УДК 512.624.95 + 517.772

ЧИСЛО ІЗОМОРФІЗМІВ ЕЛІПТИЧНОЇ КРИВОЇ ПІД ЧАС ТРАНСФОРМАЦІЙ КАНОНІЧНОЇ ФОРМИ РІВНЯННЯ

А.В. БЕССАЛОВ, В.Є. ЧЕВАРДІН

Представлено результати аналізу аналітичних виразів трансформації несуперсингулярних еліптичних кривих у канонічній формі для криптографічних цілей. Отримано нові результати оцінки верхньої границі числа ізоморфних трансформацій еліптичної кривої в канонічній формі над кінцевим полем Галуа. Так, для поля характеристики p верхня межа числа ізоморфізмів еліптичної кривої при трансформаціях із канонічної в канонічну форму зростає пропорційно p. Для трансформації еліптичної кривої над полем характеристики p із канонічної в нормальну форму верхня границя числа ізоморфізмів зростає пропорційно $p4$. Використання повної множини трансформацій базової еліптичної кривої дозволяє збільшити потужність простору можливих параметрів криптосистем на еліптичних кривих, а також використовувати їх в якості додаткового джерела ентропії. Застосування отриманих результатів для криптографічних генераторів випадкових чисел може дозволити скоротити довжину модуля поля Галуа.

ВСТУП

Актуальним науковим завданням є розробка нових аналітичних виразів, які дозволяють точніше оцінювати параметри та властивості криптографічних примітивів на основі перетворень у групах точок еліптичних кривих. Це зумовлено останніми науковими результатами, які отримані поєднанням великих обчислювальних потужностей, таких як: декодування ДНК людини, вирішення задачі дискретного логарифмування в простому полі з розрядністю чисел 1024 біти і низки інших наукових проблем. Криптоперетворення в групі точок еліптичної кривої дозволяють задовольнити зростаючі вимоги щодо стійкості та швидкодії сучасних систем захисту інформації.

Відомо, що поряд зі спеціальними задачами еліптичної криптографії виникає необхідність переходу до ізоморфних кривих, які зберігають структуру групи точок під час трансформації їх координат. При цьому слід визначити точне число ізоморфізмів або дати хоча б оцінку цього числа.

У цій роботі вказана задача вирішена для часткового випадку канонічної форми базової кривої.

Мета роботи — аналіз можливих трансформацій базової несуперсингулярної еліптичної кривої та отримання аналітичних виразів для оцінки граничних значень множини ізоморфних трансформацій кривої.

ІЗОМОРФНІ ТРАНСФОРМАЦІЇ ЕЛІПТИЧНОЇ КРИВОЇ ТА ОЦІНКА ПОТУЖНОСТІ МНОЖИНИ ІЗОМОРФІЗМІВ ДЛЯ КАНОНІЧНОЇ ФОРМИ ЕЛІПТИЧНОЇ КРИВОЇ

Нормальною формою базової кривої над полем F_p у визначеннях, що прийняті в [1, 3], називається крива виду:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_k \in F_p, \quad (1)$$

яка також є афінною версією рівняння Вейєрштрасса [2].

Лінійне ізоморфне перетворення координат цієї кривої задається формулами:

$$y = u^3\overline{y} + su^2\overline{x} + t, \quad x = u^2\overline{x} + r, \quad u \neq 0, \ u,r,s,t \in \{0,..,p-1\}. \quad (2)$$

При довільних параметрах $\{u,r,s,t\}$ перетворення отримуємо криву виду:

$$\overline{E}: \overline{y}^2 + \overline{a}_1\overline{x}\,\overline{y} + \overline{a}_3\overline{y} = \overline{x}^3 + \overline{a}_2\overline{x}^2 + \overline{a}_4\overline{x} + \overline{a}_6, \overline{a}_i \in F_p. \quad (3)$$

Необхідно отримати співвідношення, які пов'язують коефіцієнти $\overline{a}_i$ ізоморфної кривої $\overline{E}$ з коефіцієнтами базової кривої (1).

