

НОРМАЛІЗАЦІЯ СКРУЧЕНОЇ КРИВОЇ ЕДВАРДСА ТА ДОСЛІДЖЕННЯ ЇЇ ВЛАСТИВОСТЕЙ НАД F_p

Р. В. Скуратовський^{1, а}, А. А. Мовчан^{2, б}

¹Технічний ліцей НТУУ «КПІ»

²Національний університет НАУКМА

Анотація

В роботах ([1], [2], [3], [4]) були введені і отримані криві Едвардса і скручена крива Едвардса, що не мали особливостей у афінних координатах але мали особливі точки у проєктивному представленні. В данній роботі запропоновано не тільки нормалізовану криву Едвардса а ще й зроблено аналіз її класів суперсингулярних кривих. Дуже важливо знати ті криві, які є суперсингулярними (тобто мають нульовий j -інваріант), бо вони є криптографічно слабкими, хоча вони в деяких випадках не допускають поділу точки попалам. Одними з найпридатніших для швидких обчислень є криві Едвардса [2], що не мають особливих точок у афінній формі та є рекордно швидкими по виконанню групової операції додавання точок а також подвоєння точок. Згідно теореми Хассе [5] порядок групи алгебраїчної кривої $N_E = p + 1 \pm t$. Якщо слід ендоморфізма Фробеніуса $t = 0$, то маємо вироджену пару кривих (крива і крива зі скрутом) з параметром $t = 0$, тому порядки обох кривих співпадають. Такі криві є суперсингулярними кривими. В роботі показано, що скручена крива Едвардса не є еліптичною і зроблено її нормалізацію.

1. Вступ

В еліптичній криптографії дуже важливо знати ті криві, які є суперсингулярними (тобто мають нульовий j -інваріант), бо вони є криптографічно слабкими, хоча вони в деяких випадках не допускають поділу точки попалам. Одними з найпридатніших для швидких обчислень є криві Едвардса [2]. Ознакою виродженості кривої є слід ендоморфізма Фробеніуса t , якщо $t = 0$, то маємо вироджену пару кривих (крива і крива зі скрутом) з параметром $t = 0$, тому порядки обох кривих співпадають. Такі криві є суперсингулярними кривими. В роботі показано, що скручена крива Едвардса не є еліптичною і зроблено її нормалізацію.

Знайдено параметри кривої при яких має місце рівність $t = 0$ і умови максимальності підгрупи простого порядку кривої Едвардса над скінченним полем F_p .

2. Основні результати

Відомо, що якщо слід t ендоморфізма Фробеніуса: $t = 0$, то $N_E = p + 1$, тобто пара відповідних кривих має найменший порядок над даним F_p . Зрозуміло, що вироджена пара скручених кривих отримується при $d = -1$ але ми дослідили всі набори таких коефіцієнтів. Елемент (-1) при $p \equiv 3 \pmod{4}$ є квадратичним лишком [5], тобто є допустимим параметром кривої. Вдалося знайти і деякі такі набори для скрученої кривої Едвардса $E_{a,d}$ [1], що задається рівнян-

ням (1), над різними скінченними полями F_{p^n}

$$\begin{aligned} ax^2 + y^2 &= 1 + dx^2y^2, a, d \in F_p^*, \\ ad(a-d) &\neq 0, d \neq 1, p \neq 2. \end{aligned} \quad (1)$$

Зробимо нормалізацію цієї кривої, тобто знайдемо таке скінченне регулярне відображення $v : X^v \rightarrow X$, яке є біраціональним ізоморфізмом і X^v є нормальним многовидом [6], тобто з цілозамкненими (нормальними) кільцями регулярних функцій $k[X]$, де X – афінний многовид, над своїм полем дробів Q .

