НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2021 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою

«Математичні методи криптографічного захисту інформації»

зі спеціальності: **113 Прикладна математика**

на тему: **«Оцінки ефективності методів додавання точок еліптичної кривої у формі Едвардса»**

Виконала: Олефір Поліна Юріївна,
студентка II курсу групи ФІ-02мп

Керівник: к.т.н., доцент
Кучинська Наталія Вікторівна _____

Консультант: _____

Рецензент: к.т.н., доцент
_____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2021

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — другий (магістерський)
Спеціальність (освітня програма) — 113 Прикладна математика,
Освітньо-професійна програма «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2021 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Олефір Поліна Юріївна

1. Тема дисертації: «*Оцінки ефективності методів додавання точок еліптичної кривої у формі Едвардса*», науковий керівник дисертації Кучинська Наталія Вікторівна к.т.н., доцент, затверджені наказом по університету №3683-с від «05» листопада 2021р.

2. Термін подання студентом роботи: «__» _____ 2021р.

3. Об'єкт дослідження: *інформаційні процеси в системах криптографічного захисту*

4. Вихідні дані до роботи: *ДСТУ 9041:2020, опубліковані статті для тематики дослідження*

5. Перелік завдань, які потрібно розробити:

1) проаналізувати форми еліптичних кривих та їх властивості, які використовуються у сучасних криптосистемах та криптографічних стандартах;

2) дослідити можливість застосування диференціальних координат Р. Фарашахі для експоненціювання точки кривої у формі Едвардса, яка використовується у стандарті ДСТУ 9041:2020;

3) порівняти ефективність експоненціювання точки залежно від методу додавання точок.

6. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *Презентація доповіді*

7. Орієнтовний перелік публікацій. *Результати роботи частково представлено у матеріалах міжнародної науково-техічної конференції.*

8. Дата видачі завдання: «__» _____ р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Визначення орієнтовної теми дисертації із науковим керівником	Вересень-жовтень 2020 р.	Виконано
2	Огляд опублікованих джерел за темою дослідження	Листопад 2020 р. - лютий 2021 р.	Виконано
3	Дослідити наявні методи експоненціювання точки	Березень - червень 2021 р.	Виконано
4	Застосувати нові диференціальні координати до законів додавання та подвоєння точок еліптичної кривої Едвардса згідно ДСТУ 9041:2020	Вересень 2021 р.	Виконано
5	Обчислити кількость операцій експоненціювання точки за допомогою сходинок Монтгомері з диференціальними координатами	Жовтень 2021 р.	Виконано
6	Порівняти складність експоненціювання точки кривої Едвардса залежно від методу експоненціювання точки	Листопад 2021 р.	Виконано

Студент _____ Поліна Олефір

Науковий керівник _____ Наталія Кучинська

РЕФЕРАТ

Кваліфікаційна робота містить: 44 стор., 1 рисунок, 2 таблиці, 21 джерел.

Метою роботи є порівняння ефективності методів додавання точок еліптичної кривої у формі Едвардса. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є методи підвищення ефективності експоненціювання точки скрученої кривої Едвардса.

У роботі проведено дослідження покращення ефективності обчислення експоненціювання точки кривої Едвардса, шляхом застосування нових диференціальних координат Р. Фарашахі. Наведено оцінку ефективності для кожного способу додавання точок, використовуючи сходи Монтгомері. Було застосовано можливі диференціальні координати Р. Фарашахі до форми еліптичної кривої, яка використовується у стандарті ДСТУ 9041:2020. Обчислено кількість операцій для кожного виду координат з використанням сходів Монтгомері. Надано порівняння ефективності експоненціювання точки еліптичної кривої Едвардса залежно від координат.

ЕЛІПТИЧНІ КРИВІ, КРИВІ ЕДВАРДСА, ДИФЕРЕНЦІАЛЬНЕ ДОДАВАННЯ ТОЧОК, СХОДИ МОНТГОМЕРІ

ABSTRACT

The qualifying paper contains: 44 pages, 1 figures, 2 tables, 21 sources.

The aim of this work is to compare the effectiveness of methods for adding points of an elliptic curve in the form of Edwards. The object of research is information processes in cryptographic security systems. The subject of the research is the methods of increasing the efficiency of scalar multiplication of the point of the twisted Edwards curve.

The work provides research on the improvement of the efficiency of calculating of the elliptic curve in the form of Edwards by applying the new differential coordinates of R. Farashahi. An estimate of the effectiveness is given for each method of adding points, using the Montgomery ladder. Possible differential coordinates of R. Farashahi were applied to the shape of the elliptical curve used in the DSTU 9041:2020. The number of operations is calculated for each type of coordinate using the Montgomery ladder. A comparison of the efficiency of scalar multiplication of the point of the elliptic curve of Edwards depending on the coordinates is given.

ELLIPTIC CURVES, EDWARDS CURVES, DIFFERENTIAL ADDITION OF POINTS, THE MONTGOMERY LADDER

ЗМІСТ

ВСТУП

Актуальність дослідження. Швидкий розвиток технологій вимагає покращення криптографічних алгоритмів та стандартах, які б відповідали сучасним вимогам безпеки. Зазвичай у криптографічних стандартах, зокрема у стандартах цифрового підпису використовуються еліптичні криві у різних формах представлення, наприклад у формі Вейєрштрасса та Монтгомері. Проте дослідження показали, що закон експоненціювання точки для еліптичних кривих у формі Вейєрштрасса та Монтгомері значно повільніший, ніж у формі Едвардса. Тому криві Едварда викликають великий інтерес при проєктуванні криптографічних протоколів та стандартів асиметричного шифрування. Прикладом цього є введений нещодавно в дію національний стандарт України ДСТУ 9041: 2020, який використовує скручені криві Едвардса.

При реалізації криптографічних алгоритмів та протоколів на еліптичних кривих важливо імплантувати операцію скалярного добутку ефективно та безпечно, особливо від атак за стороннім каналом. На сьогодні одним з найефективніших способів протидії такому виду атак є метод Монтгомері. Сходи Монтгомері є швидкими та використовуються в апаратних реалізаціях. Також новий метод реалізації диференціального додавання точок Р. Фарахаші для еліптичних кривих у формі Едвардса є найбільш перспективним, бо показує рекордну швидкість та є стійкими до атак стороннім каналом.

Метою дослідження є порівняння ефективності методів додавання точок еліптичної кривої у формі Едвардса. Для досягнення мети необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити можливість застосування диференціальних координат для експоненціювання точки кривої у формі Едвардса, яка використовується у стандарті ДСТУ:9041;

3) порівняти ефективність експоненціювання точки залежно від координат точок;

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є методи підвищення ефективності експоненціювання точки скрученої кривої Едвардса.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, математичної статистики.

