УДК 681.3
DOI https://doi.org/10.32689/maup.it.2021.1.8

Руслан СКУРАТОВСЬКИЙ
викладач кафедри обчислювальної математики і компютерного моделювання, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039

ORCID: https://orcid.org/0000-0002-5692-6123

Ruslan SKURATOVSKYI
Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039

Бібліографічний опис статті: Скуратовський Р. Операції на скрученій кривій едварса, і її застосовність в криптографії. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 70–76. DOI: https://doi.org/10.32689/maup.it.2021.1.8

Bibliographic description of the article: Skuratovskyi, R. (2021). Operatsii na skruchenii kryvii edvarsa, i yii zastosovnist v kryptohrafii [Operations on the twisted edwars curve, and its applicability in cryptography]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 70–76. DOI: https://doi.org/10.32689/maup.it.2021.1.8

ОПЕРАЦІЇ НА СКРУЧЕНІЙ КРИВІЙ ЕДВАРСА, І ЇЇ ЗАСТОСОВНІСТЬ В КРИПТОГРАФІЇ

Анотація. *Більшість криптосистем сучасної криптографії природним чином можна «перекласти» на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінчнним полем F_{p^n}, які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей. Показано, що проективна крива $E_{a,d}$ не є еліптичною. Досліджено умови існування подільності навпіл елемента з групи точок скрученої кривої Едвардса $E_{a,d}$, що є важливим в алгоритмах. Знайдено род скрученої кривої Едвардса. Метою роботи є пошук критерію подільності точки кривої навпіл над полем F_{p^n} і аналіз властивостей скрученої кривої Едвардса необхідних для побудови генератора псевдовипадкових криптостійких послідовностей і побудова односторонньої функції для нього.*

Ключові слова**:** *скінчене поле, алгебраїчна крива, група точок еліптичної кривої, подільність точки кривої навпіл, генератор криптостійкої послідовності.*

OPERATIONS ON THE TWISTED EDWARS CURVE, AND ITS APPLICABILITY IN CRYPTOGRAPHY

Abstract. *Most cryptosystems in modern cryptography can naturally be «translated» into elliptical curves. We consider Edwards algebraic curves over a finite field, which are currently one of the most promising carriers of point sets used for fast group operations available in asymmetric cryptosystems, in particular, for constructing random cryptostable sequences. It is shown that the projective curve is not elliptical. The conditions for the existence of divisibility in half of an element from the group of points of a twisted Edwards curve, which is important in algorithms, are investigated. The genus of the twisted Edwards curve is found. The aim of this work is to find the criterion for dividing the point of the curve in half over the field and to analyze the properties of the twisted Edwards curve necessary to construct a generator of pseudo-random cryptostable sequences and construct a one-way function for it.*

Key words: *finite field, algebraic curve, group of points of an elliptic curve, divisibility of a point of a curve in half, generator of cryptostable sequence.*

Вступ. Електронний цифровий підпис з обраних засобів найбільш широко забезпечує захист від всіх можливих атак. Причиною цього є наявність в ньому вже хешфункції та закритого ключа шифрування. Найпрогресивнішою схемою є схема цифрового підпису еліптичної кривої (ECDSS – Elliptic Curve Digital Signature). Завдяки вищезгаданим можливостям вирішуються проблема управління та розподілу ключів шифрування. Ми досліджуємо ще одне сімейство кривих придатних для створення ECDSS.

Вперше криві Едвардса E_d представлено Едвардсом в роботі [1]. В еліптичній криптографії дуже важливо знати ті криві які є суперсингулярними (ті, що мають нульовий j-інварівант), бо вони є крипографічно слабкими і період побудованого на їх основі генератора псевдовипадкових чисел є меншим.

Відомо, що суперсингулярні криві, на відміну від несуперсингулярних, над алгебраїчно замкненим полем, мають не комутативне кільце ендоморфізмів. Криві у формі Едвардса над простим полем сьогодні є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, що використовуються в асимметричних криптосистемах. Найважливіші переваги: рекордна

продуктивність, універсальність закона додавання, симетричність точок і представлення нейтрального елемента групи точкою в афінних координатах. Ці властивості були помічені і обгрунтовані в роботах відомих фахівців по криптографії [2; 3; 4; 5].

