ПЕРСПЕКТИВНІ КРИПТОПЕРЕТВОРЕННЯ

ОЦІНКА ШВИДКОДІЇ ПРОГРАМНИХ ФУНКЦІЙ СКАЛЯРНОГО МНОЖЕННЯ ТА ПОШУК КОЕФІЦІЄНТІВ РІВНЯННЯ ІЗОГЕННИХ КРИВИХ З ВИКОРИСТАННЯМ MIRACL CRYPTOGRAPHIC SDK

Київ 2021

АНОТАЦІЯ

ШИФР РОБОТИ

ПЕРСПЕКТИВНІ КРИПТОПЕРЕТВОРЕННЯ

НАЗВА РОБОТИ

ОЦІНКА ШВИДКОДІЇ ПРОГРАМНИХ ФУНКЦІЙ СКАЛЯРНОГО МНОЖЕННЯ ТА ПОШУК КОЕФІЦІЄНТІВ РІВНЯННЯ ІЗОГЕННИХ КРИВИХ З ВИКОРИСТАННЯМ MIRACL CRYPTOGRAPHIC SDK

Володіючи рядом чудових властивостей, криві Едвардса над скінченними полями займають особливе місце серед різних форм представлення еліптичних кривих. Скалярний добуток для точок кривої Едвардса обчислюється мінімальним числом операцій, тому криві Едвардса викликають інтерес при проектуванні криптографічних протоколів і стандартів асиметричного шифрування.

Метою роботи є оцінка швидкодії програмних функцій скалярного множення та реалізація пошуку коефіцієнтів ізогенної кривої за допомогою алгоритму Велю з використанням MIRACL Cryptographic SDK.

Для досягнення даної мети слід виконати наступні завдання:

- проведення аналізу відомих підходів до реалізації додавання та подвоєння точок еліптичної кривої в різних базисах;
- реалізація операції скалярного множення точок кривої Едвардса;
- реалізація пошуку коефіцієнтів ізогенної кривої за допомогою алгоритму Велю.

У роботі було розглянуто форми представлення ЕК та необхідні властивості для використання кривих Едвардса в криптографії. Проведено аналіз швидкодії операцій над точками ЕК у формі Едвардса в різних базисах. Програмно реалізована функція скалярного множення точок ЕК та пошук коефіцієнтів ізогенних кривих за алгоритмом Велю з використанням MIRACL Cryptographic SDK.

Результатом роботи є нові оцінки швидкодії операцій скалярного множення точок еліптичних кривих в формі Вейєрштрасса, нові параметри часткового випадку еліптичних кривих, а саме скручених кривих Едвардса в інвертованих координатах, що надають можливість отримати максимальну швидкодію операцій над точками еліптичної кривої, які дозволені міжнародними стандартами для криптографічного застосування. Також вперше вдосконалено бібліотеку програмних функцій MIRACL, яка дозволяє реалізовувати операції над точками кривих над полем з довжиною характеристики 384 біт.

Дана наукова робота складається з двох розділів, загальний обсяг: 69 сторінок, 6 рисунків, 12 таблиць, 6 діаграм, 5 додатків та 17 використаних джерел.

Ключові слова: еліптична криптографія, еліптичні криві Едвардса, скалярне множення, ізогенії, MIRACL Cryptographic SDK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
API	–	Application Programming Interface
DSA	–	Digital Signature Algorithm
ECC	–	Elliptic Curve Cryptography
KCM	–	Karatsuba-Comba-Montgomery
Ltd.	–	Limited definition
MIRACL	–	Multiprecision Integer and Rational Arithmetic Cryptographic Library
MOV	–	Menezes, Okamoto, Vanstone
RSA	–	Rivest, Shamir і Adleman
SDK	–	Software Development Kit
ЕК	–	Еліптична крива

ВСТУП

Серед різних форм представлення еліптичних кривих особливе місце займають криві у формі Едвардса, що з'явилася в сучасній науковій літературі порівняно нещодавно [1,2], вони є найшвидшими й найперспективнішими для використання в асиметричних криптосистемах на даний момент. Особливістю таких кривих є можливість подання нейтрального елемента в афінних координатах, універсальність закону додавання та рекордна швидкість операції додавання точок еліптичної кривої, що забезпечує незаперечні переваги для використання кривих Едвардса в криптографії.

При застосуванні криптографічних алгоритмів з використанням еліптичних кривих важливим чинником є час їхньої роботи. Найбільш ресурсо- та часовитратною є операція скалярного множення точок еліптичної кривої на число. Таким чином, актуальними є дослідження способів та методів даного обчислення. Скалярний добуток для точок кривої Едвардса обчислюється мінімальним числом операцій у порівнянні з іншими відомими представленнями еліптичних кривих [2, 4]. Безсумнівно, що криві Едвардса викликають інтерес при проектуванні криптографічних протоколів і майбутніх стандартів асиметричного шифрування.

З появою потужних квантових комп’ютерів сучасні алгоритми шифрування втратять свою актуальність, так як не зможуть забезпечити конфіденційність інформації. Одним зі способів вирішення даної проблеми є використання ізогеніїв. Тому їхнє дослідження є дуже важливими.

РОЗДІЛ 1
АНАЛІЗ ВІДОМИХ ПІДХОДІВ ДО РЕАЛІЗАЦІЇ ДОДАВАННЯ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ В РІЗНИХ БАЗИСАХ ТА ПОШУШКУ ІЗОГЕННИХ КРИВИХ

У даному розділі проведено огляд базових понять про ЕК. Розглянуто алгоритми додавання та подвоєння точок еліптичних кривих у різних базисах, поняття ізогеніїв та алгоритм їх пошуку.

1.1. Базові поняття

Еліптичні криві є джерелом кінцевих абелевих груп та володіють корисними структурними властивостями. Вони забезпечують ті ж самі показники стійкості, якими володіють числові й поліноміальні криптосистеми, але відповідні показники перших вдалося отримати при істотно меншому розмірі ключа. Тому їх використовують для побудови криптографічних протоколів [1, 2].

Еліптична крива E над скінченним полем F_p називається крива, що задається рівнянням Вейєрштрасса (1.1)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

де $\{a_1, a_2, a_3, a_4, a_5, a_6\} \in F_p$.

Якщо $p \neq 2$, то лінійною заміною змінних $y \to \frac{a_1x+a_3}{2}$ крива 1.1 переходить у криву виду

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Еліптичною кривою E над скінченним простим полем $F = GF(p)$, де $p \neq 2{,}3$, змінну a_2 (з рівняння 1.2) можна прирівняти нулю. Так рівняння ЕК приймає вигляд

$$y^2 = x^3 + ax + b, \qquad \text{де } a, b \in F_p. \tag{1.3}$$

Якщо $F = GF(2^m)$, то крива E описується рівнянням:

$$2 + xy = x^3 + ax + b, \qquad \text{де } a, b \in F.$$

Дані асиметричні криптосистеми, засновані на еліптичних кривих над кінцевими полями.

Еліптичні криві можна поділити на сингулярні і не сингулярні відповіно до рівності чи не рівності нулю дискримінанта кривої $\mathrm{A} = -16(4\mathrm{a}^3 + 27b^2)$. Сингулярні криві містять самоперетин, тому з точки зору алгебри та криптографії вони не відіграють важливу теоретичну роль і не мають практичного застосування. Тому в теорії еліптичних кривих прийнято вважати, що $\mathrm{A} = 0$.

Еліптичні криві у формі Вейєрштрасса

Еліптичною кривою у формі Вейєрштрасса [13] над полем F_p, де $p \neq 2,3$, називають криву, яка в афінних координатах задається рівнянням:

$$y^2 = x^3 + Ax + B, \tag{1.5}$$

де $A, B \in F_p$.

Закон додавання точок

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases} \tag{1.6}$$

Закон подвоєння точки

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -\left(\frac{3x_1^2 - a}{2y_1}\right)x_3 + \frac{x_1^3 - ax_1 - 2b}{2y_1} \end{cases} \tag{1.7}$$

Еліптичні криві в оригінальній формі Едвардса[1]

$$x^2 + y^2 = e^2(1 + x^2y^2) \tag{1.8}$$

Закон додавання точок

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{e(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - x_1x_2y_1y_2)}\right) \tag{1.9}$$

Закон подвоєння точки

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{e(1 + x_1^2y_1^2)}, \frac{y_1^2 - x_1^2}{e(1 - x_1^2y_1^2)}\right) \tag{1.10}$$

Еліптичні криві у формі Едвардса з модифікацією Бернштейна-Ланге [4]

$$x^2 + y^2 = 1 + dx^2y^2, \tag{1.11}$$

де $d(1 - de^4) \neq 0, \left(\frac{d}{p}\right) = -1$.

Закон додавання точок

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - y_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \right) \quad (1.12)$$

Закон подвоєння точки

$$2(x_1, y_1) = \left(\frac{x_1^2 - y_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2} \right) \quad (1.13)$$

При обчисленні закон подвоєння точки працює швидше ніж закон додавання.

1.2. Аналіз математичних виразів додавання та подвоєння точок еліптичної кривої Едвардса

При роботі з точками ЕК Едвардса використовують афінні, проективні та інверсні координати. В різних координатних площинах діють свої закони алгебраїчних операцій.

Базиси подання точок еліптичної кривої Едвардса[5]

В афінних координатах точки ЕК виражається двома координатами x та y, де множина значень $x, y \in F_p$, що задовольняють рівняння 1.17.

Щодо проективних координат, то $\{(X, Y, Z) : X, Y, Z \in F_q, (X, Y, Z) \neq (0,0,0)\}$. Так як між проективними та афінними координатами існує зв'язок: $x = X/Z, y = Y/Z$, то заміною можна привести рівняння кривої E з афінних координат в проективні:

$$\text{E: } (X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2,$$
$$\text{де } X = xZ, Y = yZ.$$

Введення проективних координат є досить корисним з точки зору криптографії, оскільки воно також дозволяє більш ефективно застосовувати закони додавання та подвоєння точок без використання інверсій у базовому полі, оскільки кожна інверсія є досить складною операцією.

Використання інвертованих проективних координат пришвидшує обчислення, тому обчислення виконуються в них. Якщо ввести формальну заміну координат $x = \frac{Z}{X}, y = \frac{Z}{Y}$, тоді рівняння (1.10) матиме вигляд:

$$\frac{Z^2}{X^2} + \frac{Z^2}{Y^2} = 1 + \frac{dZ^4}{X^2Y^2}$$

Можна переписати у формі проективної кривої з інверсією координат:

$$Z^2(X^2+Y^2) = X^2Y^2 + dZ^4,$$
де $XYZ \neq 0$.

Складність групових операцій для точок повної кривої Едвардса [14]

В роботі [2] вперше було дано аналіз складності виконання групових операцій на кривій у формі Едвардса в проективних координатах і доведена суттєва перевага у порівнянні з аналогічними операціями на кривій у формі Вейєрштрасса. Слідуючи цій роботі, позначено складності виконання операцій в полі F_q: M – множення, S – піднесення до квадрату, I – інверсія, U – множення на параметр кривої. Інверсія елементів [6] є трудомісткою операцією арифметики еліптичних кривих, що оцінюється порядком $I \cong (10-50M)$. Щоб позбутися від інверсії, при виконанні криптопротоколів переходять від двовимірних афінних координат до проективних координат [2]. Такий перехід забезпечує значну перевагу в продуктивності обчислень [7].

Визначення та властивості скручених кривих Едвардса

В роботі [9] скручені криві Едвардса (twisted Edwards curves) були визначені як узагальнення кривих Едвардса $x^2+y^2 = 1+dx^2y^2$ шляхом введення нового параметра a в рівняння

$$ax^2+y^2 = 1+dx^2y^2,$$
де $a \neq d, a, d \in F_p^*, d \neq 1, p \neq 2$.

Використовуються модифіковані закони додавання і подвоєння точок [3].

$$E_a, d\colon\ x^2+ay^2 = 1+dx^2y^2,$$
де $a, d \in F_p^*, d \neq 1, a \neq d, p \neq 2$.

Одиничним класом кривих в узагальненій формі Едвардса є скручена крива Едвардса з обмеженнями на параметри a і d

$$E_{a,d} : x^2+ay^2 = (1+dx^2y^2), \tag{1.15}$$
де $a, d \in F_p^*, d \neq 1, a \neq d, \left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$.

Модифіковані закони додавання і подвоєння точок кривої (1.15) мають вигляд:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1-dx_1x_2y_1y_2}, \frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}\right) \tag{1.16}$$

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1-dx_1^2y_1^2)}, \frac{2x_1y_1}{(1+dx_1^2y_1^2)}\right) \tag{1.17}$$

Альтернативний закон додавання точок [11]

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}\right) = (x_3, y_3). \qquad (1.18)$$

Додавання точок (закон додавання (1.16))

Нехай $x = \frac{X}{Z}, y = \frac{Y}{Z}$, тоді рівняння кривої (1.15) в проективних координатах має вигляд

$$(X^2 + aY^2)Z^2 = Z^4 + dX^2Y^2, \quad X = xZ, \; Y = yZ.$$

Сума двох точок тепер записується як $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$. З урахуванням підстановок визначено координати точки згідно (1.16):

$$x_3 = \frac{X_3}{Z_3} = \frac{Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(X_1X_2 - aY_1Y_2)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)},$$
$$y_3 = \frac{Y_3}{Z_3} = \frac{Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(X_1X_2 - aY_1Y_2)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}.$$

Позначення:

$A = Z_1Z_2$; $B = A^2$; $C = X_1X_2$; $D = aY_1Y_2$; $E = dCD$; $F = B - E$; $G = B + E$

Тоді

$$Y_3 = A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D),$$
$$X_3 = A \cdot G \cdot (D - C),$$
$$Z_3 = F \cdot G.$$

Підрахунок числа елементарних операцій тут дає 10 операцій множення M, одне піднесення до квадрату S і 2 множення на параметри a і d кривої. Отже, знаходимо складність обчислення суми різних точок, виражену через число множень і піднесень до квадрату в полі $V_E = 10M + 1S + 2U$ [9].

Подвоєння точок

Використовуючи рівняння кривої (1.15), закон подвоєння (1.17) можна записати у формі, що не залежить від параметра d

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{2 - x_1^2 - ay_1^2}, \frac{2x_1y_1}{x_1^2 + ay_1^2}\right)$$

Тоді координати точки подвоєння згідно (3.3)

$$x_3 = X_3Z_3 = \left(\frac{\left(\left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)}{\left((2 - \left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)}\right) = \frac{(X_1^2 - aY_1^2)(X_1^2 + aY_1^2)}{(2Z_1^2 - X_1^2 - aY_1^2)(X_1^2 + aY_1^2)},$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{2\frac{X_1}{Z_1}\frac{Y_1}{Z_1}\left(\left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)}{\left(2 - \left(\frac{X_!}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)} = \frac{2X_1Y_1(2Z_1^2 - X_1^2 - aY_1^2)}{(2Z_1^2 - X_1^2 - aY_1^2)(X_1^2 + aY_1^2)}.$$

Позначення:

$$A = X_1^2, B = Y_1^2, C = aY_1^2, D = Z_1^2, E = (A + C), F = (A - C),$$
$$G = 2D - A - C, H = (X_1 + Y_1)^2 \Rightarrow 2X_1 \cdot Y_1 = H - A - B.$$

Тоді

$$X_3 = E \cdot F,$$
$$Y_3 = 2X_1Y_1 \cdot G,$$
$$Z_3 = E \cdot G.$$

Підрахунок числа операцій піднесення до квадрату і множення в полі дає сумарну складність групового подвоєння $T_E = 3M + 4S + 1U$ [9].

Складність додавання (альтернативний закон (1.18))

Вводячи розширені проектні координати $(X{:}Y{:}T{:}Z)$, авторам [11] вдалося скоротити число польових операцій при додаванні 2-х різних точок до $9\mathrm{M} + 1U$ в порівнянні зі складністю $10\mathrm{M} + 1S + 2U$ при реалізації додавання за формулою (4.2) [9].

При $Z \neq 0$ задано чотиривимірні проективні координати $(X{:}Y{:}T{:}Z)$, підстановкою в (1.18). Тоді

$$\frac{X_3}{Z_3} = \frac{(T_1Z_2 + Z_1T_2)}{(Y_1Y_2 + aX_1X_2)}, \qquad \frac{Y_3}{Z_3} = \frac{(T_1Z_2 - Z_1T_2)}{(X_1Y_2 - Y_1X_2)}.$$

Звідси

$$X_3 = (X_1Y_2 - Y_1X_2)((T_1Z_2 + Z_1T_2),$$
$$Y_3 = (Y_1Y_2 + aX_1X_2)((T_1Z_2 - Z_1T_2),$$
$$T_3 = (T_1Z_2 + Z_1T_2)((T_1Z_2 - Z_1T_2),$$
$$Z_3 = (Y_1Y_2 + aX_1X_2)((X_1Y_2 - Y_1X_2).$$

Нехай

$$\mathrm{A} = \mathrm{X}_1\mathrm{X}_2, \mathrm{B} = Y_1Y_2, C = T_1Z_2, D = Z_1T_2, E = C + D, F = C - D,$$
$$G = B + aA, H = (X_1 - Y_1)(X_2 + Y_2) - A + B.$$

Тоді

$$X_3 = EH, Y_3 = GF, T_3 = EF, Z_3 = GH.$$

Тому складність групової операції додавання різних точок становить $V_E^* = 9\mathrm{M} + 1U$. Якщо параметр $\mathrm{a} = \pm 1$ або менше, складність оцінюється як 9M. При подвоєнні точки кривої Едвардса в тривимірних проективних координатах складність мінімальна і становить $T_E = 3\mathrm{M} + 4S + 1U$ [9]. В роботі [11]

показано, що в розширених проективних координатах складність подвоєння зростає на одну операцію множення $T_E^* = 4\text{M} + 4S + 1U$.

Таблиця 1.1

Складність групових операцій класів кривих в різних координатах

Клас кривих, координати	Складність групової операції	
	Додавання точок	Подвоєння точок
Повні криві Едвардса, проективні координати	$10\text{M} + 1S + 1U$	$3\text{M} + 4U$
Скручені криві Едвардса, проективні координати	$10\text{M} + 1S + 2U$	$3\text{M} + 4S + 1U$
Скручені криві Едвардса, розширені проективні координати	$9\text{M} + 1U$	$4\text{M} + 4S + 1U$

Найменших обчислювальних витрат вимагають операції на повних кривих Едвардса. Особливо вони виграють при подвоєнні, яке обходиться без операції множення на параметр кривої $1U$.

1.3. Ізогенії еліптичних кривих

Криптографія з використанням ізогеніїв вважається стійкою до атак квантових комп'ютерів. Квантовий комп'ютер, який зможе утримати в зв'язаному стані декілька тисяч кубіт, дозволить знаходити закриті ключі по відкритих ключах у всіх асиметричних криптосистемах, які зараз використовуються. Число кубіт для злому RSA дорівнює подвоєному числу біт в модулі, тобто для розкладання на множники модуля RSA довжиною 2048 біт потрібно 4096 кубіт. Для злому еліптичних кривих необхідні більш скромні потужності «квантового заліза»: для вирішення завдання ECDLP для кривих над простим полем з модулем кривої довжиною n біт потрібно $6n$ кубіт, тобто для модуля в 256 біт потрібно 1536 кубіт, а для 512 біт – 3072 кубіт [10].

Ізогенія – це раціональне відображення, яке переводить точки однієї кривої E_1 в точки інший кривої E_2, або в саму себе, наступним чином: якщо на кривій E_1 обрати будь-які дві точки A_1 і B_1 і відобразити їх в точки A_2 і B_2 на кривій E_2, тоді те ж саме відображення обов'язково переведе їх суму – точку $\text{C}_1 = A_1 + B_1$ в точку $\text{C}_2 = A_2 + B_2$ – суму їх відображень. Ця властивість називається збереженням операції, а таке відображення є гомоморфізмом. Ізогенію можна

виразити за допомогою раціональної функції: точка (x, y) відображається в точку з координатами $\left(\frac{f_1(x,y)}{f_2(x,y)}, \frac{g_1(x,y)}{g_2(x,y)}\right)$, де f_1, f_2, g_1, g_2 – поліноми. Якщо між двома кривими існує таке відображення, то вони є ізогенними. Окремий випадок ізогенії, ендоморфізм – це ізогенія кривої на саму себе [16].

Теорема Тейта

Дві криві над одним кінцевим полем ізогенні тоді і тільки тоді, коли порядки їх груп рівні.

Приклад 1 (ендоморфізм):

Скалярне множення точки на число: $n * P$ на кривій $y^2 = x^3 + Ax + B$ для $n = 2$ та $P = (x, y)$:

$$2 * P = \left(\frac{x^4 - 2Ax^2 - 8Bx - A^2}{4(x^3 + Ax + B)}, \frac{(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B - A)y}{8(x^3 + Ax + B)^2}\right)$$

Для довільного n аналогічна, але довша, формула може бути отримана рекуррентно за допомогою поліномів ділення (division polynomials).

