КІБЕРНЕТИКА

УДК 621.391.15 : 519.7

А.В. БЕССАЛОВ
Київський університет імені Бориса Грінченка, Київ, Україна,
e-mail: *a.bessalov@kubg.edu.ua.*

С.В. АБРАМОВ
Київський університет імені Бориса Грінченка, Київ, Україна,
e-mail: *s.abramov.asp@kubg.edu.ua*.

ОСОБЛИВІ ВЛАСТИВОСТІ ЗАКОНУ ДОДАВАННЯ ТОЧОК НЕЦИКЛІЧНИХ КРИВИХ ЕДВАРДСА

Анотація. Проведено аналіз особливих властивостей двох класів квадратичних і скручених кривих Едвардса, що враховують їхню нециклічну структуру, а також неповноту закону додавання точок. Обидва класи кривих містять особливі точки 2-го і 4-го порядків за однією нескінченною координатою, що породжують точки з невизначеністю $0/0$ в одній з координат суми, які названо нечіткими точками. Сформульовано і доведено п'ять теорем, що дають змогу розв'язати ці невизначеності і задати умови, за якими закон додавання точок у таких класах кривих є повним.

Ключові слова: крива в узагальненій формі Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, особлива точка, нечітка точка, колесо точок, квадратичний лишок, квадратичний нелишок.

ВСТУП

Одним із перспективних протоколів постквантової криптографії (Post Quantum Crypthography, PQC) нині є протокол відкритого обміну ключами — алгоритм CSIDH [1] на ізогеніях суперсингулярних еліптичних кривих над полем F_p з мінімальною довжиною ключа. У реалізаціях алгоритму CSIDH раніше використовували швидку арифметику ізогеній кривих Монтгомері. У роботі [2] запропоновано новий ефективний метод обчислення ізогеній непарних ступенів на повних кривих Едвардса на основі w-координат Фарашахи–Хоссейні. У роботах [3, 4] замість повних кривих Едвардса обґрунтовано і проілюстровано на прикладі імплементацію алгоритму CSIDH на квадратичних і скручених кривих Едвардса.

Значними перевагами повних кривих Едвардса з одним параметром d ($\chi(d) = -1$), визначених у роботі [5], є повнота та універсальність закону додавання точок, технологічність, афінні координати нейтрального елемента групи точок. Введення другого параметра a кривої $E_{a,d}$ в роботі [6] дало змогу розширити клас кривих Едвардса і створити згідно з прийнятою в [7–9] класифікацією два нових класи: скручені і квадратичні криві Едвардса. Ці класи утворюють пари квадратичного кручення, які є перспективними для імплементації алгоритму CSIDH [4].

Особливістю таких класів нециклічних кривих Едвардса (з трьома точками 2-го порядку) порівняно з повними кривими Едвардса є втрата властивості повноти закону додавання точок [6]. Це означає, що існують пари точок, сума яких породжує особливі точки, де одна координата є нескінченною (нуль у знаменнику формул додавання), а також за допомогою програмування було виявле-

но пари доданків, що утворюють невизначеності 0 / 0 в цих формулах. У певному сенсі ці точки можна вважати небезпечними, бо вони призводять до збою програм обчислень групових операцій. Це зумовило проведення детального аналізу подібних проблем. Мета цієї статті — аналіз особливих властивостей квадратичних і скручених кривих Едвардса, пов'язаних з неповнотою закону додавання точок. Це дає змогу сформувати та визначити умови, які забезпечують коректне обчислення скалярних добутків у таких класах кривих Едвардса. Зокрема, вибір випадкової точки в алгоритмі CSIDH для кожної ізогенної кривої з високою ймовірністю утворює точку парного порядку, потенційно небезпечну.

Аналіз у цій роботі базується на низці властивостей квадратичних і скручених кривих Едвардса, які утворюють пари квадратичного кручення [6–9]. Суперсингулярні криві цих класів, що мають однаковий порядок $N_E = p+1 = 2^m n$, $m \geq 3$ (де n — непарне), існують лише для $p \equiv 3 \bmod 4$ [9–11]. Мінімальний парний кофактор порядку таких кривих дорівнює 8, тоді справедливо $p \equiv 7 \bmod 8$. У цій роботі ми не обмежуємось суперсингулярними кривими Едвардса, а розглядаємо також для повноти випадок $p \equiv 1 \bmod 4$ (розд. 3).

У розд. 1 наведено короткий огляд властивостей класів кривих Едвардса за класифікацією, прийнятою в [7, 9]. У розд. 2 розглянуто специфічні аспекти неповноти закону додавання точок квадратичних кривих Едвардса, сформульовано та доведено три теореми про точки з нулями у знаменниках формул додавання, наведено приклад. У розд. 3 такі ж самі результати з доведенням двох теорем отримано для скручених кривих Едвардса за умови $p \equiv 3 \bmod 4$ і $p \equiv 1 \bmod 4$, що спричиняє суттєві розбіжності у порядках цих кривих. Найбільш важливим результатом розд. 2 і 3 є доведення повноти закону додавання точок для точок непарного порядку цих кривих та їхніх підгруп, що не містять особливих точок.

1. КЛАСИ КРИВИХ В УЗАГАЛЬНЕНІЙ ФОРМІ ЕДВАРДСА

Розглянемо деякі специфічні властивості нециклічних кривих Едвардса [7, 9]. Еліптична крива в узагальненій формі Едвардса визначається рівнянням

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2 y^2,\ a, d \in F_p^*,\ a \neq d,\ d \neq 1. \tag{1}$$

Якщо квадратичний характер $\chi(ad) = -1$, крива (1) є ізоморфною повній кривій Едвардса [5] з одним параметром d

$$E_d: x^2 + y^2 = 1 + dx^2 y^2,\ \chi(d) = -1. \tag{2}$$

Ця крива циклічна, для неї справджується повний закон додавання точок [5] і не є предметом нашого аналізу.

У випадку $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ має місце ізоморфізм кривої (1) з квадратичною кривою Едвардса [7]

$$E_d: x^2 + y^2 = 1 + dx^2 y^2,\ \chi(d) = 1,\ d \neq 1, \tag{3}$$

яка має (на відміну (2)) параметр d, визначений як квадратичний лишок. Для обох кривих (2) і (3) зазвичай приймають $a = 1$. У роботі [6] криву (3) і криву (2) названо кривими Едвардса. Водночас відмінність квадратичних характерів цих кривих зумовлює кардинально різні їхні властивості. Виходячи з цього, було запропоновано нову класифікацію [7].

