УДК 681.3.06

ИЗОМОРФИЗМ НЕСУПЕРСИНГУЛЯРНЫХ КРИВЫХ НАД ПОЛЯМИ ХАРАКТРЕИСТИКИ 2 И КРИВЫХ ЭДВАРДСА С ОДНИМ ПАРАМЕТРОМ

А.В. БЕССАЛОВ, А.А. ДИХТЕНКО

Рассмотрены аффинное и проективное представления эллиптической кривой в форме Эдвардса над полями $F_2{}^m$. Даны оценки сложности выполнения групповых операций в проективных координатах. Получены условия существования несуперсингулярной кривой, изоморфной кривой Эдвардса с одним параметром d. Для известных стандартных кривых, удовлетворяющих этим условиям, найдены изоморфные им кривые Эдвардса.

Ключевые слова: расширенное поле характеристики 2, несуперсингулярная кривая, кривая Эдвардса, кривая Коблица, групповой закон.

ВВЕДЕНИЕ

Форма Эдвардса эллиптической кривой над полем характеристики $p > 3$ задает симметричную относительно координат кривую с порядком, кратным 4 [1, 2, 5, 6]. Для всех кривых этого класса групповая операция выполняется рекордно малым числом арифметических операций в поле [2, 5]. Наряду с простыми полями большой характеристики в криптографии широко применяются расширенные поля $F_2{}^m$ характеристики 2. Несмотря на различия в форме записи, кривым Эдвардса над полями $F_2{}^m$ и F_p (при $p > 3$) присущи сходные свойства [3, 4, 7]. Для двух типов кривых Эдвардса нуль абелевой группы представляется парой аффинных координат, а соответствующий групповой закон справедлив для произвольной пары точек кривой (включая совпадающие, обратные точки, и нуль группы) [2, 3]. Минимальный кофактор в порядке кривой Эдвардса над полем $F_2{}^m$ равен 2. Задачей работы является поиск кривых Эдвардса, приемлемых для криптографии.

Настоящая работа рассматривает кривые в форме Эдвардса над расширенными полями $F_2{}^m$. Анализ оценок сложности операций сложения и удвоения точек кривой Эдвардса над полем $F_2{}^m$ приводит к выводу, что наибольшая производительность присуща кривым с одним параметром $d = d_1 = d_2$. Между несуперсингулярными кривыми и кривыми Эдвардса в общем виде над полями $F_2{}^m$ существует изоморфизм [3]. В разделе 3 мы находим условия, при которых для данной эллиптической кривой найдется изоморфная кривая Эдвардса с одним параметром d. Для известных канонических кривых из национальных стандартов (ДСТУ 4145 – 2002 [8, 9] и FIPS 186-2 – 2000 [8]), удовлетворяющих полученным условиям, мы нашли изоморфные кривые Эдвардса с одним параметром d . В случае ДСТУ 4145 – 2002 таких кривых две, в американском стандарте FIPS 186-2 – 2000 данные условия выполняются для четырех кривых Коблица.

1. КРИВЫЕ ЭДВАРДСА НАД РАСШИРЕННЫМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Кривая Эдвардса над полем $F_2{}^m$ описывается уравнением в аффинных координатах [3]

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

где d_1, d_2 - пара элементов поля, удовлетворяющих условиям $d_1 \neq 0$ и $d_2 \neq t^2+t \quad \forall t \in F_{2^m}$. Закон сложения точек кривой (1) $(x_1, y_1)+(x_2, y_2)=(x_3, y_3)$ универсален и имеет вид

$$x_3 = \frac{d_1(x_1+x_2)+d_2(x_1+y_1)(x_2+y_2)+(x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)},$$

$$y_3 = \frac{d_1(y_1+y_2)+d_2(x_1+y_1)(x_2+y_2)+(y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1+(y_1+y_1^2)(x_2+y_2)}. \tag{2}$$

Полнота закона (2) – наиболее весомый аргумент для включения кривых Эдвардса над полями $F_2{}^m$ в проекты будущих стандартов шифрования. Нуль группы $O=(0,0)$, как видно из (2), не изменяет координат другой точки в сумме. Прочие свойства кривых Эдвардса над полями четных и нечетных характеристик подробно рассмотрены в работах [3, 4, 7] и [1, 2, 5, 6] соответственно. Очевидно, что производительность криптосистемы в значительной мере зависит от ее параметров, и в случае кривых над полями $F_2{}^m$, актуален вопрос нахождения таких коэффициентов d_1, d_2 кривой Эдвардса, при которых будет достигаться максимальная скорость выполнения операций.