Наукова новизна Вперше для диференціальних координат модифікованої еліптичної кривої у формі Едвардса обчислено ефективність експоненціювання точок.

Практичне значення. Результати цієї роботи можуть застосовуватись у розробці та удосконаленню криптографічних протоколів та стандартів.

Апробація результатів та публікації. Частина результатів була оприлюднена на І Міжнародної науково-технічної конференції «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку», м. Київ, 25 листопада 2021 року, доповідь «Дослідження ефективності методів додавання точок еліптичної кривої у формі Едвардса».

1 ЗАСТОСУВАННЯ ЕЛІПТИЧНИХ КРИВИХ У СУЧАСНИХ КРИПТОСИСТЕМАХ

У даному розділі досліджено еліптичні криві, які застосовуються у сучасних криптосистемах: криві Вейєрштрасса, Монтгомері та криві Едвардса. Розглянуто міжнародні стандарти, які рекомендують до використання криві Едвардса. Проаналізовано алгоритм Монтгомері, який дозволяє швидко та безпечно експоненціювати точку.

1.1 Сучасні форми еліптичних кривих, що використовуються у криптосистемах

В.Міллер та Н.Кобліц запропонували у роботах [3] і [4] використовувати еліптичні криві у криптографії. Еліптичні криві представлені у різноманітних формах: рівняння Лежандра, кубічна форма, форма Вейєштрасса, форма Монтгомері та інші. На сьогодні та на перехідний до постквантового період криптосистеми на еліптичних кривих є одними з найперспективніших, оскільки дозволяють забезпечити аналогійчний рівень криптографічної стікості, використовуючи ключі меншого розміру, у порівнянні з RSA.

1.1.1 Еліптичні криві у формі Е.Вейєрштрасса

Рівняння еліптичної кривої E над скінченним полем K в узагальненій формі Е.Вейєрштрасса:

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

де $a_1, a_2, a_3, a_4, a_6 \in K$, $\Delta \neq 0$, Δ — дискримінант на K.

Над простим полем $K = F_p$, якщо характеристика поля не дорівнює 2 та 3, то рівняння (1.1) можна поділити на 2 та виконати заміну. У результаті цього отримаємо коротку форму рівняння еліптичної кривої у формі Вейєрштрасса:

$$y^2 = x^3 + Ax + B, \tag{1.2}$$

де A,$B \in F_p$, $\Delta = 4a^3 + 27b^2 \neq 0$.

Над полем $K = F_{2^m}$ крива E називається несуперсингулярною кривою, а рівняння (1.1) можна переписати так:

$$y^2 + xy = x^3 + Ax^2 + B, \tag{1.3}$$

де A,$B \in F_{2^m}$, $\Delta = b \neq 0$.

Закон додавання точок $P = (x_1, y_1)$, $Q = (x_2, y_2)$ та подвоєння точки для кривої Вейєрштрасса у формі (1.2) має вигляд:

$$P + Q = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1)$$

$$2P = ((\frac{3x_1^2 + A}{2y_1})^2 - 2x_1, -(\frac{3x_1^2 - A}{2y_1})x_3 + \frac{x_1^2 - Ax_1 - 2B}{2y_1}) \tag{1.4}$$

1.1.2 Криві у формі Монтгомері

Крива Монтгомері над полем $F_q, q = p^m$

$$M_{C,D} : Dv^2 = u^3 + Cu^2 + u, \tag{1.5}$$

де C,$D \in F_q$, $C^2 \neq 4$.

Закон додавання точок $P = (x_1, y_1)$, $Q = (x_2, y_2)$ та подвоєння точки

для кривої Монтгомері (1.5) має вигляд:

$$P+Q=((\frac{y_2-y_1}{x_2-x_1})^2-C-x_1-x_2,(\frac{y_2-y_1}{x_2-x_1})^2(x_1-x_2)-y_1)$$

$$2P=(D(\frac{3x_1^2+2Cx_1+1}{2Dy_1})-C-2x_1,(\frac{3x_1^2+2Cx_1+1}{2Dy_1})(x_1-x_2)-y_1) \quad (1.6)$$

1.1.3 Криві Едвардса

Г. Едвардс представив нормальну форму еліптичних кривих та закон додавання [8], на основі результатів Ейлера та Гауса. При цьому показав, що ті криві, які мають кофактор кратний чотирьом (порядок кривої кратний чотирьом) можуть бути перетворені у нормальну форму.

Оригінальна крива Едвардса, визначена над полем F з характеристикою $p \neq 2$, рівнянням:

$$x^2+y^2=a^2(1+x^2y^2), a \in F \quad (1.7)$$

Закон додавання точок $P=(x_1,y_1)$, $Q=(x_2,y_2)$ та подвоєння точки має вигляд:

$$\begin{aligned} P+Q &= (\frac{x_1y_2+x_2y_1}{a(1+dx_1x_2y_1y_2)}, \frac{y_1y_2-x_1x_2}{a(1-dx_1x_2y_1y_2)}) \\ 2P &= (\frac{2x_1y_1}{a(1+x_1^2y_1^2)}, \frac{y_1^2-x_1^2}{a(1-x_1^2y_1^2)}) \end{aligned} \quad (1.8)$$

Криві існують над полями з ненульовою характеристикою та над скінченними полями F_p. Оберненою точкою до точки $P=(x,y)$ є точка $-P=(-x,y)$). Нейтральним елементом є $(0,a)$. За законом додавання $(x,y)+(-x,y)=(0,a)$. З закону подвоєння маємо точку другого порядку $D_0=(0,-e)$.

Варто зауважити, що у криптографії цікавими є криві над F_q, де $q=p^m$. Але дані криві мають низку недоліків, тому її не рекомендують використовувати у криптологічних додатках. Наведемо недоліки кривих

виду (1.7):

– якщо $e = 1$, то крива не еліптична;

– подвоєння точки $P = (1,1)$ породжує невизначеність для координати y;

– нециклічні криві;

– серед точок 2–го та 4–го є особливі точки (точки на нескінченності)

.

1.1.4 Повні криві Едвардса

Д. Бернстейн та Т. Ланге [5] розширили результат Г. Едвардса та ввели нову форму еліптичної кривої, щоб цим охопити більший клас еліптичних кривих. Автори ввели у рівняння кривої новий параметр d, який є нелишком у полі F_{p^m} з характеристикою $p \neq 2$:

$$E_{e,d} : x^2 + y^2 = e^2(1 + dx^2y^2), \tag{1.9}$$

де $c \neq 0$, $d \neq 0$, $dc^4 \neq 1$.

