DOI: 10.58254/viti.5.2024.19.215

УДК 004.056.5

д-р техн. наук Чевардін В. Є. ORCID: 0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)
Лаврик І. В. ORCID: 0000-0002-3433-9083 (ВІТІ ім. Героїв Крут)

КРИПТОСИСТЕМИ НА ОСНОВІ ІЗОМОРФНИХ ПЕРЕТВОРЕНЬ ЕЛІПТИЧНИХ КРИВИХ

У статті розглянуто напрями розробки та вдосконалення постквантових криптографічних систем, заснованих на ізоморфних перетвореннях еліптичних кривих, потенційно стійких до квантового криптоаналізу. Проведено аналіз недоліків та переваг існуючих асиметричних криптосистем, в тому числі таких, які побудовані на основі ізоморфних перетворень. Досліджено підходи до побудови криптографічних алгоритмів на основі ізогеній еліптичних кривих, що можуть стати основою для створення стійких до квантових атак криптосистем.

У процесі проведених досліджень було розроблено програмні функції для реалізації операцій над ізогеніями еліптичних кривих різного порядку, які забезпечать зазначені в стандарті [12] рівні безпеки: 256, 384, 512. Розроблена програмна реалізація операцій скалярного множення точки кривої та операцій над ізогеніями еліптичної кривої, на основі якої отримано експериментальні значення часу на обчислення скалярного добутку з використанням розпаралелювання. Проведено експерименти порівняння з класичного множення точки кривої з представленням скаляру k у вигляді послідовності 4-бітових слів, що дозволило прискорити операцію скалярного множення в 30 разів, для 8-бітових слів прискорення склало 18,8 разів.

Напрямком подальших досліджень є розробка методів генерації та верифікації цифрового підпису, на основі перетворень над точками ізогенії еліптичної кривої з використанням розпаралелювання операцій скалярного множення точки кривої.

Ключові слова: *асиметричні криптосистеми, еліптична крива, ізоморфні перетворення еліптичної кривої, ізогенія еліптичної кривої.*

V. Chevardin, I. Lavryk Cryptosystems based on isomorphic transformations of elliptic curve points.

The article presents research in the field of development and improvement of cryptographic systems based on elliptic curves isomorphic transformations potentially resistant to quantum cryptanalysis. Analysis results of existing asymmetric cryptosystems disadvantages and advantages, including those based on isomorphic transformations, are presented. The approaches to the construction of cryptographic algorithms based on isogenies of elliptic curves, which can become the basis for creating cryptosystems resistant to quantum attacks, are investigated.

In the course of the research, program functions were developed to implement operations on elliptic curves isogenies of different orders, which will ensure the security levels specified in the standard: 256, 384, 512. A software implementation of the operations of a curve point scalar multiplication and operations on elliptic curve isogenies has been developed, on the basis of which experimental values of the time to perform the scalar product using parallelization have been obtained. Experiments have been conducted to compare the classical multiplication of a curve point with the representation of the scalar k as a sequence of 4-bit words, which made it possible to speed up the scalar multiplication operation by 30 times, for 8-bit words the speedup was 18.8 times.

The direction of further research is the development of methods for the generation and verification of a digital signature, based on transformations over the isogeny points of the elliptic curve using the parallelization of operations of scalar multiplication of the curve point.

Keywords: *asymmetric cryptosystems, elliptic curve, isomorphic transformations of an elliptic curve, isogeny of an elliptic curve.*

Постановка проблеми та актуальність дослідження

Одним із найважливіших досягнень цього століття стала поява квантових комп’ютерів, що викликало реальну потребу оцінки стійкості існуючих асиметричних криптопримітивів, які використовуються в системах електронно-цифрового підпису, системах та комплексах автентифікації та розмежування доступу, генерації загальних секретних ключів для шифрування та автентифікації даних. У більшості існуючих та широко розповсюджених алгоритмів використовують стандартизовані перетворення в групі точок еліптичної кривої, які визначені стандартами ДСТУ 4145-2002, IEEE P.1363, AIS 2.0. Основні напрямки досліджень розділилися. Частина робіт була спрямована на підвищення стійкості класичних асиметричних криптосистем, що базуються на складності рішення задач DLP, ECDLP та інших

еквівалентних ним [3]. Інша спрямована на розробку нових криптопримітивів, стійких до квантового криптоаналізу [3; 4]. Враховуючи, що розробка принципово нових криптопримітивів викликає потребу в додаткових витратах на впровадження в інформаційні системи, реалізацію нових програмно-апаратних засобів та систем, актуальною науково-технічною задачею є вдосконалення існуючих криптоперетворень з підвищеними показниками стійкості до квантового криптоаналізу.

Аналіз останніх публікацій та наукових результатів

Початком розвитку систем асиметричного шифрування, цифрового підпису, інкапсуляції криптографічних ключів тощо стала поява однонаправлених функцій, для яких задача обчислення прообразу потребує надзвичайно великого обсягу обчислювальних витрат. Першим прикладом таких задач стали системи Діффі – Геллмана, RSA та подібні їм [1]. Наприклад, криптосистема RSA базується на складності задачі факторизації. Знаходження ефективних алгоритмів факторизації цілого числа N призвели до потреби постійно збільшувати його бітову довжину.

З часом з'явилася альтернатива цим алгоритмам. Замість RSA-подібних перетворень стали застосовувати перетворення, які базуються на еліптичних кривих, що розглянуті в роботах [5–9]. Для побудови криптосистем на еліптичних кривих використовують нормальну форму (форму Веєрштрасса [5]) чи канонічну форму кривої з параметром $q \neq 2,3$, ($q \neq 2^m$) у спрощених видах (криві Монтгомері, криві Коблиця, криві Едвардса та інші). Перехід від RSA-подібних систем до систем на еліптичних кривих дозволив отримати можливість зниження довжини ключа криптосистеми з 1024 біт до 160 біт без зниження криптостійкості системи. Найбільш цікавими результатами вдосконалення або розробки нових перетворень на еліптичних кривих є використання ізоморфних трансформацій нормальної форми кривої до інших скорочених форм [10–12]. Зазначений підхід надає можливість спростити число примітивних операцій для виконання скалярного множення точок і підвищити швидкодію криптоперетворень. З іншого боку, перехід накладає додаткові обмеження на параметри кривої та умови виконання операції скалярного множення. Наприклад, для кривих Едвардса [6] обираються криві, порядок яких не є простим числом і є кратним 4, що вважається уразливістю для криптографічно стійких кривих. Перехід до еліптичних кривих у формі Едвардса дозволяє в середньому підвищити швидкодію операцій скалярного множення в два рази, але не забезпечує стійкість до квантового криптоаналізу.