Скручену криву Эдвардса визначено в роботі [7] як окремий випадок кривої (1) для $\chi(ad) = 1,\ \chi(a) = \chi(d) = -1$.

Модифікований закон додавання точок кривої (1) запишемо у вигляді

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 x_2 - a y_1 y_2}{1 - d x_1 y_1 x_2 y_2}, \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 y_1 x_2 y_2} \right). \tag{4}$$

Закон подвоєння точки (x_1, y_1) відповідно має вигляд

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2 y_1^2}, \frac{2x_1 y_1}{1 + dx_1^2 y_1^2} \right). \tag{5}$$

За допомогою (5) легко перевірити, що будь-яка крива Едвардса містить точку 2-го порядку $D_0 = (-1, 0)$ та, за винятком скручених кривих Едвардса, — дві точки 4-го порядку $\pm F_0 = (0, \pm 1)$. У цій роботі ми аналізуємо особливості закону додавання точок для нециклічних кривих Едвардса (1) за умови $\chi(ad) = 1$, тобто для класів квадратичних та скручених кривих Едвардса. Головною їхньою відмінністю від циклічних повних кривих (2) є наявність двох нових особливих точок 2-го порядку з нескінченною y-координатою, що породжує нециклічну підгрупу 4-го порядку точок 2-го порядку. У свою чергу, це призводить до неповноти закону додавання точок (1) і проблем під час програмування обчислень скалярних добутків точок.

Рівняння (1) можна записати раціональними функціями

$$y^2 = \frac{1 - x^2}{a - dx^2}, \; x^2 = \frac{1 - ay^2}{1 - dy^2}.$$

Нулі у знаменниках цих функцій породжують особливі точки 2-го та 4-го порядків

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty \right), \; \pm F_1 = \left(\infty, \pm \frac{1}{\sqrt{d}} \right). \tag{6}$$

Знак ∞ ми ставимо у разі ділення на нуль. З використанням правил граничного переходу і формули (5) отримаємо

$$2F_1 = \left(\frac{a\infty^2}{-d\frac{a}{d}\infty^2}, \frac{2x_1\infty}{dx_1^2\infty^2} \right) = (-1, 0) = D_0,$$

де D_0 — точка 2-го порядку будь-якої кривої Едвардса така, що $2D_0 = (1, 0) = O$ (O — нейтральний елемент групи точок). Аналогічно можна переконатися, що $2D_{1,2} = (1, 0) = O$. Із формул (6) випливає, що над простим полем F_p особливі точки $D_{1,2}$ існують в обох класах квадратичних і скручених кривих Едвардса, а точки 4-го порядку $\pm F_1$ — тільки в класі квадратичних кривих Едвардса.

Отже, всі нециклічні криві Едвардса містять три циклічні підгрупи 2-го порядку $G_2^{(0)} = \{O, D_0\}$, $G_2^{(1)} = \{O, D_1\}$, $G_2^{(2)} = \{O, D_2\}$, одну циклічну підгрупу G_n точок непарного порядку n, а квадратичні криві Едвардса, крім того, містять дві циклічні підгрупи 4-го порядку: $G_4^{(0)} = \{O, F_0, D_0, -F_0\}$, $G_4^{(1)} = \{O, F_1, 2F_1 = D_0, 3F_1 = -F_1\}$.

Згідно з (4) сума довільної точки (x_1, y_1) і однієї з точок 2-го або 4-го порядку має координати:

$$(x_1, y_1) + (-1, 0) = (-x_1, -y_1), \tag{7}$$

$$(x_1, y_1) + (0, \pm 1) = (-(\pm) ay_1 \pm x_1), \tag{8}$$

$$(x_1, y_1) + \left(\pm\sqrt{\frac{a}{d}}, \infty \right) = \left(\pm\sqrt{\frac{a}{d}} \cdot x_1^{-1}, \frac{\pm 1}{\sqrt{ad}} \cdot y_1^{-1} \right), \tag{9}$$

$$(x_1, y_1) + \left(\infty, \pm \frac{1}{\sqrt{d}} \right) = \left(\pm \frac{-1}{\sqrt{d}} \cdot x_1^{-1}, \pm \frac{1}{\sqrt{d}} \cdot y_1^{-1} \right). \tag{10}$$

Зокрема, якщо (x_1, y_1) — точка непарного порядку, то суми (7) та (9) визначають точку парного порядку $2n_1$, а суми (8) та (10) — точку парного порядку $4n_1$. Зауважимо, що проблеми з неповнотою закону додавання точок виникають тільки для точок (9) і (10), утворених за допомогою особливих точок, що мають одну нескінченну координату.

2. ОСОБЛИВОСТІ ЗАКОНУ ДОДАВАННЯ ТОЧОК КВАДРАТИЧНИХ КРИВИХ ЕДВАРДСА

Розглянемо квадратичні криві (3), що містять усі особливі точки (6). Нехай деяка підгрупа цих кривих містить точки 4-го порядку $\pm F_1 = (\infty, \pm 1/\sqrt{d})$, для яких, як зазначено вище, $\pm 2F_1 = (-1, 0) = D_0$. Ця циклічна підгрупа є прямою сумою $G_4^{(1)} \oplus G_n$ і має порядок $4n$. Крива (3) з мінімальним кофактором 8 має порядок $N_E = 8n$ (n — непарне число), до того ж максимальний порядок точки дорівнює $4n$. Нехай $P = (x_1, y_1)$, $Ord\, P = 4n$. Тоді $nP = F_1$, $2nP = D_0$, $3nP = -F_1$, $4nP = O = (1, 0)$. Підгрупа $\langle P \rangle = \{kP \mid k = 1, \ldots, 4n\}$ пробігає всі точки «колеса точок» (рис. 1), причому кожна діагональ колеса згідно з (7) зв'язує точки (x, y) і $(-x, -y)$ з протилежними за знаком координатами. Іншою важливою властивістю колеса точок є горизонтальна асиметрія точок: точки верхнього та нижнього півкола обернені одна до одної ($kP \Leftrightarrow -kP$), тобто мають однакові x-координати та протилежні y-координати. Звідси випливає, що відносно вертикальної діагоналі симетричні точки мають протилежні за знаком x-координати і однакові за знаком y-координати. Ці властивості кривих (2) і (3), що породжуються подвійною симетрією координат їхніх точок, дають змогу легко (без обчислень) побудувати всі точки колеса за відомими точками першого лівого квадранта [8].

