УДК 681.3.06

Бессалов А.В., Діхтенко А.А., Яценко О.І.

Загальносистемні параметри криптосистеми на кривій Едвардса над розширеннями малих простих полів

У задачі пошуку прийнятних для криптографії кривих Едвардса запропоновано підхід, що полягає в побудові кривої мінімального порядку 4 над малими полями F_5 і F_7 із наступним розширенням цих полів. Знайдено 5 кривих, які можна рекомендувати для використання в майбутніх криптосистемах .

In the task of finding suitable for cryptography Edwards curves, an approach based on selection of the curve with minimum order 4 over small fields F_5 and F_7 with the following prime extension of these fields was suggested. Five curves were found that can be recommended for use in projecting cryptosystems.

Вступ

Асиметричні криптосистеми на еліптичних кривих понад десятиріччя успішно використовуються на основі дійсних національних і міжнародних стандартів [5]. Пошуки більш досконалих алгоритмів останніми роками привели до альтернативи канонічної форми кривих – кривим у формі Едвардса [1 – 4]. Їх головні переваги: рекордна продуктивність і простота групових операцій та програмування. Однак криві Едвардса поки що не стандартизовані, для них необхідно ініціювати пошук кривих з майже простим порядком $N_E = 4n$, де n – просте число. Мінімальний кофактор 4 у порядку кривої пов'язаний з існуванням точок 4-го порядку в усіх кривих Едвардса. В загальному випадку для пошуку надійних кривих Едвардса слід адаптувати відомі алгоритми SEA або Satoh [5].

В цій роботі пропонується найбільш простий шлях знаходження кривої Едвардса майже простого порядку $4n$. За аналогією з кривими Коблица над полями характеристики 2, ми пропонуємо знайти дві криві Едвардса мінімального порядку $N_{E1} = 4$ над малими простими полями F_5 и F_7 , після чого знайти порядки цих кривых над расширениями степеню m цих полів з наступним відбором при простих m потрібного майже простого порядку $4n$. В результаті нами були знайдені кілька кривих в межах криптографічних значень параметрів.

Знаходження кривих Едвардса майже простого порядку над розширеннями малих полів

Криві Едвардса над кінцевими полями характеристики $p > 3$ описуються рівнянням [1,2]

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

Різні значення параметру c породжують ізоморфні криві, тому можна прийняти c = 1, $\tilde{d} = d$, тоді різні криві визначаються лише одним параметром d у рівнянні

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

Спочатку розглянемо криву над полем F_5, де значеннями параметру d, які допустимі, є квадратичні нелишкі 2 и 3. Вони є мультіпликативно оберненими, тому утворюють пару кривих кручення [3]. Межі Хассе $p + 1 \pm 2\sqrt{p}$ при p = 5 знаходяться в интервалі 2…10, в цих межах для кривих Едвардса допустимі лише 2 значення порядку N_E кривої, які рівні 4 и 8. Згідно з твердженням 1 в [3] точки 8-го порядку існують, якщо $1 - d$ – квадратичний лишок, і не існують в протилежному випадку. При d = 2 значення $(1 - d)$ = 4mod5 – квадратичний лишок, і відповідна крива має порядок 8. При d = 3 значення $(1 - d)$ = 3mod5 – квадратичний нелишок, тоді крива має порядок 4. Вона містить лише обов'язкові 4 точки усіх кривих Едвардса $(0, \pm 1)$, $(\pm 1, 0)$ при c = 1.

Таким чином, ми приймаємо d = 3, тоді з $N_{E1} = p + 1 - t_1 = 4$ слід рівняння Фробеніуса t_1 = 2. Розрахуємо порядки кривих над розширеннями $F_p{}^m$ за відомою формулою [5]

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

де для визначення параметру t_m скористаємось рекурентною формулою

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

Результати розрахунків по формулам (2), (3) с відбором простих значень $n = N_{Em}/4$ надані в таблиці 1. У другої колонці таблиці надані округлені значення для довжини модуля поля $m_b = m\log p/\log 2$ в бітах. Тестування числа n на простоту за допомогою тесту Міллера-Рабіна здійснювалось спеціальною прикладною програмою.