Наведемо деякі положення з теорії еліптичних кривих.

Криві Веєрштрасса

Крива (1) називається кривою Веєрштрасса або нормальною формою еліптичної кривої над скінченним полем F_q.

$$y^2 + a_1xy + a_2y = a_3x^3 + a_4x^2 + a_5x + a_6,\ a_i \subset F_p. \quad (1)$$

Гладкою (неособливою) еліптичною кривою порядку n над полем F_q називається множина точок, які задовольняють рівнянню (1), де многочлен ступеня[1] m з коефіцієнтами $A \subset F_p$, $B \subset F_p$, де $q = p$ – просте число. Для криптографічних цілей для еліптичної кривої виконуються вимоги: дискримінант $\Delta(E) \neq 0$, j-інваріант $j \neq \{0,12^3\}$.

Представлення кривої (1) над полем характеристики $q = p$ з фіксованими параметрами $a_1 = 0$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$ дає канонічну форму кривої (скорочену форму Веєрштрасса):

$$y^2 = x^3 + Ax + B. \quad (2)$$

[1] Ступінь багаточлена є максимальним ступенем одночленів, з яких він складається.

Крива (1) над полем характеристики $q = 2^m$ трансформується до форми (3):

$$y^2 + xy = x^3 + Ax^2 + B \quad (3)$$

Криві (2, 3) є більш розповсюдженими для застосування в криптографічних додатках та системах електронного цифрового підпису, а саме в системі ЕЦП на основі ДСТУ 4145-2002, в протоколі генерації спільного секрету Діффі – Геллмана IEEE 1363–2000 та інших стандартизованих криптопротоколах стандарту 1363а-2004. Від основної форми Веєрштрасса (1) можемо перейти до інших форм еліптичних кривих завдяки ізоморфним трансформаціям. Найбільш популярними з відомих трансформацій кривої (1) стали криві Монтгомері та Едвардса [6; 7], які дозволили зменшити обчислювальну складність скалярного множення точок кривої. Так, криві Едвардса дозволили прискорити скалярне множення точки кривої в два рази.

Скалярним множенням точки кривої є k-кратне додавання точки кривої, $\boldsymbol{k * P = P + P + \ldots + P}$. Скалярне множення є складно оберненою операцією, для якої зворотним перетворенням є дискретне логарифмування в групі точок еліптичної кривої. Враховуючи математичну конструкцію скалярного множення точки кривої, існує два основних напрямки вдосконалення криптоперетворень у групі точок еліптичних кривих, а саме підходи, спрямовані на зменшення обчислювальної складності, та підходи, спрямовані на підвищення криптографічної стійкості. Розглянемо переваги перетворень у групі точок еліптичної кривої.

1. Використовуючи ізоморфізм $E_p \equiv G^*{}_{p'}$, кожна точка $Q \in E_p$ може бути представлена як цілочисельний елемент поля $c \in F_{p'}$. Це дозволяє переходити від операцій над точками кривих до операцій над цілими числами в простому полі. Зазначена властивість викликала вимогу до перебільшення бітової довжини поля p в 30 разів над бітовою довжиною p'. Це дозволило перейти від перетворень у скінченному полі до перетворень у групі точок еліптичної кривої.

2. Використання в асиметричних алгоритмах перетворень над точками еліптичної кривої дозволяє змінювати параметри криптосистеми шляхом лише зміни коефіцієнтів A та B з фіксованим значенням p. Так, еліптичні криві з різними коефіцієнтами, але з однаковим значенням (4) вважаються ізоморфними і дозволяють змінювати криві зі сталим значенням характеристики поля E_p.

$$j(E) = \frac{1728(4A^3)}{4A^3 + 27B^2} \neq 0 \cdot \quad (4)$$

3. Перетворення в групі точок еліптичної кривої дозволяє отримати можливість розпаралелювання найбільш обчислювально складної операції скалярного множення точки кривої на потоки, що надає можливість збільшити швидкість множення точок кривої на скаляри [8; 9]. Так, якщо зафіксуємо еліптичну криву E з коефіцієнтами A та B над скінченним полем $F(p)$, то для довільної точки кривої $P \in E_{A,B,p}$ можна виконати скалярне множення точки кривої, а саме $Q = k * P$. Нехай існує умовний l_k-розрядний регістр, що реалізує скалярне множення точки P на число k, довжина якого дорівнює l_k. Якщо представити значення k у вигляді суми цілих чисел довжиною l_{ki}, а саме $k = k_1 + k_2 + \ldots + k_n = \sum_{i=0}^{i=n-1} k_i$, де $n = l_k / l_{ki}$, тоді замість множення $k * P$ з l_k -розрядним регістром виникає можливість виконати n множень з використанням l_{ki}-розрядних регістрів. Результат обчислення точки Q в такому випадку матиме вигляд: $Q = k * P = \sum_{i=0}^{i=n-1} k_i * P$. У такому випадку реалізація алгоритму скалярного множення у вигляді паралельних потоків, які будуть виконувати операції $k_i * P$, дозволить потенційно прискорити процес множення в n разів.

Розглянемо недоліки або обмеження перетворень у групі точок еліптичної кривої.

1. Для генерації параметрів еліптичної кривої необхідно обрати такі значення *A*, *B* та *p*, які забезпечать вимоги до порядку еліптичної кривої. Визначення порядку кривої потребує обчислювальних витрат, які викликані складністю алгоритму Schoof-Atkin-Elkies (SEA) [8; 9].