Закон додавання точок $P = (x_1, y_1)$, $Q = (x_2, y_2)$ та подвоєння точки має вигляд:

$$P + Q = (\frac{x_1y_2 + x_2y_1}{e(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - dx_1x_2y_1y_2)}) \tag{1.10}$$

$$2P = (\frac{2x_1y_1}{e(1 + dx_1^2y_1^2)}, \frac{y_1^2 - x_1^2}{e(1 - dx_1^2y_1^2)}) \tag{1.11}$$

Відсутність особливих точок (повнота закону додавання), циклічна структура кривої — це все свідчіть про кардинально різні властивості кривих (1.7) та (1.9).

Результат вчених Д. Берштейна та Т. Ланге у роботі [5] вперше визначає алгоритм обчислення групових операцій над проєктивними координатами для кривої (1.9). Операція інверсії у полі є досить

складною операцією, тому для криптографічних додатків зручно використовувати проєктивні координати.

Афінну точку (x, y) можна розглядати у проєктивній системі координат $P^2(F_q)$. Точка з проєктивними координатами $(X : Y : Z)$ відповідає точці з афінними координатами $(\frac{X}{Z}, \frac{Y}{Z})$, де $Z \neq 0$. Рівняння кривої (1.9) в проєктивних координатах:

$$(X^2 + Y^2)Z^2 = c^2(Z^4 + dX^2Y^2) \tag{1.12}$$

Нейтральним елементом є точка $(0 : c : 1)$, а оберненим до точки $(X_1 : Y_1 : Z_1)$ є точка $(-X_1 : Y_1 : Z_1)$.

Нехай, $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$, тоді закон додавання (1.10) у проєктивних координатах виражається через наступні формули:

$$\begin{aligned} &A = Z_1Z_2, && B = A^2, && C = X_1X_2, \\ &D = Y_1Y_2, && E = d \cdot C \cdot D, && G = B + E \end{aligned} \tag{1.13}$$

Отримуємо:

$$\begin{aligned} X_3 &= AF((X_1 + Y_1)(X_2 + Y_2) - C - D) \\ Y_3 &= AG(D - C) \\ Z_3 &= C \cdot F \cdot G \end{aligned} \tag{1.14}$$

Нехай, M — обчислювальна складність множення елементів поля, S — обчислювальна вартість піднесення в квадрат, C — вартість множення на константу c, D — вартість множення на константу d, a — вартість додавання. Тоді складність додавання точок у проєктивних координатах (1.14) дорівнює $C(P_1 + P_2) = 10M + 1S + 1C + 1D + 7a$. При змішаному додаванні, коли $Z_2 = 0$, тобто множник $A = Z_1 \cdot Z_2$ можна виключити, то тоді $C(P_1 + P_2) = 9M + 1S + 1C + 1D + 7a$.

Також у роботі [5] наведено вартість подвоєння, яка дорівнює

$C(2P_1) = 3M + 4S + 3C + 6a$.

Отже, загальна складність додавання та подвоєння точок кривої (1.9): $C(P_1 + P_2, 2P) = 13M + 5S + 4C + 1D$.

1.1.5 Скручені криві Едвардса (Twisted Edwards Curves)

У роботі [7] Д. Бернштейна, П. Біркнера та інших представлено скручені криві Едвардса, які є узагальненням повних кривих Едвардса та показали, що вони охоплюють значно більше еліптичних кривих. Ефективність додавання та подвоєння точок є досить високою у порівнянні з повними кривими Едвардса.

Скручена еліптична крива над F_q з $\chi(ad) = \pm 1$, де χ – символ Лежандра, задається рівнянням:

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2 \tag{1.15}$$

де a,$d \in F_q$, $d \neq 1$, $d(a - d) \neq 0$, $p \neq 2$.

Нехай, $P = (x_1,y_1)$ та $Q = (x_2,y_2)$, де $P, Q \in F_q$, тоді закон додавання та подвоєння точок для кривої Едвардса визначено так:

$$P + Q = (\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}) \tag{1.16}$$

$$2P = (\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2}) \tag{1.17}$$

Обернена точка $-P = (-x,y)$, точка порядка два (0,-1), точка порядка чотири $(\pm\frac{1}{\sqrt{a}}; 0)$.

Відповідна скручена крива Едвардса у проєктивній системі координат, де $(X : Y : Z)$ в $P^2(F_q)$ визначається так:

$$(aX^2 + Y^2)Z = Z^4 + dX^2Y^2$$

Додавання у проєктивних координатах записується так

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ та обчислюється за такими правилами:

$$A = Z_1Z_2, \qquad B = A^2, \qquad C = X_1X_2, \qquad G = B + E$$
$$D = Y_1Y_2, \qquad E = dCD, \qquad F = B - E.$$

Отримуємо:

$$\begin{aligned} X_3 &= AF((X_1 + Y_1)(X_2 + Y_2) - C - D) \\ Y_3 &= AG(D - aC) \\ Z_3 &= FG \end{aligned}$$

Складність закону додавання $10M+1S+2D$, де M — обчислювана вартість множення у полі, S — обчислювана вартість піднесення в квадрат, D — множення на a та d. Складність подвоєння точки $3M + 4S + 1D$.

Загальна складність додавання та подвоєння точки для скручених кривих Едвардса $C(P+Q,2P) = 13M+5S+3D$, що є меншою у порівнянні з повними кривими Едвардса.

Варто зауважити, що Х. Хісіл та К.Вонг у роботі [11] досліджували покращення ефективності додавання точок у скручених кривих Едвардса виду (1.15) та отримали новий закон додавання точок, а саме:

Нехай, $P = (x_1,y_1)$ та $Q = (x_2,y_2)$, де $P, Q \in F_q$:

$$P + Q = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2x_1}{x_1y_2 - x_2y_1}\right) \tag{1.18}$$

У роботі [11] також було введено розширені проєктивні координати $(X : Y : T : Z)$ для кривої (1.15). При $Z \neq 0$ закон додавання (1.18) виражається розширеними проєктивними координатами за такими

правилами: $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, $t = \frac{xy}{Z}$, $T = \frac{XY}{Z}$. Тоді:

$$\begin{aligned} X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2) \\ Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2) \\ T_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2) \\ Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2) \end{aligned} \tag{1.19}$$

Складність додавання точок $9M + 1U$, де U — складність множення на параметри кривої. Цей результат є меншим, ніж у роботі Д. Бернштейна та П. Біркнера. Але закон додавання (1.18) містить особливі точки, при яких знаменник дорівнює нулю.

1.2 Класифікація кривих Едвардса

Крива Монтгомері (1.5) шляхом раціонального перетворення координат [7], [6]: $y = u, x = u - 1 \to u = 1 + x, v = u$ відображається в біраціонально еквівалентну узагальнену криву у формі Едвардса задану рівнянням:

$$E_{a,d} : x^2 + ay^2 = 1 + dx^2y^2, \tag{1.20}$$

де a,$d \in F_q$, $d \neq 1$, $a \neq d$, $p \neq 2$.