Приклад 2 (ізогенія між різними кривими):

Нехай є крива $E_1: y^2 = x^3 + x + 1$ над полем $GF(19)$ і крива $E_2: y^2 = x^3 + 4x + 13$ над тим же полем. Порядки їхніх груп, тобто число точок на кривій, у E_1 і E_2 рівні: $\#E_1 = \#E_2 = 21$.

По теоремі Тейта рівність $\#E_1 = \#E_2$ означає, що між E_1 та E_2 існує ізогенія. Групи точок кривих не ізоморфні тому, що j-інваріант $E_1 = 6$, а j-інваріант $E_2 = 4$. Ізогенія, яка відображає точки з E_1 на E_2 може бути представлена за допомогою наступного раціонального відображення:

$$\varphi: (x, y) \to \left(\frac{x^3 - 4x^2 - 8x - 8}{x^2 - 4x + 4}, \frac{x^3y - 6x^3y + 5xy - 6y}{x^3 - 6x^2 - 7x - 8}\right)$$

Наприклад, точки A_1 (9, 6) і B_1 (14, 2) кривої E_1 та їх сума – точка C_1 з координатами (5, 6), якщо підставити їх в формулу вище, то буде отримано їх відображення на криву E_2, відповідні їм точки на $E_2 - A_2, B_2, C_2$. Обрахунок проведено за допомогою програми написаної на мові програмування Python (додаток А). Результати проведених обрахунків відображені на рис. 1.3.1.

```
E:\Program-work\CALC_ECC\venv\Scripts\python.exe E:/Program-work/CALC_ECC/main.py
A1(9,6)->A2(14,1)
B1(14,2)->B2(17,4)
C1(5,6)->C2(8,5)
```

Рис. 1.3.1. Результати відображення точок кривої E_1 на криву E_2

$\mathrm{C}_2 = A_2 + B_2$, тобто точка $\mathrm{C}_1 = A_1 + B_1$ переходит в точку $\mathrm{C}_2 = A_2 + B_2$, звідси: $\varphi(A + B) = \varphi(A) + \varphi(B)$.

Число можливих ізогеніїв для конкретної кривої дорівнює кількості підгруп в групі її точок. Існує детермінований алгоритм який придумав математик Велю (Velu') в 1971 році.

Загальна схема алгоритму Велю:

1. На вхід подається крива $E_1: y^2 = x^3 + Ax + B$ і одна з її підгруп C (*isogeny kernel*).

2. На виході отримується крива $E_1: y^2 = x^3 + A'x + B'$, яка ізогенна кривій E_1 та раціональне відображення $\left(\frac{f_1(x,y)}{f_2(x,y)}, \frac{g_1(x,y)}{g_2(x,y)}\right)$.

В результаті отримуються коефіцієнти і для ізогенної кривої і формули з дробом. Підгрупа C – будь-яка з підгруп кривої. C – ядро ізогенія: всі її елементи переходять в точку на нескінченності. Якщо крива E_1 ізогенна до кривої E_2, то вірно і зворотне: E_2 ізогенна до E_1. Складність алгоритму: $O(\#C)$ кроків, де $\#C$ – порядок.

Так як і для мультиплікативних груп кінцевого поля і еліптичних кривих, для ізогеніїв існує своя складна задача, яка підвищує криптостійкість криптографічних алгоритмів заснованих на ізогеніях еліптичних кривих [16].

Складне завдання для ізогеніїв

Дано дві ізогенні криві E_1 і E_2 з різними j-інваріантами, про які відомо, що вони є ізогенними, але не відомо за допомогою якої підгрупи було отримано цю ізогенію. Число підгруп має бути великим настільки, щоб було обчислювально складно знайти ізогенію простим перебором, підставляючи підгрупи в алгоритм Велю.

Висновки. Все більшої популярності набувають криптосистеми побудовані на еліптичних кривих через те, що на основі їх застосування вдалося забезпечити ті ж показники стійкості, якими володіють числові і поліноміальні

криптосистеми, але відповідні показники перших вдалося отримати при істотно меншому розмірі ключа. Так, наприклад 160-бітний ключ криптосистеми побудованої на еліптичних кривих Едвардса забезпечує таку ж крипостійкість як і 1024-бітний ключ RSA.

Володіючи рядом чудових властивостей, криві Едвардса над скінченними полями дуже перспективні для використання в асиметричних криптосистемах. Закон додавання для точок кривої Едвардса має властивості універсальності і повноти [2], що робить їх лідерами в швидкості обчислення групових операцій.

Аналіз показав, що найменших обчислювальних витрат при додаванні точок ЕК вимагають скручені криві Едвардса над розширеними проективними координатами, а при подвоєнні точок ЕК – повні криві Едвардса над проективними координатами.

З появою потужних квантових комп’ютерів сучасні алгоритми шифрування втратять свою актуальність, так як не зможуть забезпечити конфіденційність інформації. Одним зі способів вирішення даної проблеми є використання ізогеніїв. Тому їхнє дослідження є дуже важливими.

РОЗДІЛ 2

РЕАЛІЗАЦІЯ ОПЕРАЦІЙ СКАЛЯРНОГО МНОЖЕННЯ ТОЧОК КРИВОЇ ЕДВАРДСА ТА ПОШУКУ КОЕФІЦІЄНТІВ РІВНЯННЯ ІЗОГЕННОЇ КРИВОЇ ЗА АЛГОРИТМОМ ВЕЛЮ

2.1. Скалярне множення точок еліптичної кривої [18]

Операція скалярного множення являє собою множення цілого числа n на точку P еліптичної кривої, яке можна представити наступним чином: $nP = \underbrace{P + P + \cdots + P}_{n \text{ раз}}$. Обчислення nP вимагає n додавань, що є найбільш ресурсо- та часовитратною операцією, тому актуальними є дослідження способів та методів даного обчислення.

Порівняльний аналіз швидкодії скалярного множення точки для кривих у формі Едвардса і Вейєрштрасса [8]

Всі оцінки складності для додавання та подвоєння точок ЕК Едвардса наведено в таблиці 1.1.

Наведено складності всіх польових операцій до складності множення M. Беручи обчислювальну складність зведення в квадрат 1S = 0.67M [2], а множення на параметр кривої $1U = 0.5M$, отримано оцінки складності додавання і подвоєння на кривій Едвардса $V_p = 10M + 1S + 1U = 11{,}17M$, $T_W = 3M + 4S = 5.67M$. Подвоєння в проективних координатах майже в два рази швидше додавання. При використанні інвертованих проективних координат отримано $V_{EI} = 9M + 1S + 1U = 10{,}17M$, $T_{EI} = 3M + 4S + 1U = 6.17M$. Для еліптичної кривої у формі Вейєрштрасса відповідно, $V_W = 12M + 2S = 13.33M$, $T_W = 7M + 5S = 10.33M$. Нехай v_1 - відносна частота знаків «1» в двійковій послідовності числа k. Тоді в загальній формі перевага в продуктивності обчислення скалярного множення на кривій Едвардса в порівнянні з тим же обчисленням на кривій у формі Вейєрштрасса дорівнює

$$\gamma(v_1) = \frac{T_W + v_1 V_W}{T_E + v_1 V_E} = \frac{10.33 + 13.33 v_1}{5.67 + 11.17 v_1}. \quad (2.1)$$

Для обчислень в інвертованих проективних координатах отримано

$$\gamma(v_1) = \frac{T_W + v_1 V_W}{T_{EI} + v_1 V_{EI}} = \frac{10.33 + 13.33 v_1}{6.17 + 10.17 v_1}. \quad (2.2)$$

Використання повних кривих Едвардса дозволяє в 1.5 – 1.6 рази прискорити виконання криптопротоколів в порівнянні з іншими формами кривих [6].

Продуктивність скалярного множення точки в розширених проективних координатах [12]

Скручена крива Едвардса E в розширених проективних координатах має відповідні показники складності $V_E^* = 9\text{M} + 1U, T_E^* = 4\text{M} + 4S + 1U$, звідси $V_E^* = 9.5M,\ T_E^* = 7.17\text{M}$.

$$\gamma(v) = \frac{10.33 + v13.33}{7.17 + v9.5}.$$

Продуктивність скалярного множення точки в проективних координатах

Показники складності в проективних координатах: $V_E = 11.67M, T_E = 6.17M$. Звідси:

$$\gamma(v) = \frac{10.33 + v13.33}{6.17 + v11.67}.$$

Для порівняння виграшу продуктивності скалярного множення точок кривих Едвардса в порівнянні з кривими в канонічній формі Вейєрштрасса результати розрахунків коефіцієнтів $\gamma(v)$ занесено в таблицю 2.1.

Таблиця 2.1

Результати розрахунків коефіцієнтів $\gamma(v)$

Клас кривих, координати	Виграш $\gamma(v)$	
	(v = 0.5)-подвійне k	(v = 0.33)-потрійне k
Повні криві Едвардса, проективні координати	1.51	1.574
Скручені криві Едвардса, проективні координати	1.416	1.47
Скручені криві Едвардса, розширені проективні координати	1.426	1.429

Отже, використання закону додавання в розширених проективних координат дає дуже незначний приріст продуктивності обчислень на кривій

Едвардса в порівнянні з повним універсальним законом додавання (2.2). При потрійному скалярному множенні точки скрученої кривої Едвардса класичний закон додавання (2.2) в проективних координатах дає невеликий виграш в порівнянні з альтернативним законом додавання в розширених координатах. Найкращі результати у швидкодії скалярного множення, забезпечують повні криві Едвардса, що не мають надмірного параметра a. Слід підкреслити, що в порівнянні з канонічними кривими обидві арифметичні дії дають приріст швидкості скалярного множення приблизно в 1.5 рази.

2.2. Опис MIRACL Cryptographic SDK [15]

MIRACL Crypto SDK – високоточна цілочисельна та раціональна арифметична криптографічна бібліотека програмного забезпечення написана на мовах програмування C та C++, яка широко розглядається розробниками як золотий стандарт SDK з відкритим кодом для криптографії еліптичної кривої (ECC).

Можливості MIRACL:

- Скорочення коду програми;
- Значне спрощення розробки програми;
- Продуманий API;
- Швидка реалізація, використання вбудованого коду, прикладів програм та інших нововведень.

Ці унікальні якості MIRACL використання програмних рішень побудованих на ній в сотнях організацій по всьому світу, включаючи BAE Systems, Hitachi, Intel, Panasonic, Toyota та багато інших.

Особливості та переваги MIRACL

MIRACL [15] надає широкий та унікальний спектр переваг, що дозволяє розробникам безпечно та легко забезпечити швидку роботу програми в різних середовищах. В порівнянні з іншими подібними SDK він має:

- Вбудована C ++ обгортка системного виклику, що значно спрощує розробку програми;

- Більше 25-ти прикладних програм на C і C ++, що охоплюють широкий спектр застосувань, дають можливість почати розробку на їхній базі;

- Оптимізація вбудованих процесорів і оперативної пам’яті, щоб допомогти розробникам подолати обмеження пристрою та пам’яті;

- Сумісність з технологіями безпеки, включаючи шифрування AES, криптографія відкритого ключа RSA, обмін ключами Diffie-Hellman, цифровий підпис DSA та інші;

- Набір інструментів, які дозволяють швидко реалізувати будь-яку нову теоретико-числову функцію.

Бібліотека MIRACL складається з понад 100 процедур, які охоплюють усі аспекти високоточної арифметики. Визначено два нових типи даних - big для великих цілих чисел та flash для великих раціональних чисел. Великі цілі підпрограми засновані на алгоритмах Кнута, описаних у 4 розділі його класичної праці «Мистецтво комп’ютерного програмування». Арифметика з плаваючою косою рисою, яка працює з округлими дробами, спочатку була запропонована Д. Матулою та П. Корнеруп. Усі програми були ретельно оптимізовані для швидкості та ефективності, в той же час залишаючись стандартними, портативними *C*. Однак додаткові альтернативи швидкомовної мови монтажу для певних критичних для часу процедур також включені, особливо для популярних моделей процесорів Intel 80x86. Також надається інтерфейс C++ з включеним вихідним кодом.

Прослідковування помилок

MIRACL Ltd. використовує JIRA для взаємодії з користувачами та відстеження помилок. Якщо користувачем було знайдено помилку, то він повинен повідомити про помилки в трекері помилок MIRACL. Якщо користувач знайшов помилку, про яку вже повідомлялося, він можете додати власний коментар про неї або змінити її статус на "Підтверджено".

Співтовариство MIRACL Ltd.

MIRACL Ltd. - це найбільше співтовариство однодумців, що займаються інформаційною безпекою, які вважають, що криптографічний захист є

необхідним інструментом для захисту конфіденційності. ТОВ MIRACL надає інструменти, які можна використовувати для захисту інформації та захисту конфіденційності. Кожен, хто використовує код або послуги MIRACL Ltd., є частиною цієї глобальної спільноти.

2.3. Оцінка швидкодії програмної функції скалярного множення точок еліптичної кривої Едвардса з використанням MIRACL Cryptographic SDK

В роботі використовувались нові параметри скручених кривих Едвардса в нормальній формі [1], а також в інверсних координатах точок кривої Едвардса [4]. Варіанти кривих, які були згенеровані під час досліджень наведено в додатку В. Для визначених кривих було перевірено виконання вимог щодо стійкості до відомих методів криптоаналізу, а саме MOV-умова [6, 11], стійкість до атак ρ-Поларда і λ-Поларда та вимог до коефіцієнтів кривої Едвардса. В роботі використовувались скручені еліптичні криві у формі Едвардса над скінченним полем F_p, для простого числа $p \equiv 5 mod\ 8$ та з порядком групи точок еліптичної кривої $N_E = 4/n$, тобто з мінімальним кофактором 4 та простим числом n.

Під час розробки алгоритму програмного додатку було визначено ряд необхідних програмних функцій криптографічної бібліотеки MIRACL (табл. 2.2). Використання даних функцій значно пришвидшує реалізацію та час роботи програми. Докладний опис цих функцій відображено в додатку Б.

Таблиця 2.2

Рекомендовані функції MIRACL для роботи з ЕК

Функція	Виконувана дія
bigbits	Генерує big число заданої бітової довжини.
cinnum	Зчитує big/flash значення з файлу та присвоює його змінній.
cotnum	Вивід big/flash числа на екран або у файл.
divide	Ділить одне big число на інше.
ecurve_mult	Множить точку на еліптичній кривій $GP(p)$ на ціле число.
epoint_free	Звільняє пам’ять від точки ЕК.
epoint_get	Повертає значення координат точки ЕК.
epoint_init	Виділяє пам'ять точці на еліптичній кривій та ініціалізує її як точку на нескінченності.
epoint_set	Задає координати точці еліптичної кривої.
mirkill	Знищує big/flash – число прирівнюючи його до нуля та звільняє пам’ять від нього.
multi_inverse	Знаходить модульну інверсію багатьох чисел одночасно.

Програма надає можливість зчитувати з файлу координати як в нормальній формі так і в інвертованій (рис.2.1).

```
Read from file parameters in normal form - 1
Read from file parameters in inverted form - 2
Enter your choise:
```

Рис.2.1. Меню вибору форми зчитуваних з файлу координат

Точка ЕК множиться на задану кількість скалярів, що дає змогу встановлювати необхідну кількість виконання скалярного множення (рис.2.2).

```
Enter how many times do calculations:
```

Рис.2.2. Меню вводу кількості виконуваних операцій скалярного множення

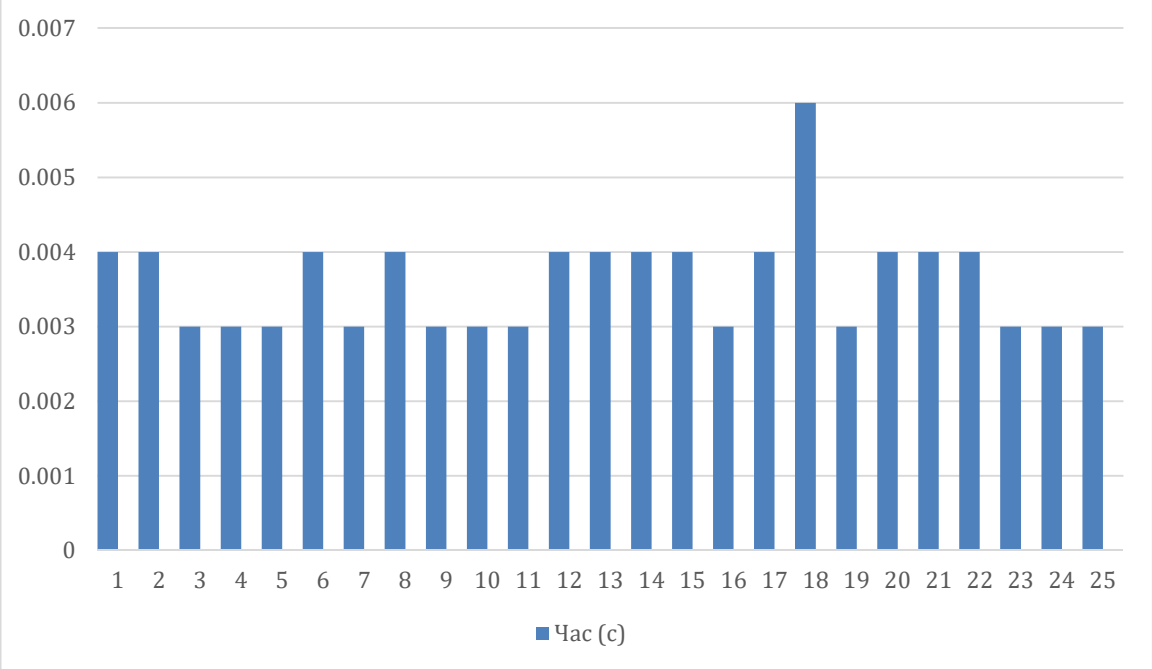
Скаляром при множенні виступає випадково згенероване за допомогою функції bigbits big-число, бітовий розмір якого дорівнює бітовому розміру характеристики поля.