2. Можливість розпаралелювання процесу скалярного множення точок кривої викликає підвищення апаратно-програмної складності реалізації скалярного множення. З іншого боку, можливість розпаралелювання операції скалярного множення з появою квантових комп'ютерів створило загрозу швидкого зламу існуючих асиметричних криптосистем з використанням алгоритму Шора, а для симетричних з використанням алгоритму Гровера [4].

3. Здійснення MOV-атаки [12] завдяки зведенню операцій в групі точок еліптичної кривої до операцій в скінченному полі цілих чисел. Так, для забезпечення рівня стійкості 128 біт для алгоритмів на основі еліптичних кривих ключ сьогодні повинен мати довжину 240 біт, а для алгоритмів RSA – 2800 біт.

4. Здійснення атаки на основі аналізу потужності, яка описана в [13]. Як правило, цей тип атаки називають Simple Power Analysis (SPA). Він використовується також для більшості асиметричних криптосистем, захист від яких включає, як правило, організаційно-технічні аспекти.

Враховуючи переваги та недоліки перетворень у групі точок еліптичної кривої, одним з перспективних напрямків вважається використання ізоморфних трансформацій, які дозволяють отримати зменшення кількості примітивних операцій для скалярного добутку точки кривої та генерації еліптичної кривої з однієї сторони, а з іншої, збільшити криптографічну стійкість криптоперетворень у групі точок еліптичної кривої завдяки збільшенню кількості варіантів шифрованих текстів. Використання множини ізоморфних кривих [7–8] дозволило відкрити новий шлях збільшення стійкості криптоперетворень, у тому числі і до квантового криптоаналізу.

Так, під час генерації еліптичної кривої генеруються параметри ізоморфної трансформації кривої, що дозволяє покращити показники стійкості алгоритмів генерації ПВП до відтворення та передбачення. Використання ізоморфних трансформацій еліптичної кривої надало змогу збільшити число внутрішніх станів генератора без суттєвих втрат часу та продовжити використання генераторів ПВП цього класу до переходу на постквантову криптографію.

Найбільш ефективним застосуванням ізоморфних трансформацій еліптичної кривої сьогодні є побудова криптоалгоритмів на основі ізогенії еліптичної кривої, яка є ядром ізоморфної трансформації кривої. Це дозволяє збільшити множину як сеансових, так і спільних ключів в алгоритмі Діффі – Геллмана при фіксованому розмірі характеристики скінченного поля. Сьогодні схема обміну ключів Діффі – Геллмана вже запропонована з використанням ізогенії еліптичної кривої, а саме схема Supersingular Isogeny Key Exchange (SIKE). Порівняно з іншим постквантовим кандидатом NTRUEncrypt з бітовою довжиною ключа 600 байтів, SIKE дозволяє використовувати 330-байтові ключі для однакового рівня безпеки 128 біт. Це робить SIKE більш привабливим для реалізації в системах електронного документообігу, мережах Bitcoin, Tor та інших. Існуючі програмні реалізації SIKE запропоновано з параметрами: SIKEp182, SIKEp217, SIKEp503, SIKEp610 і SIKEp751. Однак, в роботі [20] представлено алгоритм відтворення ключа цього алгоритму за реальний час, а саме для SIKEp503 – 20 хв, SIKEp610 – 55 хв та SIKEp751 – 3 год 15 хв. Це створило умови для виключення цього алгоритму зі списків постквантових кандидатів з метою опрацювання і вдосконалення. У зв'язку з цим, виникла потреба у пошуку шляхів для вдосконалення криптографічних схем та перетворень на основі ізоморфних трансформацій еліптичної кривої, що викликало необхідність цього дослідження.

Метою роботи є визначення шляхів удосконалення сучасних криптосистем, представлених в якості постквантових кандидатів, побудованих з використанням операцій над ізогеніями еліптичних кривих.

Викладення основного матеріалу

Для досягнення поставленої мети необхідно оцінити можливості щодо зменшення обчислювальних витрат на виконання криптографічних операцій та здатності зазначених операцій до збільшення криптографічної стійкості. Для цього проведемо аналіз перетворень в групі та підгрупі точок кривої, наведемо відомий підхід прискорення операцій завдяки розпаралелюванню скалярного множення точки кривої, побудуємо операції над ізогеніями еліптичної кривої, оцінимо потужність простору ізогеній кривої з метою використання параметру ізоморфної трансформації для збільшення криптостійкості.

Група та підгрупи точок еліптичної кривої

Позначимо скінченне поле F характеристики q як F_q [5], порядок якого $q = ord(F)$. Тоді якщо $q = p$, де p – просте число, скінченне поле назвемо простим полем F_p.

Позначимо еліптичну криву E з коефіцієнтами A та B визначену виразом (2) над полем F_p як $E_{p,A,B}$. Крива $E_{p,A,B}$ є скінченною множиною точок $P_i \in E_{p,A,B}$, для яких можемо побудувати операцію додавання (подвоєння) точок кривої, деталі отримання виразів додавання та добутку точок кривої, обрання параметрів еліптичної кривої наведено в роботах [5; 6; 9].

Приклад. Зафіксуємо криву $E_{11,3,4}: y^2 = x^3 + 3x + 4$. Так, як порядок кривої $ord(E_{11,3,4}) = 14$, то група точок складається з підгруп простого порядку 2 та 7. Позначимо підгрупу порядку 7 як subE1, а підгрупу порядку 2 як subE2. Наведемо точки, що входять до цих підгруп з урахуванням нейтрального елементу точки O.

Група subE1: {(0,2);(0,9);(4,5);(8,10);(8,1);(4,6);O}, з порядком підгрупи $ord(subE) = 7$,

Група subE2: {(10,0);O}, з порядком підгрупи $ord(subE) = 2$.

Порядок точок кривої $E_{11,3,4}$ наведено в таблиці 1.