Проблема инверсии в формулах сложения (2) для кривой, заданной в аффинных координатах, решается переходом к проективным координатам. Подставив в уравнение (1) $x = \frac{X}{Z}, y = \frac{Y}{Z}$ и умножив обе его части на Z^4 (при $Z \neq 0$) получим однородное уравнение кривой Эдвардса над полем $F_2{}^m$ с теми же параметрами d_1, d_2:

$$d_1(X+Y)Z^3+d_2(X^2+Y^2)Z^2=XYZ^2+XY(X+Y)Z+X^2Y^2,$$

где $X,Y,Z\in F_{2^m}$ (3)

Помимо точек вида $(\alpha X:\alpha Y:\alpha Z)$ при $Z\neq 0$ и $a\in F_2{}^{m*}$, которые соответствуют точкам (x,y) аффинного представления, уравнению (3) удовлетворяют еще две точки с проективными координатами $(1:0:0)$ и $(0:1:0)$. Обе являются сингулярными.

2. СЛОЖНОСТЬ ВЫПОЛНЕНИЯ ГРУППОВЫХ ОПЕРАЦИЙ НА КРИВОЙ ЭДВАРДСА, ЗАДАННОЙ В ПРОЕКТИВНЫХ КООРДИНАТАХ

Согласно [3], сложение в проективных координатах для кривых Эдвардса в общем случае реализуется за $V_{E\,d_1,d_2}=21M+1S+4D$ операций в поле. Аналогичная величина для удвоения составляет и $W_{E\,d_1,d_2}=2M+6S+3D$ операций. Здесь M, S, D – сложность умножения, возведения в квадрат и умножения на параметры d_1,d_2 в поле $F_2{}^m$. Главным преимуществом кривых Эдвардса над полями $F_2{}^m$, как отмечалось, является полнота и универсальность закона сложения (2) [3, 4]. Производительность же данных кривых в общем случае не является максимальной [3]. Однако приведенные оценки сложности можно улучшить, если принять значения параметров кривой Эдвардса над полем $F_2{}^m$ равными между собой. Другими словами, при $d_1=d_2=d$ имеем аффинную кривую вида

$$E_d:\ d(x+y+x^2+y^2)=xy+xy(x+y)+x^2y^2 \tag{4}$$

с соответствующим представлением в проективных координатах:

$$d\left((X+Y)Z^3+(X^2+Y^2)Z^2\right)=XYZ^2+XY(X+Y)Z+X^2Y^2,$$

$d,X,Y,Z\in F_{2^m}$, $d\neq 0$ и $d\neq t^2+t$, $\forall t\in F_{2^m}$. (5)

Для этого случая формулы сложения и удвоения будут иметь меньшую сложность: $V_{E\,d}=16M+1S+4D$ и $W_{E\,d_1,d_2}=2M+5S+2D$ операций в поле $F_2{}^m$ [3].

Логично поставить вопрос, при каких условиях для данной канонической кривой можно найти изоморфную кривую Эдвардса вида (4) над полем F_{2^m} и как связаны параметры таких кривых.