Для цього зробимо проєктивізацію кривої (1), нехай $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, тоді $a\frac{x^2}{z^2} + \frac{y^2}{z^2} = 1 + d\frac{x^2y^2}{z^4}$, звідси $F(x, y, z) = ax^2z^2 + y^2z^2 - z^4 - dx^2y^2$ перевіримо умови гладкості (для алгебраїчних кривих поняття гладкості і нормальності співпадають [7])

$$\begin{cases} \frac{\partial F(x, y, z)}{\partial x} = 2axz^2 - 2dxy^2 = 0, \\ \frac{\partial F(x, y, z)}{\partial y} = 2yz^2 + 2dx^2y = 0, \\ \frac{\partial F(x, y, z)}{\partial z} = 2axx^2 + 2zy^2 - 4z^3 = 0, \end{cases}$$

тут розв'язком очевидно є $(0, 0, 0)$ але не вона не належить \mathbb{P}^3 і при $z = 0$ точки $(x_0, 0, 0) = (1, 0, 0)$ і $(0, y_0, 0) = (0, 1, 0)$. Тобто маємо 2 фундаментальні точки $p_1 = (1, 0, 0)$ і $p_2 = (0, 1, 0)$. Це прості особливості. Отже, розв'язками є лише фундаментальні точки (нескінченно віддаленні точки) $(1, 0, 0)$ і $(0, 1, 0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах $A^1 : az^2 + y^2z^2 = z^4 + dy^2$ і $A^2 : ax^2z^2 + z^2 = z^4 + dx^2$.

Застосуємо нормалізаційні заміни, що є біраціональними відображеннями, які дозволяють виразити старі змінні x, y, z через нові регулярно: $x : z = u : w = t : v$, $y : z = t : u = v : w$. Отже, відношення зі змінними $x : z, y : z, x : y$ виражаються регуляр-

^аrqout@ukr.net

^бmovchan.anatolii@ex.ua

но через нові функції які теж є відношеннями. Це перетворює нашу криву (її афінні компоненти) у просторову криву (у тривимірному проективному просторі), що задана двома рівняннями:

$$\begin{cases} au^2 + v^2 = w^2 + dt^2 \\ uv = wt \end{cases}$$

Друге рівняння є рівняння цілої залежності. Таким чином, було зроблено розширення двома новими елементами. Перехід між A^1 і A^2 можна зробити так; нехай $s = v : w$, $r = u : w$, тоді $x : z = rs^{-1}$ і $y : z = sr^{-1}$.

Позначимо $\delta_p = \dim \tilde{\mathcal{O}}_p / \mathcal{O}_p$ розмірність фактора як векторного простору або це геометричний род кривої. Оскільки, базис розширення $\tilde{\mathcal{O}}_p$ над локальним кільцем точки \mathcal{O}_p складається з одного елемента, то $\delta_p = 1$. Тут $\tilde{\mathcal{O}}_p$ – цілозамкнене кільце, $\tilde{\mathcal{O}}_p \simeq k[x, y]_{xy}$. Головний ідеал $m = \langle x, y \rangle = xy$ цього кільця є дво породжений, бо це особлива точка типу самоперетин, тому існує 2 дотичні, що в результаті дають 2 твірні. Аналогічну будову має локальне кільце в точці $p' = (0, 1, 0)$, тому $\delta_{p'} = 1$ теж. Оскільки додали два нові елементи, кожен з яких відповідає своєму локальному кільцю особливої точки, яких теж дві, то $\delta_p = 1$ і $\delta_{p'} = 1$. Отже, підрахуємо род (взагалі род кривої це кількість ЛНЗ регулярних диференціалів) кривої $F(x, y, z) = ax^2z^2 + y^2z^2 - z^4 - dx^2y^2$. При $a \neq d$ ми маємо нерозкладну проективну криву степені 4, тоді згідно [7] род алгебраїчної незвідної проективної кривої:

$\rho^*(C) = \rho_\alpha(C) - \sum_{p \in E} \delta_p = \frac{(n-1)(n-2)}{2} - \sum_{p \in E} \delta_p = 3 - 2 = 1$, де $\rho_\alpha(C)$ – арифметичний род кривої C , параметр $n = \deg C = 4$. Оскільки вона роду 1, то вона ізоморфна плоскій кубічній кривій.