Швидкість роботи програмної функції скалярного множення знаходиться для кожного випадку окремо, після чого обраховується їхнє середнє арифметичне значення. Це робить оцінку швидкості роботи програми більш точною. Результати скалярного множення точки ЕК на ці скаляри відображено на рис.2.3.

```
Output data:

-----Scalar multiplication Q=k1*P------
k1 -> BD1254C454617C8FD1C09807890001137F4615B16484201C3066A87BD261CB62673C03DD3564C91195F2076AC358FBAB
Q(x, y)
X: 2F3C6F1948EBA2D598F61EBBC2A27B5B406B7A36A8F79A59B6153CAD15EB5D9D15F121653E8022394FD3405106D0C4B9
Y: 170237DC41F44AADCC6FF85B6F1536005D5FAC801E46B6FC62E8FA18F5A2032A4D5F96722BC34C6AE6A3E121A965C52B
___________________Timer ___________________: 0.018

-----Scalar multiplication Q=k2*P------
k2 -> 367E79341D9067CA3B8E014279691F4BB5CC05CF353358156A9A9F455BD727465428BC6C9D713AF6F261D231D2678CCD
Q(x, y)
X: 75B3C96E69F9D2C6320375BAFC1CF6D5A1F709860EAE3436188CEF0FF04DACC33CBDE3DF5AFB1078E404EB2AF08F0E63
Y: DFBEA06BC9AD2990A8EDCA807800BACC46436E3D755C5E446639AC4C2E41B5EAFF16DF934CD4E6CC980BAB81827A5957
___________________Timer ___________________: 0.02

-----Scalar multiplication Q=k3*P------
k3 -> 3596B73F2F27C5D11EE4AEE6AEAB3A6C9E94EB86AB285EC464FD2AC87C95FCEB92217699C96027C817574D563BAC18CB
Q(x, y)
X: 3BAB4DF5C91328FAAE12502BCC2B67158ABA3438F6CC0683E56CAE394221DFEE80EBCDD81FCAA00F0BCA86E47C897DA2
Y: 9A821EADA040F289EBDC5DD44824C032021B14C8CEC7BC69AA3E86D0A1287DC77BEBE2568398467F4765D765649A2223
___________________Timer ___________________: 0.022

-----Scalar multiplication Q=k4*P------
k4 -> 2CCF717F183424184192EC0177357FBA8189BE35D52F0B9A87C4160D95BD98B4700636954C08DAC448CE3DC6B3C58355
Q(x, y)
X: C140A42C7A703FA06933C98E5D0AE05098DA72943695A8D30C27661C630E8CB795D1BCC2D52ED269DBD522D7697CDCE1
Y: DBD2234F63C5F33F30BF7B8DB923FAF1AB1E9FB28CE40E0B742FFA4A56CB4E613CF587346B629B3394AC0D6D3A8E47B
___________________Timer ___________________: 0.021

-----Scalar multiplication Q=k5*P------
k5 -> 5B131958F6534ADD51C359F6989E1B628F5FCFC3A3CF6C135A70978719B2D9848141750DD1AB38E2812B9FB9A291FEA
Q(x, y)
X: E78A922C90ED6BE8935F7DE2854CC0077CFFBB3D24688CC02F350A129B54C665F121BF547703ACCAF67BAA97EAB3C034
Y: 679849DF050532354BA6088C0F88A9E7819E56EBC4B51778BF9DE645279B6FF5C57F23D3DD600DD5BF9E59EB8ABBAF57
___________________Timer ___________________: 0.018
---------------------------------------------------
Average time: 0.0198
---------------------------------------------------
```

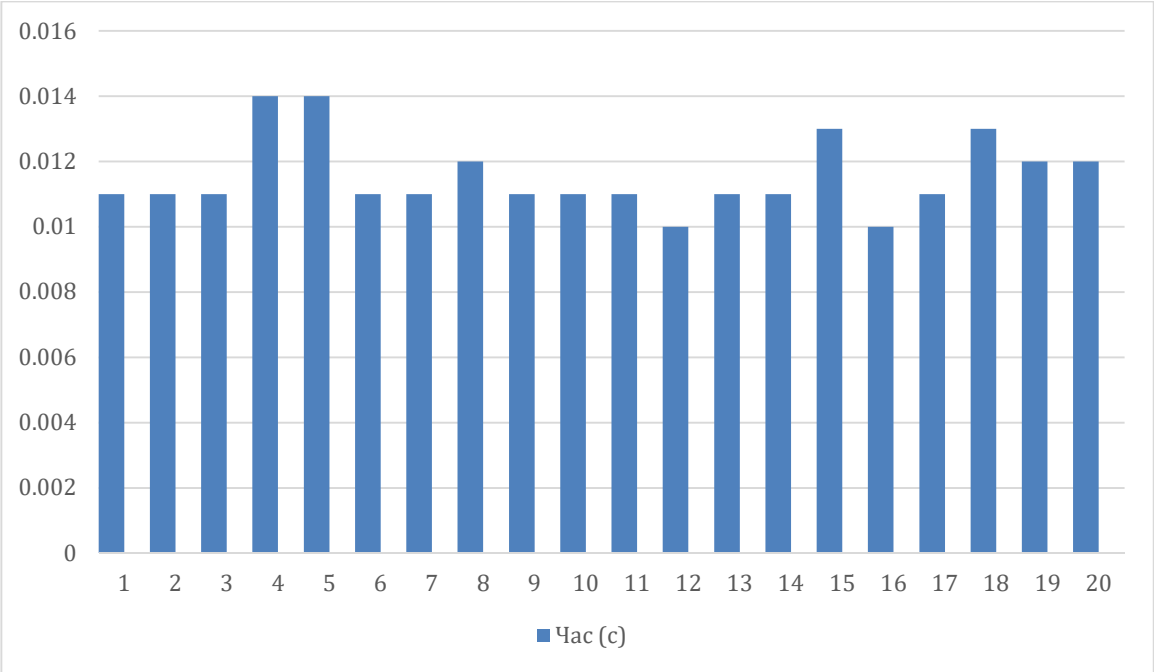
Рис.2.3. Результат роботи програми

Скалярне множення реалізовано в інвертованих координатах ЕК Едвардса з бітовими величинами характеристики поля 256, 384 та 512 біт. За результатами оцінки швидкодії побудовано діаграму часу виконання програмної функції скалярного множення. Результати цих обрахунків відображено в додатку Г.



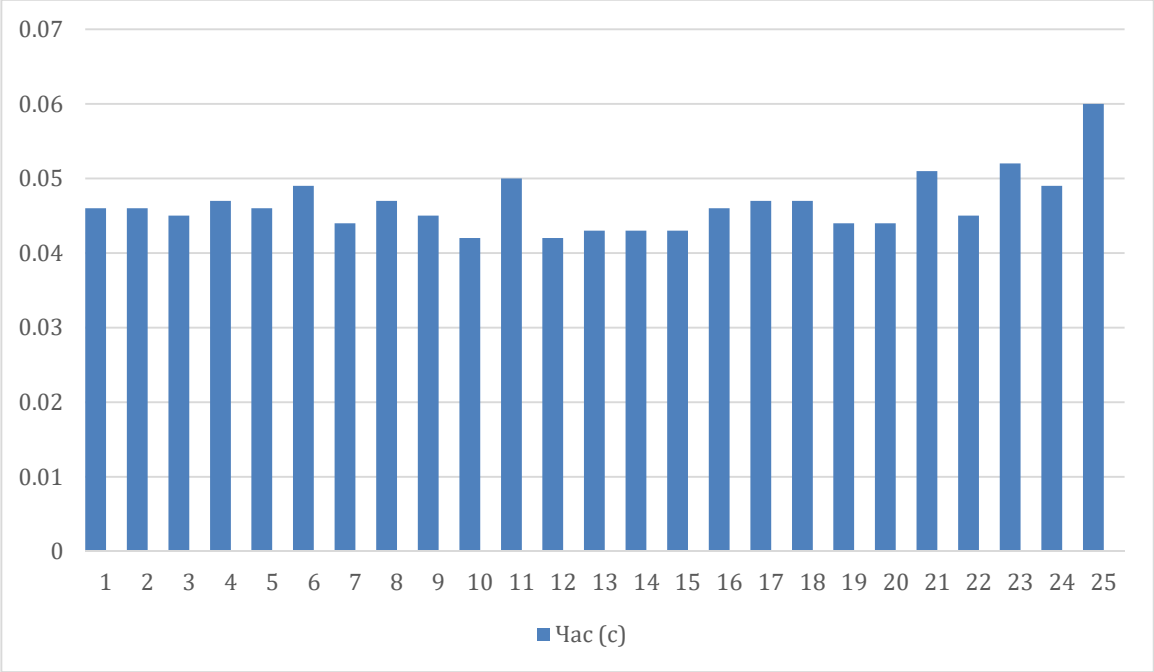
Діаграма 2.1. Час виконання програмної функції скалярного множення для точок ЕК Едвардса з бітовою величино характеристики поля 256 біт

З діаграми 2.1 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}004\ (c)$.



Діаграма 2.2. Час виконання програмної функції скалярного множення для точок ЕК Едвардса з бітовою величино характеристики поля 384 біт

З діаграми 2.2 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}011\ (c)$.



Діаграма 2.3. Час виконання програмної функції скалярного множення для точок ЕК Едвардса з бітовою величино характеристики поля 512 біт

З діаграми 2.3 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}047\ (c)$.

2.4. Програмна реалізація пошуку коефіцієнтів рівняння ізогенної кривої за алгоритмом Велю

На вхід алгоритму Велю подається крива $E_1: x^3 + Ax + B$ та одна з її підгруп C (ядро ізогенії).

Епатпи алгоритма Велю:

1. Відкидання точки на нескінченності.
2. Пошук C_2 – безліч точок парного порядку з C. R – всі інші.
3. Розбиття R на дві частини – R_+ та R_-, якщо точка P в R_+, то обернена їй в R_-.
4. Множина $S = C_2 \cup R_+$.

Для кожної точки $Q = (x_Q, y_Q)$ з S:

1) $g_Q^x = 3x_Q^2 + A$
2) $g_Q^y = -2y_Q$
3) $if(Q = -Q)\{\, v_Q = g_Q^x\} \, else\{\, v_Q = 2g_Q^x\}$
4) $u_q = \left(g_Q^y\right)^2$
5) $v = \sum_{Q \in S}(v_Q)$

6) $w = \sum_{Q \in S}(u_Q + x_Q y_Q)$

Коефіцієнти A' і B'для рівняння кривої E':

$$A' = A - 5v$$
$$B' = B - 7w$$

Обрахунок відображення $(x, y) \to (\alpha, \beta)$:

$$\alpha = x + \sum_{Q \in S}\left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2}\right)$$

$$\beta = y - \sum_{Q \in S}\left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2}\right)$$

Вихідні дані алгоритму Велю:

- Коефіцієнти A' і B'ізогенної кривої;
- Формула для відображення точок $(x, y) \to (\alpha, \beta)$.

Даний алгоритм для пошуку коефіцієнтів ізогенної кривої реалізовано програмно на мові C++ з використанням MIRACL Cryptographic SDK.

Приклад розрахунку ізогенії описаної в розділі 1.3:

Вхідні дані алгоритму Велю:

$y^2 = x^3 + x + 1$ над полем $GF(19)$ і підгрупа C: $\{O, (2,7), (2,12)\}$.

1. Відкидання точки на нескінченності.
2. Точок парного порядку в C немає.
3. Обрання для R_+ точки $(2,7)$. Точка $(2,12)$ – обернена їй. Так як $7 = -12 mod 19$.
4. Множина $S = \{(2,7)\}$.

Наступний пункт це виконання циклу з одним повторенням, так як множина S містить одну точку:

$Q = (2,7)$, її координати $x_Q = 2, y_Q = 7$
$g_Q^x = 3 * 2^2 + 1 = 13$
$g_Q^y = -2 * 7 = -14 \, mod \, 19 = 5$
$v_Q = 2 * 13 = 26 \, mod \, 19 = 7$
$u_Q = 5^2 \, mod \, 19 = 6$
$v = 7$
$w = 6 + 2 * 7 = 20 \, mod \, 19 = 1$
$A' = A - 5v = 1 - 5 * 7 = -34 \, mod \, 19 = 4$
$B' = B - 7w = 1 - 7 * 1 = -6 \, mod \, 19 = 13$

Результат роботи програми для обрахунку коефіцієнтів ізогенної кривої зображено на рис. 2.4.1. Вхідна параметри можна змінити в файлі “*parameters.ecs*”.

```
Incoming data:
A->1
B->1
m->19
x->2
y->7

Calculation results:
Gq^x -> 13
Gq^y -> 5
Vq -> 7
Uq -> 6
v -> 7
w -> 1

Isogenic curve coefficients:
A' -> 4
B' -> 13
```

Рис. 2.4.1. Результати обрахунків коефіцієнтів ізогенної кривої

Обрахунок відображення $(x, y) \to (\alpha, \beta)$:

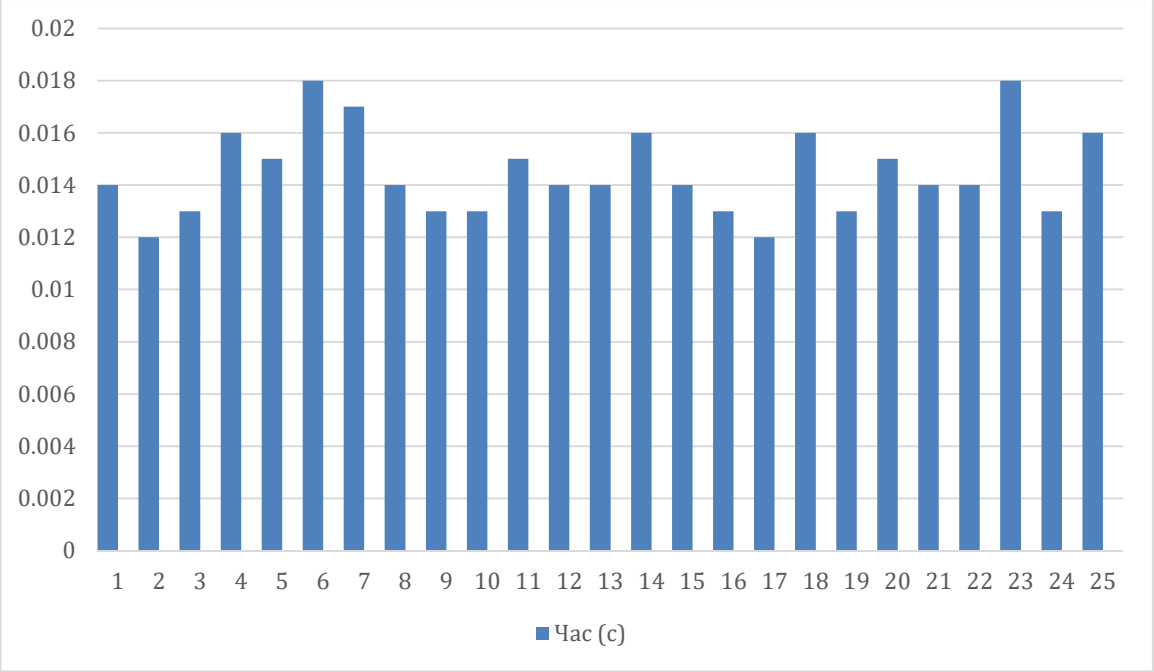
$$\alpha = x + \frac{7}{x-2} + \frac{6}{(x-2)^2} = \frac{x^3 - 4x^2 - 8x - 8}{x^2 - 4x + 4}$$

$$\beta = \frac{x^3 y - 6x^2 y + 5xy - 6y}{x^3 - 6x^2 - 7x - 8}$$

Дані коефіцієнти було знайдено для всіх кривих описаних в додатку В. Пошук коефіцієнтів ізогенної кривої реалізовано в інвертованих координатах ЕК Едвардса з бітовими величинами характеристики поля 256, 384 та 512 біт. За результатами оцінки швидкодії побудовано діаграму часу виконання програмного пошуку коефіцієнтів ізогенної кривої за алгоритмом Велю (рис.2.4.2). Результати цих обрахунків відображено в додатку Д.

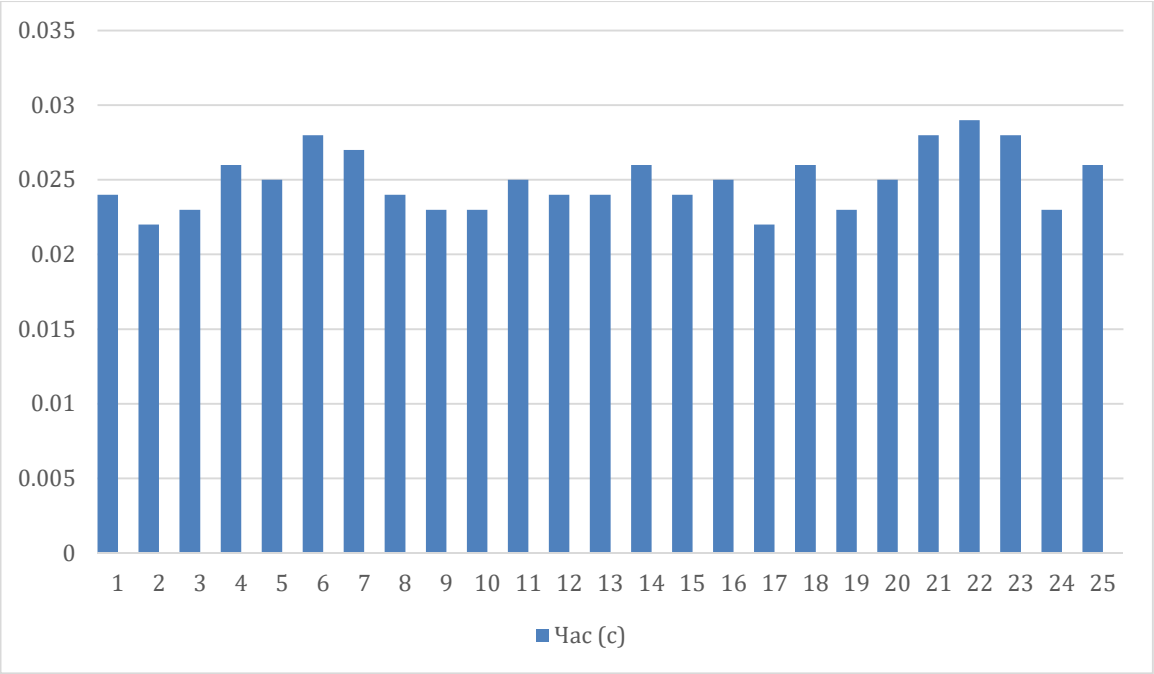
```
Incoming data:
A-> 2
B-> 18
m-> 4000000000000000000000000000000029E26087789BC2815BDFF97093543CCF
x-> 37FB10FEF3EAC946BDDDAF6AA23C0A087495D05F9EF4E68E34E6451864D56B2F
y-> 61DC4918C4BC3234240B0C8A9934F41B6C134D54864F827E12CE2B2557A803AC

Calculation results:
Gq^x -> 326525C888CE8CCC99C96EB30B43F24192A7D93160D566F6FB0653A836F77F0A
Gq^y -> 3C476DCE76879B97B7E9E6EACD9617C9CF62E774D5D0050949E38F779E00EBE4
Vq -> 24CA4B91119D19993392DD661687E482FB6D51DB490F0B6C9A2CADDFDA9AC145
Uq -> 90570170EAD2A1685B27B51BBACCC95979C3400A4847E137875AAF881FB8C31
v -> 24CA4B91119D19993392DD661687E482FB6D51DB490F0B6C9A2CADDFDA9AC145
w -> 3532BB6A2D246FDC8C1FC528EB6342D255B7BB8E9A5143F7C981254B6A45B010

Isogenic curve coefficients:
A' -> 80C862AA7EE8001FE21AD018F5889719484884DFC880E6510C086F274F6F016
B' -> B9CE018C400F0F82B219BE190492C40A34822469B6DB341A4B7D3938C119C82
____________________Timer ____________________: 0.016
```

Рис. 2.4.2. Результати обрахунків коефіцієнтів ізогенної кривої з характеристикою поля $p = 256$ біт.



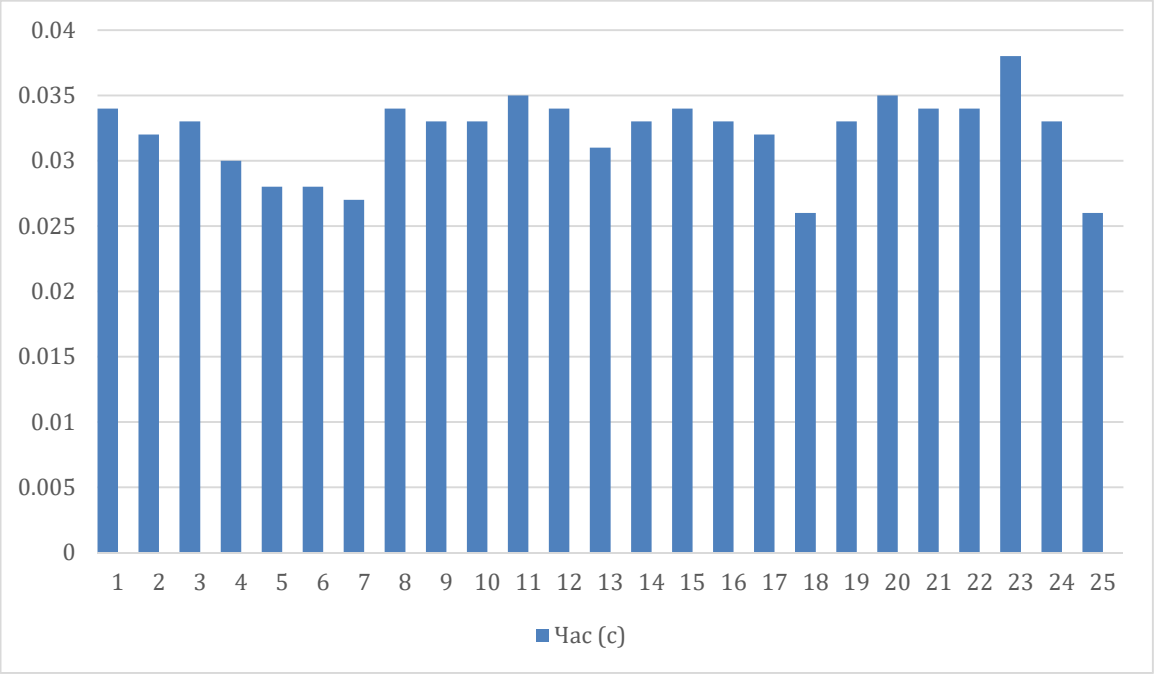
Діаграма 2.4.1. Час виконання програмної функції пошуку коефіцієнтів ізогенної кривої з бітовою величино характеристики поля 256 біт

З діаграми 2.4.1 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}014\ (c)$.



Діаграма 2.4.2. Час виконання програмної функції пошуку коефіцієнтів ізогенної кривої з бітовою величино характеристики поля 384 біт

З діаграми 2.4.2 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}024\ (c)$.



Діаграма 2.4.3. Час виконання програмної функції пошуку коефіцієнтів ізогенної кривої з бітовою величино характеристики поля 512 біт

З діаграми 2.4.3 можна зробити висновок, що $t_{\text{сер}} \approx 0{,}031\ (c)$.