А. Бессалов у роботі [6] запропонував змінити x на y у рівнянні скрученої кривої Едвардса (1.15), тоді закон додавання та подвоєння точок наступний:

Закон додавання точок $P = (x_1, y_1)$, $Q = (x_2, y_2)$ та подвоєння точки має вигляд:

$$P + Q = (\frac{x_1y_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}) \tag{1.21}$$

$$2P = (\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}) \tag{1.22}$$

Якщо $-P = (x, -y)$ обернена точка, тоді згідно (1.21) нейтральний елемент

групи точок $O = (x,y)+(x,-y) = (1,0)$. Точка другого порядку згідно (1.22) визначається як $2D_0 = (1,0)$.

Параметри a та d визначають властивості еліптичної кривої у формі Едвардса, тому залежно a та d визначають точки кривої. А саме, особливі точки на нескінченності, якщо $\chi(ad) = 1$, $\chi(d) = 1$: точки другого порядку $D_{1,2} = (\pm\sqrt{\frac{a}{d}},\infty)$, точки четвертого порядку $\pm F_1 = (-\infty, \pm\frac{1}{\sqrt{d}})$. Точки на осі точки 4–го порядку $\pm F_0 = (0, \pm\frac{1}{\sqrt{a}})$, для яких $\pm 2F_0 = D_0 = (-1,0)$ та $\chi(a) = 1$.

Якщо $\chi(ad) = -1$, де χ– символ Лежандра, крива (1.20) ізоморфна повній кривій Едвардса [5] з одним параметром d:

$$E_d : x^2 + y^2 = 1 + dx^2y^2, \chi(d) = -1, d \neq 0, 1 \tag{1.23}$$

де $\chi(d) = -1, d \neq 0, 1$.

Якщо $\chi(ad) = 1$ та $\chi(a) = \chi(d) = 1$, то маємо, що крива Монтгомері (1.5) ізоморфна квадратичній кривій Едвардса [6]:

$$E_d : x^2 + y^2 = 1 + dx^2y^2, \tag{1.24}$$

де $\chi(d) = 1, d \neq 0, 1$. А. Бессалов у роботі [6] дослідив властивості еліптичної кривої у формі Едвардса в залежності від параметрів a, d та запропонував нову класифікацію кривих, що дозволило розділити їх на класи, які не перетинаються. Хоча Д. Берштейн у роботі [7] не розділяє криві Едвардса на окремі класи.

Розділення на класи та доведення їх базується на бірaціональній еквівалентності кривої Монтгомері та кривої Едвардса, яка доведена у роботі [7].

Маємо:

$$\begin{aligned} C &= 2\frac{a+d}{a-d}, & D &= \frac{4}{a-d}, & C^2 &\neq 4, \\ a &= \frac{C+2}{D}, & d &= \frac{C-2}{D} \end{aligned} \tag{1.25}$$

Якщо виконати заміну параметрів D та C у рівнянні кривої Монтгомері (1.5), то отримаємо біраціонально еквівалентну скручену криву Едвардса.

Коротко опишемо випадки розділення на класи кривих Едвардса.

Перший випадок класу кривих Едвардса з умовою $\chi(ad) = -1$. Криві цього класу — циклічні криві. Для дослідження цих кривих у роботі [6] розглядають дві можливі комбінації параметрів a та d: у першому випадку — a – нелишок за $\pmod p$ та d – лишок за $\pmod p$, у другому випадку — a – лишок за $\pmod p$ та d – нелишок за $\pmod p$. Дані комбінації параметрів з заміною $d \to d^{-1}$ утворюють клас ізоморфних повних кривих Едвардса з параметром $a = 1$. З такою комбінацією параметрів (тобто заміною a на d) утворює пару квадратичного крутіння.

Щодо класу кривих з $\chi(ad) = 1$, то вони нециклічні. Також розглядається два випадки комбінації параметрів: $\chi(a) = \chi(d) = -1$ та $\chi(a) = \chi(d) = 1$, які мають кардинально різні властивості. Еліптичні криві з умовою $\chi(a) = \chi(d) = -1$ не містять точок четвертого порядку при $p = 1 mod 4$. Щодо другого випадку криві містять чотири точки або вісім точок четвертого порядку, серед яких міститься дві особливі точки. Ці можливі випадки комбінації параметрів утворюють пару квадратичного крутіння, де $a \to ca$ та $d \to cd$, $\chi(c) = -1$.

Отже, ті криві, які є ізоморфними кривим з параметром $a = 1$ А.Бессалов у роботі [6] запропонував розділяти на два класи, а саме повні криві Едвардса з умовою $\chi(d) = -1$ і квадратичні криві Едвардса з умовою $\chi(d) = 1$. А під терміном скручені криві Едвардса мати на увазі криві, що мають умову $\chi(a) = \chi(d) = -1$.

Класи кривих Едвардса залежно від параметрів кривої:

1) повні криві Едвардса з $\chi(ad) = -1$;

2) скручені криві Едвардса з $\chi(a) = \chi(d) = -1$;

3) квадратичні криві Едвардса з $\chi(a) = \chi(d) = 1$.

Важливо відмітити, що для криптологічних додатків підбирають криві порядку $N = 4n$, якщо число n–непарне. Якщо криві повні з $\chi(ad) = -1$, то половина цих кривих мають порядок $N = 4n$. Вони

циклічні та мають порядок кратний чотирьох. Якщо $\chi(a) = \chi(d) = 1$, то криві не циклічні і мають три точки 2–го порядку та чотири точки 4–го порядку. Тому ця група кривих містить нециклічну підгрупу порядка 8. Отже, криві з порядком $N = 4n$ необхідно вибирати серед групи скручених кривих Едвардса з умовою $\chi(a) = \chi(d) = -1$.

У роботі [9] зазначається, що при $p = 1mod4$ всі скручені криві Едвардса з умовою $\chi(a) = \chi(d) = -1$ мають порядок $N = 4n$, де n–непарне.

Унікальним для скручених кривих Едвардса є те, що генератор G знаходиться подвоєнням точки P. Оскільки будь-яка точка P нециклічної кривої має порядок n чи $2n$.

Максимальної ефективності групових операцій можна досягнути, якщо вибрати параметр $a \in \{2, 3\}$ [6].

$\frac{3}{8}$ кривих Едвардса з кофактором 4 безпечно використовуються у криптологічних додатках.

1.3 Кількість кривих Едвардса [16]

Варто зауважити, що криві Едвардса і криві Монтгомері бірaціонально еквівалентні, якщо вони мають точки четвертого порядку при $p \equiv 3mod4$ [6]. Для скрученої кривої Едвардса з $\chi(ad) = -1$ порядок кривої $N_t \equiv 0mod8$. Для кривої з порядком $N_t \equiv 0mod8$ квадратичним крученням є крива з умовою $\chi(ad) = 1$ та її порядок $N_E \equiv 0mod8$. Тому сума числа точок пари квадратичного крутіння при $p \equiv 3mod4$ [6] рівна $N_E + N_t = 2(p + 1) = 2(4k + 3 + 1) \equiv 0mod8$. А сума числа точок пари квадратичного крутіння при $p \equiv 1mod4$ [6] рівна $N_E + N_t = 2(p + 1) = 2(4k + 1 + 1) \equiv 0mod4$.