Складові рівняння (1), які отримані на основі формули (2), дорівнюють:

$$y^2 = u^6\overline{y}^2 + s^2u^4\overline{x}^2 + t^2 + 2u^5s\overline{x}\,\overline{y} + 2u^3ty + 2u^2stx,$$

$$a_1xy = a_1(u^5\overline{x}\,\overline{y} + u^4s\overline{x}^2 + u^2t\overline{x} + u^3r\overline{y} + u^2sr\overline{x} + rt),$$

$$a_3y = a_3(u^3\overline{y} + u^2s\overline{x} + t),$$

$$x^3 = u^6\overline{x}^3 + 3u^4r\overline{x}^2 + 3u^2r^2\overline{x} + r^3,$$

$$a_2x^2 = a_2(u^4\overline{x}^2 + 2u^2r\overline{x} + r^2),$$

$$a_4x = a_4(u^2\overline{x} + r).$$

Порівнюючи коефіцієнти з (1) та (3), отримаємо:

$$\begin{cases} u\overline{a}_1 = (a_1 + 2s)u^6, \\ u^3\overline{a}_3 = (a_3 + a_1r + 2t)u^6, \\ u^2\overline{a}_2 = (a_2 + 3r - a_1s - s^2)u^6, \\ u^4\overline{a}_4 = (a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)u^6, \\ u^6\overline{a}_6 = (a_6 + a_4r + r^2a_2 + r^3 - ta_3 - rta_1 - t^2)u^6. \end{cases} \quad (4)$$

Тепер рівняння в координатах $\overline{x}, \overline{y}$ має вид:

$$u^6\overline{y}^2 + u^5(a_1 + 2s)\overline{x}\,\overline{y} + u^3(a_3 + a_1r + 2t)y = u^6\overline{x}^3 +$$

$$+ u^4(a_2 + 3r - a_1s - s^2)\overline{x}^2 + u^2(a_4 - sa_3 + 2ra_2 -$$

$$- (t + rs)a_1 + 3r^2 - 2st)\overline{x} + a_6 + a_4r + r^2a_2 + r^3 - ta_3 - rta_1 - t^2.$$

Заміною $\widetilde{y} = u^3\overline{y}$ та $\widetilde{x} = u^2\overline{x}$ це рівняння приводиться до незалежного від параметра u виду:

$$\widetilde{y}^2 + (a_1 + 2s)\widetilde{x}\widetilde{y} + (a_3 + a_1 r + 2t)\widetilde{y} = \widetilde{x}^3 + (a_2 + 3r - a_1 s - s^2)\widetilde{x}^2 +$$
$$+ (a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)\widetilde{x} +$$
$$+ (a_6 + a_4 r + r^2 a_2 + r^3 - ta_3 - rta_1 - t^2).$$

Помноживши це рівняння на u^6 з новою заміною $Y = \widetilde{y}u^3$ та $X = \widetilde{x}u^2$, отримаємо нове рівняння:

$$Y^2 + \overline{a}_1 XY + \overline{a}_3 Y = X^3 + \overline{a}_2 X^2 + \overline{a}_4 X + \overline{a}_6,$$

де

$$\begin{cases} \overline{a}_1 = (a_1 + 2s)u, \\ \overline{a}_3 = (a_3 + a_1 r + 2t)u^3, \\ \overline{a}_2 = (a_2 + 3r - a_1 s - s^2)u^2, \\ \overline{a}_4 = (a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)u^4, \\ \overline{a}_6 = (a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - rta_1 - t^2)u^6. \end{cases} \quad (5)$$

Рівняння в координатах X, Y тотожно рівнянню (1) у координатах $\overline{x}, \overline{y}$, тому ці позначення рівнозначні.

Детальний вивід виразів (5) нам знадобився у зв'язку з помилкою, яку припущено в роботі [1]. У рівняннях (4), що наведені в [1], були втрачені співмножники u^6 у правих частинах. Тому, співмножники u^i відповідних коефіцієнтів з'явилися в лівих частинах рівнянь, а не в правих, як у рівняннях (5). Слід зазначити, що ця помилка не є катастрофічною, так як при $u \neq 0$ в поле F_p, при $p \neq 2, 3$ завжди існує зворотній елемент $v = u^{-1}$.