За відомими $P = (x_1, y_1)$ і $(n-1)P = (x_2, y_2)$ відповідно до формули (4) отримуємо особливу точку 4-го порядку

$$\left(\frac{x_1 x_2 - y_1 y_2}{1 - d x_1 y_1 x_2 y_2}, \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 y_1 x_2 y_2} \right) = F_1 = \left(\infty, \frac{1}{\sqrt{d}} \right).$$

Звідси випливає рівність $1 - d x_1 y_1 x_2 y_2 = 0$.

За вертикальною асиметрією x-координат точок колеса для точки $(n+1)P = (-x_2, y_2)$ (яка є симетричною точці (x_2, y_2)) у разі додавання з точкою $P = (x_1, y_1)$ отримаємо в знаменнику y-координати суми точок вираз $1 + d x_1 y_1 x_2 y_2 = 0$. Цей результат є наслідком неповноти закону додавання точок парного порядку кривих (3). Умовно кажучи, закон додавання точок у цьому випадку не є коректним. Із перетворення в нуль знаменника y-координати в наступній точці після точки $F_1 = (\infty, 1/\sqrt{d})$ не завжди можна отримати особливу точку 2-го порядку. Підгрупа $\langle P \rangle$ містить тільки неособливу точку 2-го порядку $2nP = D_0$. Насправді у формулі (4) в y-координаті виникає невизначеність $0/0$, яку потрібно розв'язати. Точку, в якій за законом додавання (4) виникає така невизначеність, назвемо нечіткою.

Під час програмування групових операцій із випадковими точками поява нечіткої точки призводить до збою обчислень, що потребує захисних заходів. Оскільки відомою є точка $F_1 - 2P = (x_3, y_3)$, координати нечіткої точки, яку потрібно отримати, визначаються як $F_1 + 2P = (-x_3, y_3)$. Той самий результат можна одержати за допомогою формули (10). Доведемо таку теорему.

Теорема 1. Нехай циклічна підгрупа $\langle P \rangle$ квадратичної кривої Едвардса (3), що генерується точкою $P = (x_1, y_1)$ порядку $Ord\, P = 4n$, містить особливу точку 4-го порядку $F_1 = (\infty, 1/\sqrt{d})$. Тоді суми точок $kP + (n+k)P$ і $kP + (3n+k)P$, $k < n/2$, породжують дві нечіткі точки: $(n+2k)P$ та $(3n+2k)P$.

Доведення. Циклічна підгрупа $\langle P\rangle$ за умовами теореми є сумою підгруп $\{G_4^{(1)} = \{O, F_1, 2F_1 = D_0, 3F_1 = -F_1\}\} \oplus G_n$. Вона має порядок $4n$ і містить точки $nP = F_1, 2nP = D_0, 3nP = -F_1$ та $4nP = O = (1, 0)$, серед яких є дві особливі точки $\pm F_1$ 4-го порядку. Послідовне експоненціювання точки P в першому квадранті колеса точок $\{kP \mid k = 1\ldots n\}$ визначає сегмент неособливих точок $\{kP \mid k = 1\ldots n-1\}$ і особливу точку $nP = F_1 = (\infty, 1/\sqrt{d})$. Позначимо $\{kP = (x_k, y_k)\}$, тоді згідно з (7) і з урахуванням вертикальної асиметрії x-координат точок колеса справедлива рівність $(x_{n+k}, y_{n+k}) = (-x_{n-k}, y_{n-k})$. Згідно з (4) у разі додавання точок $kP + (n-k)P$ отримаємо

$$\left(\frac{x_k x_{n-k} - y_k y_{n-k}}{1 - dx_k y_k x_{n-k} y_{n-k}}, \frac{x_k y_{n-k} + y_k x_{n-k}}{1 + dx_k y_k x_{n-k} y_{n-k}}\right) = F_1 =$$

$$= \left(\infty, \frac{1}{\sqrt{d}}\right) \Rightarrow 1 - dx_k y_k x_{n+k} y_{n+k} = 0. \qquad (11)$$

Для суми точок $kP + (3n-k)P$, що містять обернену точку $3F_1 = -F_1$, аналогічно отримаємо

$$\left(\frac{x_k x_{3n-k} - y_k y_{3n-k}}{1 - dx_k y_k x_{3n-k} y_{n-k}}, \frac{x_k y_{3n-k} + y_k x_{3n-k}}{1 + dx_k y_k x_{3n-k} y_{3n-k}}\right) = 3F_1 =$$

$$= \left(\infty, \frac{-1}{\sqrt{d}}\right) \Rightarrow 1 - dx_k y_k x_{3n+k} y_{n3+k} = 0. \qquad (12)$$

Замінимо в цих рівностях точку $(n-k)P$ на точку $(n+k)P$ та точку $(3n-k)P$ на $(3n+k)P$ і з урахуванням властивості $(x_{n+k}, y_{n+k}) = (-x_{n-k}, y_{n-k})$ отримаємо суми точок $(n+2k)P$ та $(3n+2k)P$:

$$\left(\frac{x_k x_{n+k} - y_k y_{n+k}}{1 - dx_k y_k x_{n+k} y_{n+k}}, \frac{x_k y_{n+k} + y_k x_{n+k}}{1 + dx_k y_k x_{n+k} y_{n+k}}\right) =$$

$$= \left(\frac{-x_{k1} x_{n-k} - y_k y_{n-1}}{1 + dx_k y_k x_{n-k} y_{n-k}}, \frac{x_1 y_{n-k} - y_k x_{n-k}}{1 - dx_k y_k x_{n-k} y_{n-k}}\right) =$$

$$= (n+2k)P = (x_{n+2k}, y_{n+2k}) = (-x_{n-2k}, y_{n-2k}), \qquad (13)$$

$$\left(\frac{x_k x_{3n+k} - y_k y_{3n+k}}{1 - dx_k y_k x_{3n+k} y_{3n+k}}, \frac{x_k y_{3n+k} + y_k x_{3n+k}}{1 + dx_k y_k x_{3n+k} y_{3n+k}}\right) =$$

$$= \left(\frac{-x_{k1} x_{3n-k} - y_k y_{3n-1}}{1 + dx_k y_k x_{3n-k} y_{3n-k}}, \frac{x_1 y_{3n-k} - y_k x_{3n-k}}{1 - dx_k y_k x_{3n-k} y_{3n-k}}\right) =$$