Таблиця 1.1 – Кількість кривих з мінімальним кофактором 4 для різних p

Модуль поля	Клас кривої	Кількість кривих
$p \equiv 1 mod 4$	повні	$\frac{(p-5)}{4}$
	скручені	$\frac{(p-5)}{4}$
$p \equiv 3 mod 4$	повні	$\frac{(p+1)}{4}$

1.4 Міжнародні стандарти, які використовують еліптичні криві Едвардса

Зазвичай у криптографічних стандартах, зокрема цифрового підпису використовуються еліптичні криві у різних формах представлення. Проте дослідження різних форм еліптичних кривих, показали, що закон експоненціювання точки для еліптичних кривих у формі Вейерштараса та Монтгомері значно повільніший, ніж в еліптичних кривих у формі Едвардса. Перевагою використання кривих Едвардса є застосування однорідного закону додавання. Для кривих Вейєрштраса додавання двох різних точок і додавання двох однакових точок (тобто подвоєння) здійснюється за різними формулами. При цьому швидкість виконання цих операцій також різна. Вплив цієї різниці на швидкість високорівневих криптографічних операцій може призвести до атак сторонніми каналами. Закон додавання на кривих Едвардса не має цієї особливості. Також для кривих Едвардса властива ефективність операцій у групі точок. У наслідок цього ця перевага допускає побудову більш швидких реалізацій.

Стандарт цифрового підпису виданий NIST

У США Д. Берштейном, Т. Ланде було розроблено алгоритм цифрового підпису EdDSA (Edwards-curve Digital Signature Algorithm) на основі скручених кривих Едвардса [18].

E/F_q — еліптична крива Едвардса ($Ed25519$) над простим полем

2^{255-19} має порядок кривої рівний $2^c L$, де $c = 3$ та

$$L = 2^{252} + 27742317777372353535851937790883648493$$

. Еліптична крива, яка використовується у стандарті, задається рівнянням:

$$-x^2 + y^2 = 1 - \frac{121665}{121666} x^2 y^2, \tag{1.26}$$

Крива E/F_q біраціонально еквівалентна кривій Монтгомері (відома як $Curve25519$) з перетворенням координат:

$$\begin{aligned} x &= \frac{u}{v} \cdot \sqrt{-486664} \\ y &= \frac{u-1}{u+2} \end{aligned} \tag{1.27}$$

Крива Монтгомері ($Curve25519$) задається рівнянням:

$$y^2 = x^3 + 486662x^2 + x \tag{1.28}$$

Стандарт ГОСТ Р 50.1.114-2016

Стандарт ГОСТ Р 50.1.114-2016 [19] — це стандарт Російської Федерації «Параметри еліптичних кривих для криптографічних алгоритмів та протоколів». Параметри, для еліптичної кривої у формі Едвардса, які надаються у стандарті, рекомендується застосовувати спільно з алгоритмами формування та перевірки електронного цифрового підпису відповідно до ГОСТ Р 34.10, а також з алгоритмами узгодження ключів при захисті інформації.

У стандарті рекомендуються використовувати еліптичну криву Едвардса у формі (1.2), можливі комбінації та значення наведені у стандарті, а саме p — модуль еліптичної кривої, e,d — коефіцієнти рівняння скрученої еліптичної кривої у формі Едвардса, m — порядок групи точок, q — порядок циклічної групи, (u,v) — координати точки P,

яка належить скрученій кривій Едвардса.

ДСТУ 9041:2020

ДСТУ:9041 [17] — це національний стандарт України «Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених кривих Едвардса». Даний стандарт надає алгоритм шифрування коротких повідомлень (інкапсуляції ключів) на еліптичних кривих у формі Едвардса над простими полями.

Скручена крива Едвардса над полем F_p, яка використовується у стандарті з рекомендованими параметрами, задається рівнянням:

$$x^2 + 2y^2 = 1 + dx^2y^2, \tag{1.29}$$

де $a = 2, d \in \overline{Q_p}$, а $\overline{Q_p}$ — множина квадратичних нелишків за модулем p ($p \equiv 5 mod 8$), $a \neq d$, d — найменший квадратичний нелишок за якого порядок кривої дорівнює $4n$.

Висновки до розділу 1

У даному розділі розглянуто форми еліптичних кривих у афінних та проєктивних координатах, які застосовуються у сучасних криптосистемах. Особливо розглянуто еліптичні криві Едвардса, які на сьогодні є найбільш перспективними у розробці криптографічних алгоритмів та стандартах. Наведена класифікація кривих Едвардса та їх перевага у порівнянні з іншими еліптичними кривими. Також розглянуто форми кривих Едвардса, які використовуються у міжнародних стандартах, особливо у стандарті Україні ДСТУ 9041:2020. Наведено оцінки ефективності обчислення експоненціювання точок еліптичних кривих. У результаті дослідження оцінок складності експоненціювання точки все ж таки залишається відкритим питання покращення швидкості обчислення скалярного множення в алгоритмах криптосистем на еліптичних кривих.

2 ПОРІВНЯННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ДИФЕРЕНЦІАЛЬНИХ КООРДИНАТ ДО ЕЛІПТИЧНОЇ КРИВОЇ У ФОРМІ ЕДВАРДСА

У даному розділі розглянуто новий метод диференціального додавання точок для еліптичних кривих у формі Едвардса, а саме диференціальні координати Р. Фарашахі. Новий метод покращує ефективність обчислення добутку точки на скаляр (або експоненціювання точки). Досліджено застосування диференціальних координат Р. Фарашахі до форми еліптичної кривої згідно ДСТУ 9041:2020. Отримано оцінки кількості операцій для кожного виду координат, особливо з використанням сходинок Монтгомері для протидії атакам за побічним каналом. Також зроблено висновок, які координати є кращими.

2.1 Метод бінарного експоненціювання

Скалярне множення є найважливішою, ресурсовитратною, часовитратною операцією над еліптичними кривими, тому на сьогодні існує багато алгоритмів пришвидшення експоненціювання точки еліптичної кривої. Скалярне множення над еліптичними кривими використовується в алгоритмах цифрового підпису ($ECDSA$) [20] та багатьох інших криптографічних протоколах. Головним при реалізації таких протоколів є виконання операції скалярного добутку ефективно та безпечно.

Нехай, E — еліптична крива над над скінченним полем F_q, P,$Q \in E$, k — задане ціле число.