Висновки. В даному розділі було розглянуто операцію скалярного множення точок ЕК Вейєрштрасса та Едвардса та проведено їхній порівняльний аналіз. Було описано MIRACL Cryptographic SDK. Визначено необхідні для обрахунку скалярного множення функції криптографічної бібліотеки MIRACL. Проведено оцінку швидкодії програмної функції скалярного множення для точок ЕК та функції пошуку коефіцієнтів ізогенної кривої з характеристиками поля 256, 384 та 512 біт. Перспективою подальших досліджень є операції на ізогенних кривих, які забезпечують стійкість операцій на еліптичних кривих до квантового криптоаналіза Шора.

ВИСНОВКИ

Під час виконання роботи було досліджено форми та властивості деяких форм представлення еліптичних кривих. Проведено аналіз відомих базисів подання точок ЕК Едвардса. Розглянуто основні арифметичні дії на еліптичних кривих над скінченними полями. Порівняльний аналіз групових операцій показав, що найменших обчислювальних витрат при додаванні точок ЕК вимагають скручені криві Едвардса над розширеними проективними координатами, а при подвоєнні точок ЕК – повні криві Едвардса над проективними координатами.

У другому розділі було розкрито важливість швидкості виконання скалярного множення точок ЕК та проведено порівняння цієї операції на ЕК Едвардса та Вейєрштрасса, який показав, що криві Едвардса є лідером в швидкості обчислення. Описано золотий стандарт SDK з відкритим кодом для криптографії еліптичної кривої. Визначено необхідні для обрахунку скалярного множення функції криптографічної бібліотеки MIRACL. Проведено оцінку швидкодії програмної функції скалярного множення для точок ЕК з характеристиками поля 256, 384 та 512 біт. Розкрито питання ізогенії та необхідність дослідження в даному напрямку.

Результатом роботи є нові оцінки швидкодії операцій скалярного множення точок еліптичних кривих в формі Вейєрштрасса, нові параметри часткового випадку еліптичних кривих, а саме скручених кривих Едвардса в інвертованих координатах, що надають можливість отримати максимальну швидкодію операцій над точками еліптичної кривої, які дозволені міжнародними стандартами для криптографічного застосування, а також програмна реалізація пошуку коефіцієнтів ізогенних кривих за алгоритмом Велю. Також вперше вдосконалено бібліотеку програмних функцій MIRACL, яка дозволяє реалізовувати операції над точками кривих над полем з довжиною характеристики 384 біт. Результати досліджень були враховані розробниками ДСТУ 9041:2020 [17].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422.
2. Bernstein D.J. Faster addition and doubling on elliptic curves. — 3 edition. — 2007. — P. 29–50.
3. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.
4. Bernstein D.J., Lange T. Inverted Edwards coordinates. National Science Foundation under grant ITR–0716498, 2007, 331 – 8 and in part by the European Commission through the IST Programme under Contract IST–2002–507932 ECRYPT.
5. C. Washington. Elliptic Curves. Number Theory and Cryptography. Second Edition. CRC Press, 2008.
6. Koblitz N., Menezes A.J., A Riddle Wrapped in an Enigma. Technical Reports CACR-2015-14. Available: www.cacr.math.uwaterloo.ca.
7. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.
8. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.
9. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. //IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.
10. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія, практика, застосування: монографія. – Харків: Видавництво «Форт», 2012. – 870с.

11. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, Dawson Ed. Twisted Edwards Curves Revisited // ASIACRYPT. – 5350. – New York: Springer, 2008. – PP. 326-343.

12. Miller V.S. Use of Elliptic Curves in Cryptography. Advances in Cryptology – Proceedings of CRYPTO”85, Springer Verlag Lecture in Computer Science 218, 1986. – PP. 417-726.

13. W. P. Reinhardt and P. L. Walker, Weierstrass Ellipticand Modular Functions, in NIST Handbook of Mathemat-ical Functions (Cambridge University Press, Cambridge,2010), Chap. 23.

14. Silverman J.H. The arifmetic of Elliptic Curve / J.H. Silverman. – GTM 106, Springer – Verlag, New York, 1986. – 868 p

15. MIRACL [Електронний ресурс]: https://github.com/miracl/MIRACL.

16. Craig Costello, “Supersingular isogeny key exchange for beginners”.

17. ДСТУ 9041:2020 Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса.

18. Прийма О.О., Чевардін В.Є., Пономарьов О.А. «Оцінка швидкодії програмних функцій скалярного множення з використанням MIRACL CRYPTOGRAPHIC SDK».

ДОДАТКИ

Додаток А

1. Програмний код обчислення перетворення точок за теоремою Тейта на мові програмування Python.

```
def invert_num(num, mod):
    i = 1
    while True:
        if (num * i) % mod == 1:
            return i
        else:
            i = i + 1


def calc_izo_coordinate(x, y, mod):
    # x
    numerator1 = (pow(x, 3, mod) - 4 * pow(x, 2) - 8 * x - 8) % mod
    denominator1 = (pow(x, 2) - 4 * x + 4) % mod
    x_iz = (numerator1 * invert_num(denominator1, mod)) % mod
    # y
    numerator2 = (pow(x, 3) * y - 6 * pow(x, 2) * y + 5 * x * y - 6 * y)
% mod
    denominator2 = (pow(x, 3) - 6 * pow(x, 2) - 7 * x - 8) % mod
    y_iz = (numerator2 * invert_num(denominator2, mod)) % mod
    return x_iz, y_iz


# test
print("A1(9,6)->A2"+str(calc_izo_coordinate(9, 6, 19)).replace(" ", ""))
print("B1(14,2)->B2"+str(calc_izo_coordinate(14, 2, 19)).replace(" ",
""))
print("C1(5,6)->C2"+str(calc_izo_coordinate(5, 6, 19)).replace(" ", ""))
```

2. Програмний код оцінки швидкодії програмної функції скалярного множення на мові програмування C++.

```
#include "stdio.h"
#include "iostream"
#include <ctime>
#include <windows.h>

using namespace std;

extern "C" {
#include "miracl.h"
#include "mirdef.h"
}

void funckInvers(big& x_inv, big& y_inv, big& n, big x, big y)
{
    big xtemp, ytemp;
    xtemp = mirvar(0);
    ytemp = mirvar(0);
    if (multi_inverse(1, &y, n, &xtemp))
    {
```

```
        divide(xtemp, n, n);

        if (epoint_x(xtemp) == FALSE) { printf("It`s not curve point \n");}
    }
    if (multi_inverse(1, &x, n, &ytemp)) { divide(ytemp, n, n); }
    x_inv = xtemp;
    y_inv = ytemp;
}

int main(void)
{
    FILE *f;
    int bit, choose, q;
    double t = 0, duration;
    clock_t startEnc;
    big p, n, a, b, x, y, Qx, Qy, k;
    epoint *Q, *P;
    miracl *mip = mirsys(500, 10);
    p = mirvar(0);
    n = mirvar(0);
    a = mirvar(0);
    b = mirvar(0);
    x = mirvar(0);
    y = mirvar(0);
    Qx = mirvar(0);
    Qy = mirvar(0);
    k = mirvar(0);
    P = epoint_init();
    Q = epoint_init();

    f = fopen("ProgDate384_1.ecs", "rt");
    fscanf(f, "%i\n", &bit);

    printf("Read from file parameters in normal form - 1\nRead from file
parameters in inverted form - 2\nEnter your choose: ");
    cin >> choose;
    system("CLS");
    printf("Enter how many times do calculations: ");
    cin >> q;
    system("CLS");

    mip->IOBASE = 16;

    cinnum(p, f);
    cinnum(a, f);
    cinnum(b, f);
    cinnum(n, f);
    cinnum(x, f);
    cinnum(y, f);
    fclose(f);
    printf("Input data:\n");
    printf("p -> ");
    cotnum(p, stdout);
    printf("A -> ");
    cotnum(a, stdout);
    printf("B -> ");
```

```
    cotnum(b, stdout);
    printf("n -> ");
    cotnum(n, stdout);
    printf("X -> ");
    cotnum(x, stdout);
    printf("Y -> ");
    cotnum(y, stdout);
    ecurve_init(a, b, p, MR_AFFINE);
    if(choose==1){funckInvers(x, y, p, x, y);}
    epoint_set(x, y, 0, P);
    if (choose == 1) {
        epoint_get(P, x, y);
        printf("P_inv(x, y)\n");
        printf("X -> "); cotnum(x, stdout);

        printf("Y -> "); cotnum(y, stdout);
    }
    mirkill(p);
    mirkill(a);
    mirkill(b);
    mirkill(n);
    mirkill(x);
    mirkill(y);
    printf("\nOutput data:\n");
    for (int i = 0; i < q; i++) {
        if(i>=1){
            epoint_free(Q);
            Q = epoint_init();
        }
        bigbits(bit, k);
        ////////////////////////Timer//////////////////
        startEnc = clock();
        ecurve_mult(k, P, Q);
        duration = (clock() - startEnc) / (double)CLOCKS_PER_SEC;
        ////////////////////////////////////////////////
        t += duration;
        printf("\n-----Scalar multiplication Q=k%i*P------\n", i + 1);
        printf("k%i -> ", i + 1);
        cotnum(k, stdout);
        epoint_get(Q, Qx, Qy);
        printf("Q(x, y) \nX: ");
        cotnum(Qx, stdout);
        printf("Y: ");
        cotnum(Qy, stdout);
        cout << "___________________Timer ___________________: " << duration <<
'\n';

    }
    cout << "-------------------------------------------------\nAverage time:
" << t/q << "\n-------------------------------------------------";
    epoint_free(P);
    epoint_free(Q);
    mirkill(Qx);
    mirkill(Qy);
    mirkill(k);
    return 0;
```

```
}
```

3. Програмний код обчислення коефіцієнтів ізогенної кривої за теоремою Велю на мові програмування C++.

```
#include "stdio.h"
#include "iostream"
#include <ctime>
#include <windows.h>

using namespace std;

extern "C" {
#include "miracl.h"
#include "mirdef.h"
}


big inverse_nres(big x)
{
    big buff,  buff_nres;
    buff = mirvar(0);
    buff_nres = mirvar(0);
    nres(x, buff_nres);
    redc(buff_nres, buff);
    return buff;
}


int main()
{
    FILE *f;
    double duration;
    clock_t startEnc;
    miracl *mip = mirsys(500, 10);
    big A, B, A_i, B_i, x, y, m, Vq, Uq, Gx, Gy, buff, pow2, buff_nres, v, w;

    A = mirvar(0);
    B = mirvar(0);
    A_i = mirvar(0);
    B_i = mirvar(0);
    x = mirvar(0);
    y = mirvar(0);
    pow2 = mirvar(2);
    m = mirvar(0);
    Vq = mirvar(0);
    Uq = mirvar(0);
    Gx = mirvar(0);
    Gy = mirvar(0);
    v = mirvar(0);
    w = mirvar(0);
    buff = mirvar(0);
    buff_nres = mirvar(0);

    mip->IOBASE = 16;

    fopen_s(&f, "param\\parameters_512_5.ecs", "rt");
    printf("Incoming data:\n");
    cinnum(A, f); printf("A-> ");  cotnum(A, stdout);
    cinnum(B, f); printf("B-> ");  cotnum(B, stdout);
    cinnum(m, f); printf("m-> ");  cotnum(m, stdout);
    cinnum(x, f); printf("x-> ");  cotnum(x, stdout);
    cinnum(y, f); printf("y-> ");  cotnum(y, stdout);
```

```
fclose(f);

prepare_monty(m);//all operation in nres form doing by mod(m)

printf("\nCalculation results:\n");

//////////////////////////Timer start//////////////////////////
startEnc = clock();
//////////////////////////////////////////////////////////////

//Gq^x=3x^2+A
powmod(x, pow2, m, buff);
premult(buff, 3, buff);
add(buff, A, buff);
Gx=inverse_nres(buff);
printf("Gq^x -> "); cotnum(Gx, stdout);

//Gq^y=-2Yq
buff = mirvar(-2);
multiply(buff, y, buff);
Gy=inverse_nres(buff);
printf("Gq^y -> "); cotnum(Gy, stdout);

//if(Q=-Q)
//(x1,y1)=(x2,-y1)
nres(y, buff_nres);//buff_nres = -y mod m
if(!mr_compare(y, buff_nres)){ //return 0 if y == buff_nres
    //Vq=Gx
    Vq = Gx;
    printf("Vq -> "); cotnum(Vq, stdout);
}
else{
    //Vq=2Gx
    premult(Gx, 2, buff);
    Vq = inverse_nres(buff);
    printf("Vq -> "); cotnum(Vq, stdout);
}

//Uq=Gy^2
powmod(Gy, pow2, m, Uq);
printf("Uq -> "); cotnum(Uq, stdout);

//v=Vq
v = Vq;
printf("v -> "); cotnum(v, stdout);
//w=Uq+x*Vq
multiply(x, Vq, buff);
add(Uq, buff, buff);
w = inverse_nres(buff);
printf("w -> "); cotnum(w, stdout);

printf("\nIsogenic curve coefficients:\n");

//A'=A-5v
premult(v, 5, buff);
subtract(A, buff, buff);
A_i = inverse_nres(buff);
printf("A' -> "); cotnum(A_i, stdout);

//B'=B-7w
premult(w, 7, buff);
subtract(B, buff, buff);
B_i = inverse_nres(buff);
printf("B' -> "); cotnum(B_i, stdout);
```

```
    ////////////////////////////////////////////////////////////
    duration = (clock() - startEnc) / (double)CLOCKS_PER_SEC;
    cout << "____________________Timer ____________________: " << duration << '\n';
    ////////////////////////////////////////////////////////////
}
```

multi_inverse

Функція: BOOL **multi_inverse**(m,x,n,w)
int m;
big n;
big *x,*w.

Файл: mrxgcd.c

Опис: Знаходить модульну інверсію багатьох чисел одночасно, використовуючи спостереження Монтгомері, що $x^{-1} = y.(xy)^{-1}, y^{-1} = x.(xy)^{-1}$. Оскільки модульна інверсія повільно обчислюється, то для підвищення швидкодії використовується дана операція.
Параметри: кількість потрібних обертів m, масив $x\,[.]\,M$ чисел, інверсне значення яких шукається, модуль n та отриманий масив обертів $w\,[.]$.

Повернене значення: *TRUE*, якщо операція успішна, в іншому випадку *FALSE*.

Обмеження: Параметри x і w повинні бути чіткими.

divide

Функція: void **divide**(x,y,z)
big x,y,z;

Файл : mrarth2.c

Опис: Ділить одне велике число на інше.

Параметри: Три великі числа x, y і z. На виході $z = x / y$; $x = x \bmod y$. Показник повертається лише тоді, коли x і z однакові, а решта лише якщо y і z однакові.

Повернене значення: Жодне

Обмеження: Параметри x і y повинні бути різними, а y повинен бути ненульовим.

Приклад: divide(x, y, y);
Ця функція присвоює значенню x залишок, від ділення x на y. Частка не повертається.

epoint_init

Функція: epoint* **epoint_init**()

Файл : mrcore.c

Опис: Виділяє пам'ять точці на еліптичній кривій $GF(p)$ і ініціалізує її до "точки на нескінченності".

Параметри: Немає.

Повернене значення: Точка p.

Обмеження: Всі точки еліптичної кривої, ініціалізовані викликом цієї функції, в кінцевому рахунку звільняються від виклику на *epoint_free*.

cinnum

Функція: int **cinnum**(x,f)
flash x;
FILE *f;

Файл : mrio2.c

Опис: Інформація на вході flash-число з клавіатури або файлу, використовуючи як число поточне значення змінної екземпляра IOBASE. Флеш-число можна вводити за допомогою косої риски "/" для позначення чисельника та знаменника, або точкою.

Параметри: $Big/flash\ x$ та дескриптор файлу f. Для введення з клавіатури f вказується як stdin, або значення з відкритого файлу. Щоб примусити ввести фіксовану кількість байтів, встановіть змінну екземпляра INPLEN на потрібне число, безпосередньо перед викликом cinnum.

Повернене значення: Кількість введених символів.

Обмеження: Немає.

Приклад:
```
mip->IOBASE=256;
mip->INPLEN=14;    */ Вводить 14 байт з fp і
cinnum(x,fp);     перетворює їх у велике число x  */
```

epoint_get

Функція: int **epoint_get**(p,x,y)
epoint *p;
big x,y;

Файл : mrcurve.c

Опис: Нормалізує точку і повертає значення її (x, y) координат на активній еліптичній кривій $GF(p)$.

Параметри: Точка p і два великі цілі числа x і y. Якщо x і y однакові при введенні, повертається лише значення x.

Повернене значення: Найменше значущий біт y. Можна реконструювати точку з її координати x і лише найменшого значущого біта y. Часто такий «стислий» опис точки є корисним.

Обмеження: Точка p повинна бути на використовуваній кривій.

Приклад: $i = epoint\_get(p, x, x)$; /* витяг x координата і найменшого значущого біта y */

ecurve_mult

Функція: void **ecurve_mult**(k,p,pa)
big k;
epoint *p,*pa;

Файл : mrcurve.c

Опис: Множить точку на еліптичній кривій $GP(p)$ на ціле число.
Використовується метод додавання/віднімання.

Параметри: Велике число k, дві точки p і pa.
На виході $pa = k * p$.

Повернене значення: Жодне.

Обмеження: Точка p повинна бути на використовуваній кривій.

cotnum

Функція: int **cotnum**(x,f)
flash x;
FILE *f;

Файл : mrio2.c

Опис: Виведе big/flash-число на екран або в файл, використовуючи в якості бази числа значення, яке в даний час присвоюється змінній екземпляра IOBASE.

Флеш-число буде перетворено для подання в точці, якщо змінна RPOINT = ON. В іншому випаде його як частку.

Параметри: big/flash – число x та дескриптор файлу *f*. Якщо $f - stdout$, вихід буде на екран, якщо ні, то в файл, відкритий дескриптором *f*.

Повернене значення: Кількість вихідних символів.

Обмеження: Немає.

Приклад: mip->IOBASE=16;
cotnum(x,fp);
Виводить *x* у шістнадцятковій формі до файлу *fp*.

mirkill

Функція: void **mirkill**(x)
big x;

Файл : mrcore.c

Опис: Знищує big/flash – число, прирівнюючи його до нуля звільняє від нього пам'ять.

Параметри: big/flash – число *x*.

Повернене значення: Жодне.

powmod

Функція: void **powmod**(x,y,z,w)
big x,y,z,w;

Файл : mrpower.c

Опис: Підносить число до степеня та бере його по великому модулю. Внутрішньо використовує арифметику Монтгомері, якщо модуль *z* непарний.
Цю функцію можна додатково пришвидшити для конкретних модулів шляхом виклику спеціальних процедур (якщо ваш компілятор дозволяє). Модульний множник *KCM* буде автоматично викликаний, якщо *MR_KCM* був визначений у *mirdef.h* та встановлений на відповідний розмір. Альтернативно, модульний множник *Comba* буде використовуватися, якщо *MR_COMBA* визначений таким чином, і модуль має вказаний розмір. Експериментальний копроцесорний код буде викликаний, якщо визначено *MR_PENTIUM*. Слід визначити лише один із цих умов.

Параметри: big x,y,z,w.
На виході $w = x^y mod\ z$.

Повернене значення: Жодне.

Обмеження: Значення *y* повинно бути додатнім. Параметри w і z повинні бути цілими.

bigbits

Функція: int **bigbits**(n, x)
int n;
big x;

Файл : mrbits.c

Опис: Створює випадкове big-число заданої бітової довжини. Використовується вбудований простий генератор випадкових чисел irand.

Параметри: Велике число *x* і цілі числа *n*. На виході *x* містить велике випадкове число *n* біт завдовжки.

Повернене значення: Жодне

Обмеження: Немає.

Приклад: bigbits(100,x);

Генерує 100-бітове випадкове число.