$$= (3n+2k)P = (x_{3n+2k}, y_{3n+2k}) = (-x_{3n-2k}, y_{3n-2k}). \qquad (14)$$

З пар рівностей (11), (13) і навіть (12), (14) випливає, що нуль у знаменнику x-координати (11) перемістився у знаменник y-координати в рівності (13). Те саме справедливо для пари рівностей (12) і (14). Нуль у знаменнику y-координати може породжувати особливі точки 2-го порядку (6) або нечіткі точки. Перший випадок неможливий, оскільки підгрупа $\langle P\rangle$ містить тільки дві особливі точки $\pm F_1$ підгрупи $G_4^{(1)}$. До того ж координати доданків точок відомі з правила вертикальної асиметрії x-координат точок колеса і визначені в (13), (14). Тоді для чисельників їхніх y-координат справедливі рівності

$$x_k y_{n+k} + y_k x_{n+k} = y_{n+2k}(1 + dx_k y_k x_{n+k} y_{n+k}) = 0,$$

$$x_k y_{3n+k} + y_k x_{3n+k} = y_{3n+2k}(1 + dx_k y_k x_{3n+k} y_{3n+k}) = 0.$$

Отже, y-координати точок $(n+2k)P$ та $(3n+2k)P$, що отримані як суми $kP + (n+k)P$ та $kP + (3n+k)P$, можна представити як невизначеності $0/0$, а відповідні точки $(n+2k)P$ та $(3n+2k)P$ є нечіткими. Теорему доведено.

Наслідок 1. Твердження теореми 1 справедливе для заміни $n \to \nu, \nu \mid n$.

Доведення. Цей наслідок має місце, оскільки будь-яка підгрупа $G_\nu \subset G_n$ кривої непарного порядку ν утворює у разі підсумовування з підгрупою $G_4^{(1)}$ підгрупу $G_4^{(1)} \oplus G_\nu$ порядку 4ν, що містить особливі точки $\pm F_1$ 4-го порядку.

Теорема 2. Нехай циклічна підгрупа $\langle P \rangle$ квадратичної кривої Едвардса (3), що генерується точкою $P = (x_1, y_1)$ порядку $Ord\, P = 2n$, містить одну особливу точку 2-го порядку $D_{1,2} = (\pm 1/\sqrt{d}, \infty)$. Тоді сума точок $kP + (n+k)P$, $k < n/2$, утворює одну нечітку точку $(n+2k)P$.

Доведення. У цьому разі циклічна підгрупа $\langle P \rangle_{2n}$ порядку $2n$ будується як пряма сума груп $G_2^{(1)} \oplus G_n$ або $G_2^{(2)} \oplus G_n$. За умовами теореми $nP = D_{1,2} = (\pm 1/\sqrt{d}, \infty)$, $2nP = O = (1, 0)$. Послідовне експоненціювання точки P у верхньому півколі колеса точок $\{kP \mid k = 1 \ldots n\}$ утворює неособливі точки $\{kP \mid k = 1 \ldots n-1\}$ та особливу точку $nP = D_1 = (1/\sqrt{d}, \infty)$ або $nP = D_2 = (-1/\sqrt{d}, \infty)$, що лежить на горизонтальній діаметральній лінії. Точки $\{-kP \mid k = 1 \ldots n-1\}$ нижнього півкола колеса є оберненими до точок верхнього півкола. Нехай $kP = (x_k, y_k)$, тоді на підставі (7) і властивості горизонтальної асиметрії y-координат точок колеса має місце рівність $(x_k, y_k) = (x_{-k}, -y_{-k})$. Згідно з (4) сума точок $(n-k)P + kP$ визначає точку D_1 або D_2, тоді

$$\left(\frac{x_k x_{n-k} - y_k y_{n-k}}{1 - dx_k y_k x_{n-k} y_{n-k}}, \frac{x_k y_{n-k} + y_k x_{n-k}}{1 + dx_k y_k x_{n-k} y_{n-k}} \right) = D_{1,2} =$$

$$= \left(\frac{\pm 1}{\sqrt{d}}, \infty \right) \Rightarrow 1 + dx_k y_k x_{n-k} y_{n-k} = 0. \qquad (15)$$

Однак сума точок $(n+k)P + kP = (n+2k)P$ не є особливою точкою:

$$\left(\frac{x_k x_{n+k} - y_k y_{n+k}}{1 - dx_k y_k x_{n+k} y_{n+k}}, \frac{x_k y_{n+k} + y_k x_{n+k}}{1 + dx_k y_k x_{n+k} y_{n+k}} \right) =$$

$$= \left(\frac{x_k x_{n-k} - y_k y_{n-k}}{1 + dx_k y_k x_{n-k} y_{n-k}}, \frac{x_k y_{n-k} - y_k x_{n-k}}{1 - dx_k y_k x_{n-k} y_{n-k}} \right) =$$

$$= (n+2k)P = (x_{n+2k}, y_{n+2k}) = (x_{n-2k}, -y_{n-2k}). \qquad (16)$$

З цих рівностей випливає, що нуль у знаменнику y-координати (15) перемістився в знаменник x-координати рівності (16). Нуль у знаменнику x-координати відповідає особливим точкам 4-го порядку (6), які вилучені з циклічної підгрупи $\langle P \rangle$ порядку $2n$. Оскільки ненульові координати цих точок відомі за правилом горизонтальної асиметрії y-координат точок колеса і визначені в (16), справедлива рівність

$$x_k x_{n+k} - y_k y_{n+k} = x_{n+2k}(1 - dx_k y_k x_{n+k} y_{n+k}) = 0.$$

Отже, x-координата точки $(n+2k)P$ $(k<n/2)$, що отримана згідно з (4) для суми точок $(n+k)P+kP$, породжує невизначеність $0/0$, а відповідна точка $(n+2k)P$ є нечіткою. Теорему доведено.

Зауважимо, що для підгруп, які містять особливі точки 4-го порядку, невизначеності $0/0$ в нечітких точках завжди виникають в x-координатах, тоді як для підгруп, що містять особливі точки 2-го порядку, вони виникають в y-координатах.

Теорема 3. Для точок непарних порядків циклічної підгрупи G_n квадратичної кривої Едвардса (3), що генерується точкою $P=(x_1, y_1)$ порядку $Ord\ P=n$, а також точок парних порядків $2n$, $4n$, які генерують циклічні підгрупи, що не містять особливих точок, закон додавання точок (4) є повним.

