УДК 681.3.06

О. Б. Теліженко, аспірант

Інститут Служби зовнішньої розвідки України, м. Київ

СТРУКТУРА ГРУПИ ТОЧОК КРИВОЇ ЕДВАРДСА, ЩО НЕ МІСТИТЬ ТОЧОК ВОСЬМОГО ПОРЯДКУ

Розглядаються криві Едвардса, що не містять точок восьмого порядку. Наведений опис всіх підгруп і всіх суміжних класів.

Ключові слова: *крива Едвардса, підгрупа, суміжні класи.*

Вступ. Еліптичні криві в формі Едвардса (криві Едвардса) [1] є найбільш перспективними для використання в асиметричних криптографічних системах.

Ці криві мають ряд переваг у порівнянні з відомими еліптичними кривими у канонічній формі [2], таких як швидкодія, універсальність закону додавання та наявність афінних координат нейтрального елемента (нуля) абелевої групи точок. Із симетрії точок кривих Едвардса відносно обох координатних осей випливають цікаві та зручні властивості цих кривих.

Ці властивості були виявлені та обґрунтовані вже в першій роботі [2] фахівців з криптографії.

Переваги побудови асиметричних систем саме на кривих Едвардса привернули до них увагу як закордонних (див., напр. [1, 2, 4]), так і вітчизняних авторів [5–8]. Нині криві Едвардса активно досліджуються у всьому світі, зокрема, вивчається можливість розробки нових стандартів цифрового підпису, що базуються на кривих Едвардса. Особливо цікавими з практичної точки зору є криві Едвардса, у яких порядок дорівнює $4N$, де N — велике просте число. Криві Едвардса, порядок яких ділиться на 8, є занадто надлишковими — адже для побудови підпису все одно використовується підгрупа простого порядку.

Стійкість цифрового підпису на еліптичних кривих базується на складнорозв'язувальності задачі *DLP* у підгрупі групи точок кривої. Для того, щоб ця задача мала лише експоненційні алгоритми розв'язку, на криву накладаються певні обстеження ([9]): великий порядок поля, або великий простий степінь розширення, наявність підгрупи великого простого поля, MOV-умова, тощо. При порушенні будь-якої з перелічених вимог цифровий підпис стає вразливим до атак певних типів.

Серед атак на криптосистеми, що базуються на задачі *DLP*, особливе місце займають так звані спеціальні атаки — такі, що використовують особливості самої циклічної групи, в якій розглядається ця задача. Тому при побудові такої криптосистеми необхідно вивчити структуру відповідної групи, її певні особливості.

Для розв'язання задачі *DLP* важливе значення має структура групи точок кривої Едвардса [1, 2]. Потужність групи точок кривої Едварда завжди кратна 4 [1, 2].

В цій роботі ми повністю описуємо структуру групи кривої Едвардса, а саме всі підгрупи цієї групи та усі класи суміжності за цими підгрупами.

Основні терміни та позначення. У цьому розділі ми наведемо основні терміни, позначення та математичні результати, які будуть використовуватися у цій роботі.

Крива Едвардса над простим полем F_p, де $p \neq 2$ [1] задається рівністю

$$E: x^2 + y^2 = 1 + dx^2 y^2,\ d \in F_p^*,\ d \neq Q_p. \qquad (1)$$

Для множини точок кривої Едвардса задається операція додавання, відносно якої множина буде циклічною абелевою групою, що породжується деякою точкою $G = (x, y) \in E$, $x \in F_p$, $y \in F_p$: $E =< G >$. Точку G можна знайти, наприклад, згідно алгоритму, що описаний у [3].

Правила додавання точок кривої Едвардса задаються формулою

$$\forall R, S \in E,\ R = (x_1, y_1),\ S = (x_2, y_2):$$

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right), \qquad (2)$$

де $1 - dx_1 x_2 y_1 y_2 \neq 0$, $1 + dx_1 x_2 y_1 y_2 \neq 0$, $\forall x_1, x_2, y_1, y_2 \in F_p^*$.