Дані криві задовольняють самим сильним вимогам по стійкості до MOV-атаки, про що неодноразово зазначалось у працях вітчизняних та закордонних вчених [6; 7]: неможливість застосувати цей метод забезпечується через відсутність можливості вкласти групу точок кривої в мультиплікативну групу поля достатньо малого порядку. Для цього достатньо, щоб мінімальне натуральне t, $p^t \equiv 1 mod |N_E|$ було достатньо великим. Для скручених кривих Едвардса $t = |N_E| - 1$, що є максимально можливим. Великою перевагою є можливість побудови скрученої кривої Едвардса порядку $4p$, $p \in \mathbf{P}$, тому не може бути використана атака підміни точки, що належить рекомендованій кривій на точку зі скрученої кривої тобто так званої кривої кручення. Також це не дає противнику використовувати китайську теорему про лишки для визначення секретного ключа, бо маємо великий множник p в $|N_E|$. З точки зору алгебраїчної геометрії, крива не є еліптичною, бо є сингулярною.

Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що має в порядку групи кривої множник Цікавою є можливість побудови скрученої кривої Едвардса порядку $N_E = 4p$, $p \in \mathbb{P}$, тобто такої, яка має мінімальний кофактор. Тому природньо досліджувати такі криві і клас кривих, який узагальнює ці криві – скручені криві Едвардса. Частково, викладені результати представлено в тезах [8] та попередні дослідження є у статті [3].

З точки зору алгебраїчної геометрії, крива Едвардса не є еліптичною, бо є сингулярною. Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що має в порядку групи кривої множник Як зазначено в роботі [11] для побудови “elliptic curve power generator” генератора і генератора ”Naor–Reingold” використовують не суперсингулярну еліптичну криву і її точку P великого простого порядку, якщо ж порядок l точки P не простий, то вибирають початкове заповнення e таке, що $(e,l) = 1$.

Нашою метою є дослідження властивостей цих кривих що необхідні для її застосування в асиметричній криптографії а також в криптоаналізі, зокрема дослідження цієї кривої на предмет сингулярності.

Постановку проблеми полягає у виявленні ресурсів математичного апарату, що дозволить максимально швидко здійснювати групову операцію пов’язану з додавання точки до себе. Тобто операцію «експонеціювання» точки кривої, яка лежить в основі проблеми дискретного логарифма.

Аналіз особливостей скрученої кривої Едвардса.

Розглянемо скручену криву Едвадрса $E_{a,d}$

$$ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in F_p^*,\ ad(a-d) \neq 0,\ d \neq 1,\ p \neq 2,\ a \neq d, \qquad (1)$$

При $a = d$ перетворимо криву $ax^2 + y^2 = 1 + ax^2y^2$ до вигляду $ax^2 - ax^2y^2 - 1 + y^2 = 0$ або $ax^2(1-y^2) - (1-y^2) = 0$. Отже, крива розкладається у добуток двох пар прямих $(ax^2 - 1)(y^2 - 1) = 0$. Якщо $a = 1$, то $E_{a,\mathrm{d}}$ перетворюється у криву E_{d}. З умови гладкості знаходимо особливі точки афінної кривої.

Знайдемо особливі точки. Позначимо $F(x,y) = ax^2 + y^2 = 1 + dx^2y^2$, $a,d \in F\mathrm{p}^*$, d ≠ 1, $p \neq 2$, $a \neq d$. $\begin{cases} \dfrac{\mathrm{F}(x,y)}{\partial x} = 0 \\ \dfrac{\mathrm{F}(x,y)}{\partial y} = 0 \end{cases}$,

$$\begin{cases} 2ax = 2dxy^2 \\ 2y = 2dx^2y \end{cases}, \quad \begin{cases} ax - dxy^2 = 0 \\ y - dx^2y = 0 \end{cases} \quad \begin{cases} x(a - dy^2) = 0 \\ y(1 - dx^2) = 0 \end{cases} \quad \left[\begin{array}{l} \begin{cases} x = 0 \\ y = 0 \end{cases} \\ \begin{cases} (a - dy^2) = 0 \\ (1 - dx^2) = 0 \end{cases} \end{array} \right. \quad \left[\begin{array}{l} (0,0) \\ \left(\pm\sqrt{\dfrac{1}{d}}, \pm\sqrt{\dfrac{a}{d}} \right) \end{array} \right.$$

Але точка $(0,0)$ кривій $E_{a,\mathrm{d}}$ не належить не залежно від поля.