Таблиця 1

Порядок точок кривої $E_{11,3,4}$

P_i	(5,10)	(4,6)	(7,4)	(8,10)	(9,1)	(0,9)	(10,0)	(0,2)	(9,10)	(8,1)	(7,7)	(4,5)	(5,1)	O
$ord(P_i)$	14	7	14	7	14	7	2	7	14	7	14	7	14	1

Точки порядку 14 не використовують, так як точки (4,6), (4,5), (8,10), (8,1), (0,9), (0,2) створюють циклічну підгрупу порядку 7, що зменшує кількість операцій, які повинні виконати криптоаналітику. В зазначеному прикладі точка (10,0) має порядок 2 і в якості генератора групи не використовується також. Для криптографічних додатків завжди обирають циклічні підгрупи точок кривих простого порядку.

Особливістю операцій над точками еліптичної кривої є можливість розпаралелювання операції скалярного множення точки кривої. Розглянемо сутність процесу розпаралелювання операції скалярного множення точки кривої.

Розпаралелювання скалярного множення точки кривої

Нехай, еліптична крива $E_{p,A,B}$ має скінченну множину точок $P_i \in E_{p,A,B}$. Точка $P \in E_{p,A,B}$ є базовою точкою (має великий простий порядок). Тоді операцію скалярного множення $k * P$ можна представити як $k * P = (k_1 + k_2) * P = k_1 * P + k_2 * P$ на основі асоціативності операції додавання точок кривої. Для виконання операцій $k_1 * P$ та $k_2 * P$ використовують два різних обчислювача (регістра) або ядра процесора, що суттєво прискорює

виконання операції $k * P$. Є різні підходи щодо використання розпаралелювання скалярного множення точки кривої з використанням комбінації Double-and-add та Halve-and-add алгоритмів та Montgomery-halving алгоритму, результати аналізу ефективності яких наведено в роботах [11], а саме скалярне множення точки кривої визначається виразом:

$$I = (\omega + l)I_{dbl} + (\frac{l}{\omega+1} + 2^{\omega-1})I_{add},$$

де I_{dbl} – складність операції подвоєння точки 2P кривої; I_{add} – складність операції додавання точок P+Q кривої.

Сутність прискорення скалярного множення з використанням цих алгоритмів полягає в різноманітних формах розкладання цілого числа k, що скорочує кількість операцій додавання та подвоєння точки кривої, які здійснюються під час виконання основної операції множення $k * P$. Так,

$$k = k' \times 2^{-\delta} mod N = k_1 + k_2 = (k'_l 2^{l-\delta} + \ldots +_{\square} k'_\delta) + (k'_l 2^{-1} + \ldots +_{\square} k'_0 2^{-\delta}) \text{ mod N},$$

звідки

$$k * P = (k'_l 2^{l-\delta} + \ldots +_{\square} k'_\delta) * P + (k'_l 2^{-1} + \ldots +_{\square} k'_0 2^{-\delta}) * P$$

скалярний добуток можна реалізувати δ паралельними процесами (потоками).

Розглянемо модель реалізації скалярного добутку з використанням розпаралелювання скалярного множення точки еліптичної кривої.

Нехай для скалярного множення обрано скаляр k, який поданий у вигляді бітової строки довжиною n. Представимо значення скаляру k послідовністю ω-бітових слів α_i, довжина якої дорівнює δ, $k = \alpha_1||\alpha_2||\alpha_3||\ldots||\alpha_\delta$. В такому випадку число $\delta = \frac{n}{\omega}$.

Позначимо процес множення точки на скаляр, що виконує обчислювач (регістр) або ядро процесора, pr_i, де $1 \le i \le N_{pr}$, N_{pr} – кількість процесів, якими реалізований скалярний добуток (складність обчислювальної системи). Позначимо час виконання скалярного множення точки P кривої як t_k. З метою зменшення обчислювальної складності або часу t_k необхідно розрахувати значення параметру N_{pr} залежно від значення ω та δ. Проведемо обчислення залежності t_k від ω та δ на ПЕОМ з параметрами Processor 11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz, 2496 Mhz, 8 Core(s), 16 Logical Processor(s) Installed Physical Memory (RAM) 40.0 GB.

Приклад наведено у таблицях 2, 3.

Таблиця 2

Параметри еліптичної кривої та базової точки для проведення експерименту

p:	10061
A:	6451
B:	1036
Px:	10056
Py:	9389
scalar 256 bit:	87034285127702403403987564460963533267302939201657370815850986418735890857122
Qx:	3498
Qy:	6874

Таблиця 3

Параметри еліптичної кривої та базової точки для проведення експерименту

ω (біт)	t_k (сек)
4	0.0000419
8	0.0000676
16	0.0001070
32	0.0001969
64	0.0003782
128	0.0006585
256	0.0012763

За результатами експерименту встановлено, що представлення скаляру *k* послідовністю 4-бітових слів надає можливість прискорити операцію скалярного множення *k*P* в 30 разів, завдяки встановленню значення $N_{pr} = 30$.

Операції над ізогеніями еліптичної кривої

Нехай E_1 та E_2 – гладкі еліптичні криві (2) над полем *F*, які визначаються рівнянням (2) з відповідними коефіцієнтами. Кожна крива визначена значеннями: #*E*, Δ, *j*(*E*). Існування ізоморфізмів для еліптичних кривих надає можливість використовувати весь простір еквівалентних кривих для створення більш стійких модифікацій існуючих криптоалгоритмів [14–18]. Ізогенія еліптичної кривої є одним із різновидів ізоморфних трансформацій кривої в еквівалентну.

Визначення 1. Ізогенія еліптичної кривої є неконстантним раціональним відображенням кривої E_1 над скінченним полем *F* в криву E_2, яке також називається груповим гомоморфізмом та подається у вигляді:

$$\phi(x;y) \to \left(\frac{f_1(x;y)}{f_2(x;y)}, \frac{g_1(x;y)}{g_2(x;y)}\right) = \left(\frac{p_{(x)}}{q_{(x)}}, yr(x)\right),$$

де f_1, f_2, g_1, g_2 – поліноми.