Для подальшого викладання нам знадобиться низка наступних відомих результатів.

Як було зазначено, порядок кривої Едвардса E завжди ділиться на 4. Для криптографічних застосувань, як правило, використовуються криві Едвардса такі, що $|E| = 4N$, де N — (велике) просте число. У цій роботі ми будемо розглядати саме такі криві.

За теоремою Лагранжа [3], для довільної підгрупи $H < E$ виконується рівність

$$|E| = (E : H) \cdot |H|.$$

Як відомо [3], група точок кривої Едвардса E є циклічною. Тому, за теоремою про властивості циклічної групи [2], для будь-якого дільника d порядку групи $|E|$ існує рівно $\varphi(d)$ елементів порядку d.

Якщо $|E| = 4N$, де N — просте, то у групі E існує одна точка першого порядку (це точка $O = (0,1)$), одна точка другого порядку — точка $D = (–1, 0)$ та дві точки четвертого порядку: $\pm F = (\pm 1, 0)$. Далі, у

цій групі існує $\varphi(N) = N-1$ точок порядку N, $\varphi(2N) = N-1$ точок порядку $2N$ та $\varphi(4N) = 2(N-1)$ точок порядку $2N$.

Згідно теореми про циклічну групу [2], у групі E існує єдина підгрупа H_1 порядку 1, єдина підгрупа H_2 порядку 2, єдина підгрупа H_4 порядку 4, єдина підгрупа H_N порядку N, єдина підгрупа H_{2N} порядку $2N$, єдина підгрупа H_{4N} порядку $4N$. Підгрупи H_1 та H_{4N} називаються тривіальними.

Згідно теореми Лагранжа, для будь-якої $H < E$ існують такі $g_1,...,g_k \in E$, де $k = \dfrac{|E|}{|H|} = (E:H)$, що

$$E = (g_1 + H) \bigcup ... \bigcup (g_k + H),$$

де $g_i + H$, $i = \overline{1,k}$ — різні ліві класи суміжності групи E за підгрупою H, причому при $i \neq j$ виконується

$$g_i + H \bigcap g_j + H = \varnothing.$$

Основні результати. У цьому розділі ми визначимо класи суміжності за всіма нетривіальними підгрупами групи E. Також покажемо, які елементи можуть породжувати ці класи.

Теорема 1. Нехай G — утворюючий елемент групи E, $H_{2N} =< 2G >$. Тоді:

1) $|H_{2N}| = 2N$;

2) $$E = H_{2N} \bigcup (G + H_{2N}). \qquad (3)$$

Доведення. Спочатку доведемо, що $|H_{2N}| = 2N$. За теоремою про властивість циклічної групи [3],

$$\operatorname{ord} 2G = \frac{|E|}{(|E|,2)} = \frac{4N}{2} = 2N.$$

Оскільки $H_{2N} =< 2G >$, то $|H_{2N}| = \operatorname{ord} 2G = 2N$. Перше твердження доведено.

Оскільки $|E| = 4N$, то за теоремою Лагранжа [3] в групі E існує $\dfrac{4N}{2N} = 2$ класи суміжності за підгрупою H_{2N}, і $E = H_{2N} \bigcup (A + H_{2N})$ для деякого $A \in E$. Тому для доведення (3) достатньо довести, що класи суміжності H_{2N} та $G + H_{2N}$ є різними. Дійсно, якщо ці класи співпадають, то за властивостями класів суміжності [3] $G \in H_{2N}$. За умови теореми, $< G >= E$ і якщо $G \in H_{2N}$, то $E \subset H_{2N}$. Маємо протиріччя з тим, що $|H_{2N}| = 2N$, а $|E| = 4N$. Друге твердження доведено.