В межах Хассе є ще одна крива з мінімальним порядком $N_{E1} = p + 1 - t_1 = 4$ при p = 7 и t_1 = 4. Вона також має параметр d = 3, який є квадратичним нелишком у полі F_7, при цьому $1 - d$ = 5 – також нелишок. Прості множники n порядків цієї кривої над розширеннями $F_7{}^m$, що обчислені за допомогою (2), (3), наведені в таблиці 2.

$p = 5$ Таблиця 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

$p = 7$ Таблиця 2

m	m_b	$n = N_{Em}/4$
5	14	4261
7	19	205759
17	47	58157621574673
43	120	54595359399794914922465326744889728 3
47	132	13108345791890759086345450437985587821 83
127	356	53136273114200417711082595776474056083298454184099962702599160022401657332487956399341333796788130398754359
223	626	71581852226941622933299737411659197932981104415173763451661527073195598927924017803839396075711488567742585548737657165186060208128204445456219597545912695038457513147335447096716383526039

Нажаль, наші апріорні очікування достатньо великої кількості придатних для криптографії кривих Едвардса над розширеннями малих простих полів характеристики p > 3 не підтвердились. Як випливає з таблиць 1 і 2, в межах стандартних вимог до порядку генератора криптосистеми і близьким до нього розширенням $2^{mb}(m_b \cong 180 \ldots 600)$ ми знайшли всього 3 криві Едвардса: 2 криві над полем F_5^m зі степенями $m = 181$ и $m = 227$, і одну криву над полем F_7^m зі степенем $m = 127$. До них, однак, можна додати ще 2 криві з $m = 353$ (при $p = 5$) і з $m = 223$ (при $p = 7$), тобто з надмірним рівнем стійкости і значенням $m_b > 600$.

Як приклад, розглянемо визначення координат точки кривої Едвардса простого порядку n нал полем F_5^{181}. Для даного розширення був знайдений примітивний поліном мінімальної ваги $P(z) = z^{181} + z^3 + z^2 + 3z + 3$, який

застосовується в арифметиці поля при додаванні точок кривої. Відбираємо випадкову координату $x = x(z)$ = [3 0 2 4 0 2 3 1 1 4 0 0 1 0 3 1 4 3 2 3 0 4 3 1 4 4 3 0 1 4 1 4 2 3 4 4 2 1 4 4 1 3 1 0 1 1 0 0 3 4 4 1 3 3 0 1 2 3 0 0 3 3 2 1 0 3 4 2 3 1 4 4 3 1 1 2 2 1 3 1 1 2 2 3 2 0 4 3 0 2 2 0 4 0 2 0 3 3 1 0 2 2 4 0 1 3 3 2 4 2 2 1 1 0 1 2 2 2 3 1 4 3 4 4 3 3 0 3 1 1 3 2 4 0 2 2 3 1 1 1 1 2 1 3 2 3 3 3 4 0 4 2 4 2 3 2 0 2 1 1 4 3 0 4 2 4 4 1 2 0 3 0 1 3 1 2 2 4 2 1], обчислюємо згідно (1) значення y^2 як $a = (1 - x^2)\cdot(1 - 3x^2)^{-1}$ = [0 3 2 2 4 1 0 0 4 2 2 4 3 0 0 4 1 1 1 0 2 4 4 4 2 1 3 1 3 4 0 4 2 3 1 4 0 0 0 4 1 4 2 1 3 4 0 3 3 2 1 4 3 4 4 0 3 0 0 0 1 3 0 1 0 1 3 1 3 4 4 4 0 1 2 3 3 4 3 2 1 4 3 2 4 2 1 0 3 1 0 4 3 4 1 3 1 1 0 1 1 2 3 2 3 3 2 4 3 0 1 4 3 1 0 0 4 3 1 0 4 2 3 1 4 4 4 1 0 4 0 0 2 3 1 4 2 1 0 4 4 2 4 0 3 1 3 1 2 3 2 3 2 0 1 3 1 1 4 1 1 4 3 2 0 1 3 0 4 3 2 2 0 2 0 1 0 4 0 2 4] (молодша степінь – зліва). Визначення квадратного кореня з елементу a виконаємо за допомогою експоненціювання [5]. У нашому випадку $p = 5 \equiv 1 \bmod 4$, $q = 5^{181} \equiv 5 \bmod 8$. В мультиплікативній групі поля F_q , якщо $a = y^2$ – квадратичний лишок, маємо елементи підгрупи F_5^*