3. УСЛОВИЯ ИЗОМОРФИЗМА КАНОНИЧЕСКОЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД ПОЛЕМ $F_2{}^m$ И КРИВОЙ ЭДВАРДСА С ОДНИМ ПАРАМЕТРОМ

Каноническая эллиптическая кривая (или несуперсингулярная кривая) задана над полем $F_2{}^m$ аффинным уравнением

$$v^2+uv=u^3+a_2u^2+a_6,\qquad \text{где } a_6\neq 0. \tag{6}$$

При построении кривых Эдвардса вида (1), изоморфных кривым вида (6) в работе [7] мы выбирали значение параметра d_1 так, чтобы выполнялись два условия: $Tr(d_1)=Tr(a_2)+1$ и $Tr\left(\frac{\sqrt{a_6}}{d_1{}^2}\right)=1$. Далее вычисляли значение другого параметра по формуле $d_2=d_1{}^2+d_1+\frac{\sqrt{a_6}}{d_1{}^2}$ [3, 7]. Пусть для кривой (6) существует изоморфная кривая Эдвардса вида (4). Тогда, принимая $d_1=d_2=d$, получим систему

$$\begin{cases} d=d^2+d+\dfrac{\sqrt{a_6}}{d^2} \\ Tr(d)=Tr(a_2)+1 \\ Tr(\dfrac{\sqrt{a_6}}{d^2})=1 \end{cases} \tag{7}$$

Возьмем функцию следа от обеих частей первого уравнения системы, тогда с учетом $Tr(d)=Tr(d^2)$ получим $Tr(d)=Tr(\frac{\sqrt{a_6}}{d^2})$. Теперь из 2-го и 3-го уравнений сразу следует, что

$$Tr(a_2) = 0 \qquad (8)$$

Первая формула в системе (7) позволяет вычислить для изоморфной кривой Эдвардса единственное значение параметра *d*

$$d^2 + \frac{\sqrt{a_6}}{d^2} = 0, \qquad \Rightarrow d = \sqrt[8]{a_6}\ . \qquad (9)$$

Условие $d \neq 0$ в (4) и существование квадратного корня у каждого элемента поля $F_2{}^m$ обеспечивает разрешимость данного равенства.

Равенства (8), (9) задают изоморфизм между кривыми вида (6) и (4). Из всех несуперсингулярных кривых ровно половина кривых со следом $Tr(a_2) = 0$ отвечает этим условиям. Так как 8 не делит порядок мультипликативной группы поля $(2^m - 1)$, для каждого ненулевого параметра a_6 кривой (6) существует единственное значение параметра $d = \sqrt[8]{a_6}$ изоморфной кривой Эдвардса и обратно: $a_6 = d^8$ – единственное значение для каждого *d*.

Из (8) следует, что все несуперсингулярные кривые и изоморфные им кривые Эдвардса вида (4) имеют порядок, кратный 4. В качестве примера можем взять две кривые действующего украинского стандарта ДСТУ 4145 – 2002 над полями со степенью расширения $m = 173,\ m = 257$ соответственно, которые удовлетворяют условиям (8), (9). В таблице 1 приведены параметры кривых в форме Эдвардса вида $d(x + y + x^2 + y^2) = xy + xy(x + y) + x^2y^2$ изоморфных данным кривым в канонической форме над соответствующим полем, а также координаты генераторов криптосистемы.

Таблица 1

Кривые Эдвардса, изоморфные каноническим кривым над полями $F_2{}^m$ при $m = 173,\ m = 257$ для случая украинского стандарта ДСТУ 4145 – 2002

m = 173	**$P(x) = x^{173} + x^{10} + x^2 + x + 1$, n=800000000000000000000189B4E67606E3825BB2831**
d =	194E92F31C2F97583B5B079A66498651CFF964D4EDC1
x_G =	7F533BD52D2DDEAA0A26A9B1547AD25257F26E7E1BD
y_G =	1310000C9C9510CA7EEAE41922062276B7C0EAE85512
m = 257	**$P(x) = x^{257} + x^{12} + 1$, n=800000000000000000000000000000006759213AF182E987D3E17714907D470D**
d =	1A561C01C65FDA18821A29F0299C88C26C8A85C4F5F326BF152B115950E5AB7A6
x_G =	12F1EFDA68924370FA29955383A6FCAB88CAD1E67BF61411F5D796838FA9F38B0
y_G =	18E4BCBC54AD766E6834C60BBC8630661D42C8B075E024A3671922801063456FD