Отже отримали аж 4 точки, за умови, що при цьому для F_p коефіцієнти a і d в F_p повинен бути таким, що $\left(\frac{d}{p}\right) = 1$ і $\left(\frac{ad}{p}\right) = 1$, тобто $\left(\frac{d}{p}\right) = 1$ і $\left(\frac{a}{p}\right) = 1$. Отже наявні 4 особливі точки з урахування того, що точка $(0,0)$ кривій не належить.

Як відомо [2] проективна крива дала можливість отримати більш швидкі швидкі операції над точками кривої. Тому проаналізуємо особливі точки в проективному замиканні кривої.

Для цього зробимо проективізацію кривої. Нехай $x = \frac{X}{Z}, y = \frac{X}{Z}$, 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 в проективних координатах співпадають:

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

$ax^2 + y^2 - 2z^2 = 0$ з другого рівняння слідує, що $y = 0$ або $z = \pm\sqrt{d}$ тут розв'язком очевидно є $(0,0,0)$ і точка $(x_0,0,0)$.

Пошукаємо інші корені в припущенні $z = 0$ коренем є також точка $(0,y_0,0) = (0,1,0)$. Тобто маємо 2 особливі проективні точки $p_1 = (1,0,0)$ і $p_2 = (0,1,0)$. Це прості особливості.

Отже, розв'язками є лише особливі точки (нескінченно віддаленні точки) $(1,0,0)$ і $(0,1,0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах

$$A^1 : az^2 + y^2z^2 = z^4 + dy^2 \text{ і } A^2 : \ ax^2z^2 + z^2 = z^4 + dx^2$$

Опишемо будову локального кільця в точці p_1, його елементами є дроби з функцій виду $F(x,y,z) = \frac{f(x,y,z)}{g(x,y,z)}$, знаменники яких не обертаються в 0 у точці p_1. Локальне кільце, що має особливості в 2-ух точках має функції у яких знаменники не діляться на $(x-1)(y-1)$.

Знайдемо $\delta_{\mathrm{p}} = \dim \bar{\mathcal{O}}_{\mathrm{p}} / \mathcal{O}_p$, де $\mathcal{O}_{\mathrm{p}}$ – локальне кільця в особливій точці p, це кільце породжується відношеннями регу лярних функцій: $\mathcal{O}_{\mathrm{p}} = \left\{ \frac{f}{g} : (g,(x-1)(y-1)) = 1 \right\}$, $\bar{\mathcal{O}}_{\mathrm{p}}$ – ціле замикання локального кільця в особливій точці p. Позначимо $\delta_p = \dim \bar{\mathcal{O}}_p / \mathcal{O}_p = 1$ розмірність фактора як векторного простору. Оскільки, базис розширення $\bar{\mathcal{O}}_p$ над $\mathcal{O}_p$ складається з одного елемента в кожній з двох особливих точок, то $\delta_p = 1$.

Отже, підрахуємо род кривої за Рідом: $\rho^*(C) = \rho_\alpha(\mathrm{C}) - \sum_{p \in E} \delta_p = = \frac{(n-1)(n-2)}{2} - \sum_{p \in E} \delta_p = 3 - 2 = 1$ бо $n = 4$. де $\rho_\alpha(C)$ – арифметичний рід кривої C, параметр $n = degC = 4$.