Доведення. Додавання будь-якої пари точок непарних порядків утворює точку непарного порядку. У підгрупі G_n, таким чином, вилучені особливі точки (6) порядків 2 і 4 і знаменники координат сумарної точки (4) мають вигляд $1\pm dx_1y_1x_2y_2\neq 0$. З доведення теорем 1 і 2 також випливає, що і нечіткі точки з невизначеністю $0/0$ в координатах сумарної точки вилучені. Отже, у підгрупі G_n кривої (3) закон додавання (4) повний.

У циклічних підгрупах парних порядків, утворених прямими сумами $G_2^{(0)}\oplus G_n$ і $G_4^{(0)}\oplus G_n$ і які не містять особливих точок (6), за законом (4) для всіх пар точок, що додаються, виконується нерівність $1\pm dx_1y_1x_2y_2\neq 0$, отже, закон додавання повний. Теорему доведено.

Проілюструємо прикладом результати теорем.

Приклад 1. Нехай $p=23$, крива задана рівнянням (3) з параметром $d=2=5^2$. Вона є суперсингулярною і має порядок $N_E=p+1=24$. У табл.1 наведено координати точок всіх її підгруп порядків $4n=12$, $2n=6$ та $n=3$, а рис. 1 ілюструє колесо точок для підгрупи з особливою точкою F_1 (*а*) і підгрупи без особливої точки (*б*). Рис. 2 ілюструє два колеса точок для $2n=6$, які містять або точку 2-го порядку D_1 (*а*), або точку D_0 (*б*). Одна точка $P=(6,11)$ генерує підгрупу максимального порядку, що містить 12 точок, записаних у другому рядку табл. 1. При цьому $3P=F_1=(\infty,9)$ — особлива точка 4-го порядку. Згідно з (4) і відповідно до теореми 1 сума точок $P+(3+1)P=5P$ утворює рівність

$$\left(\frac{6\cdot(-5)-11\cdot(-10)}{1-2\cdot6\cdot(-5)11\cdot(-10)},\frac{6\cdot(-10)+(-5)\cdot11)}{1+2\cdot6\cdot(-5)11\cdot(-10}\right)=\left(\frac{-12}{2},\frac{0}{0}\right)=\left(-6,\frac{0}{0}\right).$$

Отримали нечітку точку з невизначеністю $0/0$ в y-координаті на позиції $5P$. Той самий результат маємо у разі додавання точок $(3n+1)P+P=(9+2)P$.

Квадратичні криві Едвардса містять вдвічі більше особливих і нечітких точок, ніж скручені, що потрібно враховувати у разі використання в алгоритмах точки парних порядків.

3. ОСОБЛИВОСТІ ЗАКОНУ ДОДАВАННЯ ТОЧОК СКРУЧЕНИХ КРИВИХ ЕДВАРДСА

Визначимо пару квадратичної та скрученої кривої Едвардса як пару квадратичного кручення з параметрами $\chi(ad)=1$, $a'=ca$, $d'=cd$, $\chi(c)=-1$ [7]. Для квадратичної кривої Едвардса $\chi(a)=\chi(d)=1$ можна прийняти $a=1$, тоді для скрученої кривої Едвардса $a'=c$, $d'=cd$, $\chi(d)=1$, $\chi(c)=-1$.

Розглянемо спочатку приклад, коли $p\equiv 3 \bmod 4$. Зауважимо, що при цьому існують суперсингулярні криві Едвардса порядку $N_E\equiv 0 \bmod 8$ [10]. До того ж $\chi(-1)=-1$ та можна вважати, що $c=-1$. Тоді рівняння скрученої кривої Едвардса згідно з (1) запишемо у вигляді

$$E_{-1,-d}\colon x^2-y^2=1-dx^2y^2,\ d\in F_p^*,\ d\neq 1,\ \chi(d)=1. \qquad (17)$$

Таблиця 1. Точки циклічних підгруп квадратичної кривої (3) порядку $N_E = 24$ для $p = 23,\ d = 2$

Номер підгрупи	Координати точок за назвами											
	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$
1	(6, 11)	(5, – 10)	**(∞, 9)**	(–5, – 10)	(–6, 11)	(–1, 0)	(–6, – 11)	(–5, 10)	**(∞, – 9)**	(5, 10)	(6, – 11)	(1, 0)
2	(10, 5)	(5, 10)	(0, 1)	(–5, 10)	(–10, 5)	(–1, 0)	(–10, – 5)	(–5, – 10)	(0, – 1)	(5, – 10)	(10, – 5)	(1, 0)
3	(11, 6)	(–5, – 10)	**(–9, ∞)**	(–5, 10)	(11, – 6)	(1, 0)						
4	(–11, 6)	(–5, 10)	**(9, ∞)**	(–5, – 10)	(11, – 6)	(1, 0)						
5	(5, 10)	(–5, 10)	(–1, 0)	(–5, – 10)	(5, – 10)	(1, 0)						
6	(–5, 10)	(–5, – 10)	(1, 0)									

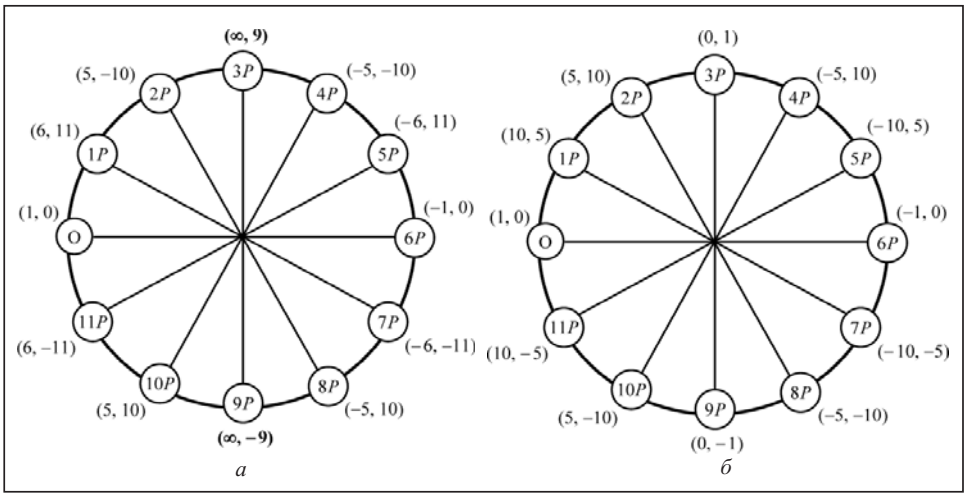


Рис. 1. Колесо точок підгруп порядку $4n = 12$, що містять точки $\pm F_1$ (*а*) або точки $\pm F_0$ (*б*) квадратичної кривої Едвардса порядку $N_E = 24$ для $p = 23,\ d = 2$