Теорема 2. Нехай G — утворюючий елемент групи E, $H_N =< 4G >$. Тоді:

1) $|H_N| = N$;

2) $$E = H_N \bigcup (G + H_N) \bigcup (2G + H_N) \bigcup (3G + H_N). \quad (4)$$

Доведення. Доведемо, що $|H_N| = N$. За теоремою про властивість циклічної групи [3],

$$\text{ord}4G = \frac{|E|}{(|E|, 4)} = \frac{4N}{4} = N.$$

Оскільки $H_N =< 4G >$, то $|H_N| = \text{ord}4G = N$. Перше твердження доведено.

Оскільки $|E| = 4N$, то за теоремою Лагранжа [3] в групі E існує $\frac{4N}{N} = 4$ класи суміжності за підгрупою H_N, і $E = H_N \bigcup (A_1 + H_N) \bigcup$ $\bigcup (A_2 + H_N) \bigcup (A_3 + H_N)$ для деяких $A_i \in E$, $i = \overline{1,3}$. Для доведення (4) достатньо довести, що класи суміжності H_N, $G + H_N$, $2G + H_N$, $3G + H_N$ — різні.

Дійсно, якщо суміжні класи $iG + H_N$ та $jG + H_N$, $i = \overline{0,3}$, $j = \overline{0,3}$, $j > i$ мають спільний елемент, то існують точки $R_1 \in H_N$ та $R_2 \in H_N$ такі, що $iG + R_1 = jG + R_2$. Звідси випливає, що

$$R_1 - R_2 = jG - iG = (j - i)G \in H_N =< 4G >.$$

Маємо, що $j - i = 4k$, де $k \in Z$, або $j = i + 4k$. Ця рівність виконується тільки тоді, коли $k = 0$, або $j = i$. Тобто класи $iG + H_N$ та $jG + H_N$ співпадають. Друге твердження доведене.

Теорема 3. За підгрупою H_4 група E розкладається на N суміжних класів:

$$E = H_4 \bigcup (G + H_4) \bigcup (2G + H_4) \bigcup ... \bigcup ((N-1)G + H_4). \quad (5)$$

Доведення. У групі E існує тільки одна підгрупа порядку 4 [2] $H_4 = \{(0,1), (1,0), (-1,0), (1,1)\}$.

Оскільки $|E| = 4N$, то за теоремою Лагранжа [3] в групі E існує $\frac{4N}{4} = N$ класів суміжності за підгрупою H_4, і $E = H_4 \bigcup (A_1 + H_4) \bigcup$ $\bigcup (A_2 + H_4) \bigcup ... \bigcup (A_{n-1} + H_4)$ для деяких $A_i \in E$, $i = \overline{1, n-1}$. Для доведення (5) достатньо довести, що класи суміжності $jG + H_4$, де $j = \overline{0, N-1}$ — різні.

Дійсно, якщо суміжні класи $iG + H_4$ та $jG + H_4$, $i = \overline{0, N-1}$, $j = \overline{0, N-1}$, $j > i$ мають спільний елемент, то існують точки $R_1 \in H_4$ та $R_2 \in H_4$ такі, що $iG + R_1 = jG + R_2$. Звідси випливає, що

$$R_1 - R_2 = jG - iG = (j-i)G \in H_4,\ i = \overline{0, N-1},\ j = \overline{0, N-1},\ j > i.$$

Маємо протиріччя із структурою групи H_4, якщо $jG \neq iG$. Теорема доведена.

Теорема 4. За підгрупою H_2 група E розкладається на $2N$ суміжних класів.

$$E = H_2 \cup (G + H_2) \cup (2G + H_2) \cup ... \cup ((2N-1)G + H_2). \qquad (6)$$

Доведення. У групі E існує тільки одна підгрупа порядку 2 [3] $H_2 = \{(-1, 0), (0, 1)\}$.

