DD0B4D1E8CB620D1226E7D8C9FDFE138F617C0
m = 191	**$P(x) = x^{191} + x^9 + 1$, n=40000000000000000000000069A779CAC1DABC6788F7474F**
$d_1 =$	8
$d_2 =$	3E9D061E228EDCA3D70943FBA58882CEED93F23D2F0888B
$x_G =$	4753A3DEE912C24C9298B9F06AA7E27583949BF09462C67A
$y_G =$	389B5804EE0CD12CB108D2034603B930855979CB5AD30776
m = 233	**$P(x) = x^{233} + x^9 + x^4 + x + 1$, n=1000000000000000000000000000013E974E72F8A6922031D2603CFE0D7**

Продолжение табл.2

d_1 =	4
d_2 =	168D50202F1C874FE7BCE08CF64ABF78D959DB56A53EE3387E963C84AD
x_G =	F2F608558FED69CC31BDAA9BB4842265F9E9AD8457596273801744D0E0
y_G =	2C00AB6DBB76D5BE58ACED3FD4B0794E0ECE21E84A41F38C10C1893A64
m = 257	**$P(x) = x^{257} + x^{12} + 1$, n=800000000000000000000000000000006759213AF182E987D3E17714907D470D**
d_1 =	1
d_2 =	129412CB0FA992A6B6A6BEFEF740F83E1AE6C17BE4D4F3616F639B2F27688D001
x_G =	9FD3727044903DF7449203878D034D87964052D64664D583A0ED69B37D4D6A61
y_G =	1A898787363EBB480F20A1AC759F498378375F5066468A137351346F50E16373
m = 307	**$P(x) = x^{307} + x^8 + x^4 + x^2 + 1$, n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC079C2F3825DA70D390FBBA588D4604022B7B7**
d_1 =	6
d_2 =	6A577FE886FF3BD047B314D9E094DCDC2E9F042EE3338869E776CB6075C4A0A169BE053417AD7
x_G =	6AAD22CC933A1BE6349B802D17DA70E48C480A6FA4C6C099F39CFEB270178D49A64BF92A8D262
y_G =	1055BE77CBB48AF00CF6A4C7E6D27EBA27D77442C4D0A58B99893D978369163FD8A908125CCD8
m = 367	**$P(x) = x^{367} + x^{21} + 1$, n=4000000000000000000000000000000000000000000009C300B75A3FA824F22428FD28CE8812245EF44049B2D49**
d_1 =	2
d_2 =	47AE47377615E10041C7DF34C9FC6EFB9A589B6405C6BC15BA9AAC186B3CE4C09446C5AB4DFFC199CD94F1C37373
x_G =	7934BB36E0E76EDC55C2BC68476B3E8157C6C731EF07B9D0B9D31623CEAC1A46C4A7B6B0EBAFC2C16D93E3794997
y_G =	4471E442DC9FC47DFB60CE95E312B2209FC50000CBEABA9294DC2E7D612CFC5246894A55B9702DE055892B2B7DE2
m = 431	**$P(x) = x^{431} + x^5 + x^3 + x + 1$, n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBA3175458009A8C0A724F02F81AA8A1FCBAF80D90C7A95110504CF**
d_1 =	8
d_2 =	26C08DD2E5BE99638D8123FAAA6FFEE4965F85CBDA46C906F1A42F66150C49928B00BE2B4A6A3E9D1F7AE09D9984B681F2DB7EA2973
x_G =	198E2AD22D178117E7FEBF738913EFAF8C655BC49E96E3F314B3D788671C872ECFE6D93BBE561A114E6B4A251503BC2F58803E2FF
y_G =	61A19032C14D0A9CE7A5A0289AF4299C9FEC94BEB2A5F86F8B095FEB7657403A00EF759C9BA4DEDE26D4C5CDF018DF47245781C23EE

Всего было найдено еще по пять изоморфных кривых Эдвардса для каждого случая – в общей сложности получено 90 кривых для различных степеней m расширения поля F_{2^m}. Для поля определенной битовой длины полученные кривые Эдвардса равнозначны стандартным каноническим с точки зрения стойкости и обладают высокой производительностью. Приведенные в данной работе кривые Эдвардса с малыми значениями параметра d_1 требуют выполнения меньшего числа операций в поле, что дает дополнительный выигрыш.

Выводы

Рассмотрена альтернативная форма эллиптической кривой над расширенным полем характеристики 2, а именно – форма Эдвардса эллиптической кривой. Эта форма имеет ряд характерных свойств, интересных для практического применения рассматриваемых кривых. Даны формулы изоморфного преобразования между формой Вейерштрасса и формой Эдвардса кривой над полями характеристики 2. На основе общесистемных параметров двух действующих стандартов (ДСТУ 4145 – 2002 и FIPS 186-2 – 2000) приведены кривые Эдвардса, изоморфные каноническим эллиптическим кривым в этих стандартах. Для каждой из найденных кривых Эдвардса также рассчитаны и приведены в соответствующих таблицах координаты генератора криптосистемы.

Главными преимуществами кривых в форме Эдвардса перед каноническими эллиптическими кривыми являются высокая скорость вычислений, полнота закона сложения и наличие аффинных координат нейтрального элемента аддитивной группы точек кривой.

Список литературы: 1. *Edwards, H.M.* A normal form for elliptic curves // Bulletin of the American Mathematical Society. – Volume 44, Number 3, July 2007. – PP. 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 Reza Rezaeian.* Binary Edwards curves // Cryptographic hardware and embedded systems – CHES 2008, 10th international workshop. – Washington, D.C., USA, August 10-13, 2008. – PP. 224-256. 4. *Bernstein Daniel J.*, Batch binary Edwards // Advances in cryptology – Crypto 2009, 29th annual international cryptology conference, Santa Barbara, CA, USA, August 16-20, 2009. – PP. 317-336. 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. – 2011. – №4. – С.33-36. 6. *Бессалов, А.В.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. – 2011. – Вып. 167. – С. 203-208. 7. *Бессалов, А.В., Гурьянов, А.И., Дихтенко, А.А.* Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника. – 2012. – №2. – С. 225-227. 8. *Бессалов, А.В., Дихтенко, А.А., Яценко, А.И.* Параметры криптосистемы на кривой Эдвардса над расширениями малых простых полей // Прикладная радиоэлектроника. – 2013. – Т. 12, №2. – С.95-99. 9. *Бессалов, А.В., Дихтенко, А.А.* Криптостойкие кривые Эдвардса над простыми полями // Прикладная радиоэлектроника. – 2013. – Т. 12. №2. – С.107-113. 10. *Бессалов, А.В.* Деление точки на два для кривой Эдвардса над простым полем // Прикладная радиоэлектроника. – 2013. – Т. 12, №2. – С.95-101. 11. *Бессалов, А.В., Телиженко, А.Б.* Криптосистемы на эллиптических кривых : учеб. пособие. – К. : ІВЦ «Політехніка», 2004. – 224с. 12. *Державний* стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка ДСТУ 4145-2002. Видання офіційне. – К. : Держстандарт України, 2003. – 39с.

Национальный технический
университет Украины «КПИ»,
Донецкий национальный университет

Поступила в редколлегию 11.11.2013