Одним із найважливіших для криптографічної стійкості криптоперетворень, які будуються на основі ізогеній, є їхній ступінь, який визначає розмір множини ізоморфних трансформацій.

Визначення 2. Степінь ізогенії – є степенем раціонального відображення, що знаходиться як максимум зі степенів поліномів $p(x)$ та $q(x)$:

$$deg(\phi(x;y)) = max(deg(p(x), deg(q(x)))),$$

де *p(x), q(x)* – поліноми.

Для сепарабельних ізогеній $deg(\phi(x;y)) = \#ker\phi(x;y)$. Якщо криві $E1 = E2,$ то $\phi(x;y)$ – ендоморфізм.

Теорема Tate [19]. Нехай E_1 та E_2 – криві над скінченним полем *F*. Тоді криві E_1 та E_2 є ізогенними кривими тоді і тільки тоді, коли порядки їх груп дорівнюють $\#E_1 = \#E_2$.

Приклад. Для обраної раніше кривої $E_{11,3,4}$ порядку 14 оберемо циклічну підгрупу простого порядку 7. Для обраної кривої над полем F_{11} отримаємо всі ізоморфні криві

порядку 14, як мають у своєму складі підгрупу порядку 7. Кількість таких кривих для визначених умов дорівнює кількості пар коефіцієнтів *A* та *B*, для яких порядок циклічної підгрупи однаковий. Для обраних параметрів в таблиці 4 наведено трансформації всіх кривих ізоморфних базовій кривій $E_{11,3,4}$, де *n* – порядок кривої над полем характеристики 11.

Таблиця 4

n	*6*	*7*	*8*	*9*	*10*	*11*	*13*	*14*	*15*	*16*	*17*	*18*
A, B	*1, 8*	*2, 7*	*1, 9*	*1, 4*	*1, 10*	*1, 5*	*1, 6*	*1, 1*	*1, 7*	*1, 2*	*2, 4*	*1, 3*
	3, 10	*6, 6*	*2, 10*	*2, 2*	*2, 5*	*2, 8*	*2, 3*	*2, 6*	*2, 9*	*2, 1*	*6, 5*	*3, 1*
	4, 2	*7, 2*	*3, 3*	*3, 5*	*3, 7*	*3, 9*	*3, 2*	*3, 4*	*3, 6*	*3, 8*	*7, 9*	*4, 9*
	5, 6	*8, 10*	*4, 5*	*4, 1*	*4, 8*	*4, 4*	*4, 7*	*4, 3*	*4, 10*	*4, 6*	*8, 1*	*5, 5*
	9, 7	*10, 8*	*5, 4*	*5, 3*	*5, 2*	*5, 1*	*5, 10*	*5, 9*	*5, 8*	*5, 7*	*10,3*	*9, 4*
			6, 7	*6, 8*	*6, 9*	*6, 10*	*6, 1*	*6, 2*	*6, 3*	*6, 4*		
			7, 6	*7, 10*	*7, 3*	*7, 7*	*7, 4*	*7, 8*	*7, 1*	*7, 5*		
			8, 8	*8, 6*	*8, 4*	*8, 2*	*8, 9*	*8, 7*	*8, 5*	*8, 3*		
			9, 1	*9 ,9*	*9, 6*	*9, 3*	*9, 8*	*9, 5*	*9, 2*	*9, 10*		
			10, 2	*10, 7*	*10, 1*	*10, 6*	*10, 5*	*10, 10*	*10, 4*	*10, 9*		

Зафіксуємо значення порядку кривої $n = 6$ та отримаємо всі ізоморфні трансформації точок для кожної ізоморфної кривої (табл. 5).

Таблиця 5

A_i, B_i	$\{P_i\}$	$\{P_i\}$	$\{P_i\}$	$\{P_i\}$	$\{P_i\}$	$\{P_i\}$
1, 1	*(0, 1)*	*(3, 3)*	*(6, 6)*	*(6, 5)*	*(3, 8)*	*(0, 10)*
2, 6	*(1, 3)*	*(10, 6)*	*(5, 3)*	*(5, 8)*	*(10, 5)*	*(1, 8)*
3, 4	*(0, 2)*	*(4, 6)*	*(8, 1)*	*(8, 10)*	*(4, 5)*	*(0, 9)*
4, 3	*(0, 5)*	*(5, 4)*	*(10, 8)*	*(10, 3)*	*(5, 7)*	*(0, 6)*
5, 9	*(0, 3)*	*(1, 9)*	*(2, 7)*	*(2, 4)*	*(1, 2)*	*(0, 8)*
6, 2	*(3, 5)*	*(5, 6)*	*(6, 10)*	*(6, 1)*	*(5, 5)*	*(3, 6)*
7, 8	*(3, 1)*	*(8, 2)*	*(4, 1)*	*(4, 10)*	*(8, 9)*	*(3, 10)*
8, 7	*(1, 4)*	*(9, 7)*	*(2, 8)*	*(2, 3)*	*(9, 4)*	*(1, 7)*
9, 5	*(0, 4)*	*(9, 1)*	*(7, 2)*	*(7, 9)*	*(9, 10)*	*(0, 7)*
10, 10	*(4, 2)*	*(7, 4)*	*(9, 2)*	*(9, 9)*	*(7, 7)*	*(4, 9)*

Обчислимо ізогенію для ізоморфних кривих E_1: $y^2 = x^3 + x + 1$ та E_2: $y^2 = x^3 + 4x + 13$, побудованих над скінченним полем F_{19}, та перевіримо правильність ізоморфної трансформації точок кривої E_1.