Оскільки вона роду 1, то вона ізоморфна плоскій кубічній кривій але не є еліптичною, бо має особливості в проективній частині. Крива Едварса як і скручена крива Едаварса ізоморфна деякій афінній частині еліптичної кривої. Нормалізація кривої Едвардса – крива в формі Веєрштраса, що запропонована Монгомері E_M отримана шляхом біраціонального відображення $u = (1+y)/(1-y)$, $v = u/x$ [12], яка вже є еліптичною. При аналізі цієї теореми де було розглянуто цю біраціональну еквівалентність авторами Бессаловим А.В., Циганковою О. В. у статті [13] даремно критикуюь теорему 3.2 з авторитетного джерела [12], де аналізується ця біраціональна еквівалентність, допускають плутанину, підмінюючи термін біраціональна еквівалентність на ізоморфізм кривих у теоремі 1 зі своєї статті [13]. Також ними [13] допущено неточності в кінці розділу 1 в теоремі 1, де стверджують існування ізомормізму між скрученою кривою Едварса і кривою Монтгомері що неможливо, бо крива завжди розглядається над полем а не над його частиною як автори стверджують у теоремі 1 дарма називаючи теорему 3.2 з [12] не коректною. Один з можливих підходів до розв'язання сингулярності у цих двух точках є застосування нормалізазаційних замін, що є біраціональними відображеннями, які дозволяють виразити старі змінні x,y,z через нові регулярно: $x:z = u:w = t:v$, $y:z = t:u = v:w$.

Це перетворить нашу криву у просторову криву (у тривимірному проективному просторі), що задана двома рівняннями:

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

Оскільки вона роду 1, вона ізоморфна плоскій кубічній кривій. Остання кри ва не має особливостей і тому елемент яким ми розширили поле часток локального кільця є цілим алгебраїчним.

Властивості скрученої кривої Едвардса.

Лема 1. Якщо (x,y) точка кривої $E_{a,d}$, тоді має місце рівність

$$\left(\frac{1-dx_1^2}{p} \right) = \left(\frac{1-ax_1^2}{p} \right).$$

Доведення. З рівняння скрученої кривої Едвардса $ax^2+y^2=(1+dx^2y^2)$ отримуємо $y^2-dx^2y^2=1-ax^2$ $y^2-dx^2y^2=1-ax^2$ звідки $y^2(1-dx^2)=(1-ax^2)$. А оскільки квадратичність лівої частини визначається лише множником $(1-dx^2)$, то має місце конгруентність $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$.

Лема 2. Якщо (x,y) точка кривої $E_{a,d}$, тоді має місце рівність

$$\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right).$$

Доведення. З рівняння скрученої кривої Едвардса $ax^2+y^2=(1+dx^2y^2)$ отримуємо $ax^2-dx^2y^2=1-y^2$ звідки $x^2(a-dy^2)=1-y^2$. А оскільки квадратичність лівої частини визначається лише множником $a-dy^2$, то має місце конгруентність $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$.

Твердження 1. Для довільної точки (x_1,y_1), яка не є точкою порядку 2 чи 4, кривої (1) при $e=1$ виконується рівність

$$\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right).$$

Доведення. Для точки $P=(x_1,y_1)$ з що задовольняє рівняння кривої (1) розглянемо добуток

$$(a-dy_1^2)(1-ax_1^2)=a+adx_1^2y_1^2-a^2x_1^2-dy_1^2=ay_1^2-dy_1^2=(a-d)y_1^2.$$

Згідно з лемою 2 маємо $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$ підставивши це в останню рівність замість $(a-dy_1^2)$ отримуємо нову рівність лишків $\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right)$ що і потрібно було довести.

Можливість виконання оберненої операції до операції подвоєння точки ще й досі не досліджена для скрученої кривої Едвардса, наступна теорема дає відповідь на це питання.

Зауважимо, що під подільністю точки (X; Y) навпіл розумітимемо знаходження її праобразу тобто точки (x; y), яка додавалася до себе при застосуванні формули подвоєння точки [1].

Теорема. Для довільної точки $G=(X,Y)$ скрученої кривої Едвардса (1), що не є точкою 2-го чи 4-го порядка, існують точки поділу на 2 тоді і тільки тоді, коли $\left(\frac{1-aX^2}{p}\right)\neq -1$.