Додаток В

Таблиця 3.1

Параметри кривої Едвардса майже простого порядку над полем з характеристикою поля $p = 2^{256}$

1	**Dec**	**Hex**
p	115792089237316195423570985008687907853269984665640564039457584007913129639501	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE4D
n	28948022309329048855892746252171976963373169931171801824889495879912655174863	4000000000000000000000000000000029E26087789BC2815BDFF97093543CCF
d	24	18
X	25320802586794500263203547481190957015558063656385909487478718360165689944879	37FB10FEF3EAC946BDDDAF6AA23C0A087495D05F9EF4E68E34E6451864D56B2F
Y	44263557162068748502919190978710306369602874782592811177776285379660209456044	61DC4918C4BC3234240B0C8A9934F41B6C134D54864F827E12CE2B2557A803AC

2	**Dec**	**Hex**
p	115792089237316195423570985008687907853269984665640564039457584007913129639349	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDB5
n	28948022309329048855892746252171976963373169931171801824889495879912655174863	4000000000000000000000000000000003A02AE2178C1BA11BD9C4805BC8C6829
d	319	13F
X	18336267022793275410964528580037856763177526592039354128520883460488832032447	2889F59837465E702D9A1FFD5725079CF5A44786D295107DABA01E2D8F0D1EBF
Y	31337192652039744007921008289133309869444260564823666081120281371384797542521	454838F54D5E9B9332D12B2F60274D7689CBF060F78BC81C665C1A1A3A513879

Продовження таблиці 3.1

3	**Dec**	**Hex**
p	115792089237316195423570985008687907853269984665640564039457584007913129639013	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC65
n	28948022309329048855892746252171976963357524003033751936551228399944822236563	4000000000000000000000000000000001E1D14B6ED53005C107434A962152593
d	107	6B
X	47556993841100739599424433290368298966202815917097662198812481846395255609889	69244DFCA2DA84637C7C0D8D2CD59E391078AE07E3F248722122A9BEF8735A21
Y	34044891700198722664598583844526653582950099841318639922151360849104869553857	4B44B9D0F04ADF1FA3C57D958BD9E83C4787F2114F444D8D7218798C308076C1

4	**Dec**	**Hex**
p	115792089237316195423570985008687907853269984665640564039457584007913129638637	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAED
n	28948022309329048855892746252171976963368905359188240366612659790205947058519	4000000000000000000000000000000026AD0CE5A034E9970A0131EDD7919957
d	68	44
X	104961043095557246864111245059024768339963503805376124293211059788221507559317	E80DD85A537A44FD65DB1799048A60F324827E3ED2D280ABFB37661CD941DF95
Y	21242416729692867371974626096097394263911919881993621979141041541317911378284	2EF6C823E475BE6B03665F228F1DB65F3AEEB076EE53044482674E6D0E8FF96C

Продовження таблиці 3.1

5	**Dec**	**Hex**
p	115792089237316195423570985008687907853269984665640564039457584007913129638397	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFF9FD
n	28948022309329048855892746252171976963194920896565118575978537791938089771029	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFA3C8D C9AC1EDAE7723F05213DC50E015
d	94	5E
X	102210527511116257065164977241992110528580721726822461754176861682179775922980	E1F91BC517A66C51A0CD1B7194C3BA26EE83D 1F2EB431E0A5D3F64E4AFD40324
Y	58052323272934185741891857335940880274867462404750853533431956677041616194734	8058735974E50F868276CAEAA1A5849BE694A04 1E35E2C3AF8100244D7CA0CAE

Таблиця 3.2

Параметри кривої Едвардса майже простого порядку над полем

з характеристикою поля $p\ =\ 2^{384}$

1	**Dec**	**Hex**
p	394020061963944792122790401001436138050797392704654466679482934042457217714972106114142625488491564080662799030466 9	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFF79D
n	985050154909861980306976002503590345126993481761636166698734240194831149331612477994593809865442793064701305978439 9	400000000000000000000000000000000000000000 0000000AF905B73674AC7D4AF38C53331DC208 A517DCB3F340EECF
d	532	214
X	378605099923611775822585344176526745571001455847209534083111347984587035202012457786807657785870884173242153300900 97	F5FC151B6264CB53A4B879AA9A1F4A5156BBF 063B56AAA912617C0E4CEFF15D2DF497D9AEF 12374A22D22C3B402B2C71
Y	260129509132952349786225203482071189933725997538504879752092777989029134090282419473324707561401813312992987967927 53	A9027207E88074F4AFA3D44D4590DD04BAFBF 6AE3D321091F500C783F4707940B7F5EBDD9332 5C5391843F9A78526BB1

Продовження таблиці 3.2

2	**Dec**	**Hex**
p	39402006196394479212279040100143613805079739 270465446667948293404245721771497210611414266 25488491564080662799030253 3	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFEF45
n	98505015490986198030697600250359034512699348 17616361666987627714008946833997268206183865 72629454856970129870536412 9	4000000000000000000000000000000000000000000 000000169BD1B903298994262820E2A3E73B4AA 252FB924D3974A1
d	67	43
X	58261320653658379748556555332812600319995683 55126384120151619444654264107330221621026497 63612464683964782869399162 4	25DA67A2BCA7B317923BD7537E3F781E433EB2 8F0224070701BBDF3DF0D63D26BA5409747D7A B030E2BB6FE78593C0C8
Y	49745883148293005848933408879821983901630890 24561755804282844284952514128201362112745717 47310112557972024005216956 2	20520FB9FCABB124725D8FF3AD5B2004DC296 B245A1D57C689962B2A9D0EABCFD94CC4157E 7CD0809055711EB35DEB5A

3	**Dec**	**Hex**
p	39402006196394479212279040100143613805079739 270465446667948293404245721771497210611414266 25488491564080662799029954 1	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFE395
n	98505015490986198030697600250359034512699348 17616361666989053325453926932465648799219726 44617234304508946622883419 9	4000000000000000000000000000000000000000000 00000050BFE5AEE2F9642045CBA3B5673EC7020 317A99B7A2A7F97
d	772	304
X	37098545717916464853110998994376441061355470 43282155949177820506247648379209503696225854 69804943066827365916237284 26	F108BBC769E3358598060F9C1C5EB79C6492860 F58967AC7D7E50B23B21767B3D8A360C346B2A A22A801E0DD652CAD2A
Y	20049086756029240168979067176197058613587066 20638871338691888900925084081584712575399853 01561159333561733112088305 14	8242F49FA453B08E85B033A3399C0EECFB57522 496A9DFE1FC8423C009951649DD1FF90F9B49A A9C6E28AD374A67B632

Продовження таблиці 3.2

4	Dec	Hex
p	3940200619639447921227904010014361380507973927046544666794829340424572177149721061141426625488491564080662799029934 9	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE2D5
n	9850501549098619803069760025035903451269934817616361666989878774642711096478812296247202615001159915611335154572127	400000000000000000000000000000000000000000000007269FD2518A6AC30A3FA9F3931A347FA8BAC4843ECF19B5F
d	276	114
X	3513707725219091949658796810197634540844119017132350111701373596942375995375706286050590110379595744070963846948 2028	E44A4A622DAA298B94A167989E99ADFF06180D11EAA618386D7B173C82C4C1E9822C47B7C7F5B26663C8BF3074C4762C
Y	1283161111137128310193428852483192371844145313206807988910496554097149273335698041371152664277808279071740886954 0214	535E607ABF5739C3E5A946F9AD44C899C33BF00B04CAE695080D622B28DA64CA0B55AB041BF971382D956739A3AAE176

Таблиця 3.3

Параметри кривої Едвардса майже простого порядку над полем

з характеристикою поля $p = 2^{512}$

1	Dec	Hex
p	13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006083221	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC95
n	3351951982485649274893506249551461531869841455148098344430890360930441007518405126134457362200665151479341001585987474750943073636601341402240469528982943	40000000000000000000000000000000000000000000000000000000000000028A3CE52209E2BD4952882D5574165192C46C0D0311FEA6BF9FECE70EE63B59F
d	269	10D
X	43046380597677236918434480114169121317872065204166094567972647848418035311036617847132303732294365245200452952546226446182213573646727679140845605672 47872	5230A1EE747050A072BD7319741586EA520388B6B53094571C821A2FC9A9E83D56665346B5DB04C43E75261DBDA512728FAAFAC48AE9260A5A184E2933E3A400
Y	27374793099677091760423610510556576343089791514222859156372319061778945606835359017625712614128131082361634424969394591431079444280718851729740138316 0453	53A0D50CC63C9219762F451978AEF214DBCFCC3A5CB5EF27124991A86B42B3A1A832724A0E6B930FDD1DA2E27A540D6B675E4422C444F529C508F0BAE7D0A85

Продовження таблиці 3.3

2	**Dec**	**Hex**
p	13407807929942597099574024998205846127479365 82059239337772356144372176403007354697680187 42981669034276900318581864860508537538828119 46569946433649006082269	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFF8DD
n	33519519824856492748935062495514615318698414 55148098344430890360930441007518370586201943 87154673316589859146005262089761738039690723 85036612444932871161 97	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFDC46E59CE4C BBB6248CFE7BB582E1F490FD5F9F74433AE745 EFE6351254BCDA5
d	377	179
X	88597343811717371087556294075707525932477409 08886513363817185271029862755816849123937823 55447264488990570054063409518125212820747786 99361696050167293332 43	A9297AC52D51EF4745E5E558F6217B302052A39 544DFE6DC04FE427850225E232BC379E11F6C51 FDB0C9D0C2511BC3E945E25B9829B00C4DD92 843328606ADFB
Y	86455503668724465625333164807242986656488138 32725284029798720279497293062458262197550131 70011799670050813851866997665179879350569198 96000476523800855311 19	A51291E6175265F4C5755445CF271E51E9248C72 8D01CC388C3938E477F3A94C69F21873F7CB97C 64AE7D33A1056B41BB0E95436F88A03555C7291 1F313331EF

Продовження таблиці 3.3

3	**Dec**	**Hex**
p	13407807929942597099574024998205846127479365 82059239337772356144372176403007354697680187 42981669034276900318581864860508537538828119 46569946433649006080637	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFF27D
n	33519519824856492748935062495514615318698414 55148098344430890360930441007518407480050918 05097884849023290546744883643236649541028702 82562972013832191670 99	40000000000000000000000000000000000000000000 00000000000000000000002DD8135044F2810D554 443F2E2BD624D526C8798402AB63951BFA991E6 087F7B
d	175	AF
X	88362013022735650739457696274545086569028078 87394026515909596547743730643485300826964440 03100689333011836929730516718068952498496561 74420366544920049970 48	A8B673C87778EE5D31B9A404334AB9B5A572C8 EB536C2C91443F112F8961B1E1BBE4E7AC851E 8AA509F0B9AD2D9C203A816B67E0796AD7FF2 9726D262EA957B8
Y	67610772410924923539045835968188318906223094 45547158112661771293181461536708813664770037 66540142516982685036311802911107883359778203 38331989349516026254 03	81177507F05F730D44D26B9D14B0FFAC6558F68 34314F0414A9D6A9E48608C5F08507D8273AF13 26ABD50A49B901462F3BE8005B63FC8FF851B8 53FF48B31B7B

Продовження таблиці 3.3

4	Dec	Hex
p	13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006079621	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEE85
n	3351951982485649274893506249551461531869841455148098344430890360930441007518396353790343801270711865654675947715856811848087560072076516114450014792038811	400000000000000000000000000000000000000000000000000000000000000153ED5CAB52ECFB1E3832493DD7A1C06617A6790626B88DFAC45D806A147B99B
d	969	3C9
X	4403167501809402372946958312821261725702600416103728084786199165375897394442739369540011463346443928036136454990468558451417724853226831333756059727381050	54123C034D18682F739A011463EE02332B35825602C853A8EDE6DD1657894A47C2D6E1D2EF39DC434504051DB60A690FAFFA10B9053E37268D3AF352F18B423A
Y	8956091467824468059616554275589900393507022555100483100644056648682675845369599847044504726771800163369277184311974057611335242353710810420013399548874515	AB0076944360C99551AE3AB73E24473AD55987DFD6378DD3A6D89A4B2C88576F837341D4141E791B512483B6AEED65E09F68A64CE5B3B78AF16924634C2BCF13

5	Dec	Hex
p	13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006077517	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE64D
n	3351951982485649274893506249551461531869841455148098344430890360930441007518397574859115342105504421968358115142292868933144305181031055780134069835884667	40000000000000000000000000000000000000000000000000000000000000017F1EF80AF949ECB3AC390D869E51ACD0E05576A5B2F6A96416B8365C69B687B
d	85	55
X	5456069801766800420335846677506187906982782937321353853441030055636984730642647514848735897405040367405894214761212463806053364021517067680380714875038403	682CB6B299DBE8983409E0A21839FC9D80066C91E7239D532251AE3FF4AC87F549C0005883852A1BACC4236B8FF08492519B7947D292779AD512D14A83732AC3
Y	3832946029017571358479004656254719722797009150216531011598486336024328071059966751102034859233360777371137719488844629808294099758508429376318289005082204	492F0CC7E947498364D0E4E15A82EF57ACB975FFD09C0FCD3BA967A7DACE72FD2151648FEB11A12F3ED9F1297469285D2C26A1CFB2DDDF23B946E540A8B5765C

Додаток Г

Таблиця 3.4

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{256}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
P (x,y)	37FB10FEF3EAC946BDDDAF6AA23C0A087495D05F9EF4E68E34E6451864D56B2F, 61DC4918C4BC3234240B0C8A9934F41B6C134D54864F827E12CE2B2557A803AC
k_1	B25F0539178DC46B0D7E504550FC71EC835BC884A086C91195F2076AC358FBAB
Q_1 (x,y)	FC88C48510DB7415CEE2CEC0014D9F8F600D36B9DE8AE9F089C6543279B20E94, 9A29536CEFF9119986DDDE64F670B1AF105FABE59DD343449560C665C73F9D53
t_1	0.003
k_2	CF5035BB5229D6891A389FCDC8153ED1A34C11FF97E8A96E29AA3AF64C90EAA3
Q_2 (x,y)	BD185C24120D194793AAE1B46E6EE9BC954A86A4C678CA1210705C43527D3AA7, C9BAD8362ABB91392A207A814D1FCA03912E77BDF0F569D01D15A391A7334C83
t_2	0.004
k_3	F80F55D5D203071626143B45E27219FDA2F579C2107E81516077697B4941B40F
Q_3 (x,y)	CA3123F00D710ADC2FA98A7815A07B8EE79049EFBF4526FCCD6358DA337C02E5, F381D56459251196E0B808C6861D4539061B46CB044D7F57C9C111283E43FB61
t_3	0.004
k_4	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF
Q_4 (x,y)	E2FA5C61D4A882AD464ED222CFB0FFEE14C362A6210C8162A7B93ECC06709092, CC32C3BD53B35309409956DF48A37BAF39630B36598AC67DE753DF7BAB5C77B
t_4	0.003
k_5	B5C85EA4C5B62C885CA2AFC54D972952D8B219DCA286A5CC3FF8EFF8D14FFF1C
Q_5 (x,y)	7501C41677457DE0DE8DED18711546BCB1EC7C192F0227DBBCA1225C121C159E, 60BF3F7E8984AD36CD3DD9F0735B02E418F2B3F78A8A5E04CFA7BF99490CDFCA
t_5	0.004
$t_{сер}$	0.0036

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
P (x,y)	2889F59837465E702D9A1FFD5725079CF5A44786D295107DABA01E2D8F0D1EBF, 454838F54D5E9B9332D12B2F60274D7689CBF060F78BC81C665C1A1A3A513879
k_1	B25F0539178DC46B0D7E504550FC71EC835BC884A086C91195F2076AC358FBAB
Q_1 (x,y)	D497C3C4C29E33F4E70C54C83B0AFBA3A015C330980DE76D61BC7F8F907854FB, DFD72A7D2B65D3EB6471B053A4AC4B6BE3D481C2A3198F352D3BA74FCCB047E3
t_1	0.004
k_2	CF5035BB5229D6891A389FCDC8153ED1A34C11FF97E8A96E29AA3AF64C90EAA3
Q_2 (x,y)	AECEBEF810CBC477D289BB8A60ADFC7AFE41C6A25051493249E53B1296AE0C51, C20833D17BFC231E3BE2CAE574484C54868F9912BF9204DE8B0608DD31F87F8D
t_2	0.003
k_3	F80F55D5D203071626143B45E27219FDA2F579C2107E81516077697B4941B40F
Q_3 (x,y)	4F9F18766E119F882722CD4533057BBBCC363D27BF86C345306FE67855990B63, F045789BE3BC923CCA1926C91C32E25FD0C1D1438FB9A782ACE57BACDD79907B
t_3	0.004
k_4	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF
Q_4 (x,y)	F53AA4763C99A22BC12339F3BACC711FAA5E57BA695FDBE7330F3206641DAF29, D08F367C06610D740BD57EFBB83F06D370E1A7AFF1F9CFC43F4DC47D911F30DA
t_4	0.003
k_5	B5C85EA4C5B62C885CA2AFC54D972952D8B219DCA286A5CC3FF8EFF8D14FFF1C
Q_5 (x,y)	8F46E503513BA897FAE2DFB3A5B3C5BA9EBE78C36E42018800FB89991AC712C8, 80C23B757EAEC5F9C80526629D067CC67EDD82BC302D84B21A1944112437733C

t_5	0.003
$t_{сер}$	0.0034

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
P (x,y)	69244DFCA2DA84637C7C0D8D2CD59E391078AE07E3F248722122A9BEF8735A21, 4B44B9D0F04ADF1FA3C57D958BD9E83C4787F2114F444D8D7218798C308076C1
k_1	B25F0539178DC46B0D7E504550FC71EC835BC884A086C91195F2076AC358FBAB
Q_1 (x,y)	11A18CAAAF789B95D3B5DE7B0B355F8025924DCEFBF9C79815CFBBBEF14DDA2F, 11BCC3C6748157522D703C300B8DA49A56AFE856D8980EF34B2FCA29FC2562DF
t_1	0.003
k_2	CF5035BB5229D6891A389FCDC8153ED1A34C11FF97E8A96E29AA3AF64C90EAA3
Q_2 (x,y)	7F86330AFAE452DD3ECD5B0E712D1CE177713A9EF847D1DA51D08D2316E7A62B, 544C3A826A4F71CE9971F9ABD56113D909D328EB0E29CCBF68881C5CC9081FC2
t_2	0.004
k_3	F80F55D5D203071626143B45E27219FDA2F579C2107E81516077697B4941B40F
Q_3 (x,y)	C6600133EEE4098C6C4B09527AC48CA07AF3E355577D3A1E5250C2D10AFAB0D2, 66FB746D5A99A491291979333A91A8806C6E307050BFE78EDBB19E66A848C732
t_3	0.004
k_4	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF
Q_4 (x,y)	55B2BE545AA7E1709342F2BDC9E1C3F259CCCAB3CBE5A66DA3D68111FDE916E9, C41EA8DA3BEE7FAD4D5B74F94DA43382FE9B5FDC08D6F8B536E0C57A7510413E
t_4	0.004
k_5	B5C85EA4C5B62C885CA2AFC54D972952D8B219DCA286A5CC3FF8EFF8D14FFF1C
Q_5 (x,y)	1F5303C06CAC426CBC33CA94487E3AABEDDABBA79318FF98BC41A70DE63CADBA, 505C31E09A4FD9807C617C3D58CACB97EBD2FADB1C765B9EA4C1AE65FA71983A
t_5	0.004
$t_{сер}$	0.0038

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
P (x,y)	E80DD85A537A44FD65DB1799048A60F324827E3ED2D280ABFB37661CD941DF95, 2EF6C823E475BE6B03665F228F1DB65F3AEEB076EE53044482674E6D0E8FF96C
k_1	B25F0539178DC46B0D7E504550FC71EC835BC884A086C91195F2076AC358FBAB
Q_1 (x,y)	A1918F9BEB2030910139E578F4C5E9217C20248DF3FABC2CCBEE3F0798D9B360, 28240EE304E088AE7F04503857D39F2E31EACC824068B876B2F65FAF7215E317
t_1	0.003
k_2	CF5035BB5229D6891A389FCDC8153ED1A34C11FF97E8A96E29AA3AF64C90EAA3
Q_2 (x,y)	12A8735D3F4784433825E5EC9F62BFE14A948156CB5B0F398FECCDA8781C08FA, 524D88C98332D0CD81429FBD2E7BF22122AF51DC77904E968611BD1E7442E982
t_2	0.004
k_3	F80F55D5D203071626143B45E27219FDA2F579C2107E81516077697B4941B40F
Q_3 (x,y)	67BAA6ADAD7B88B68E8984EEB285F6CD00154630314F1E717F8A1D8F6B1409B8, 6C03DA1601C010E20D4F76B73A20E8DC17D0D9B6114DCFA6124BB7C6A38FEB9C
t_3	0.006
k_4	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF
Q_4 (x,y)	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF, 33D02B50E25F0DF7520CD0C9920D8D45848F81458449DB05B243D7184398E5C4
t_4	0.003
k_5	B5C85EA4C5B62C885CA2AFC54D972952D8B219DCA286A5CC3FF8EFF8D14FFF1C
Q_5 (x,y)	B6EBDDDA9605FF56A83F88887343261ECAD996CA757EF68E5BBD0D74B66B52EA, 316BF982CCC8C967601A9F082C7D7A959654849938671364A63F1507DF47F0B4