Скалярне множення (або експоненціювання точки) — це k-кратне

додавання точки P:

$$Q = kP = \underbrace{P + P + \ldots + P}_{k \text{ раз}}$$

Найпростішим способом виконання скалярного множення kP еліптичної кривої є бінарні алгоритми, які є аналогом піднесення до квадрата та множення за модулем [21].

Метод бінарного експоненціювання базується на тому, що ціле число k представляється як $k = k_{l-1}2^{l-1} + k_{l-2}2^{l-2} + \ldots + k_0$, де $k_{l-1} = 1$ та $k_i \in \{0,1\}$, $i = 0,1,2,\ldots,l-1$. Далі метод перебирає біти точки k зліва на право, якщо біт дорівнює одиниці, то виконується додавання точок та подвоєння точки, якщо біт рівний нулю, то тільки подвоєння. Після перебору всіх бітів отримуємо $Q = kP$. Бінарний метод вимагає $l-1$ подвоєнь точки та $\frac{l-1}{2}$ додавань точок.

Наприклад, нехай $k = (109)_{10} = (1101101)_2$. Обчислимо $109P$:

$$\begin{gathered} P \\ 2P + P \\ 2\left(2P + P\right) \\ 2\left(2\left(2P + P\right)\right) + P \\ 2\left(2\left(2\left(2P + P\right)\right) + P\right) + P \\ 2\left(2\left(2\left(2\left(2P + P\right)\right) + P\right) + P\right) \\ \underbrace{2\left(2\left(2\left(2\left(2\left(2P + P\right)\right) + P\right) + P\right)\right) + P}_{} \\ \Downarrow \\ 109P \end{gathered}$$

Рисунок 2.1 – Множення точки на скаляр методом бінарного експоненціювання

2.2 Диференціальне додавання точок та сходи Монтгомері

Зазвичай обчислення kP для точки P на еліптичній кривій E над скінченним полем F_q і заданим цілим числом k виконується рекурсивно

за допомогою формул додавання та подвоєння точок. Але даний метод не є ефективним, оскільки різниця в часі між реалізацією додавання та подвоєння може виявити інформацію про біти k. Це робить даний метод незахищеним від атак сторонніми каналами.

Одним зі способів обчислення скалярного добутку є сходи Монтгомері, які є стійкими до атак за побічним каналом і досить швидкими. Стійкість до атаки пояснюється тим, що на кожному етапі алгоритму, незалежно від поточного обробленого біта скаляра k, виконується одночасно операція подвоєння однієї точки, а також операція додавання. З кожною ітерацією змінюється лише порядок обчислення бітів. Таким чином, для захисту від атак стороннім каналом, сходи Монтгомері широко використовуються, особливо в апаратних реалізаціях.

Було запропоновано декілька модифікацій основних операцій додавання та подвоєння точок. Введемо деякі означення:

Нехай E — еліптична крива над F_q та $P, Q \in E(F_q)$. Тоді диференціальне додавання точок P та Q — це обчислення $P + Q$ та $Q - P$.

Нехай, w — раціональна функція з координатами в $E(F_q)$, де $w(P) = w(-P)$ для будь-якої точки P з $E(F_q)$. Диференціальне додавання та подвоєння w-координат означає обчислення $w(P + Q)$ та $w(2Q)$ через задані значення $w(P)$ та $w(Q)$ та обчислення $w(P - Q)$, де $P, Q \in E(F_q)$.

Алгоритм 2.1. Алгоритм Монтгомері
Вхід: $k = \sum_{i=0}^{m-1} k_i 2^i$ і $k_i \in \{0,1\}$, $k = (k_{m-1}, k_{m-2}, \ldots, k_0)_2$, $P \in F_q$
Вихід:kP
1) $(R_0, R_1) \leftarrow (P, 2P)$
2) для $i = m - 1$ до 0 виконується:
3) якщо $k_i = 0$, то $(R_0, R_1) \leftarrow (2R_0, R_0 + R_1)$
4) якщо $k_i = 1$, то $(R_0, R_1) \leftarrow (R_0 + R_1, 2R_1)$
5) повернути R_0.

Як бачимо, з пунктів алгоритму 3 та 4 різниця $R_1 - R_0$ ніколи не

змінюється з кроком алгоритму та різниця завжди рівна P [14]. Отже, $R_1 = R_0 + P$. Після i-тої ітерації циклу ми маємо:

$$\begin{aligned} R_0 &= (k)_i P, \\ R_1 &= ((k)_i + 1)P, \end{aligned} \tag{2.1}$$

де $(k)_i = \frac{k}{2^i}$.

Формули (2.1) доводять правильність алгоритму: у рядку 7, коли завершили ітерацію, то повертаємось до $R_0 = k_0 P = kP$.

Нехай, $k = 23_{10} = (10111)_2$, тоді у циклі алгоритму Монтгомері отримаємо такі пари R_0,$R_1 : \{2R_0$,$R_1\}, \{3R_0$,$2R_0\}$,$\{6R_0$,$5R_0\}$,$\{11R_0$,$12R_0\}$,$\{23R_0$,$24R_0\}$.

Для кривої Монтгомері (1.5) у роботі [2] було виведено формули для координат суми та подвоєння точки з заданою різницею. Наведемо формули: $P_i = (x_i, y_i), i = \overline{0,4}\ P_0 = P_1 - P_2, P_3 = P_1 + P_2, P_4 = 2P_1$:

$$x_0 x_3 = \frac{(x_1 x_2 - 1)^2}{(x_1 - x_2)^2} \tag{2.2}$$

$$x_4 = \frac{(x_1^2 - 1)^2}{4x_1((x_1 + 1)^2 + (A + 2)x_1)} \tag{2.3}$$

У проєктивних координат $(X : Z)$ формули (2.2) та (2.3) виглядають наступним чином:

$$\begin{aligned} X_3 &= ((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2))^2 \\ Z_3 &= X_0((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2))^2 \\ X_4 &= (X_1 - Z_1)^2 (X_1 + Z_1)^2 \\ Z_4 &= 4X_1 Z_1((X_1 + Z_1)^2 + eX_1 Z_1), e = A + 2 \end{aligned} \tag{2.4}$$

Складність додавання та подвоєння точок

Нехай, M — обчислювальна вартість множення елементів поля, S — обчислювальна вартість піднесення в квадрат, U — вартість множення на константу e. Вартість додавання точок $C(P_1 + P_2) = 3M + 2S$, вартість

подвоєння $C(2P_1) = 2M+2S+1U$. Сумарно $C(P_1+P_2,2P_1) = 5M+4S+1U$.

2.3 Нове диференціальне додавання та подвоєння точок

Р. Фарашахі та С. Хоссейні у роботі [1] запропонували нові формули диференціального додавання та подвоєння для скручених кривих Едвардса. Нові формули додавання та подвоєння точки утворюються шляхом застосування раціональних функцій $w(x,y) = dx^2y^2$ та $w(x,y) = \frac{ax^2}{y^2}$ до звичайних законів додавання та подвоєння точок скрученої кривої Едвардса.