Доведення. Для скрученої кривої Едвардса закон подвоєння має форму [11]

$$2(x_1,y_1)=\left(\frac{2x_1y_1}{y^2+ax_1{}^2},\frac{y_1^2-ax_1{}^2}{1-dx_1{}^2y_1^2}\right)=(X,\mathrm{Y})$$

звідси, скориставшись рівнянням кривої ми виводимо модифіковану формулу додавання точки до самої себе:

$$2(x_1,y_1)=\left(\frac{2x_1y_1}{1+dx_1{}^2y_1^2},\frac{y_1^2-ax_1{}^2}{1-dx_1{}^2y_1^2}\right)=(X,Y)=G. \qquad (3)$$

Розглянемо рівняння

$\frac{2x_1y_1}{1+dx_1{}^2y_1{}^2}=X$, що рівносильне $dXx^2y^2-2xy+X=0$ і зробимо заміну $t=x_1y_1$ після чого отримаємо рівняння

$$dXt^2-2t+X=0,$$

розв'язок, якого існує якщо і тільки якщо $\left(\frac{1-dX^2}{p}\right)=1$ (або $1-dX^2\equiv 0(\mathrm{mod}\,p)$).

Розв'язки мають вигляд $t_{1,2}=\frac{1\pm\sqrt{1-dX^2}}{dX}$, вони існують як тільки $\left(\frac{1-dx_1^2}{p}\right)=1$. Згідно з Лемою 1 $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$. Для точки $P=(x_1,y_1)$ з що задовольняє рівняння кривої (1) розглянемо добуток

З рівності (2) маємо для першої ще одне рівняння

$$\frac{2x_1y_1}{y_1^2+ax_1^{\,2}}=X$$

Зробимо заміну $u=\frac{y}{x}$ отримаємо $\frac{2u}{u^2+a}=X$ або $2u=X(u^2+a)$ перепишемо як квадратне рівняння відносно u $Xu^2-2u+Xa=0$ з визначником $D_2=4(1-aX^2)$. Отже, згідно з Лемою 1 рівняння $dXt^2-2t+X=0$ і $Xu^2-2u+Xa=0$ розв'язні одночасно, що дає вираз для координат точки $P_j=(x_j,y_j)$: $x_j=\sqrt{t_ju_j^{-1}}, y_j=\sqrt{t_ju_j}$ $j\in\{0,1\}$

Прирівнюючи ліві частини рівностей $\frac{2x_1y_1}{1+dx_1^{\,2}y_1^{\,2}}=X$ і $\frac{2x_1y_1}{y^2+ax_1^{\,2}}=X$ отримуємо $ax_1^2+y_1^2=1+dx_1^2y_1^2$, тобто отримані пари (x_i,y_j) задовольняє рівнянню кривої, що також слідує з замкнутості групової операції. Помітимо, що разом з (x_1,y_1) вище вказані рівняння задовольняють $(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$

$$Y^2=\frac{1-aX^2}{1-dX^2}=\frac{1-a\frac{4t^2}{(y^2+ax^2)^2}}{1-d\frac{4t^2}{y^2+ax^2}}=\frac{(y^2+ax^2)^2-4at^2}{(y^2+ax^2)^2-4dt^2}=\frac{(y^2+ax^2)^2-4at^2}{(1+dt^2)^2-4dt^2}=\frac{(y^2-ax^2)^2}{(1-dt^2)^2}=\frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}$$

Отже, отримали рівняння, що задає другу координату після подвоєння точки (x_1,y_1), піднесене до квадрату. Це рівняння ми використаємо для вибору правильного з додаткових коренів $(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$ до істинного кореня (x_1,y_1). Таким чином друге рівняння задовольняють точки (x_1,y_1) і $(-x_1,-y_1)$. Помітимо, що $(-x_1,-y_1)=(x_1,y_1)+D$