Продовження таблиці 3.4

t_5	0.004
$t_{сер}$	0.004

Результати скалярного множення точки № 5 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
P (x,y)	E1F91BC517A66C51A0CD1B7194C3BA26EE83D1F2EB431E0A5D3F64E4AFD40324, 8058735974E50F868276CAEAA1A5849BE694A041E35E2C3AF8100244D7CA0CAE
k_1	B25F0539178DC46B0D7E504550FC71EC835BC884A086C91195F2076AC358FBAB
Q_1 (x,y)	B4D82B30839481E459A5E98A3C6D2AA4EDBD5E5E8FB309FD236F6CE413DA0491, 1131724884D1DD83B453A64B59241531666E6FABC0D7D9957E7EDDD02CC58F6D
t_1	0.004
k_2	CF5035BB5229D6891A389FCDC8153ED1A34C11FF97E8A96E29AA3AF64C90EAA3
Q_2 (x,y)	EC79644551A427DED90329EF514D959D2C49A003AD504E5603768C7BE949A604, 6721F4B248734DBF384C593C0134034A9A35C88BAE507A22F80174035BCCC0C1
t_2	0.004
k_3	F80F55D5D203071626143B45E27219FDA2F579C2107E81516077697B4941B40F
Q_3 (x,y)	A1B65EFA7C9EE5DBDF875CF4D4E0CF9795DE123DB08996730A8C807807693A5F, A08D7D879AE38C8220AAE0568E657BA954E1F4638C722D2EC4B2D1C311BC73FB
t_3	0.003
k_4	C78247DBF9F9685B349747675818E996D1802BABE252A0DCC6039DC4AFDE9EFF
Q_4 (x,y)	427B1AB0ED8D83C9375820B5456BB9B056EA396D5645B154FAFA567C019115F2, 84A228B6C3D7CA4F75A2586C6D282BEA3077CA6F3751A438F64758D138656044
t_4	0.003
k_5	B5C85EA4C5B62C885CA2AFC54D972952D8B219DCA286A5CC3FF8EFF8D14FFF1C
Q_5 (x,y)	315B58E53A708F54401E633C694251D2A8834C3C64DB7E74A685123BBDD3BDB2, CF1EED745F1BC85176D07659D502A1A35826E82A4EFE0AF8336C5E66C6F231D1
t_5	0.003
$t_{сер}$	0.0034

Таблиця 3.5

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{384}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
P (x,y)	2B8D5997842C553D8A8F7CD8C62D7AAAE37EF7E52E5CBD98D2427258DEAA77F43B224E6C1E46BC50F3BB7838D9C77379, 45653A0F9C3558B3C89A5266F6442DBF7979C763B20535EAB352DB9F5E656D2CC14BD8C1B16FC6A7FE41784530B1EEB3
k_1	BD1254C454617C8FD1C09807890001137F4615B16484201C3066A87BD261CB62673C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	2F3C6F1948EBA2D598F61EBBC2A27B5B406B7A36A8F79A59B6153CAD15EB5D9D15F121653E8022394FD3405106D0C4B9, 170237DC41F44AADCC6FF85B6F1536005D5FAC801E46B6FC62E8FA18F5A2032A4D5F96722BC34C6AE6A3E121A965C52B
t_1	0.011
k_2	367E79341D9067CA3B8E014279691F4BB5CC05CF353358156A9A9F455BD727465428BC6C9D713AF6F261D231D2678CCD
Q_2 (x,y)	75B3C96E69F9D2C6320375BAFC1CF6D5A1F709860EAE3436188CEF0FF04DACC33CBDE3DF5AFB1078E404EB2AF08F0E63, DFBEA06BC9AD2990A8EDCA807800BACC46436E3D755C5E446639AC4C2E41B5EAFF16DF934CD4E6CC980BAB81827A5957

t_2	0.011
k_3	3596B73F2F27C5D11EE4AEE6AEAB3A6C9E94EB86AB285EC464FD2AC87C95FCEB92217699C96027C817574D563BAC18CB
Q_3 (x,y)	3BAB4DF5C91328FAAE12502BCC2B67158ABA3438F6CC0683E56CAE394221DFEE80EBCDD81FCAA00F0BCA86E47C897DA2, 9A821EADA040F289EBDC5DD44824C032021B14C8CEC7BC69AA3E86D0A1287DC77BEBE2568398467F4765D765649A2223
t_3	0.011
k_4	2CCF717F183424184192EC0177357FBA8189BE35D52F0B9A87C4160D95BD98B4700636954C08DAC448CE3DC6B3C58355
Q_4 (x,y)	C140A42C7A703FA06933C98E5D0AE05098DA72943695A8D30C27661C630E8CB795D1BCC2D52ED269DBD522D7697CDCE1, DBD2234F63C5F33F30BF7B8DB923FAF1AB1E9FB28CE40E0B742FFA4A56CB4E613CF587346B629B3394AC0D6D3A8E47B
t_4	0.014
k_5	5B131958F6534ADD51C359F6989E1B628F5FCFC3A3CF6C135A70978719B2D9848141750DD1AB38E2812B9FB9A291FEA
Q_5 (x,y)	E78A922C90ED6BE8935F7DE2854CC0077CFFBB3D24688CC02F350A129B54C665F121BF547703ACCAF67BAA97EAB3C034, 679849DF050532354BA6088C0F88A9E7819E56EBC4B51778BF9DE645279B6FF5C57F23D3DD600DD5BF9E59EB8ABBAF57
t_5	0.014
$t_{сер}$	0.0122

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
P (x,y)	470E08D8AE8685B8EB2E3A49147E146AACF4155B06F27E27A2F4C87B69D627D405B5107B5327CBDA389E7F3CDD3A4342, 4D9DCA8CA3FC5344C384F81370E56BA789CB3DBE102B98CAC8F4632C2A618B4D0B759D991F71C5B416018800B5366AE
k_1	BD1254C454617C8FD1C09807890001137F4615B16484201C3066A87BD261CB62673C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	7973CFF7D1581325F8F7E301604BC783BA07F5195F884D3824B3B3492D621046449DE04EBD3DA4DB8FED1D4D63CB1FDF, 12CAD32B3DBEC6B1F5B44A44D12375652346A8EC4ED804D488FC6C11725A7C51CB6FF55C828C0CB8BEC62017B82AE198
t_1	0.011
k_2	367E79341D9067CA3B8E014279691F4BB5CC05CF353358156A9A9F455BD727465428BC6C9D713AF6F261D231D2678CCD
Q_2 (x,y)	14278491F02F14A441ADDF561D03EFD1D7E8E25E9E76F7390AAD36499157B3F2B65B2F69E096DA90417BAAAB787C8245, 33D01816D4E580BD66311E9E4A9B8353521423A5BBA81883763720F9F0AF4E1F5A49113E6E8FC50F5C1B385917AAAD0C
t_2	0.011
k_3	3596B73F2F27C5D11EE4AEE6AEAB3A6C9E94EB86AB285EC464FD2AC87C95FCEB92217699C96027C817574D563BAC18CB
Q_3 (x,y)	CF8A7D26C64B0A3E33AC2AB98C57945D43BCC541DB1A69E926129B152551D0F0D3A121AEA7560CDFDE9F31BB5E1E32F0, 6291D596ED6E81BBDF4E16D8E0BE167C4D32DEBEE06E4DF38578BEF2BE51A3DAD20402E2B20640A79D8AB06145CE8A95
t_3	0.012
k_4	2CCF717F183424184192EC0177357FBA8189BE35D52F0B9A87C4160D95BD98B4700636954C08DAC448CE3DC6B3C58355
Q_4 (x,y)	BE4333BECC335528A853CB1ADAEBB84BDB2CE7B4FF91C19C33DD08D2AD803D39C102F48D68B4A4ACA5E7ADC698619F69, 813C8A78D37D5B6253813933A094667A9FA18AF8AA6FE66B18CB56B28BE9960EEFE64BF104C068B72DA07DCACBF7EC1C
t_4	0.011

k_5	5B131958F6534ADD51C359F6989E1B628F5FCFC3A3CF6C135A70978719B2D9848141750DD1AB38E2812B9FB9A291FEA
Q_5 (x,y)	B754A6E3AB8FB505D263A7A225517D4606467130680BB8CBA170BB5C3DD48B377595CD0AA084C8DA7075E4EC8968B40F, DBED1574D31459E4672166B3D39F82CA29437EFF9145214BA16939D4CBA5A42C87F7CFA9C92A3D845E0A90EC7BACF06
t_5	0.011
$t_{сер}$	0.0112

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
P (x,y)	523ABC1A5AF820063D26B084EAD0FBC7C731F654CDD1A69DF390DDCECBDEC6AF7E158B144EDEF81612C5B3E595DD484F, B855C45CD16694B9C35D9D1368E839FA56D4BAB0401736259818DE0900BF7E18D543992257A7FAD84E3137A78797F833
k_1	BD1254C454617C8FD1C09807890001137F4615B16484201C3066A87BD261CB62673C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	C77B0767AD037C8A79353EF0F451A52296407F3840A0DC39D0A5E0A90C7D81ABCEF3D005A6C81ACB3E2B821C8C5BB870, 6C5B02EEBFC2AC78BA5159563A4C5B346B6FDC9A1433E1D8E0890DB0C87584E993B26FA75EA3226C6137F9F9C1D09FA7
t_1	0.011
k_2	367E79341D9067CA3B8E014279691F4BB5CC05CF353358156A9A9F455BD727465428BC6C9D713AF6F261D231D2678CCD
Q_2 (x,y)	1D2190F8AC4A2D0FE1975BDF46F4228B3DCA000D4904EC561F988A48C80678A9589F465EE7765B1C45F6F0C9011B348E, 97DD84041CBEE9BE3C3D4A016C0227C9C39046E32FE0A7D60624420DC0651D2D7A658C18CC219A08596AA2F48136223D
t_2	0.01
k_3	3596B73F2F27C5D11EE4AEE6AEAB3A6C9E94EB86AB285EC464FD2AC87C95FCEB92217699C96027C817574D563BAC18CB
Q_3 (x,y)	E7971CF0BD56B079AF3C544A468CF413B611B22DA251EBA0C6C8B46B71843DBDE5E80F58C205622995F39C0F3D85A152, 3D866AC2F7C54D620E01CAE3D734711D82C40348514891B2FEFF4B7D104D65C7DC6350862CB77E4E734D8FA4B831BF61
t_3	0.011
k_4	2CCF717F183424184192EC0177357FBA8189BE35D52F0B9A87C4160D95BD98B4700636954C08DAC448CE3DC6B3C58355
Q_4 (x,y)	FA7A0E7DF3DBB0791CDFCC4314499FD7503678E1ACCB7DDA4BE73C2716A5AB596E958061C2A126F758C3EBC5F1D6BD97, D9B951E6540D62F2A7A2C53B07DA7607C303AD46ADA30B424A2807004AEFE10A493F4B2B23015D9BA23463160830A527
t_4	0.011
k_5	5B131958F6534ADD51C359F6989E1B628F5FCFC3A3CF6C135A70978719B2D9848141750DD1AB38E2812B9FB9A291FEA
Q_5 (x,y)	DA2FF125ED86A75B0003A816729E123A865DCD9653C9BF474750F055D19268214866B8D17C1B6C95E4DBF7BEDF1E6B0C, 2702ADB1202C9A6505AC12DE322D95935235AD755E3D6758A0B3ECB3B4C73B3EC696F1296993DF800403365F96CF06FC
t_5	0.013
$t_{сер}$	0.0112

Продовження таблиці 3.5

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
P (x,y)	4F501508724598418F99869CADBF875E2F3B4A17A74AEB9A414538D4A532906030F8D64D0CB9EE0E3D0B1C25A77DE77E, AFC9472BE3F1874919B90E69246C0F84B5F5DD062EEFE449B4439816D4E3BE4AAC08007BC463EB813B441202BD0863F6
k_1	BD1254C454617C8FD1C09807890001137F4615B16484201C3066A87BD261CB62673C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	3E43627C489B0714A72EF371F2DD3F9563C0FDCC5A059C1A9B3AA9D427560AFCD4272AC4B5BFBB6DDDCF8C0187C455A3, EE947DC9F75E521E0DD8A81B177DA09388F0524CBDEBB341014C8E21471DA120AF968BC9F6F55F8E0766C1CB3BE9DB8
t_1	0.01
k_2	367E79341D9067CA3B8E014279691F4BB5CC05CF353358156A9A9F455BD727465428BC6C9D713AF6F261D231D2678CCD
Q_2 (x,y)	A2342AFC2C85ADEF118F4836468F3D873D2B9DB339DE46759B0ECC83D37D72C957B4371E080C654CABB002F684A146E, 186D0B16FAB6F88EE92FD4DCC9C9343242980B1ED8F493C951E189222EEDC55F53AE0951F3C246233ED4C7EC491B3959
t_2	0.011
k_3	3596B73F2F27C5D11EE4AEE6AEAB3A6C9E94EB86AB285EC464FD2AC87C95FCEB92217699C96027C817574D563BAC18CB
Q_3 (x,y)	D39293954F31075C15B0ADC1B241327F4AA53F25A2A9A1A7B9C1F5B8CD79769A129CC3F557E1C57437F3F8C741273536, 3A1FC6F767B648FFCD71E6882214259D917AC212EF23AEB611B623DE02741A8F37349D36755D1B8183FCAA7C31DD2B91
t_3	0.013
k_4	2CCF717F183424184192EC0177357FBA8189BE35D52F0B9A87C4160D95BD98B4700636954C08DAC448CE3DC6B3C58355
Q_4 (x,y)	2C8D6767FA176D391C86760C0A6CAFC085A0744B47241F14A8A1748788A53AD53EDE161352F7F2B6AC56E108BDAF0C66, 89497F62B172DA93F6C3824B45574CB7956E5266915FEA466CC677F6BB6F86018D83E2F3B2EB05A4E8A79F3A92313E82
t_4	0.012
k_5	5B131958F6534ADD51C359F6989E1B628F5FCFC3A3CF6C135A70978719B2D9848141750DD1AB38E2812B9FB9A291FEA
Q_5 (x,y)	77833285143AAACFE23F53933A2BD5EB60E66FF15F97A42F86730766CE19C4A77D0AEC9728CE8883D090B98595AF7A6B, DF76FD9223E8099B6A2250655086A1A23F9129B6DEC2D6AB2B9493116C5C37AA597116721E8EA98C6DF5E9F413D772F8
t_5	0.012
$t_{сер}$	0.0116

Таблиця 3.6

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{512}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
P (x,y)	39DBCA29BDE102C9E4AF8B86AAAFC6591A1F8035DA10194D311A2C29A894ADCA0529EF80C4C84282187ED732F40FACF3E0D4236703FDDB14A01A7EB05594072F, 7E9625B235C54B7DEA64C8B5C0B6ACC8F7C4AFF995EC4B71A39B486B84D53927697CEB356EE89F84E9F90E82B1BEAA4B5AAC56496A62F0046EC0152C9C4EA659
k_1	BA76FAE790DCB4A9F15290A2D80D4389187E4E68F90CF520AE9B686E3D67D985611A1931489E8E72D2BD4681BBF31B1DFD5C03DD3564C91195F2076AC358FBAB

Q_1 (x,y)	C2334FDF36CEF73CB3E0D6F41BD6B88FFD3160689E320FDD7D14FE9DCBD7AB15DA392803 521333C43749024FBB2DEAF15E3981C6BA9024C99F09F2C31FE89F96, E31D72479BDC64350EB978F514C2D7C39418F6C9D6653FFCA6A5D61E10188686743C7BF5B3F F5B6290591CDA48C29568AA70CFF3D7450A458F10CDCCBE2ECE5C
t_1	0.046
k_2	A5420B393140DBEDC6BC39AF65FFC573BE0A49821C8768F9F9BCF009CF3CC42D373A838B5 FC26D54DDAE75ACD6CB72C8328053A0B2F481516077697B4941B40F
Q_2 (x,y)	DDDFDB25FF4FDAB6F878B4DAE99FCAFB93DF4504048FD7005A943DC7DF516A1098F101B6 E1B199F038FB277B226B910D223D26FBD3572C764C9E0CCB7FFE960, C2BB9AB91137DBCEC2ED08CAB88BBC194FFAACC4CD9FD1C31CFA943650D9DAD8372583 FCB488C4D1CA05F3BEDC3BD1DAEFE0E2A05C04BBAEA1E5A500E4717EC0
t_2	0.046
k_3	2F1DBB39EBBBDB43B9D502AB0B4CCBFFB94DDF17E951589934501D51DAA2E66986F7C8B AC818D6BAEDB3DB4F48B016E2E5679E899198A5CC3FF8EFF8D14FFF1C
Q_3 (x,y)	93A5D9CA5DA80C304556B964CD522E9563EEAC28A1CE8B93A7A50E3E0E5A54D714EC7E87 CB489A311B7EE54A698AF7AF3357D8C50A69A85EF6C879790850B4F0, B7257667CDD6EC84C45A6C64E1DDA129E97192906C6849B859D5157B39BD8CE2FB3B23C5A 052C6EFC670C7EB0A252CE35A1AF5B271D7DA7D7E7F0C6A41464AC8
t_3	0.045
k_4	EA60D512DE6A1B05FC4EFD5666C4BC247B4EE54F97F8D95F90454EF47003B6598C11E99D20 A1DD10E318529F30EA193ED861C1206C638CD736CC678DF6ACDDD1
Q_4 (x,y)	91BEA7B59C5CC539F9D512B09E76CDEFEC67457795C5B6B93D5522F09D21847ABD3AED011 CAA475DE572272B39D655AD43635D26AEA2C0888C3E3D277F8CDAFB, 4208983150F1F46797EBFDDE8034C637C273ACC684ABA1E81AC78B4275C1070E8B32813DEA B288F39A99C4F9DB24DD043F0F267CFECBC7B63DF43741E8ED7E9C
t_4	0.047
k_5	E65D14E10FC782EAE2D51D94FB55967CE30A9904BF0F53B29CB825CB89CEB4D89E829E9BB 0044B14092FA6930C39B047A581A1B49449F997EDFB12ADB73C04A
Q_5 (x,y)	ADC44D91BACC714E5EDC75493EF56B833681E99F10A2991E2DA17B639630105DDC5DFBAE 74C6263F845DC6EEA691CBC34F98E2531EACEFCDFCDE3E478CC30978, 563B89D6F61F0D89958709C1EB9219DD01F202331EFED3A71FA31020BBC9FB0B74A68B914B B17D22B4614247E16F9817389ABEA1E0D6014B78046EEEA6F2A272
t_5	0.053
$t_{сер}$	0.0474

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
P (x,y)	47396FEDE8B433E8B6EE416E61FA9A3A61774A4AD8358581E481E0F456495E2ACD6472CBE4DB1D C69FB426F3D09F31B98B0C5E0E9BA35D4319949FB79D420E3F, CFBD2EAE8F8F41DC96121BF256F1A3C01AD0771CA7459221026E3F5486B995BD37B5F9A4DC6DD D208FF2A69AF044EB1DBC13DFE58D603460EF0FA86909C2A3F6
k_1	BA76FAE790DCB4A9F15290A2D80D4389187E4E68F90CF520AE9B686E3D67D985611A193148 9E8E72D2BD4681BBF31B1DFD5C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	B9796418AC510DE8B72600D6D959E92B14EA0EC0F5C578981905F3DF20D2079C260DF30DF93 A5A1864769D3BCEA9408635764CEDA0EE7FDBB1707B6D30FE8949, A823AD551C7EDF2016359F7AB1EB38199AFEC2F6AC8D55FE8A3B13124BD67ACBA5F6BF8C 5EFFAC1EC2D99D89FE77B6B8619F9234A6D5998F7FF44015CB55DDF2
t_1	0.049
k_2	A5420B393140DBEDC6BC39AF65FFC573BE0A49821C8768F9F9BCF009CF3CC42D373A838B5 FC26D54DDAE75ACD6CB72C8328053A0B2F481516077697B4941B40F
Q_2 (x,y)	426D79C97E0D9DD7557452A8FD145B68CB6783F9EC2F8D1A093793ED8352512A2805893DCED4A2 1C665DD773A926622445EFFD3CA56D5AC42D41AE1512BE90E3, 6DB1AE56106D1D21532A74BB14FFC6F39595A759ECBCB766C402B25CE73439AA746EF5DF9C66D E29CDE35FC7FF31D17AEA06E9B20521462E3774AFBF399FC44
t_2	0.044
k_3	2F1DBB39EBBBDB43B9D502AB0B4CCBFFB94DDF17E951589934501D51DAA2E66986F7C8BAC818 D6BAEDB3DB4F48B016E2E5679E899198A5CC3FF8EFF8D14FFF1C