Взяв за основу американский стандарт FIPS 186-2 – 2000 и принимая во внимание условия (8), (9), можем заметить, что каждой из 4-х кривой Коблица с параметром $a = 0$ изоморфна кривая Эдвардса с параметрами $d_1 = d_2 = 1$, над различными полями F_{2^m} простых степеней расширения. В таблице 2 мы приводим координаты генераторов криптосистемы на кривых Эдвардса вида $x + y + x^2 + y^2 = xy + xy(x + y) + x^2y^2$ изоморфных данным кривым Коблица над соответствующим полем.

Таблица 2

Кривые Эдвардса, изоморфные кривым Коблица над полями $F_2{}^m$ при $m = 233,\ m = 283,\ m = 409,\ m = 571$ для случая американского стандарта FIPS 186-2 – 2000

K-233:	**$P(x) = x^{233} + x^{74} + 1$, n=8000000000000000000000000000069D5BB915BCD46EFB1AD5F173ABDF**
x_G =	FACA9831F3C99277CF551679FE7245D52B11A048FC45C0B78BCEE6BF32
y_G =	19BCD68FB073EBC8437C67422B12751BB1279087397553C8819C72CBE2

K-283:	$P(x) = x^{283} + x^{12} + x^7 + x^5 + 1$, **n=1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE9AE2ED07577265DFF7F94451E061E163C61**
x_G =	5AD205F99526557BC0731B3991187B66FCE4D30386D0864AE5318A21FFB4A96BD88CE9B
y_G =	10142CE6C38325511BB593DEA87393A70D9CDB25D097DEF259E343850310470CF940318
K-409:	$P(x) = x^{409} + x^{87} + 1$, **n=7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE5F83B2D4EA20400EC4557D5ED3E3E7CA5B4B5C83B8E01E5FCF**
x_G =	1CE08B54A8E78B891EB7E8D1DF23A74B0A4976E3C2FD33E984FEA99D2CD03AA3633127ADA8858E3854E7EBDF442F300FAE480
y_G =	CCFE11FE0FD07C5F196CCA8672276D10C9489D344C33E230185BA43CDF3F505BE98285BCD2547BB274707811736A323B7E6FE7
K-571:	$P(x) = x^{571} + x^{10} + x^5 + x^2 + 1$, **n=20000000000000000000000000000000000000000000000000000000000000000000000000000131850E1F19A63E4B391A8DB917F4138B630D84BE5D639381E91DEB45CFE778F637C1001**
x_G =	1653830605B1343AC3BB092259163566A374B13FF921A3EE4DD9C8B189443DE17B83D18B37B79870DFE06ABF1DCD13F22B4EC5918DC4DBA0BD6FA3F3EC86F59724215EC35A2D4E8
y_G =	7CC37E95C30C6C3DC8286F24323FAFF14BF2EC60F0574DEBAA9F2AD2F08622CBCFEBA00DE29CA7D6B31E8F4AE96D3B9857908C1572263F94285E765FC3A94230BA175C142CDDB68

Закон сложения для кривых Коблица не обладает свойством полноты и универсальности (в отличие от случая кривых Эдвардса), и это можно трактовать как их недостаток. Однако, сложность групповой операции в случае кривых Коблица все же будет меньшей, чем в случае изоморфных кривых Эдвардса, поэтому нельзя сделать однозначный вывод о превосходстве одной формы рассматриваемых кривых над другой.

ЗАКЛЮЧЕНИЕ

Среди множества форм представления эллиптических кривых кривые в форме Эдвардса особенно интересны с практической точки зрения. В настоящей работе мы рассмотрели кривые Эдвардса над расширенными полями F_{2^m}. Закон сложения для данных кривых обладает свойством универсальности и полноты, а его сложность варьируется в зависимости от выбранных параметров кривой.