Для $i = 0,1,2,3,4$, нехай $w_i = w(P_i)$, де $P_i \in E(F)$. Позначимо $w_0 = w(P_1 - P_2)$, $w_3 = w(P_1 + P_2)$ та $w_4 = w(2P_1)$. З формул додавання та подвоєння точок (1.17) і (1.17) скрученої кривої Едвардса у формі (1.15) отримано:

$$w_4 = \frac{4w_1((w_1+1)^2 - ew_1)}{(w_1^2-1)^2} \tag{2.5}$$

$$w_3w_0 = \frac{(w_1-w_2)^2}{(w_1w_2-1)^2}, \tag{2.6}$$

де $e = \frac{4a}{d}$.

Якщо w_0 – це елемент поля, а входи w_1, w_2 та виходи w_3, w_4 представлено як дроби для $i = 1,2,3,4 : w_i = \frac{W_i}{Z_i}$, то формули (2.5) та (2.6) у проєктивних координатах наступні:

$$\begin{aligned} \frac{W_4}{Z_4} &= \frac{4W_1Z_1(W_1+Z_1)^2 - eW_1Z_1)}{(W_1-Z_1)^2(W_1+Z_1)^2} \\ \frac{W_3}{Z_3} &= \frac{Z_0(W_1Z_2 - W_2Z_1)^2}{W_0(W_1W_2 - Z_1Z_2)^2}, \end{aligned} \tag{2.7}$$

де $e = \frac{4a}{d}$.

Проєктивні w — координат формули диференціального додавання та подвоєння на одному кроці алгоритму Монтгомері мають загальну

складність, яка дорівнює $C(P_1 + P_2, 2P_1) = 6M + 4S + 1U$.

Якщо встановити $Z_0 = 1$ та виконати наступну заміну у формулах (2.7):

$$A_1 = (W_1 + Z_1) \qquad B_1 = (W_1 - Z_1) \qquad E = A_1^2 + B_1^2$$
$$A_2 = (W_2 + Z_2) \qquad B_2 = (W_2 - Z_2)$$
$$C = A_1 B_2 \qquad D = A_2 B_1$$

Отже, змішані проєктивні w — координат формули диференціального додавання та подвоєння мають вигляд:

$$\begin{aligned} W_4 &= E(A_1^2 - (\frac{e}{4})E) \\ Z_4 &= A_1^2 B_1^2 \\ W_3 &= (C - D)^2 \\ Z_3 &= W_0(C + D)^2 \end{aligned} \tag{2.8}$$

Загальна складність змішаних проєктивних w — координат формул диференціального додавання та подвоєння (2.8) дорівнює $C(P_1 + P_2, 2P_1) = 5M + 4S + 1U$.

2.4 Застосування диференціальних координат до форми кривої згідно ДСТУ:9041

2.4.1 Порівняння швидкості експоненціювання точки кривої Едвардса та кривої Вейєрштрасса

А.Безсалов, Л.Ковальчук, Н.Кучинська у роботі [10] показали можливість застосування раціональної функції, запропонованої Р. Фарашахі, виду $w(x,y) = dx^2y^2$ до законів додавання та подвоєння точок скрученої кривої Едвардса виду (1.20). Також було отримано оцінку ефективності застосування раціональної функції $w(x,y) = dx^2y^2$ на

одному кроці сходів Монтгомері. Оцінка вартості обчислення на одному кроці сходів Монтгомері складає $C(P_1 + P_2,2P_1) = 5M + 4S + 1U$. Якщо прийняти оцінку $1S = 0{,}67$, то $C(P_1 + P_2, 2P_1) = 7{,}67M$.

Також у роботі [10] оцінений виграш у швидкості обчислення експоненціювання точки скручених кривих Едвардса з використанням диференціальних координат Фарашахі у порівнянні з кривими Вейєштрасса. Алгоритм Монтгомері застосовується для будь-якого типу кривої, тому для кривих Вейєштрасса вартість обчислення точки на скаляр на одному кроці сходів Монтгомері складає $C(P_1 + P_2, 2P_1) = 19M + 7S$. Якщо прийняти оцінку $1S = 0{,}67$, то $C(P_1 + P_2, 2P_1) = 23{,}67M$. Отже, потенційний виграш у швидкості обчислення експоненціювання точки з використанням диференціальних координат на кривих Едвардса у порівнянні з кривими у формі Вейєрштрасса дорівнює 3,09 раз. Варто зауважити, що використання класичного методу послідовних подвоєнь та додавань точок скрученої кривої Едвардса забезпечує максимальний виграш у швидкодії до 1,61 раза у порівнянні з кривою Вейєштрасса [12].

2.4.2 Застосування диференціальних координат до кривої Едвардса згідно ДСТУ:9041

Покажемо застосування координати виду $w(x,y) = \frac{ax^2}{y^2}$ до скрученої кривої Едвардса у формі згідно ДСТУ:9041 (1.20).

Додавання та різниця точок

Нехай, $P_i = (x_i,y_i)$, $w_i = w(P_i) = a\frac{x_i^2}{y_i^2} \rightarrow w_i = a\frac{y_i^2}{x_i^2}$. Позначимо, $P_0 = P_1 - P_2$, $P_3 = P_1 + P_2$, $w_0 = w(P_0)$, $w_3 = w(P_3)$. Тоді згідно з (1.21):

$$P_o = (x_0,y_0) = (\frac{x_1x_2 + ay_1y_2}{1 + dx_1x_2y_1y_2}, \frac{-x_1y_2 + x_2y_1}{1 - dx_1x_2y_1y_2}) \tag{2.9}$$

$$P_3 = (x_3,y_3) = (\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}) \tag{2.10}$$

$$w_0 w_3 = (a y_0 x_0^{-1} y_3 x_3^- 1)^2 =$$

$$= a^2 (\frac{-x_1 y_2 + x_2 y_1}{1 - d x_1 x_2 y_1 y_2} \cdot \frac{1 + d x_1 x_2 y_1 y_2}{x_1 x_2 + a y_1 y_2} \cdot \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2} \cdot \frac{1 - d x_1 x_2 y_1 y_2}{x_1 x_2 - a y_1 y_2})^2$$

Після спрощення отримуємо:

$$w_0 w_3 = a^2 (\frac{x_2 y_1 - x_1 y_2}{x_1 x_2 + a y_1 y_2} \cdot \frac{x_2 y_1 + x_1 y_2}{x_1 x_2 - a y_1 y_2})^2$$

$$= a^2 (\frac{(x_2 y_1)^2 - (x_1 y_2)^2}{(x_1 x_2)^2 - (a y_1 y_2)^2})^2 \tag{2.11}$$