Отже, у процесі нормалізації кривої скрученої Едвардса $E_{a,d}$ стало зрозуміло, що це кубічна крива з двома особливостями типу завузлення. Саме ці завузлення підвищують її степінь до 4. Нормалізацією кожного вузла є пряма.

Дослідимо які класи таких кривих є суперсингулярними.

Теорема 1. Якщо $p \equiv 3 \pmod{4}$ і p – просте, то кількості точок кривої $x^2 + y^2 = 1 + 2x^2y^2$ та кривої $x^2 + y^2 = 1 + 2^{-1}x^2y^2$ співпадають і рівні $N_E = p + 1$ при $p \equiv 3 \pmod{8}$ та $N_E = p - 3$ при $p \equiv 7 \pmod{8}$.

Отже, потрібно показати, що число N_2 , рівне кількості точок на кривій

$$y^2 = (x^2 - 1)(2x^2 - 1), \quad (2)$$

задовільняє умову $N_2 \equiv 1 \pmod{p}$ для $p \equiv 3 \pmod{8}$ і $N_2 \equiv -1 \pmod{p}$ для $p \equiv 7 \pmod{8}$. Тоді матимемо $N_2 = p + 1$ для $p \equiv 3 \pmod{8}$ та $N_2 = p - 1$ для $p \equiv 7 \pmod{8}$. (Випадки $N_2 = 1$ або $N_2 = 2p - 1$ неможливі, бо $N_2 \geq 2$ і $N_2 \leq 2p - 2$). Звідси слідує твердження про кількість точок на початковій кривій (1).

Для фіксованого значення x кількість розв'язків рівняння (2) дорівнює $1 + \left(\frac{(x^2-1)(2x^2-1)}{p}\right)$, де $\left(\frac{a}{p}\right)$ – символ Лежандра. Як відомо, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$, тому для фіксованого x кількість розв'язків рівняння (2) порівнянна за модулем p з $1 + ((x^2 - 1)(2x^2 - 1))^{\frac{p-1}{2}}$. Отже, підсумовуючи за всіма x , маємо

$$\begin{aligned} N_2 &\equiv \sum_{x=0}^{p-1} 1 + ((x^2 - 1)(2x^2 - 1))^{\frac{p-1}{2}} \equiv \\ &\equiv p + \sum_{x=0}^{p-1} (x^2 - 1)^{\frac{p-1}{2}} (2x^2 - 1)^{\frac{p-1}{2}} \pmod{p}. \end{aligned} \quad (3)$$

Розкривши дужки в $(x^2 - 1)^{\frac{p-1}{2}} (2x^2 - 1)^{\frac{p-1}{2}}$, отримуємо, що $a_{2p-2} = 1^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$. Отже,

$$N_2 \equiv -\left(\frac{2}{p}\right) - a_{p-1} \pmod{p}. \quad (4)$$

Нам потрібно було довести, що $N_2 \equiv 1 \pmod{p}$ при $p \equiv 3 \pmod{8}$ і $N_2 \equiv -1 \pmod{p}$ при $p \equiv 7 \pmod{8}$. Тобто треба було показати, що $N_2 \equiv -\left(\frac{2}{p}\right) - a_{p-1} \pmod{p}$ для $p \equiv 3 \pmod{4}$. Це буде слідувати з (3), якщо ми покажемо, що $a_{p-1} \equiv 0 \pmod{p}$. Визначимо a_{p-1} згідно з формулою бінома Ньютона a_{p-1} рівний коефіцієнту при x^{p-1} в добутку двох дужок $\in (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^j)^2$. Нескладно доводитися,

що $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j \equiv 0 \pmod{p}$ при $p \equiv 3 \pmod{4}$. Це завершує доведення.

Важливим параметром кривої є її кофактор [2], бо він визначає її підгрупу простого порядку, ми довели, що для $E_{a,d}$ (1) мінімальний кофактор рівний 4. Для дослідження умов існування точки 8-го порядку на скрученій кривій Едвардса використано формули подвоєння координат точки $2(x, y) = \left(\frac{2xy}{1+dx^2y^2}, \frac{y^2-ax^2}{1-dx^2y^2}\right)$.