Оскільки $|E| = 4N$, то за теоремою Лагранжа [3] в групі E існує $\frac{4N}{2} = 2N$ класів суміжності за підгрупою H_2, і $E = H_2 \cup (A_1 + H_2) \cup \cup (A_2 + H_2) \cup ... \cup (A_{2N-1} + H_2)$ для деяких $A_i \in E$, $i = \overline{1, 2N-1}$. Для доведення (6) достатньо довести, що класи суміжності $jG + H_2$, де $j = \overline{0, 2N-1}$ — різні.

Дійсно, якщо суміжні класи $iG + H_2$ та $jG + H_2$, $i = \overline{0, 2N-1}$, $j = \overline{0, 2N-1}$, $j > i$ мають спільний елемент, то існують точки $R_1 \in H_2$ та $R_2 \in H_2$ такі, що $iG + R_1 = jG + R_2$. Звідси випливає, що

$$R_1 - R_2 = jG - iG = (j-i)G \in H_2,\ i = \overline{0, 2N-1},\ j = \overline{0, 2N-1},\ j > i.$$

Маємо протиріччя із структурою групи H_2, якщо $jG \neq iG$. Теорема доведена.

Висновки. Отже, у роботі описані всі можливі підгрупи групи точок кривої Едвардса E та всі класи суміжності за цими підгрупами.

Список використаних джерел:

1. Edwards H. M. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*. July 2007. Vol. 44, N 3. P. 393–422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. *IST Programme under Contract IST-2002-507932 ECRYPT*. 2007. P. 1–20.
3. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра: В 2-х т. М.: Гелиос-АРВ, 2003.
4. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christinne. Twisted Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498, 2008. P. 1–17.
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. Kovalchuk L., Bessalov A. Exact Number of Elliptic Curves in the Canonical Form, Which are isomorphic to Edwards Curves over Prime field. *Cybernetics and Systems Analysis.* 2015. Vol. 51. I. 2. P. 165–172.
7. Ковальчук Л. В., Бессалов А. В., Беспалов А. Ю. Алгоритм генерации базовой точки кривой Эдвардса с использованием критериев делимости точки. *Кибернетика и системный анализ.* 2016. Т. 52. № 5. С. 14–24.
8. Бессалов А. В., Цыганкова О. В. Новые свойства кривой Эдвардса над простым полем. *Радиотехника*. 2015. № 180. С. 137–143.
9. Державний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, 2003.

Edwards curves are considered which have no points of the order eight. The description is given for all subgroups and all correspondent adjacement classes.

Key words: *Edwards curve, subgroup, adjacement classes.*

Одержано 28.02.2017

УДК 004.383.3

Р. Б. Трембач*, канд. техн. наук, доцент,
Б. Р. Трембач,** аспірант,
А. І. Сидор*,** аспірант,
Г. В. Возна*,** студентка

* Тернопільський національний технічний університет імені І. Пулюя, м. Тернопіль,
** Національний університет «Львівська політехніка», м. Львів,
*** Тернопільський національний економічний університет, м. Тернопіль

СТРУКТУРА ТА СИСТЕМНІ ХАРАКТЕРИСТИКИ СПЕЦПРОЦЕСОРІВ ВИЗНАЧЕННЯ ХЕММІНГОВОЇ ВІДДАЛІ РЕАЛІЗОВАНИХ В РІЗНИХ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСАХ

В роботі розглядається структура та системні характеристики компонентів багаторозрядних спецпроцесорів. Розроблено спецпроцесор сканування та визначення Хеммінгової віддалі між кодами представленими в унітарному теоретико-числовому базисі перетворення у двійковий код Радемахера.

Ключові слова: *спецпроцесор, теоретико-числовий базис, Хеммінгова віддаль.*

Вступ. Теоретичні основи елементної бази структурних та функціональних компонентів універсальних цифрових процесорів та спецпроцесорів закладені в багатьох роботах відомих вчених та спе-