Приклад. Нехай скінченне поле буде F_{19}, а криві над цим полем E_1: $y^2 = x^3 + x + 1$ та E_2: $y^2 = x^3 + 4x + 13$. Порядок кривих E_1 та E_2 дорівнює $\#E_1 = \#E_2 = 21$, інваріанти кривих дорівнюють один одному, $j(E_1) = j(E_2)$. Для заданої кривої була обчислена гомоморфна трансформація, а саме вирази $f1(x;y)$, $f2(x;y)$, $g1(x;y)$, $g2(x;y)$:

1. $f1(x; y) = x^3 - 4x^2 - 8x - 8$;
2. $f2(x; y) = x^3 - 4x + x$;
3. $g1(x; y) = x^3y - 6x^2y + 5xy - 6y$;
4. $g2(x; y) = x^3 - 6x^2 - 7x - 8$.

Ступінь знайденої ізогенії дорівнює 3.

Обчислення ізогенії еліптичної кривої

Побудуємо ізогенію кривої E_1: $y^2 = x^3 + x + 1 \; mod \; 19$ за допомогою алгоритму Велю з ядром ізогенії C: $\{O, (2, 7), (2, 12)\}$, де ядро ізогенії – це циклічна підгрупа простого порядку.

Алгоритм Велю для ядра C: $\{O, (2,7), (2,12)\}$ кривої E_1

1. Відкинути точку на нескінченності.

2. Знайти C_2 – множини точок парного порядку. R – решта точок. Точок парного порядку в підгрупі C немає.

3. Розбити R на дві частини – R_+ та R_-. Для R_+ обрано точку (2,7). Точка (2,12) обернена до неї, так як $7 = -12 \; mod \; 19$.

4. Отримати множину $S = \{(2,7)\}$. Для кожної точки $Q = (x_Q, y_Q)$ із S знайти v та w.

Цикл виконується лише один раз, оскільки множина S містить лише одну точку $Q = (2,7)$, з координатами $x_Q = 2, y_Q = 7$.

$g_Q^x = 3 * 2^2 + 1 = 13, g_Q^y = -2 * 7 = 5, v_Q = 2 * 13 = 7, u_Q = 5^2 = 6, v = 7,$

$w = 6 + 2 * 7 = 1.$

5. Обчислити коефіцієнти A' та B' для ізогенної кривої E'.

$A' = 1 - 5 * 7 = 4, B' = 1 - 7 * 1 = 13.$

6. Обчислити формулу для раціонального відображення $(x, y) \to (\alpha, \beta)$ з використанням ядра C: $\{O, (2,7), (2,12)\}$ кривої (1):

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2} \right), \alpha = x + \frac{7}{x-2} + \frac{6}{(x-2)^2} = \frac{x^3 - 4x^2 + 11x - 8}{x^2 - 4x + 4};$$

$$\beta = y - \sum_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right), \beta = \frac{x^3 y - 6x^2 y + 5xy - 6y}{x^3 - 6x^2 + 12x - 8}.$$

7. Обчислити $(x, y) \to (\alpha, \beta)$ з використанням C: $\{O, (2,7), (2,12)\}$ кривої E_1: $y\text{^}2 = x\text{^}3 + x + 1 \; mod \; 19$ на E_2: $y^2 = x^3 + 4x + 13 \; mod \; 19$.

Обрано точки кривої E_1 та виконано перевірку правильності ізоморфної трансформації точок кривої. Взято випадкові точки кривої $P_1 = (9;6)$ та $P_2 = (14;2)$. $P_1 + P_2 = P_3 = (5;6)$. Ізоморфною точкою для P_1 на кривій E_2 буде точка $Q_1 = (14;1)$, відповідно $Q_2 = (17;4)$. Обчислимо $Q_1 + Q_2 = Q_3 = (8;5)$. Трансформація точки $P_3 = (5;6)$ на криву E_2 дає точку Q_3, що підтверджує правильність ізоморфної трансформації.

$$\alpha = \frac{x^3 - 4x^2 + 11x - 8}{x^2 - 4x + 4} = 72 * \; 9^{-1} = 72 * 8 \; mod \; 19 = 8 \, , x = 5.$$

$$\beta = \frac{x^3 y - 6x^2 y + 5xy - 6y}{x^3 - 6x^2 + 12x - 8} = -36 * \; 27^{-1} = -36 * 12 \; mod \; 19 = 5, x = 5, \text{y} = 6.$$

Відображення точок кривої E_1: $y^2 = x^3 + x + 1 \; mod \; 19$ на криву E_2: $y^2 = x^3 + 4x + 13 \; mod \; 19$ подано в таблиці 6. З використанням отриманого раніше перетворення φ: $(x, y) \to (\alpha, \beta)$ на основі значень $P_i \in E_1$ були отримані значення $Q_i \in E_2$.

Таблиця 6

Відображення точок кривої E_1 на криву E_2

№	1	2	3	4	5	6	7	8	9	10	11	12
P_i	(0,1)	(7,16)	(14,17)	(0,18)	(7,3)	(14,2)	(5,6)	(10,2)	(16,16)	(5,13)	(10,17)	(16,3)
Q_i	(17, 15)			(17, 4)			(8, 5)			(8, 14)		
№	13	14	15	16	17	18	19	20	21			
P_i	(9,6)	(13,11)	(15,3)	(9,13)	(13,8)	(15,16)	(2,7)	(2,12)	O			
Q_i	(14, 1)			(14, 18)			O					

Таким чином, ізогенія кривої знайдена, побудована операція перетворення точок з використанням ізогенії для E_1 та E_2, що надає можливість її застосування в криптопримітивах.

Оцінка кількості ізогеній для фіксованої форми еліптичної кривої

Для оцінки кількості ізогеній скористаємось кривою (2) над F_{11} і F_{19} та перебираючи всі коефіцієнти кривої A та B, отримаємо кількість ізогеній для кожного випадку, але використаємо лише ізогенії простого порядку. В таблиці 7 наведено фрагмент отриманих даних.