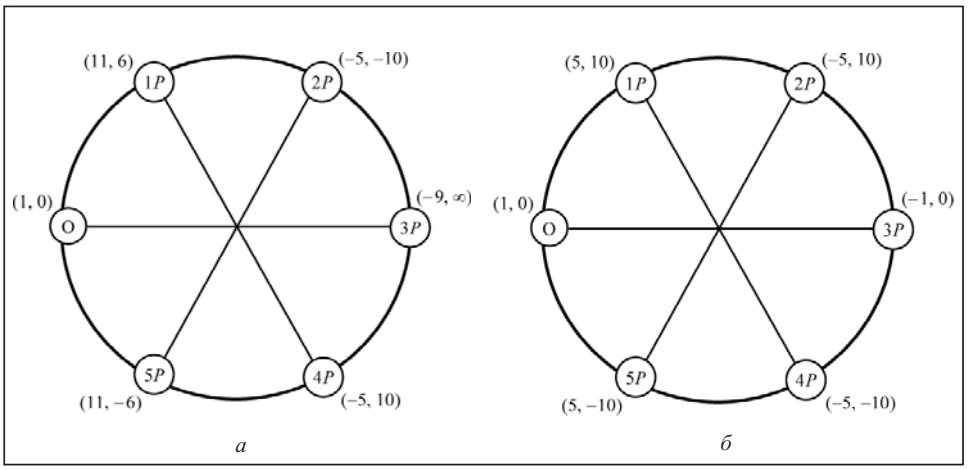


Рис. 2. Колесо точок підгруп порядку $2n = 6$, що містять точку D_1 (*а*) або D_0 (*б*) квадратичної кривої Едвардса порядку $N_E = 24$ для $p = 23,\ d = 2$

Зазначимо, що ця крива не містить ні класичних точок 4-го порядку $\pm F_0 = (0, \pm 1)$, ні особливих точок 4-го порядку (6). Разом з тим існують неособливі точки 4-го порядку [7, теорема 2.1]:

$$\pm F_2 = \left(\sqrt[4]{\frac{a}{d}}, \pm \sqrt{\frac{-1}{\sqrt{ad}}} \right), \ \pm F_3 = \left(-\sqrt[4]{\frac{a}{d}}, \pm \sqrt{\frac{-1}{\sqrt{ad}}} \right), \tag{18}$$

подвоєння яких визначає особливі точки 2-го порядку D_1 та D_2 з (6). Дійсно, згідно з (5) маємо

$$2F_2 = \left(\frac{\sqrt{\frac{a}{d}} - a\frac{-1}{\sqrt{ad}}}{1 - d\sqrt{\frac{a}{d}}\frac{-1}{\sqrt{ad}}}, \frac{2\sqrt{\frac{a}{d}}\frac{-1}{\sqrt{ad}}}{1 + d\sqrt{\frac{a}{d}}\frac{-1}{\sqrt{ad}}} \right) = \left(\frac{2\sqrt{\frac{a}{d}}}{2}, \frac{\sqrt{\frac{a}{d}} - a\frac{-1}{\sqrt{ad}}}{1 + d\frac{-1}{d}} \right) = \left(\sqrt{\frac{a}{d}}, \infty \right) = D_1.$$

Друге значення квадратного кореня $-\sqrt{\frac{a}{d}}$ відповідає подвоєнню $2F_3 = D_2$. Тоді крива (17) містить дві циклічні підгрупи 4-го порядку, які містять особливі точки 2-го порядку:

$$G_4^{(2)} = \{O, F_2, 2F_2 = D_1, 3F_2 = -F_2\}, \ G_4^{(3)} = \{O, F_3, 2F_3 = D_2, 3F_3 = -F_3\}. \tag{19}$$

Прямі суми цих груп з підгрупою точок непарного порядку утворюють циклічні підгрупи кривої (17) порядку $4n$, що містять особливі точки 2-го порядку. Ці ж самі точки належать до підгруп порядку $2n$, утворених у вигляді сум $G_2^{(1)} \oplus G_n$ та $G_2^{(2)} \oplus G_n$. Ці властивості кривої (17) використовують в теоремах, наведених нижче. Важливою відмінністю властивостей підгруп точок порядків $2n$ і $4n$ скручених кривих Едвардса з особливими точками від властивостей квадратичних кривих є втрата властивості вертикальної асиметрії на колесі точок (див. (7)–(10)).

Теорема 4. Нехай циклічна підгрупа $\langle P \rangle$ скрученої кривої Едвардса (17), що генерується точкою $P = (x_1, y_1)$ порядку $Ord\ P = 4n$ або $Ord\ P = 2n$, містить одну особливу точку 2-го порядку $D_{1,2} = (\pm 1/\sqrt{d}, \infty)$. Тоді за умови $Ord\ P = 4n$ сума точок $kP + (2n + k)P$ породжує одну нечітку точку $(2n + 2k)P$, а за умови $Ord\ P = 2n$ сума точок $kP + (n + k)P$ породжує одну нечітку точку $(n + 2k)P$.

Доведення. Циклічна підгрупа $\langle P \rangle$ скрученої кривої Едвардса (17) порядку $4n$ з особливою точкою $D_1 = (1/\sqrt{d}, \infty)$ або $D_2 = (-1/\sqrt{d}, \infty)$ є сумою $G_4^{(2)} \oplus G_n$ або $G_4^{(3)} \oplus G_n$, де підгрупи 4-го порядку визначено в (19). У першому випадку, коли $Ord\ P = 4n$, виконується $2nP = D_1$, у другому випадку, коли $Ord\ P = 2n$, маємо $2nP = D_2$, і ці точки на горизонтальному діаметрі колеса точок замикають його верхнє півколо. Обчислено його неособливі точки kP, $k < 2n$, тоді відомі й обернені точки, а саме $-kP$. Запишемо дві рівності:

$$kP + (2n - k)P = 2nP = \left(\frac{1}{\sqrt{d}}, \infty \right),$$

$$kP + (2n + k)P = (2n + 2k)P = (x_{2n+2k}, y_{2n+2k}). \tag{20}$$

Другі доданки у цих сумах взаємно обернені, тоді

$$(x_{2n+k}, y_{2n+k}) = (x_{2n-k}, -y_{2n-k}). \tag{21}$$

З (4), (20) та (21) випливає $1 + dx_k y_k x_{2n-k} y_{2n-k}) = 1 - dx_k y_k x_{2n+k} y_{2n+k}) = 0$.