Q_3 (x,y)	DD34D9CB0234A4208A85FADA76C904B7D59B7AA4A546A48A9C05F37C68838BD3BD5DB64 37650592CC18EBEE054351AD5102EB459DF01D11668DB73FD1CBF0D80, 458C4B07D1DEBD9014444A94BF40CB4C94C51E9364095A7F5F87E51F6383DF86647441176AA D834CA5FD22B2F6A454E8BE79D4DDF918071EC4A9110B35B23424
t_3	0.047
k_4	EA60D512DE6A1B05FC4EFD5666C4BC247B4EE54F97F8D95F90454EF47003B6598C11E99D20A1DD 10E318529F30EA193ED861C1206C638CD736CC678DF6ACDDD1
Q_4 (x,y)	943D854B2E33E7E0CF3525EE6DE7BBDFE94E6C50D67AF3C5CE1D1E5B62BBD17D5FE1F2B267AD CCA773B60EE4EF346E8F6C127FA586326A949F26196CED98F4B, 458C4B07D1DEBD9014444A94BF40CB4C94C51E9364095A7F5F87E51F6383DF86647441176AAD834 CA5FD22B2F6A454E8BE79D4DDF918071EC4A9110B35B23424
t_4	0.045
k_5	E65D14E10FC782EAE2D51D94FB55967CE30A9904BF0F53B29CB825CB89CEB4D89E829E9BB0044B 14092FA6930C39B047A581A1B49449F997EDFB12ADB73C04A
Q_5 (x,y)	C7053FEEAA901303A52B23CDD6772E55E314871CD12E208B40B5D8B259BA7F724EB89D7C73 D43ED5398711A1828145BE5315B35D6834EBAE40BA742179154A4A, A82A2F83F9FF2D8C394A20D07A7A98B7AF2FF5CEA145FE96F8AF0D97CC991B8079A137B8D4EFE B2642F9AAE75B6F380DAC3609A537F9316CC8D79634EE2E4E7F
t_5	0.042
$t_{сер}$	0.0454

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
P (x,y)	9359CA76205C5439933F51964ACEE23C4387A16381A60D6CB7DFB308D3021B46B05AB7A249CA2B 91C9BF23A2D96EFFB14F1F9758C83DD25A9AE8FB5C0491FB7F, F90ECE5D2202A94AE21C0B5108163A4A251BE53804A4A72A8F3657F7FB025359D3C2A4F027698BF E06C54EBC108E8AFBF513D7D808E449464BBDAFF4D920845D
k_1	BA76FAE790DCB4A9F15290A2D80D4389187E4E68F90CF520AE9B686E3D67D985611A1931489E8E7 2D2BD4681BBF31B1DFD5C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	B7A6EA2BE147796C4B0DD1B13C8373A6473002B28462A3A1B449B3893C1A19BF76F9ED936F6AF7 AC764889C02E21092818C4D0FB2D1B844EF3301177C4506410, 3FA27B3A50A7279BE852AFDD59881DCD68DD2EEF46BAAF1C0D18097A4663FCE3E5CE9A9F82F9 DE3AED450523D41FCB2AC727109F650CF271314486F0E6255833
t_1	0.05
k_2	A5420B393140DBEDC6BC39AF65FFC573BE0A49821C8768F9F9BCF009CF3CC42D373A838B5FC26 D54DDAE75ACD6CB72C8328053A0B2F481516077697B4941B40F
Q_2 (x,y)	9B6C6522FCB3AE9DB1DB61A750FBBFCF85B871979807C4857A2F4ACB74DCB8E5C746D3AF089A 9462DEF670E6B7BF3209C56A019CA289406A3EFFB0D948F1FA9E, 3CA3A846B553E8754E478D625A5DCA1A9C36DAE73614FA93E0A422DEA3D233E9447AA6FCD57E 20427ADA762172F6176E42ECE42CE0F2BCEDAFA1DF9B9252EAD9
t_2	0.042
k_3	2F1DBB39EBBBDB43B9D502AB0B4CCBFFB94DDF17E951589934501D51DAA2E66986F7C8BAC818 D6BAEDB3DB4F48B016E2E5679E899198A5CC3FF8EFF8D14FFF1C
Q_3 (x,y)	E101B1F0729FCA0C76C4F6D350E30F2973D60C0BB3047C62687B40026D30FE188FB430C8B9346560 B8BBB316C3F74FAC5C30F367883522EC38A2B9EA4AC38C4C, 85A40057C0F9BCEE76A7BB08CBF7166021C832901616D8DB0A087F753E9D190D933E4C5E4271456 9B60B7D4189AC58E4C227430C93255DF6DB8DADAB5AA1940A
t_3	0.043
k_4	EA60D512DE6A1B05FC4EFD5666C4BC247B4EE54F97F8D95F90454EF47003B6598C11E99D20A1DD 10E318529F30EA193ED861C1206C638CD736CC678DF6ACDDD1
Q_4 (x,y)	9A8ADFAD29F71ED3D373FF33B06323749337AEBC4C1E39E376034DB2A0891C0FFB37E7A16FE412 0086E974256A29118316FEB2279533DF81AFA6F009262D0D9, 24E28C6848AB1EA9029F796A8F07C37860828F2F4FC6035906611DE3997083CAB2AEFC21E8CA069 E7A9888A1B57ADD566150465C7EF469AD08B1C3483E47D74B
t_4	0.043
k_5	E65D14E10FC782EAE2D51D94FB55967CE30A9904BF0F53B29CB825CB89CEB4D89E829E9BB0044B 14092FA6930C39B047A581A1B49449F997EDFB12ADB73C04A

Q_5 (x,y)	ECDD0AA1ED636248E89F1E9CC0A194BCF02F7F4299C5479A2D771C32CC36A085140A032D3C5003336B0ABEF645EF9D68F1974057654389F53D6CF66B660E1C2B, A6DE97CA7F6246A0F6D7871700356357A996A927A6DD88FD1DA572A50107ED661AD72BC307D9BC99F52B63F6643F8EDC238DC536AE79CABCD5E67849250842C1
t_5	0.043
$t_{сер}$	0.0442

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
P (x,y)	D7100BFE834D7FBEB3BCBAABA9CB2D10DDD2E9103FB5C684E2FE991A3E17F7D80CE8CB349FAC7056AB57CCCB6AB1A0ACFA5E9767CA9B864E578842A913DB52F3, 5F2DA4AA6F383835CD16BF1C476720242FD29083ACB88DF8A8908943202BE86A6D09EB2BF4F62A945AA9F1C98CD3D64A1C38B3D8D634AD1B45A7074B6E55F6F6
k_1	BA76FAE790DCB4A9F15290A2D80D4389187E4E68F90CF520AE9B686E3D67D985611A1931489E8E72D2BD4681BBF31B1DFD5C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	6E919B72480B04674A1034A4BA1C12694E57540F01976D21321F44F00BC3680D9890DF408CD64696E22DFA8338ED12492C1029052C8C8C4EEFA81E1C214AFDD3, 4201E03C60C4A44EBE094810C32E5948378925F2493861F37E42319EF885F73E936C32BC12178DAE490A75426C22ED20867E0DD47633594D7D950E7C4F080128
t_1	0.046
k_2	A5420B393140DBEDC6BC39AF65FFC573BE0A49821C8768F9F9BCF009CF3CC42D373A838B5FC26D54DDAE75ACD6CB72C8328053A0B2F481516077697B4941B40F
Q_2 (x,y)	F377A35F6BD784E4AD0FE3B73076DBEA206A7D850ACEE95F14EA73A43A1D2C4BF8124149348A5C977A4BE09439D221F20033EF08AD98481158E1ED18B3BEA3D7, 8CDF18AD7E7A7B2BA2E9BF104E81D7CFD1F22A64AB1EFD33678DA4B6F121E46E27BF1D80DDCDA96B0CEE0E7CA900BD9FB2E5D04BC3ACE9A9C36EBDCA9A6F1245
t_2	0.047
k_3	2F1DBB39EBBBDB43B9D502AB0B4CCBFFB94DDF17E951589934501D51DAA2E66986F7C8BAC818D6BAEDB3DB4F48B016E2E5679E899198A5CC3FF8EFF8D14FFF1C
Q_3 (x,y)	C5551CC52B894EF292B2849514164CC652F8B9A0132B8C1DE4254CBE790C0D63319AB76A44D25F81172403824EB53798B0FCB5410204191EC16127948600A779, 28A0AACCDB3D8B0B061F39B076763B509D4C58C3EF994DBABF87E3A6241DE6B93945409E7777D08195126DB2533CFC34A963A7B6C469F09E4A6CD0C085D3441
t_3	0.047
k_4	EA60D512DE6A1B05FC4EFD5666C4BC247B4EE54F97F8D95F90454EF47003B6598C11E99D20A1DD10E318529F30EA193ED861C1206C638CD736CC678DF6ACDDD1
Q_4 (x,y)	FAD6990274026185602442C3C7E95EF12F8D4D0FF66202CDFB1A79A4183235BFEE2CB9683204EF6B02FED176B7CC35671A1D142B194C0B59C0853B9AB0A1B483, 5F6020135110F54E46DA90BB2CA9026A4FF66E5A9C876BEC84BB3C9B314B0BDE1ED03B99FF99202B1FF9F5D0ADDDD4D47834838CB72CF7D2473C78F9FAD93918
t_4	0.044
k_5	E65D14E10FC782EAE2D51D94FB55967CE30A9904BF0F53B29CB825CB89CEB4D89E829E9BB0044B14092FA6930C39B047A581A1B49449F997EDFB12ADB73C04A
Q_5 (x,y)	8BAC2CF533BFDA1D7D3B043A2ACF8FD2D544AF00032F2721E461364C609D8272B7667AAEF10A7E47E9753B4B84EF24D92D0C898FD9FA1024D745D2569C1E9BAA, 43EBCD2D768677A30C31194F44A9D35E9346624407703D4D0B3462CAC97D054D8CCF8EBEE5FDA75D747BDDDF04ADEF7353E9255F6DF5BE4D297355F67EC16F9C
t_5	0.044
$t_{сер}$	0.0456

Продовження таблиці 3.6

Результати скалярного множення точки № 5 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
P (x,y)	682CB6B299DBE8983409E0A21839FC9D80066C91E7239D532251AE3FF4AC87F549C0005883852A1BACC4236B8FF08492519B7947D292779AD512D14A83732AC3, 492F0CC7E947498364D0E4E15A82EF57ACB975FFD09C0FCD3BA967A7DACE72FD2151648FEB11A12F3ED9F1297469285D2C26A1CFB2DDDF23B946E540A8B5765C
k_1	BA76FAE790DCB4A9F15290A2D80D4389187E4E68F90CF520AE9B686E3D67D985611A1931489E8E72D2BD4681BBF31B1DFD5C03DD3564C91195F2076AC358FBAB
Q_1 (x,y)	1BA6D699DD923A321CB1A2ADAA896BFB67C08F587A3D14806B65C70453B989EF6728BCBDF1B53CD7987E750E93A7BAA94EC39D7E4B96150CB77F37FD33B7F76B, 6056ADE99168BADABB9A750BE0A927C1C8153DFB249043C61D2F389F6E0683E17306F132049FA327EB979C40E3C7F8754D3AF9A0EFC57CA36015DE2A03F2D99E
t_1	0.051
k_2	A5420B393140DBEDC6BC39AF65FFC573BE0A49821C8768F9F9BCF009CF3CC42D373A838B5FC26D54DDAE75ACD6CB72C8328053A0B2F481516077697B4941B40F
Q_2 (x,y)	7325F1113D33069EC8D8387DC3B83888095BEAFCA2480FAD7617151882392E221D82A84D52710FF9AA034917BECF627B275879975B6B32C6A2DA7B3B17C9427F, 9745590647A7AE87D4AE618D6528989A980F9F2F44CD824D2DDE2E8B1079736881F1DF0111727752C32D05549A5BE673F514146346D0C72C3E30DA2C1DD5EEFB
t_2	0.045
k_3	2F1DBB39EBBBDB43B9D502AB0B4CCBFFB94DDF17E951589934501D51DAA2E66986F7C8BAC818D6BAEDB3DB4F48B016E2E5679E899198A5CC3FF8EFF8D14FFF1C
Q_3 (x,y)	5321BAC53D343746A198A3DF3EE1A3628D1A41DA2F716CFBF2C2D5CA51A5A93100329FD189CC80307FCBC27E16B535E06E0ECD038A8D39DC800FD26F65016E54, 6F658DCB9F57D0F26D825238C7721B5022D6DD77E4CEA0167BA90E810A87348B6064C7EC4DE368005FA7759B0E38463F706C3AFB8833E7EBB0F5569AA0D5974B
t_3	0.052
k_4	EA60D512DE6A1B05FC4EFD5666C4BC247B4EE54F97F8D95F90454EF47003B6598C11E99D20A1DD10E318529F30EA193ED861C1206C638CD736CC678DF6ACDDD1
Q_4 (x,y)	106BCE18725A208C01453E150D1E7369191620FEA33C794C0E33D78D5D34BA354409E2A67AE4DC39558DAB17CDB56E5A92BDC7A1466DBF4AC0EE0A9B2F2F5681, D2A4CC1C610116421545A9BC62C5C7DA703C055D8B5A7724857FE70DF49CCEFB4E2FB3AC5BEDCE924E77FC01AD56E146E45747224FD0858BDAEC87419863020B
t_4	0.049
k_5	E65D14E10FC782EAE2D51D94FB55967CE30A9904BF0F53B29CB825CB89CEB4D89E829E9BB0044B14092FA6930C39B047A581A1B49449F997EDFB12ADB73C04A
Q_5 (x,y)	A894865A487E0DFEAA887703D197AA8664170FE78501829DDDBDC04B846C863BE2032BE61695A36E1FD8955A9A43C3957175C97F25895A2160617136D8A44DC9, 9C3C06847E70624FDC3078036B202FEDEB953798AF8FAE25FE831727A45E33CEB54402BBD23260B365D9934D93A2DC6A54BD0A9CB3D6E06E1EA04652048031BB
t_5	0.06
$t_{сер}$	0.0514

Додаток Д

Таблиця 3.7

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{256}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
Вхідні дані	
A	2
B	18
n	4000000000000000000000000000000029E26087789BC2815BDFF97093543CCF
Q (x, y)	37FB10FEF3EAC946BDDDAF6AA23C0A087495D05F9EF4E68E34E6451864D56B2F, 61DC4918C4BC3234240B0C8A9934F41B6C134D54864F827E12CE2B2557A803AC
Результати обрахунків	
g_Q^x	326525C888CE8CCC99C96EB30B43F24192A7D93160D566F6FB0653A836F77F0A
g_Q^y	3C476DCE76879B97B7E9E6EACD9617C9CF62E774D5D0050949E38F779E00EBE4
v_Q	24CA4B91119D19993392DD661687E482FB6D51DB490F0B6C9A2CADDFDA9AC145
u_Q	90570170EAD2A1685B27B51BBACCC95979C3400A4847E137875AAF881FB8C31
v	24CA4B91119D19993392DD661687E482FB6D51DB490F0B6C9A2CADDFDA9AC145
w	3532BB6A2D246FDC8C1FC528EB6342D255B7BB8E9A5143F7C981254B6A45B010
Коефіцієнти ізогенної кривої	
A'	80C862AA7EE8001FE21AD018F5889719484884DFC880E6510C086F274F6F016
B'	B9CE018C400F0F82B219BE190492C40A34822469B6DB341A4B7D3938C119C82

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
Вхідні дані	
A	2
B	13F
n	4000000000000000000000000000000003A02AE2178C1BA11BD9C4805BC8C6829
Q (x, y)	2889F59837465E702D9A1FFD5725079CF5A44786D295107DABA01E2D8F0D1EBF, 454838F54D5E9B9332D12B2F60274D7689CBF060F78BC81C665C1A1A3A513879
Результати обрахунків	
g_Q^x	2BD9755616A820F746E6846DEEE0AB168296B416C18D934D5F14EEE42FF9C03C
g_Q^y	356F8E156542C8D99A5DA9A13FB165139A7029A27B2D9DFC6C1CA3DCC102C789
v_Q	17B2EAAC2D5041EE8DCD08DBDDC1562CCB2ABA0C0A596C89008D95C2A367184F
u_Q	6E977B7C4800DACEA000EC580E3D0A30CCF846F0733A05CA711E7166BD283A7
v	17B2EAAC2D5041EE8DCD08DBDDC1562CCB2ABA0C0A596C89008D95C2A367184F
w	27E9B68344414BC69C636C45B96CE286F86837C21DC89EE165F23FE548BC7549
Коефіцієнти ізогенної кривої	
A'	9816AA31D6EB6573AFED3B4AB3951207C2FBA06BDC455767874A33E481556C9
B'	289C02692236ED91B9480A17EE05CE505733E0588B4C4A2EEA6DA8D7B196D50D

Продовження таблиці 3.7

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
Вхідні дані	
A	2
B	6B
n	4000000000000000000000000000000001E1D14B6ED53005C107434A962152593
Q (x, y)	69244DFCA2DA84637C7C0D8D2CD59E391078AE07E3F248722122A9BEF8735A21, 4B44B9D0F04ADF1FA3C57D958BD9E83C4787F2114F444D8D7218798C308076C1
Результати обрахунків	
g_Q^x	2170F51C7710D6B1639323500F429A24F05CE90418489A917A931124BBA28183
g_Q^y	29768C5E1F6A41C0B87504D4E84C2F87CB475A02297065F94D2BAAE3C53E8337
v_Q	2E1EA38EE21AD62C72646A01E853449C29CBD51433E34C6E4B1EDA0152FDD73
u_Q	320D272FE74E18FEBAAEA082274DB23C0ED72F79FB335E0689B62379290AD4C
v	2E1EA38EE21AD62C72646A01E853449C29CBD51433E34C6E4B1EDA0152FDD73
w	58D860F3ADFBEA6DA23BC249831825FEAB30CF5FE479BE3150D5C1CB7F4410A
Коефіцієнти ізогенної кривої	
A'	31966CE359579D121C409EDF6765FA8F510D62209D1BF87998FA9088F825D256
B'	1921559563E1C9700905DAFFD6A56F60B337B9FCF95DBD267D16AFE05A675EB8

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
Вхідні дані	
A	2
B	44
n	4000000000000000000000000000000026AD0CE5A034E9970A0131EDD7919957
Q (x, y)	E80DD85A537A44FD65DB1799048A60F324827E3ED2D280ABFB37661CD941DF95 , 2EF6C823E475BE6B03665F228F1DB65F3AEEB076EE53044482674E6D0E8FF96C
Результати обрахунків	
g_Q^x	2B4AB6E4965D5E89AE5DDCAFBB6D2AE553FA83067E058DA1517EF40974A44B86
g_Q^y	22126FB837148329F93341BAE1C49341D77CB8DD63C3CAA50F33C70192033FD6
v_Q	16956DC92CBABD135CBBB95F76DA55CA8147F9275BD631AB98FCB62511B6FDB5
u_Q	17FF97DF1BEDF7DFCCA913577D5633574D76AD5BB1A48A044E0C4A060DE5B0CA
v	16956DC92CBABD135CBBB95F76DA55CA8147F9275BD631AB98FCB62511B6FDB5
w	39D91AD884FA18512ACFFB81E1DDDD59FFD8D28E85E90985B4C0A85A62867F33
Коефіцієнти ізогенної кривої	
A'	F14DB12205A4E9F30556122ADBC530BC6F23C06753ADAD41712D52256903E27
B'	2B1044145D2955C7D4501F72D2EEF28B0FCD9861B813207954C3C308334DB740

Продовження таблиці 3.7

Результати скалярного множення точки № 5 кривої Едвардса над полем з характеристикою $p = 2^{256}$	
Вхідні дані	
A	2
B	5E
n	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFA3C8DC9AC1EDAE7723F05213DC50E015
Q (x, y)	E1F91BC517A66C51A0CD1B7194C3BA26EE83D1F2EB431E0A5D3F64E4AFD40324, 8058735974E50F868276CAEAA1A5849BE694A041E35E2C3AF8100244D7CA0CAE
Результати обрахунків	
g_Q^x	7AF3CE55F8F591E40800E3A933475C84E0AB70574F002D4633315FB7155D3F0
g_Q^y	3F4F194D1635E0F2FB126A2ABCB4F6C665C30E8202E80FDDC39195D99E00470D
v_Q	F5E79CABF1EB23C81001C752668EB909C156E0AE9E005A8C6662BF6E2ABA7E0
u_Q	27B8EA570F29B262E5578362E10FF2A3C0043E0A592F5D237A9169A7E6147409
v	F5E79CABF1EB23C81001C752668EB909C156E0AE9E005A8C6662BF6E2ABA7E0
w	256758B3284A0A30A57D77E55A4794750C408273008BA1C22362A07BE073E678
Коефіцієнти ізогенної кривої	
A'	33279F0A446684D17AFF71B63FF3662C3B2692FEF27B40A267E1C8554B4778CC
B'	3A2C9319E5F9B8AB7991B8BA880AF0CADD28BDE0C5D2FC04BBFF37002A69137F