Таблиця 7

F_{11}										
коефіцієнт A	1	1	1	1	1	1	1	1	1	1
коефіцієнт B	1	2	3	4	5	6	7	8	9	10
порядок кривої #E	14	16	18	9	11	13	15	6	8	10
порядок ізогеній	(**2**,**7**)	(**2**,4,8)	(**2**,**3**,6,9,18)	(3,9)	(11)	(13)	(**3**,**5**,15)	(**2**,**3**,6)	(**2**,4)	(**2**,**5**,10)
кількість ізогеній простого порядку N_ϕ	2	1	2	1	1	1	2	2	1	2

Були проведені обчислення для інших значень полів F_{11}, F_{113}, F_{257}, результати яких наведені на рисунках 1–3.

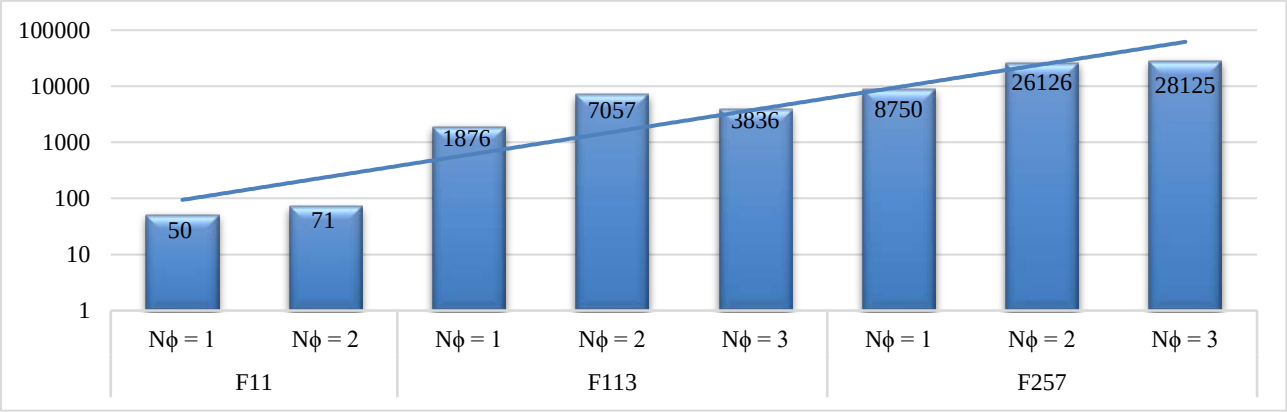

Рис. 1. Оцінка кількості кривих, які мають ядро ізогенії простого порядку (кількість циклічних підгруп простого порядку), $N_\phi = 1,2,3$

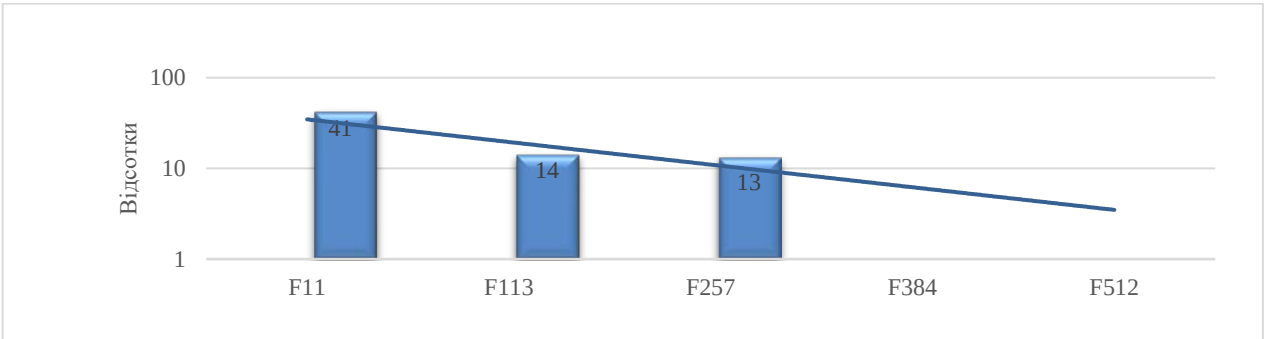

Рис. 2. Залежність кількості кривих, які мають ядро ізогенії простого порядку від #E кривої для $N_\phi = 1$

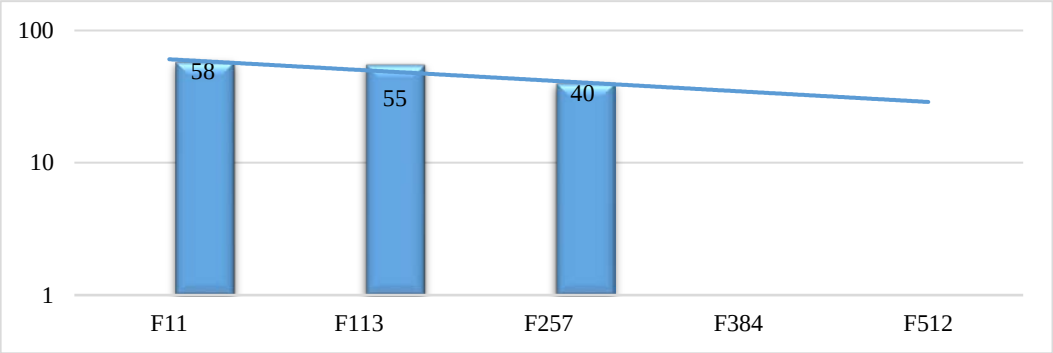

Рис. 3. Залежність кількості кривих, які мають ядро ізогенії простого порядку від #E кривої для N_ϕ = 2