Врахувавши, що $y_1^2-dx_1^2y_1^2=1-ax_1^2$ звідки $y_1^2(1-dx_1^2)=1-ax_1^2$, маємо

$$\left(\frac{1-ax_1^2}{p}\right)=\left(\frac{1-dx_1^2}{p}\right).$$

З рівності (2) для другої координати маємо визначальне рівняння

$$x_{1,2}^2=\frac{Y(\mathrm{d}(\frac{1\pm\sqrt{1-dX^2}}{dX})^2-1)\pm\sqrt{Y^2(1-\mathrm{d}\frac{1\pm\sqrt{1-dX^2}}{dX})^2+4d(\frac{1\pm\sqrt{1-dX^2}}{dX})^2}}{2d} \tag{5}$$

Крім того $y^2=\frac{t^2}{x^2}=\frac{(1+\sqrt{1-dx^2})^2}{dx^3}$ тобто елемент dx, де x визначається умовою (5), повинен бути квадратичним лишком в $\mathbb{F}_p$. Помітимо, що обидва корені рівнянь (4) і (5) є спряженими ірраціональностями, тому якщо один з них задовольняє рівняння над Z чи над $\mathbb{F}_p$, що отримане операціями додавання, множення і піднесення в натуральну степінь, то всі вони його задовольняють. Тому всі знайдені координати задовольняють рівнянню кривої (1) і рівнянням операції подвоєння точки.

Зауваження.

Разом з точкою $P=(x_1,y_1)$ рівняння (2) та (3) а також рівняння самої кривої задовольняє і точка $Q=P+D=(x_2,y_2)$.

Доведення. Випливає з комутативності групи точок тому $Q+Q=P+D+P+D=2P+O$, бо точка D має порядок 2.

Твердження. Крива Едвардса містить точку порядка 8 тоді і только тільки, коли

$$\left(\frac{1-d}{p}\right)=1.$$

Правильність твердження слідує з того, що точки 8-го порядка задовольняють рівняння $2Q=F$, де $F=(\pm1,0)$ – точки 4-го порядка. Те, що точка Q має вигляд (x,x) слідує з формул додавання точок [2, 12] і з рівняння кривої (1). Звідси з рівняння кривої маємо $2(x,x)=(\pm1,0)$, де $(\pm1,0)=F$ це координати точки 4-го порядка. Значить, точка Q лежить на диагоналі, тобто $|x|=|y|$. Звідси і з рівняння кривої маємо біквадратне рівняння $2x^2=1+dx^4$, $dx^4-2x^2+1=0$. Дискримінант якого є наступним $D=4-4d=4(1-d)$. Тому, щоб розв'язок існував необхідно і достатньо, щоб $\left(\frac{1-d}{p}\right)=1$.

Нехай $\left(e,\left|E_{1,d}\right|\right)=1$, де $e\in\mathbb{N}$, тоді в якості формули генерації псевдовипадкових послідовностей над полем $\mathbb{F}_{p^n}$ можна використати $P_j=e^jP_0$, P_0 – твірний групи кривої Едварса, її важкооборотність грунтується па проблемі дискретного логарифма. А біт складності односторонньої функції визначимо через композицію $Tr(x)=x+x^p+...+x^{p^{n-1}}$, де x – це перша координата з e^jP_0 з предикатом половинності заданим як

$$f_i=\begin{cases}0,\ Tr(x_i)<\dfrac{p-1}{2},\\ 1,\ Tr(x_i)\geq\dfrac{p-1}{2}.\end{cases}$$

Висновки. Дослідження дозволило знайти критерію суперсингулярності кривих, що дає можливість перевіряти криві на придатність до використання в якості носія групи точок для генератора псевдовипадкових послідовностей великого періоду.

Список використаних джерел:

1. Edwards H. A normal form for elliptic curves. *American Mathematical Society*. 2007. Vol. 44. No. 3. P. 393–422.
2. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*. 2008. P. 326–343.
3. Скуратовський Р., Мовчан П. В., Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp. *Збірник праць 14 Всеукраїнської науково-практичної конференції. ФТІ НТУУ «КПІ»*. 2016. Том 2. С. 102–104.
4. Скуратовський Р. Дослідження властивостей скрученої кривої Едвардса. *Конференція державної служби спеціального зв'язку та захисту інформації.* URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894
5. Сергієнко І., Задірака В., Литвин О. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. К. : Наук. думка, 2012. 400 с.
6. *Алексеев Е., Ошкин И., Попов В., Смышляев С., Сонина Л.* О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе. *Материалы XVI международной конференции «РусКрипто 2014»*. 2014. С. 24–26.
7. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*. 1993. Vol. 39. No. 5. P. 1603–1646.
8. Skuratovskii R. V. Twisted Edwards curve and its group of points over finite field Fp. *Літня школа «Алгебра, Топологія, Аналіз»*. Одеса, 2016. С. 122–124.
9. Skuratovskii R., Skruncovich U. Twisted Edwards curve and its group of points over finite field Fp. *Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf
10. Fulton W. Algebraic curves. An Introduction to Algebraic Geometry. *Third Preface – January*, 2008. 121 p.
11. Deepthi P.P., Sathidevi P.S. New stream ciphers based on elliptic curve point multiplication. *Computer Communications*. 2009. Vol. 32. P. 25–33.
12. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649.* 2008. P. 1–17.
13. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым. *Радиотехника*. 2015. Вып. 181. С. 58–63.
14. Skuratovskii R.V. Constructing of finite field normal basis in deterministic polynomial time (in Ukraine). *Bulletin of Kiev national university of Tarasa Shevchenka*. 2011. P. 49–54.

References:

1. Edwards, H. (2007). A normal form for elliptic curves. *American Mathematical Society*, vol. 44, no. 3, pp. 393–422. [in English].
2. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. (2008). Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*, pp. 326–343. [in English].
3. Skuratovskyi, R., Movchan, P. V. (2016). Normalizatsiia skruchenoi kryvoi Edvardsa ta doslidzhennia yii vlastyvostei nad Fp. *Zbirnyk prats 14 Vseukrainskoi naukovo-praktychnoi konferentsii. FTI NTUU «KPI»*, vol. 2, pp. 102–104. [in Ukrainian].
4. 9. Skuratovskyi, R. Doslidzhennia vlastyvostei skruchenoi kryvoi Edvardsa. *Konferentsiia derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894 [in Ukrainian].
5. Serhiienko, I., Zadiraka, V., Lytvyn, O. (2012). Elementy zahalnoi teorii optymalnykh alhorytmiv ta sumizhni pytannia. K.: Nauk. dumka, 400 p. [in Ukrainian].
6. Alekseev, E., Oshkin, I., Popov, V., Smyshlyaev, S., Sonina, L. (2014). O perspektivah ispolzovaniya skruchennyh ellipticheskih krivyh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove. *Materialy XVI mezhdunarodnoj konferencii «RusKripto 2014»*, pp. 24–26. [in Russian].
7. Menezes, A., Okamoto, T., Vanstone, S. (1993). Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*, vol. 39, no. 5, pp. 1603–1646. [in English].

8. Skuratovskii, R. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. *Litnia shkola «Alhebra, Topolohiia, Analiz»*, Odesa, pp. 122–124. [in English].

9. Skuratovskii, R., Skruncovich, U. Twisted Edwards curve and its group of points over finite field Fp. Akademgorodok, Novosibirsk, Russia. *Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf [in English].

10. Fulton, W. (2008). Algebraic curves. An Introduction to Algebraic Geometry. *Third Preface – January*, 121 p. [in English].

11. Deepthi, P.P., Sathidevi, P.S. (2009). New stream ciphers based on elliptic curve point multiplication. *Computer Communications*, vol. 32, pp. 25–33. [in English].

12. Daniel, J. Bernstein, Peter, Birkner, Marc, Joye, Tanja, Lange, Christiane, Peters. (2008). Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649*, pp. 1–17. [in English].

13. Bessalov, A.V., Cygankova, O.V. (2015). Proizvoditelnost gruppovyh operacij na skruchennoj krivoj Edvardsa nad prostym. *Radiotehnika*, vol. 181, pp. 58–63. [in Russian].

14. Skuratovskii, R.V. (2011). Constructing of finite field normal basis in deterministic polynomial time (in Ukraine). *Bulletin of Kiev national university of Tarasa Shevchenka*, pp. 49–54. [in English].