Таблиця 3.8

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{384}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
Вхідні дані	
A	2
B	214
n	4000000000000000000000000000000000000000000000000AF905B73674AC7D4AF38C53331DC208A517DCB3F340EECF
Q (x, y)	F5FC151B6264CB53A4B879AA9A1F4A5156BBF063B56AAA912617C0E4CEFF15D2DF497D9AEF12374A22D22C3B402B2C71, A9027207E88074F4AFA3D44D4590DD04BAFBF6AE3D321091F500C783F4707940B7F5EBDD93325C5391843F9A78526BB1
Результати обрахунків	
g_Q^x	1015A21A222ADDBAD42693B835E1996E13A70543ADE491DA5790B350E828FC745E4E511EC04B86CE0BD6763D1639836B
g_Q^y	2DFB1BF02EFF1616A0B8576574DE45F68A0812A3859BDEDC57D493435DDB186E51C972380C4DD38CBB86AD02C2E0C178
v_Q	202B44344455BB75A84D27706BC332DC274E0A875BC923B4AF2166A1D051F8E8BC9CA23D80970D9C17ACEC7A2C7306D6
u_Q	23C5C8AEE6E6FF5FF38DE73BCC9CFF57AAD022A858F6A0B2285D1094788A642DB2BB59B891E815FE4015B752F18A30C2
v	202B44344455BB75A84D27706BC332DC274E0A875BC923B4AF2166A1D051F8E8BC9CA23D80970D9C17ACEC7A2C7306D6

Продовження таблиці 3.8

w	5BF60F42AFDE428D4B06FC8F73F180B8AF021B3F0ED3F034CCA3FFD48E0F9424 34818959CB512EC01FA88F2D56FFBA7
Коефіцієнти ізогенної кривої	
A'	1F27AAFAAA5356B3B67E3ACDE53001B33B79CB5B35124D78B5440FFC91C428E C31CB79C61666020D78E6F7B8FB83AA41
B'	17C45952D30EC2E22F2CF1813D4657AF336F1414698346E8F17145CA384DDBAD7 3FAE03BEA2A3D94973E1E101D310F52

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
Вхідні дані	
A	2
B	43
n	4000000000000000000000000000000000000000000000000169BD1B903298994262820 E2A3E73B4AA252FB924D3974A1
Q (x, y)	25DA67A2BCA7B317923BD7537E3F781E433EB28F0224070701BBDF3DF0D63D26 BA5409747D7AB030E2BB6FE78593C0C8, 20520FB9FCABB124725D8FF3AD5B2004DC296B245A1D57C689962B2A9D0EABC FD94CC4157E7CD0809055711EB35DEB5A
Результати обрахунків	
g_Q^x	38E0F3BC4305333D80874151087E15BA21DD2DE45130F673DF2F1E9BE40186DE6 F3852AE96444DD57B3319EEEE8B7F3A
g_Q^y	3F5BE08C06A89DB71B44E018A549BFF647AD29B74BC550731A0B4D1CCC35BB8 899B6B99A4AD4D59423FB14E733B7128E
v_Q	31C1E778860A667B010E82A210FC2B7443BA5BC8A261ECE7A7C26B7EC4D98428 B848847A88A160605413384B8FDD89D3
u_Q	6E0343EDAC31D3F3C464E178E26AC58F0D8D2B5E604532F3469FF9209ABED9E8 0A30C8110AFD7AA1D13B2A8BA9787B8
v	31C1E778860A667B010E82A210FC2B7443BA5BC8A261ECE7A7C26B7EC4D98428 B848847A88A160605413384B8FDD89D3
w	145E31A4B4703911B4AEA6FBC2B93BD59614BA4AAA5E8F3C37CCA7D26ECCA6 27190CC607F9E05201B3A5EDE7CBEF7A32
Коефіцієнти ізогенної кривої	
A'	7367AA561CBFF98FAB772D5AB1326BAAD5C3514D4165F7A13A32D6A34669184 FF35ED25E4760B48E4EBD4CF65922167
B'	316CA47F10EE70840F396F1DACEF5D28E56EE7F5576A155ABD3ADE6A01E411A AC31EF870169373D3FD6F7160542006C8

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
Вхідні дані	
A	2
B	304
n	4000000000000000000000000000000000000000000000000050BFE5AEE2F9642045CBA 3B5673EC7020317A99B7A2A7F97

Продовження таблиці 3.8

Q (x, y)	F108BBC769E3358598060F9C1C5EB79C6492860F58967AC7D7E50B23B21767B3D8A360C346B2AA22A801E0DD652CAD2A, 8242F49FA453B08E85B033A3399C0EECFB57522496A9DFE1FC8423C009951649DD1FF90F9B49AA9C6E28AD374A67B632
Результати обрахунків	
g_Q^x	1B3B62788701F39DC633E57C3C3A4129BE7B8011E4E3E4B18A203BFF169C2B1CB9F418DFCBC6A51BEDAB9EF18BB5404D
g_Q^y	3B7A16C0B7589EE2F49F98B98CC7E22609515BB6D2AC403D9AB734EA5BB4C80DA2BA406BCDA68DD13324F59ACE05118F
v_Q	3676C4F10E03E73B8C67CAF8787482537CF70023C9C7C963144077FE2D38563973E831BF978D4A37DB573DE3176A809A
u_Q	21CA7A54F10B394E3BDCC9454B397C17D0E8CC9A1FAB1EF67695903A6FAC1BE0EBFE4BC000B744C7766CF556D865673D
v	3676C4F10E03E73B8C67CAF8787482537CF70023C9C7C963144077FE2D38563973E831BF978D4A37DB573DE3176A809A
w	A5F1BCF006CAB60E40FA7D17975B9E7BCC4C4DF63663408675CC02A30558B330824267C3A0544B026105F583B5674D5
Коефіцієнти ізогенної кривої	
A'	2FAE274AB9EC7BD641F90925A5B9745E8F2CFF4D0F1911122E7D24738CC54582197139CD0E776FF2C6C21A99EDBFFAF3
B'	37663D56FD075059C3926945ADC7EAA9D69E9DE4483493C5CDF68A36739BF9DB529A3A053858AD32FBBCB7CD54F7D05F

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{384}$	
Вхідні дані	
A	2
B	114
n	4000000000000000000000000000000000000000000000007269FD2518A6AC30A3FA9F3931A347FA8BAC4843ECF19B5F
Q (x, y)	E44A4A622DAA298B94A167989E99ADFF06180D11EAA618386D7B173C82C4C1E9822C47B7C7F5B26663C8BF3074C4762C, 535E607ABF5739C3E5A946F9AD44C899C33BF00B04CAE695080D622B28DA64CA0B55AB041BF971382D956739A3AAE176
Результати обрахунків	
g_Q^x	2F4F643D1941DD7E3F0B26153D343757EF2DFBE06C9A9682527EF0E89395120B8C5996ABA5EA95C71B2D50A9A946EA6
g_Q^y	19433F0A81518C7834AD720CA5766ECC79881FE9F66A32D747233318F83F3AFDD54487A35CF6F57F47DA0A587F7F0F31
v_Q	5E9EC87A3283BAFC7E164C2A7A686EAFDE5BF7C0D9352D04A4FDE1D1272A241718B32D574BD52B8E365AA153528DD4C
u_Q	2750C820E69C42F29E022D612CF17F192D13AF9E2D9C766D153A88C4B21A48D5A1AAC51D3378C229AC063027A45124F4
v	5E9EC87A3283BAFC7E164C2A7A686EAFDE5BF7C0D9352D04A4FDE1D1272A241718B32D574BD52B8E365AA153528DD4C
w	2EF4FFE7320175297386949C1D6949B05A2FF1CDE1FF0A6B9EFD9A2E965409E15CF96FACF19D2B482187E714EE03513D

Продовження таблиці 3.8

Коефіцієнти ізогенної кривої	
A'	226E6159D036D59118990832B9BF5D690A834293BC1F61EEFEDAA693BC6980E96C42A10DE9F0AA5E1AAFF5D9E32548E5
B'	374D00ADA1F5CBDDD751EFBB321EFC2D88B0635ED206B711558CB798779BC3FA4D0DAD9C8E8780E65B5260050B926CA3

Таблиця 3.9

Результати скалярного множення точок кривої Едвардса над полем з характеристикою $p = 2^{512}$

Результати скалярного множення точки № 1 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
Вхідні дані	
A	2
B	10D
n	4000000000000000000000000000000000000000000000000000000000000028A3CE52209E2BD4952882D5574165192C46C0D0311FEA6BF9FECE70EE63B59F
Q $(x, y$	5230A1EE747050A072BD7319741586EA520388B6B53094571C821A2FC9A9E83D56665346B5DB04C43E75261DBDA512728FAAFAC48AE9260A5A184E2933E3A400, 53A0D50CC63C9219762F451978AEF214DBCFCC3A5CB5EF27124991A86B42B3A1A832724A0E6B930FDD1DA2E27A540D6B675E4422C444F529C508F0BAE7D0A85
Результати обрахунків	
g_Q^x	13CFDFC282B0FB3C0296BD40E04BBC3FED1E3027E05CC0529238B14C6BAD64E3A34FC5C2E24BF95B0E5593B0514BFBA8F4AA2262922FF628632A4A1D91C2154D
g_Q^y	358BE55E67386DBCD13A175CD0EA21BD64860678B469421B1DB6CDCAF297A98BF39D8008DED0B9729984CE7907F6E36BBF5AF84BD8974BC6C15DB0599169A095
v_Q	279FBF850561F678052D7A81C097787FDA3C604FC0B980A524716298D75AC9C7469F8B85C497F2B61CAB2760A297F751E95444C5245FEC50C654943B23842A9A
u_Q	3745712E928216C5460747D2D621D6A5F934D6A93849C5FBD5B08DA5719694B9759289A9383F5A996E54812B0FE35013865ECA87982FE5CEFD841A6C143B9790
v	279FBF850561F678052D7A81C097787FDA3C604FC0B980A524716298D75AC9C7469F8B85C497F2B61CAB2760A297F751E95444C5245FEC50C654943B23842A9A
w	2712C87A15CB0BC1BEEB03EE54C64FB50FDA2D714F889A92344EE5420F8A8C53FBBB6B986BBC65C7F8466345E4DF06F07D2E740309260EA61D058C525BE6BA6A
Коефіцієнти ізогенної кривої	
A'	39E14266E5162FA7E61C9B773D0AA580BCD21E713C607CC649C91303CB3A0F1C41717FABAB80F1C3C54A4672300DBFCB2275AB670EA00C1C0854549C07FA017C
B'	2E7C84A96772ADB3C792E47BAE93D20C9108C1E6D343C60091D7BB31933629B4E913166FB0F012AF1FDDD741722DC8EA711C97FBB5952D9116D331F424A37442

Результати скалярного множення точки № 2 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
Вхідні дані	
A	2
B	179
n	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDC46E59CE4CBBB6248CFE7BB582E1F490FD5F9F74433AE745EFE6351254BCDA5

Продовження таблиці 3.9

Q $(x, y$	A9297AC52D51EF4745E5E558F6217B302052A39544DFE6DC04FE427850225E232BC379E11F6C51FDB0C9D0C2511BC3E945E25B9829B00C4DD92843328606ADFB, A51291E6175265F4C5755445CF271E51E9248C728D01CC388C3938E477F3A94C69F21873F7CB97C64AE7D33A1056B41BB0E95436F88A03555C72911F313331EF
Результати обрахунків	
g_Q^x	C54939BE903236BBE7FD117DF762F5D9417626D7562169E342BE209830919BF55DF14C64D8F0F1BB713C33EA44009DF6C29249441FDBECBA0C8DCC9A3A047A5
g_Q^y	35DADC33D15B34167515577461B1C35C2DB6E71AE5FC678EE78D8E371018AD6655C530C56D2F34C11F0FC7EFF067537EFD31335DA822100F811131A87D606E00
v_Q	18A92737D20646D77CFFA22FBEEC5EBB282EC4DAEAC42D3C6857C4130612337EABBE298C9B1E1E376E27867D488013BED852492883FB7D974191B99347408F4A
u_Q	39DF216B3E2102AED17BDF6CEBF6B098BE029F6F2265C51BFA51BD0FFEC7BF36587BACAA603FD5721CDB8B59C4A00E2014A352D37B1524266207FBD70E72482E
v	18A92737D20646D77CFFA22FBEEC5EBB282EC4DAEAC42D3C6857C4130612337EABBE298C9B1E1E376E27867D488013BED852492883FB7D974191B99347408F4A
w	C17EE16D632047172B0EC1FA50127C4548EB07E2E9837DB6F7B43DD63C431712A24AF87AD7022264D7570F8A7389BB27B38C929A2CD3263BF246DAED4C7C92
Коефіцієнти ізогенної кривої	
A'	4B23BE8E5E09DCA8F01D51145622658371627B96A2B1DD1F6492BA0E1A4FE865DD6FB7AC200DFAF6ADA2F0445DBDBD7E6108623F47DE8F4762426C1E654CEDA
B'	3AB587D6024A1E0E5DD298B227CF7E9A1B0192C8CB9D678FFF3A124F245A2A5E59D6D8D188EAAC7186EC864E8F055B2AF9ED21F50CF9E868BB5E7354A8346720

Результати скалярного множення точки № 3 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
Вхідні дані	
A	2
B	AF
n	4000000000000000000000000000000000000000000000000000000000000002DD8135044F2810D554443F2E2BD624D526C8798402AB63951BFA991E6087F7B
Q $(x, y$	A8B673C87778EE5D31B9A404334AB9B5A572C8EB536C2C91443F112F8961B1E1BBE4E7AC851E8AA509F0B9AD2D9C203A816B67E0796AD7FF29726D262EA957B8, 81177507F05F730D44D26B9D14B0FFAC6558F6834314F0414A9D6A9E48608C5F08507D8273AF1326ABD50A49B901462F3BE8005B63FC8FF851B853FF48B31B7B
Результати обрахунків	
g_Q^x	1E45E6F71DD338313434683DB022C1475716AE051CFAFE8D3277ED51CD460418FF0D79C17B87E12382170669D05062B63214E0AF248CEEC991CE8240F2F87627
g_Q^y	3DD115F01F4119E5765B28C5D69E00A7354E12F979D61F7D6AC52AC36F3EE742D497658C715E5EF552AB3F2AFBB05F24244EA54278DC6F2DF54DA7DAECC44671
v_Q	3C8BCDEE3BA670626868D07B6045828EAE2D5C0A39F5FD1A64EFDAA39A8C0831FE1AF382F70FC247042E0CD3A0A0C56C6429C15E4919DD93239D0481E5F0EC4E
u_Q	3230B651531A125F80711FA939AC721A4A6298D4D0A2FF0CB02FC6BCE84B9D7583DFC2C8AA6E6C8778B32F8089823529D8609555A4300343ED23313170826C63
v	3C8BCDEE3BA670626868D07B6045828EAE2D5C0A39F5FD1A64EFDAA39A8C0831FE1AF382F70FC247042E0CD3A0A0C56C6429C15E4919DD93239D0481E5F0EC4E
w	228868EA6E5AD231F4AD4DC0A61A0B91A86A48C11C480103E1C4F046C596E12732BEC80FCC16DA597F5092F2D4B77942F6212C8F569673EE8463EA7196526759

Продовження таблиці 3.9

Коефіцієнти ізогенної кривої	
A'	1144FA58D5BFCE13F5F3ED971EA47336991D33CCDE320E7C0750BACDFB43D706EEB19F02856DB9DF956F139C4A8F1064A74DDF21D3543B3EE6AD39500075DFE3
B'	E452196FB8440A24F42DFBB7549AF04651802B83A07F8E4D39D6E1098DFD7EE5428D4D27F2A0BC2D9DD0B27B9F138608EC9E675A28DAD5FA8433D2C7BE12B2C

Результати скалярного множення точки № 4 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
Вхідні дані	
A	2
B	3C9
n	4000000000000000000000000000000000000000000000000000000000000000153ED5CAB52ECFB1E3832493DD7A1C06617A6790626B88DFAC45D806A147B99B
Q $(x, y$	54123C034D18682F739A011463EE02332B35825602C853A8EDE6DD1657894A47C2D6E1D2EF39DC434504051DB60A690FAFFA10B9053E37268D3AF352F18B423A, AB0076944360C99551AE3AB73E24473AD55987DFD6378DD3A6D89A4B2C88576F837341D4141E791B512483B6AEED65E09F68A64CE5B3B78AF16924634C2BCF13
Результати обрахунків	
g_Q^x	130008D7536C68F77D85F6042B313DBA48C3B0C01C56D0100025BAD0A9AC22DBF2CC047BECF1512AB46DF1A68830B908D7D3953DB0F41939DD5395D8A95AB092
g_Q^y	29FF12D7793E6CD55CA38A9183B7718A554CF0405390E458B24ECB69A6EF512178927F1816DBEBF4B2C9D409D301DC650A0D20C8831DC62826D0C7612F56BB7C
v_Q	260011AEA6D8D1EEFB0BEC0856627B749187618038ADA020004B75A1535845B7E59808F7D9E2A25568DBE34D10617211AFA72A7B61E83273BAA72BB152B56124
u_Q	C6EED38858C11993E2076F07BDBD38A04DDC9BE99393C8A16499F984A05DB720B385AC6E2CEFCBE3E37DA5BC478CFC13629BC4FCFFCB151AF2E02332F5AF936
v	260011AEA6D8D1EEFB0BEC0856627B749187618038ADA020004B75A1535845B7E59808F7D9E2A25568DBE34D10617211AFA72A7B61E83273BAA72BB152B56124
w	D52C83E9A3C5525EFA109D52B9D377A91B10EA9B555420DB05305A93F5A461827BFBFA1B744BA9DB1693A6DDC2CCDA27D84B5B285F225F86A676EB0C6676F6A
Коефіцієнти ізогенної кривої	
A'	1FFA796BDC3E65518C463D6501396B9285B187EE49BDF5FFE86B3D95F46A368C3C45488DE1F436A9E3DFD3A468719BAB62B62483DB99E5C5F8DAD9D464C471F
B'	22BC8649C859ABF67298BB2BCEB37BA60428995C0AAB31A02DBAD85F44881557143F6E29677C8513ED25B026B5BA989B5453D73F1B3807F46FB7A937D5BB6B19

Результати скалярного множення точки № 5 кривої Едвардса над полем з характеристикою $p = 2^{512}$	
Вхідні дані	
A	2
B	55
n	4000000000000000000000000000000000000000000000000000000000000000017F1EF80AF949ECB3AC390D869E51ACD0E05576A5B2F6A96416B8365C69B687B
Q $(x, y$	682CB6B299DBE8983409E0A21839FC9D80066C91E7239D532251AE3FF4AC87F549C0005883852A1BACC4236B8FF08492519B7947D292779AD512D14A83732AC3, 492F0CC7E947498364D0E4E15A82EF57ACB975FFD09C0FCD3BA967A7DACE72FD2151648FEB11A12F3ED9F1297469285D2C26A1CFB2DDDF23B946E540A8B5765C

Продовження таблиці 3.9

Результати обрахунків	
g_Q^x	2401664B3594A1F89E631883CB5B199CEEAC9D0CF522243E992295EE33BF25C8B7C 7464E8FF117B517257BC2FD13A11DBB68D07951BD63863211F315F096A8D
g_Q^y	2DA1E6702D716CF9365E363D4AFA2150A68D14005EC7E06588AD30B04A631A0605 330562389A9A033296D03654DCFFACD1C2C29FABD2817B51B4BFB002674CB9
v_Q	4802CC966B2943F13CC6310796B63339DD593A19EA44487D32452BDC677E4B916F8 E8C9D1FE22F6A2E4AF785FA27423B76D1A0F2A37AC70C6423E62BE12D51A
u_Q	19555686D866658FFF088BA325D21F844221CADB57555F924A91FD121D0F24122BC 4D0483DB0BAE7EA976640EEA53AAB4C003D9783ABADBAD90E11A2F39FEEB2
v	4802CC966B2943F13CC6310796B63339DD593A19EA44487D32452BDC677E4B916F8 E8C9D1FE22F6A2E4AF785FA27423B76D1A0F2A37AC70C6423E62BE12D51A
w	3D39BE442F75A70C8CE817836A5DDC4B4A568590B04CED023B1BCF4A5859F9B99 BB51E1BFAF2BEB4D5D1839CB9ADBAD5B0E0017FF972C953A450E585B5EE834E
Коефіцієнти ізогенної кривої	
A'	297F2010FE831AC49D0210ADA0E70FFDEAD41DD7E6CAA958E04A624B1FA88862 A515638F959DEFFA0C4C237E8BB8D61A78E3D51E88190C6262204B78103D3EFB
B'	136BCC22B3C86EA825A75B68176EF9F0F7A2590B2DE584F0623D54F7958A2BED65 A9B9C0F06D209CC29E5CA1D1839FC38C055968AC2868D24BBA512074BA4490