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

Тоді

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

За допомогою цієї формули отримуємо y = [2 0 1 1 3 0 3 2 3 2 3 0 4 3 4 1 2 0 2 1 4 3 2 2 0 1 2 3 2 1 0 0 2 2 3 4 1 4 1 4 2 3 3 2 1 0 0 2 3 0 4 2 2 0 0 1 2 2 3 1 2 1 2 4 3 4 2 3 2 4 0 2 1 2 1 3 4 4 2 2 4 2 1 1 3 0 4 4 3 3 3 0 4 4 0 0 0 0 1 4 4 1 0 0 0 4 1 4 1 2 4 2 2 2 2 3 2 1 1 1 3 2 2 2 1 2 4 0 0 4 0 1 4 1 0 4 0 4 3 1 1 0 1 3 1 2 0 3 2 2 1 4 4 3 0 1 2 4 3 0 0 4 4 3 0 1 0 2 3 2 2 0 1 1 0 2 2 3 1 3 3]

Підстановка знайдених координат $(x, y) = P$ в рівняння (1) дає тотожність, тому ця точка існує. Далі, скалярне множення точки P на порядок n з таблиці 1 дає точку C = (1, 0) 4-го порядку, тому генератором криптосистеми порядку n є точка $G = 4P$. Її координати:

X = [0 3 2 0 1 1 2 2 1 4 2 3 0 4 2 1 1 3 0 3 1 3 2 4 2 2 3 1 0 3 4 0 1 4 4 0 4 0 3 3 4 0 1 4 1 0 1 2 4 0 2 3 3 2 4 3 1 4 0 2 3 3 3 4 3 4 3 1 2 3 0 1 2 4 3 2 0 3 3 0 0 2 0 4 2 3 1 1 1 1 2 3 0 4 3 4 0 4 4 3 0 1 2 1 1 1 4 4 1 0 2 3 1 1 0 0 4 1 4 4 2 4 1 0 0 4 3 0 1 3 3 1 4 1 4 4 1 1 1 0 3 3 0 4 2 3 1 0 1 1 3 1 3 0 4 1 2 3 1 2 1 3 4 1 0 3 1 4 0 4 1 1 2 4 4 4 2 0 0 2]

Y = [3 4 2 2 4 2 4 2 3 3 2 4 1 0 2 0 3 3 0 3 4 3 3 1 1 0 2 2 4 2 4 2 1 2 1 2 2 0 1 0 2 4 3 4 4 3 4 2 1 1 4 1 3 0 0 4 1 3 1 3 2 1 1 3 3 1 1 4 0 2 2 3 2 0 1 0 4 0 2 4 4 1 4 0 3 0 3 4 2 3 3 3 0 1 3 3 0 3 3 4 2 3 3 0 1 4 4 3 2 3 3 0 1 4 0 3 4 2 3 3 1 1 3 1 1 0 3 1 1 4 1 4 2 1 0 3 3 3 1 1 1 1 4 0 2 0 0 3 3 4 2 0 4 1 4 0 2 3 1 1 4 0 2 3 0 0 3 4 2 0 0 3 0 2 0 4 1 1 4 0 4]

У випадку, якщо при тестуванні множенням на n отримано точку 2-го порядку, генератор визначається як $G = 2P$.

Слід зазначити, що знайдені криві з мінімальним значенням параметру d = 3 забезпечать при заданій стійкості найвищу продуктивність обчислень групових операцій. В операції додавання різних точок ми економимо на однієї польовій операції множення 1U на параметр кривої [4], тому що множення на

3 замінюється трикратним додаванням у полі, тобто практично безкоштовною операцією. Арифметика обчислень в розширеннях малих полів часто є більш ефективною, ніж арифметика в простих полях великої характеристики. Вважаємо, що знайдені криві можна рекомендувати для проектів майбутніх стандартів, і також, можливо, для застосування в сучасних криптопротоколах.

Література

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. – 224с.