Твердження 1. Нами досліджена необхідна і достатня умова існування точок 8-го порядку на $E_{a,d}$ це як виявилось є квадратичність лишків відповідних виразів:

Твердження 2. Для існування точки 8-го порядку на $E_{a,d}$ необхідною і достатньою щоб за умови наявності точки 4-го порядку виконувалися умови: квадратичність лишків над F_p відповідних виразів:

$$a, \left(1 - \frac{d}{a}\right), \left(\frac{1}{d} \left(1 \pm \sqrt{1 - \frac{d}{a}}\right)\right).$$

Тобто $\left(\frac{a}{p}\right) = 1$, $\left(\frac{1-d}{p}\right) = 1$ і $\left(\frac{\frac{1}{d}(1 \pm \sqrt{1 - \frac{d}{a}})}{p}\right) = 1$, де a, d коефіцієнти $E_{a,d}$.

Для знаходження умов існування точки 8-го порядку на скрученій кривій Едвардса використаємо формулу подвоєння координат [1] точки $2(x, y) = \left(\frac{2xy}{1+dx^2y^2}, \frac{y^2-ax^2}{1-dx^2y^2}\right)$. Підставимо у неї координати то-

чки 4-го порядку $2(x, y) = (\frac{1}{\sqrt{a}}, 0)$ і знайдемо координати точки (x, y) , що задовольняє це рівняння.

$$(\frac{2xy}{1+dx^2y^2}, \frac{y^2-ax^2}{1-dx^2y^2}) = (\pm \frac{1}{\sqrt{a}}, 0)$$

Покоординатна відповідність дає систему

$$\begin{cases} \frac{2xy}{1+dx^2y^2} = \frac{1}{\sqrt{a}} \\ \frac{y^2-ax^2}{1-dx^2y^2} = 0 \end{cases} \quad (5)$$

З другої рівності маємо $ax^2 = y^2$, $y = \pm\sqrt{ax}$. Підставивши $y = \pm\sqrt{ax}$ в першу рівність маємо $\frac{2x\sqrt{ax}}{1+dx^2ay^2} = \frac{1}{\sqrt{a}}$. Звідси маємо $2ax^2 = 1+adx^4$ розв'яжемо це рівняння $adx^4 - 2ax^2 + 1 = 0$, $x^2 = \frac{a \pm \sqrt{a^2-ad}}{ad} = \frac{1}{d} \pm \frac{\sqrt{1-\frac{d}{a}}}{d} = \frac{1}{d}(1 \pm \sqrt{1-\frac{d}{a}})$. Виконаємо перевірку $x^2 = \frac{a \pm \sqrt{a^2-ad}}{ad} = \frac{1}{d}(1 \pm \sqrt{1-\frac{d}{a}})$, $x^4 = \frac{1}{d^2}(1 \pm \sqrt{1-\frac{d}{a}})^2 = \frac{1}{d^2}(1 + 1 - \frac{d}{a} \pm 2\sqrt{1-\frac{d}{a}})$, тоді

$$adx^4 - 2ax^2 + 1 = \frac{a}{d}(2 - \frac{d}{a} \pm 2\sqrt{1-\frac{d}{a}}) - \frac{2a}{d}(1 \pm \sqrt{1-\frac{d}{a}}) + 1 = \frac{2a}{d} - 1 \pm \frac{2a}{d}\sqrt{1-\frac{d}{a}} - \frac{2a}{d} \pm \frac{2a}{d}\sqrt{1-\frac{d}{a}} + 1 = 0.$$

Отже, використовується.