Отже, маємо нуль у знаменнику y-координати першої суми точок (20), а також у знаменнику x-координати другої суми точок (20). Оскільки неособлива

точка $(2n+2k)P$ має відомі координати, які можна отримати з координат оберненої точки $(2n-2k)P$, чисельник її x-координати в сумі (20) становить

$$x_{2n+2k}(1-dx_k y_k x_{2n+k} y_{2n+k}) = 0.$$

Отже, точка $(2n+2k)P$, яка утворена як сума $kP+(2n+k)P$, має невизначеність $0/0$ упродовж обчислення x-координати і є нечіткою.

Замінюючи циклічні підгрупи 4-го порядку (19) на підгрупи особливих точок 2-го порядку, отримаємо підгрупи $G_2^{(1)} \oplus G_n$ та $G_2^{(2)} \oplus G_n$ порядку $2n$, для яких $nP = D_1$ або $nP = D_2$. Наведене доведення буде справедливим після заміни $2n \to n$. У цьому випадку точка $(n+2k)P$, утворена як сума $kP+(n+k)P$, має невизначеність $0/0$ упродовж обчислення x-координати і є нечіткою. Теорему доведено.

Розглянемо випадок $p \equiv 1 \bmod 4$, який породжує тільки несуперсингулярні криві Едвардса. Це очевидно, оскільки значення $p+1 \equiv 2 \bmod 4$ не може бути порядком кривої Едвардса. Замість (17) скручені криві Едвардса визначає у цьому разі загальне рівняння (1) за умови $\chi(a) = \chi(d) = -1$. Характерною властивістю цих кривих є відсутність точок 4-го порядку [7, твердження 4.2], тоді порядок будь-якої такої кривої становить $N_E = 4n \equiv 0 \bmod 4$ [9]. Кофактор 4 кривої цього порядку визначено наявністю нециклічної підгрупи 4-го порядку $G_4 = \{O, D_0, D_1, D_2\}$ точок 2-го порядку. Ця крива містить дві підгрупи $G_2^{(1)} \oplus G_n$ та $G_2^{(2)} \oplus G_n$ порядку $2n$, для яких виконується $nP = D_1$ або $nP = D_2$. Для цих підгруп справедливе друге твердження теореми 4.

Теорема 5. Для точок непарних порядків циклічної підгрупи G_n, скрученої кривої Едвардса (1) з $\chi(a) = \chi(d) = -1$, що генерується точкою $P = (x_1, y_1)$ порядку $Ord\, P = n$, а також точок парних порядків $2n$, які генерують циклічні підгрупи, що не містять особливих точок, закон додавання точок (4) є повним.

Доведення. Твердження цієї теореми для скручених кривих Едвардса збігається з твердженням теореми 3 для квадратичних кривих Едвардса в частині, що стосується підгруп порядків n і $2n$ і його можна довести з тією ж аргументацією.

Приклад 2. Для $p = 23$ задано скручену криву (17) з параметрами $a = -1$, $d = -2$. Вона є квадратичним крученням кривої, розглянутої у прикладі 1, з тим самим порядком. У табл. 2 наведено координати точок усіх її підгруп порядків $4n = 12$, $2n = 6$, $n = 3$, а рис. 3 ілюструє колесо точок для підгрупи з особливою точкою $D_1 = (\infty, 9)$ у підгрупах порядків 12 (рис. 3, *а*) та 6 (рис. 3, *б*). Одна з її точок $P = (2, 4)$ генерує підгрупу максимального порядку 12, її точки записано у другому рядку табл. 2. Згідно з (4) та за теоремою 4 сума точок $P + (6+1)P = 8P$ визначає

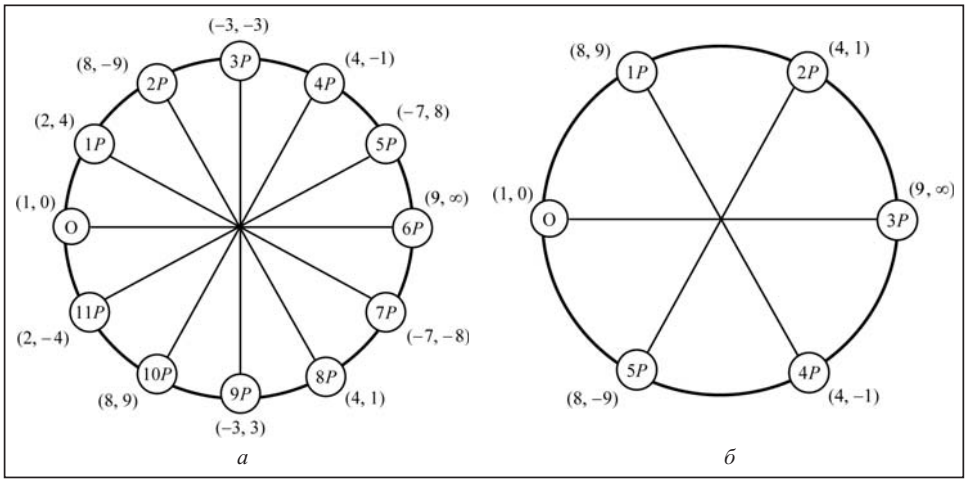
$$\left(\frac{2\cdot(-7)+4\cdot(-8)}{1+2\cdot 2\cdot 4(-7)\cdot(-8)}, \frac{2\cdot(-8)+(-7)\cdot 4}{1-2\cdot 2\cdot 4\cdot(-7)\cdot(-8)}\right) = \left(\frac{0}{0}, \frac{2}{2}\right) = \left(\frac{0}{0}, 1\right).$$

Отримали нечітку точку з невизначеністю $0/0$ в x-координаті на позиції $(n+2)P = 8P$.

За умов, коли значення k точки kP невідоме, для будь-якої точки P з підгрупи, що містить, наприклад, точку D_1, легко знайти точку Q таку, що $P + Q = D_1$ (див. (9)). Тоді точка $P - Q = S$ є нечіткою точкою з невизначеністю $0/0$ в x-координаті. Якщо відома y-координата, іншу координату можна знайти, наприклад, з рівняння кривої (1). Можна також обчислити точку $R = 2P$ та знайти суму $2P + D_1 = S$ за допомогою (9). У будь-якому випадку потрапляння на нечітку точку гальмує обчислення, і цього слід уникати.