Исходя из имеющихся оценок сложности групповой операции [3], а также, формул изоморфного преобразования [3, 7] между кривыми Эдвардса и каноническими эллиптическими кривыми над полями F_{2^m} мы получили условия существования кривой Эдвардса с одним параметром, изоморфной кривой в канонической форме. Далее, мы вычислили искомые значения параметров, соответствующие двум кривым из стандарта ДСТУ 4145 – 2002 (при $m = 173$ и $m = 257$).

В итоге можно констатировать, что сравнительно немного кривых над полями F_{2^m} из рассматриваемых стандартов удовлетворяют условию (8). Поэтому, для нахождения большего числа быстрых кривых Эдвардса необходимо искать новые кривые форме Эдвардса с почти простым значением порядка.

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 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, №4, 2011. С.33-36.

6. Бессалов А.В., Дихтенко А.А., Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника том 12 №2, 2013. С.107-113.
7. Бессалов А.В., Дихтенко А.А., Изоморфные канонической форме эллмптические кривые Эдвардса над расширенными полями характеристики 2. Статья принята к публикации в журнале «Радиотехника».
8. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.
9. 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.

ИЗОМОРФИЗМ НЕСУПЕРСИНГУЛЯРНЫХ КРИВЫХ НАД ПОЛЯМИ ХАРАКТРЕИСТИКИ 2 И КРИВЫХ ЭДВАРДСА С ОДНИМ ПАРАМЕТРОМ

Рассмотрены аффинное и проективное представления эллиптической кривой в форме Эдвардса над полями $F_2{}^m$. Даны оценки сложности выполнения групповых операций в проективных координатах. Получены условия существования несуперсингулярной кривой, изоморфной кривой Эдвардса с одним параметром d. Для известных стандартных кривых, удовлетворяющих этим условиям, найдены изоморфные им кривые Эдвардса.

Ключевые слова: расширенное поле характеристики 2, несуперсингулярная кривая, кривая Эдвардса, кривая Коблица, групповой закон.

ІЗОМОРФІЗМ НЕСУПЕРСИНГУЛЯРНИХ КРИВИХ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ 2 ТА КРИВИХ ЕДВАРДСА З ОДНИМ ПАРАМЕТРОМ

Розглянуті афінне та проективне представлення еліптичної кривої в формі Едвардса над полями $F_2{}^m$. Дані оцінки складності виконання групових операцій в проективних координатах. Отримані умови існування несуперсингулярної кривої, що ізоморфна кривій Едвардса з одним параметром d. Для відомих стандартних кривих, що задовольняють цим умовам, знайдені ізоморфні криві Едвардса.

Ключові слова: розширене поле характеристики 2, несуперсингулярна крива, крива Едвардса, крива Кобліца, груповий закон.

THE BIRATIONAL EQUIVALENCE BETWEEN THE CANONICAL ELLIPTIC CURVES OVER FIELDS OF CHARACTERISTICS 2 AND THE EDWARDS CURVES

The affine and the projective representations are considered for an Edwards curve over fields $F_2{}^m$. Evaluations are given for the group operations complexity in the projective coordinates. The conditions are obtained for the canonical curve which is isomorphic to an Edwards curve with one parameter d. The isomorphic Edwards curves are found for known standard curves, which satisfy these conditions.

Key words: extended field of characteristics 2, canonical curve, Edwards curve, Kobliz curve, group law.

Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор кафедры ММЗИ ФТИ НТУУ «КПИ». Область научных интересов: криптография, теория корректирующего кодирования.
bessalov@ukr.net
Дихтенко Алиса Анатольевна, аспирант кафедры теории упругости и вычислительной математики Донецкого национального университета. Область научных интересов: асимметричная криптография.
alice.dikhtenko@gmail.com, alice_dikhtenko@mail.ru

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри ММЗІ ФТІ НТУУ «КПІ». Область наукових інтересів: криптографія, теорія коригуючого кодування.
bessalov@ukr.net
Діхтенко Аліса Анатоліївна, аспірант кафедри теорії пружності та обчислювальної математики Донецького національного університету. Область наукових інтересів: асиметрична криптографія.
alice.dikhtenko@gmail.com, alice_dikhtenko@mail.ru