Висновки

Отже, в процесі проведених досліджень було розроблено програмні функції для реалізації операцій над ізогеніями еліптичних кривих різного порядку, які забезпечать зазначені в стандарті рівні безпеки: 256, 384, 512 з урахуванням зростання потужності квантових комп’ютерів. Отримано значення кількості ізогенних еліптичних кривих над простим полем F11, які склали 41 % (50) і 58 % (71) для N_ϕ = 1 і N_ϕ = 2 відповідно, над полем F113 ці значення складають 14 % (1876) і 55 % (7057) для N_ϕ = 1, N_ϕ = 2 відповідно, над полем F257 ці значення складають 13 % (8750) і 40 % (26126) для N_ϕ = 1 і N_ϕ = 2 відповідно від значення характеристики скінченного поля. Визначено, що удосконалення сучасних криптосистем, представлених в якості постквантових кандидатів і побудованих з використанням операцій з ізогеніями еліптичних кривих, можливо завдяки використанню розпаралелювання операцій в групі точок еліптичної кривої та з ізогенією кривої, використанню різноманітних ізогеній еліптичної кривої, потужність яких достатня для використання як додаткових секретних параметрів. Побудовано ізогенію еліптичної кривої третього порядку та отримано ізоморфну трансформацію еліптичної кривої. Отримано апроксимовані значення кількості ізогенних кривих для полів F512, N_ϕ = 2 – 28 % (73400), N_ϕ = 1 – 4 % (10485), F384, N_ϕ = 2 – 33 % (48660), N_ϕ = 1 – 8 % (11796). Підтверджено правильність побудованої ізогенії. Побудовано та перевірено операції для обчислення ізогенії заданого порядку еліптичної кривої, які дозволяють використовувати в майбутньому стандартні рівні безпеки.

Отримані експериментальні значення скалярного добутку з використанням розпаралелювання скалярного множення точки еліптичної кривої дозволили оцінити залежності часу виконання скалярного множення точки кривої t_k від параметрів ω та δ. Розроблена програмна реалізація операцій скалярного множення точки кривої, операцій над ізогеніями еліптичної кривої дозволяє обчислювати значення часу скалярного множення з визначеною потужністю обчислювальної системи, а саме з фіксованим значенням N_{pr} кількості регістрів (ядер процесору). За результатами експериментів було встановлено, що порівняно з класичним підходом до множення точки кривої, представлення скаляру k послідовністю 4-бітових слів прискорило операцію скалярного множення $k*P$ в 30 разів, завдяки встановленню значення складності обчислювальної системи $N_{pr} = 30$. Для 8-бітових слів прискорення склало 18,8 разів.

Перспективою подальших досліджень є розробка методів генерації та верифікації цифрового підпису, генераторів псевдовипадкових послідовностей на основі перетворень над точками ізогенії еліптичної кривої з використанням розпаралелювання операцій скалярного множення точки кривої.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. New York City: Association for Computing Machinery. 1978. Vol. 21, Iss. 2. P. 120–126. ISSN 0001-0782; 1557-7317. DOI: 10.1145/359340.359342.

2. Bernstein D., Lange T., Niederhagen R. Dual EC: A Standardized Back Door // Cryptology ePrint Archive, Report 2015. P. 767. URL: https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf.

3. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Foundations of Computer Science: Conference Publications. 1997. P. 1484–1509.

4. Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange – a new hope // IACR Cryptology ePrint Archive, Report 2015/1092, 2015.

5. Husemöller D., Theisen S., Forster O., Lawrence R. Elliptic Curves, Second Edition // Springer. 2002. P. 487.

6. Edwards H. A normal form for elliptic curves // Bulletin of the American Mathematical Society. Vol. 44, № 3. 2007. P. 393–422.

7. Bernstein D. J., Lange T. Inverted Edwards coordinates // Applied algebra, algebraic algorithms and error-correcting codes: 17th international symposium, AAECC-17, Bangalore, India, December 16-20, 2007, proceedings. LNCS 4851, Springer. 2007. P. 20–27.

8. Schoof R. Elliptic curves over finite fields and the computation of square roots modulo p. Bordeaux: Math. Comput. 1985. № 44. P. 483–494.

9. Schoof R. Counting points on elliptic curves over finite fields. J. Theor. Nombres. Bordeaux 7. 1995. P. 219–254.

10. Чевардин В. Е. Изоморфные трансформации эллиптической кривой над конечным полем // Международный научно-теоретический журнал «Кибернетика и системный анализ». 2013. Том 49, № 3. С. 168–171.

11. Christophe Negre, Jean-Marc Robert. New Parallel Approaches for Scalar Multiplication in Elliptic Curves over Fields of Small Characteristic // IEEE Transactions on Computers. 2015. № 64 (10). P. 2875–2890. URL: https://hal.science/hal-00908463v1/file/parallelization-ecsm8.pdf.

12. Federal Office for Information Security (BSI). BSI – Technical Guideline. Cryptographic Mechanisms: Recommendations and Key Lengths. BSI TR-02102-1. V. 2023-01.

13. Goubin L. A Refined Power-Analysis-Attack on Elliptic Curve Cryptosystems, Proceedings of Public-Key-Cryptography – PKC 2003, Lecture Notes in Computer Science 2567, Springer Verlag, 2003.

14. Stolbunov A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. Adv. in Math. of Comm. 2010. No. 4(2). P. 215–235.

15. Galbraith S., Stolbunov A. Improved algorithm for the isogeny problem for ordinary elliptic curves // Applicable Algebra in Engineering, Communication and Computing. 2013. No. 24(2). P. 107–131.

16. De Feo L., Jao D., Plˆut J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Journal of Mathematical Cryptology (to appear). 2014. URL: http://eprint.iacr.org/2011/506.

17. Costello C., Longa P., Naehrig M. Efficient algorithms for supersingular isogeny Diffie-Hellman // CRYPTO 2016. URL: https://eprint.iacr.org/2016/413.pdf.

18. Rostovtsev A., Stolbunov A. Public-key cryptosystem based on isogenies. URL: https://eprint.iacr.org/2006/145.pdf.

19. Tate J. Endomorphisms of abelian varieties over finite fields // Inventiones Mathematica. 1966. No. 2. P. 134–144.

20. Castryck W., Decru Th. An efficient key recovery attack on SIDH (PDF). In Carmit Hazay; Martijn Stam (eds.). Advances in Cryptology – EUROCRYPT 2023. International Association for Cryptologic Research. Lecture Notes in Computer Science. Vol. 14008. Springer. 2023. P. 423–447. DOI: 10.1007/978-3-031-30589-4_15. ISBN 978-3-031-30589-4.