Для базового рівняння (1), яке записане в канонічній формі маємо $a_1 = a_2 = a_3$, тоді рівняння (5) спрощується:

$$\begin{cases} \overline{a}_1 = 2us, \\ \overline{a}_3 = 2u^3 t, \\ \overline{a}_2 = (3r - s^2)u^2, \\ \overline{a}_4 = (a_4 + 3r^2 - 2st)u^4, \\ \overline{a}_6 = (a_6 + ra_4 + r^3 - t^2)u^6. \end{cases} \quad (6)$$

Нехай γ_1 — число ізоморфних кривих, які отримані трансформацією з канонічної форми в канонічну, при цьому $\overline{a}_1 = \overline{a}_2 = \overline{a}_3 = 0$ та, відповідно, $s = r = t = 0$. Тоді $\overline{a}_4 = u^4 a_4$, $\overline{a}_6 = u^6 a_6$. Число γ_1 визначається об'ємом

множин різних пар $\overline{a}_4$, $\overline{a}_6$, які залежать від значень a_4, a_6 та порядку елементів u^4, u^6 у мультиплікативній групі F_p^*.

Наприклад, при $p=7$ порядок групи $\#F_7^*=6$. Елемент $u^6=1 \bmod 7$, елемент $u^3=\pm 1 \bmod 7$, елемент $u^4 \in \{1,2,4\}$ при $u \neq 1$ має порядок 3. Це означає, що число ізоморфізмів $\gamma_1=1$ при $a_4=0, a_6 \neq 0$ (порушення останньої умови дає сингулярну криву), або $\gamma_1=3$ при $a_4 \neq 1$. Зі збільшенням p число γ_1 зростає. Так, при $p=11$, $F_{11}=10=2*5$, степені елементів u^4, u^6 парні, а самі елементи $u \neq 1$ мають порядок 5. Число різних пар елементів u^4, u^6 також дорівнює 5, тому $\gamma_1=\dfrac{p-1}{2}=5$ при $p=11$. Можна помітити, що пари елементів $(\pm u)^4, (\pm u)^6$ пробігають усі значення квадратичних від'ємників у мультиплікативній групі F_p^*, тому для будь-якого поля верхня границя буде такою:

$$\gamma_1 \leq \frac{p-1}{2}. \tag{7}$$

Звідси видно, що зріст числа ізоморфізмів у канонічній формі кривої лінійний зі збільшенням *p*.

Із рівнянь (6) очевидно, що число ізоморфізмів кривої *E* при ненульових параметрах r, s, t різко зростає. Тут перші 3 параметри кривих лінійно незалежні з розділеними змінними $r, s,$ и $t,$ що дозволяє знайти верхню границю числа ізоморфізмів під час трансформації з канонічної форми у нормальну:

$$\gamma_2 \leq \frac{1}{2}(p-1)p^3. \tag{8}$$

Величина γ_2 зростає вже пропорційно 4-му ступеню порядку p поля. Вже при $p=7$ можна отримати до $3*7^3=1029$ кривих.

Із (2) випливає, що перетворення точки в точку ізоморфної кривої має обчислювальну складність не більш п'яти множень у кінцевому полі (та не більш чотирьох множень для канонічної форми). Також використання для задач криптографії ізоморфних кривих у нормальній формі з оцінкою (8) для числа ізоморфізмів дозволяє під час фіксації цього числа приблизно в чотири рази скоротити довжину модуля поля та відповідно обчислювальну складність операцій у полі.

ВИСНОВКИ

Таким чином, у результаті проведених досліджень було отримано уточнення наведених у [1] виразів для коефіцієнтів ізоморфних еліптичних кривих під час трансформації з нормальної форми в нормальну. На їх основі було отримано нові результати для оцінки верхньої границі кількості ізоморфних

кривих, які наведені в канонічній формі. Так, трансформація кривої з канонічної форми в канонічну дає лінійну залежність (7) верхньої границі числа ізоморфізмів з ростом порядку p поля. Аналогічна границя (8) під час переходу від канонічної форми в нормальну пропорційна вже p^4. Це дозволяє значно збільшити потужність простору ізоморфних кривих у галузі криптографічних додатків, або скоротити довжину модуля поля.

Отримані результати мають користь для оцінки показників стійкості криптографічних алгоритмів на основі перетворень у групі точок еліптичної кривої.

ЛІТЕРАТУРА

1. *Husemöller D.* Elliptic Curves, Second Edition. — NY: Springer–Verlag, 2002. — 487 p.
2. *Смарт Н.* Криптография / Пер. с англ. С.А. Кулешова под ред. С.К. Ландо. — М.: Техносфера, 2005. — 528 с.
3. *Koblitz N.* Primality of the number of points on an elliptic curve over a finite field. — Pacific Journal of Mathematics. — 1988. — **131**, № 1. — P. 157–165.

Надійшла 19.09.2011