Використавши (1) знаходимо $y^2 = \frac{a}{d}(1 \pm \sqrt{1-\frac{d}{a}})$ отже, вираз має бути квадратичним лишком $\frac{a}{d}(1 \pm \sqrt{1-\frac{d}{a}})$. Перевіримо умову належності кривій (1) точок з координатами $x^2 = \frac{1}{d}(1 \pm \sqrt{1-\frac{d}{a}})$, $y^2 = \frac{a}{d}(1 \pm \sqrt{1-\frac{d}{a}})$,

$$\frac{2a}{d}(1 \pm \sqrt{1-\frac{d}{a}}) = 1 + \frac{a}{d}(1 + 1 - \frac{d}{a} \pm 2\sqrt{1-\frac{d}{a}}) = 1 \pm \frac{2a}{d} - 1 \pm \frac{2a}{d}\sqrt{1-\frac{d}{a}} = \frac{2a}{d}(1 \pm \sqrt{1-\frac{d}{a}}).$$

Отже виконується. Перевіримо чи задовольняється формула подвоєння для першої (для другої аналогічно) координати це

$$\begin{aligned} \frac{2\sqrt{ax}}{1+dx^2y^2} &= \frac{2\sqrt{a}\frac{1}{d}(1 \pm \sqrt{1-\frac{d}{a}})}{1+d\frac{a}{d^2}(1 \pm \sqrt{1-\frac{d}{a}})^2} \\ &= \frac{\frac{2\sqrt{a}}{d}(1 \pm \sqrt{1-\frac{d}{a}})}{1+\frac{a}{d}(1+1-\frac{d}{a} \pm 2\sqrt{1-\frac{d}{a}})} = \frac{-1}{\sqrt{a}}. \end{aligned}$$

Знайдемо кофактор для кривої (1), з вище сказаного можна отримати наслідок.

Наслідок 1. Кофактор скрученої кривої Едварса рівний 4 тоді і тільки тоді коли виконуються умови наявності повноти закона додавання точок (наприклад при $(\frac{a}{p}) = 1$ $(\frac{d}{p}) = -1$) і відсутності точок 8-го порядку.

Доведення ґрунтується на твердженні (2) і теоремі Лагранжа а необхідність слідує з того, що якщо

припустити існування точок 8-го порядку і врахувати, що в циклічній групі C_m для кожного $k|m$ існує підгрупа C_k , то вийде, що порядок групи ділиться на 8 але тоді це суперечить умові, де стверджується, що її кофактор 4.

Твердження 3. Необхідною і достатньою умовою подільності навіл точки (X, Y) скрученої кривої Едвардса є $e(\frac{4(1+2dX)}{p}) = 1$, $(\frac{Y^2(1-dt^2)^2+4a^2t^4}{p}) = 1$ і величини $\frac{Y(1-dt^2)\pm\sqrt{D_2}}{2}$ є квадратичними лишками по p , де $D_2 = Y^2(1-dt^2)^2 + 4a^2t^4$.

Тут під подільністю точки (X, Y) навіл розуміється знаходження її праобразу тобто точки (x, y) яка при застосуванні формули подвоєння точки [1]

$$2(x, y) = (\frac{2xy}{1+dx^2y^2}, \frac{y^2-ax^2}{1-dx^2y^2}) = (X, Y)$$

дає точку (X, Y) .

Перелік використаних джерел

1. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2008. PP. 1-17
2. H. Edwards A normal form for elliptic curves. American Mathematical Society. Volume 44, Number 3, July 2007, PP. 393-422.
3. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. Twisted Edwards Curves Revisited. ASIACRYPT 2008, LNCS 5350, PP. 326-343,
4. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme Contract 2002-507932 ECRYPT, 2007. PP. 1-20.
5. Lidl Nideraiter Introduction to Finite Fields and their Applications. By Rudolf Lidl. By Harald Niederreiter. Encyclopedia of Mathematics (No. 20). Cambridge University Press. 1996. P. 755.
6. Дрозд Ю. А. Вступ до алгебраїчної геометрії - Львів Внтл-Класика, 2004, 251 с.
7. W. Fulton Algebraic curves. An Introduction to Algebraic Geometry. Third Preface, January, 2008. P. 121.
8. Montgomery P.L., Speeding the Pollard and Elliptic Curve Methods of Factorizations, Math. Comp. 48, (1987), PP. 243-264.
9. В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева. Теория чисел в криптографии. МГТУ им. Н. Э. Баумана. Учебное пособие, г. 2011, 223 с.
10. Рид М. Алгебраическая геометрия для всех. Москва: Мир, 1991, 143 с.