Таблиця 2. Точки циклічних підгруп скрученої кривої (17) порядку $N_E = 24$ для $p = 23,\ a = -1, d = -2$

Номер підгрупи	Координати точок за назвами											
	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$
1	(2, 4)	(8, – 9)	(–3, – 3)	(4, – 1)	(–7, 8)	**(9, ∞)**	(–7, – 8)	(4, 1)	(–3, 3)	(8, 9)	(2, – 4)	(1, 0)
2	(–2, 4)	(8, 9)	(3, – 3)	(4, 1)	(7, 8)	**(–9, ∞)**	(7, – 8)	(4, – 1)	(4, – 1)	(8, – 9)	(–2, – 4)	(1, 0)
3	(8, 9)	(4, 1)	**(9, ∞)**	(4, – 1)	(8, – 9)	(1, 0)						
4	(–8, 9)	(4, – 1)	**(–9, ∞)**	(4, 1)	(–8, – 9)	(1, 0)						
5	(–4, 1)	(4, 1)	(–1, 0)	(4, – 1)	(–4, – 1)	(1, 0)						
6	(3, 3)	**(9, ∞)**	(3, – 3)	(1, 0)								
7	(–3, 3)	**(9, ∞)**	(–3, – 3)	(1, 0)								
8	(4, 1)	(4, – 1)	(1, 0)									



а *б*

Рис. 3. Колесо точок підгруп порядків $4n$ (*а*) та $2n$ (*б*), що містять точку D_1, скрученої кривої Едвардса порядку $N_E = 24$ для $p = 23,\ a = -1, d = -2$

ВИСНОВКИ

Не зважаючи на те, що частка особливих точок (6) для криптографічних застосувань мізерна (їхня відносна частка становить приблизно $1/2n$), групові операції (4) в класах нециклічних кривих Едвардса (1) ($\chi(ad) = 1$) можуть породжувати ці точки, а також нечіткі точки для близько 12.5 % ($N_E = 8n$) або 25 % ($N_E = 4n$) відомих пар доданків ($k < n/2$). Зазначимо, що цей результат справедливий для всіх дільників ν числа n, що у багато разів розширює множину небезпечних точок. Наприклад, для алгоритму CSIDH [1] з числом n, яке дорівнює добутку $K = 74$ простих чисел, кількість співмножників n складає $\sum_{s=1}^{K} C_K^s = 2^K - 1 \approx 2^{74}$. З урахуванням парних чисел кількість всіх циклічних підгруп нециклічних кривих Едвардса досягає в цьому прикладі 2^{77}. Ймовірність вибору випадкової точки парного порядку для чергової ізогенії в CSIDH у вісім разів більша, ніж точки непарного порядку. Програмуючи експоненціювання випадкових точок, це потрібно враховувати. Перехід до підгрупи G_n точок непарного порядку усуває проблему (теореми 3 і 5). Досягається це дворазовим подвоєнням будь-якої точки максимального порядку $4n$.

СПИСОК ЛІТЕРАТУРИ

1. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: An efficient post-quantum commutative group action. In: Advances in Cryptology (ASIACRYPT 2018). Peyrin T., Galbraith S. (Eds.). Cham: Springer International Publishing, 2018. P. 395–427.
2. Kim S., Yoon K., Park Y.-H., Hong S. Optimized method for computing odd-degree isogenies on Edwards curves. *Security and Communication Networks.* 2019.
3. Bessalov A., Sokolov V., Skladannyi P. Modeling of 3- and 5-isogenies of supersingular Edwards curves. *Proc. of the 2nd Intern. Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020)*. Aachen: CEUR, 2020. Vol. 2631, N I. P. 30–39.
4. Bessalov A.V. How to construct CSIDH on quadratic and twisted Edwards curves. *Кібербезпека: освіта, наука, техніка.* 2022. Т. 3, № 15. С. 148–163.
5. Bernstein D.J., Lange T. Faster addition and doubling on Elliptic curves. *Advances in Cryptology — ASIACRYPT'2007: Proc. 13th Intern. Conf. on the Theory and Application of Cryptology and Information Security* (December 2–6, 2007, Kuching, Malaysia). *Lect. Notes Comp. Sci.* Berlin: Springer, 2007. Vol. 4833. P. 29–50.
6. Bernstein D.J., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards curves. In: AFRICACRYPT 2008. *LNCS*. 2008. Vol. 5023. P. 389–405.
7. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев: Политехника, 2017. 272 с.
8. Bessalov A.V., Tsygankova O.V. Interrelation of families of points of high order on the Edwards curve over a prime field. *Problems of Information Transmission*. 2015. Vol. 51, Iss. 4. P. 391–397.
9. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. *Problems of Information Transmission.* 2017. Vol. 53, Iss. 1. P. 92–101. https://doi.org/10.1134/S0032946017010082.
10. Bessalov A.V., Kovalchuk L.V. Supersingular twisted Edwards curves over prime fields. I. Supersingular twisted Edwards curves with j-invariants equal to zero and 12^3. *Cybernetics and Systems Analysis*. 2019. Vol. 55, N 3. P. 347–353.
11. Bessalov A.V., Kovalchuk L.V. Supersingular twisted Edwards curves over prime fields. II. Supersingular twisted Edwards curves with the j-invariant equal to 66^3. *Cybernetics and Systems Analysis.* 2019. Vol. 55, N 5. P. 731–741.
12. Washington L.C. Elliptic curves. Number theory and cryptography. 2nd ed. CRCPress, 2008.

A.V. Bessalov, S.V. Abramov

SPECIAL PROPERTIES OF THE POINTS ADDITION LAW OF NON-CYCLIC EDWARDS CURVES

Abstract. The authors analyze the speclial properties of two classes of quadratic and twisted Edwards curves over a prime field, related to their non-cyclic structure and the incompleteness of the points addition law. Both classes of curves contain special points of 2nd and 4th orders with respect to one infinite coordinate, which generate points with uncertainty 0/0 in one of the coordinates of the sum, called ambiguous points. Five theorems are formulated and proved that allow resolving these uncertainties and proving the conditions whereby the points addition law in these classes of curves is complete.
.

Keywords: generalized Edwards curve, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, special point, ambiguous point, wheel of points, quadratic residue, quadratic non-residue.

Надійшла до редакції 25.05.2022