Оскільки $w_1 = a(\frac{y_1}{x_1})^2$, $w_2 = a(\frac{y_2}{x_2})^2$ та $a^2 (y_1 y_2)^2 = (x_1 x_2)^2 w_1 w_2$, то підставивши замість y_1, y_2 в (2.11) маємо:

$$w_0 w_3 = (\frac{x_2^2 x_1^2 w_1 - x_1^2 x_2^2 w_2}{(x_1 x_2)^2 - (x_1 x_2)^2 w_1 w_2})^2$$

$$= (\frac{w_1 - w_2}{1 - w_1 w_2})^2 \tag{2.12}$$

Оскільки, $w_0 = w(P)$, то сума двох різних точок обчислюється:

$$w_3 = w(P)^{-1} (\frac{w_1 - w_2}{1 - w_1 w_2})^2 \tag{2.13}$$

Подвоєння точки

Нехай, $P_1 = (x_1, y_1)$, $P_4 = 2P_1$, $w_1 = w(P_1)$, $w_4 = w(2P_1)$.

$$2P_1 = (\frac{x_1^2 - a y_1^2}{1 - d x_1^2 y_1^2}, \frac{2 x_1 y_1}{1 + d x_1^2 y_1^2})$$

Згідно з законом подвоєння маємо:

$$w_4 = a(y_1 x_1^{-1})^2 = a(\frac{2 x_1 y_1}{1 + d x_1^2 y_1^2} \cdot \frac{1 - d x_1^2 y_1^2}{x_1^2 - a y_1^2})^2$$

$$= a(\frac{2 x_1 y_1 (1 - d x_1^2 y_1^2)}{(x_1^2 + a y_1^2)(x_1^2 - a y_1^2)})^2 = a(\frac{2 x_1 y_1 (1 - d x_1^2 y_1^2)}{x_1^4 - a^2 y_1^4})^2 \tag{2.14}$$

Оскільки $y_1^4 = \frac{w_1^2 x_1^4}{a^2}$, то після підстановки в (2.14) та відкривши

квадрат отримуємо:

$$w_4 = \frac{4x_1^2y_1^2(1 - 2dx_1^2y_1^2 + d^2x_1^4y_1^4)}{x_1^8(1 - w_1^2)^2}$$

$$= \frac{4w_1}{(1 - w_1^2)^2} \cdot \frac{(1 + dx_1^2y_1^2)^2 - 4dx_1^2y_1^2}{x_1^4} \tag{2.15}$$

Оскільки $1 + dx^2y^2 = x^2 + ay^2$, то після підстановки виразу у (2.15), маємо:

$$w_4 = \frac{4w_1}{(1 - w_1^2)^2} \cdot (\frac{(x_1^2 + ay_1^2)^2}{x_1^4} - \frac{4dx_1^2y_1^2}{x_1^4})$$

$$= \frac{4w_1}{(1 - w_1^2)^2} \cdot (\frac{x_1^4(1 + w_1)^2}{x_1^4} - \frac{4\frac{d}{a}x_1^4w_1}{x_1^4})$$

Отже, у результаті наведених перетворень отримуємо:

$$w_4 = \frac{4w_1}{(1 - w_1^2)^2} \cdot ((1 + w_1)^2 - 4\frac{d}{a}w_1) \tag{2.16}$$

Наведемо алгоритми знаходження координат точки $Q = kP$ через задане значення w для двох раціональних функцій $w(x,y) = \frac{ax^2}{y^2}$ та $w(x,y) = dx^2y^2$.

Алгоритм 2.2. Алгоритм знаходження координат точки $Q = kP$ через задане значення w для $w(x,y) = dx^2y^2$

Вхід: w

Вихід: $Q = (x,y)$

1) Розв'язати квадратне рівняння для x^2. У яке необхідно підставити

замість y^2 вираз $y^2 = \frac{w}{dx^2}, dx^2 \neq 0$.

$$\begin{gathered} x^2 + ay^2 = 1 + dx^2y^2 \\ x^2 + a\frac{w}{dx^2} = 1 + w \\ x^4 - (1+w)x^2 + \frac{a}{d}w = 0 \\ D = (1+w)^2 - 4\frac{a}{d}w \\ x^2 = \frac{(1+w) \pm \sqrt{D}}{2} \end{gathered} \tag{2.17}$$

2) З двох коренів, які отримали при розв'язанні квадратного рівняння (2.17) обираємо, який є квадратичним лишком, тобто $\chi(x^2) = 1$, де χ — символ Лежандра.

3) Знайти y^2.

4) Обчислити координати точки $Q = kP = (\pm\sqrt{x^2}, \pm\sqrt{y^2})$.

Варто зауважити, що необхідно узгодження процедури однозначного вибору кореня з x^2 та y^2, що дозволить визначити результат експоненціювання точки однозначно.

Алгоритм 2.3. Алгоритм знаходження координат точки $Q = kP$ через задане значення w для $w(x,y) = \frac{ay^2}{x^2}$.

Вхід: w

Вихід: $Q = (x,y)$

1) Розв'язати квадратне рівняння для x^2. У яке необхідно підставити замість y^2 вираз $y^2 = \frac{wx^2}{a}$ та $\frac{d}{a} = 13$.

$$\begin{gathered} x^2 + ay^2 = 1 + dx^2y^2 \\ x^2 + a\frac{wx^2}{a} = 1 + dx^2\frac{wx^2}{a} \\ \frac{d}{a}wx^4 - (1+w)x^2 + 1 = 0 \\ D = (1+w)^2 - w \\ x^2 = \frac{(1+w) \pm \sqrt{D}}{9w} \end{gathered} \tag{2.18}$$

2) З двох коренів, які отримали при розв'язанні квадратного рівняння (2.18) обираємо, який є квадратичним лишком, тобто $\chi(x^2) = 1$, де χ — символ Лежандра.

3) Знайти y^2.

4) Обчислити координати точки $Q = kP = (\pm\sqrt{x^2}, \pm\sqrt{y^2})$.

Варто зауважити, що необхідно узгодження процедури однозначного вибору кореня з x^2 та y^2, що дозволить визначити результат експоненціювання точки однозначно.

2.5 Обчислення складності групових операцій на одному кроці алгоритму Монтгомері скрученої кривої Едвардса

2.5.1 Складність обчислення експоненціювання точки для скрученої кривої Едвардса

Якщо $X = xZ$ та $Y = yZ$, то скручена крива Едвардса виду (1.20) у проєктивних координатах має вигляд:

$$(X^2 + aY^2)Z^2 = Z^4 + dX^2Y^2 \tag{2.19}$$

Для підрахунку ефективності закону додавання точок (1.21) скрученої кривої Едвардса перетворимо афінні координати (x,y) у проєктивні координати $(X : Y : Z)$.

$$\begin{aligned} \frac{X_3}{Z_3} &= \frac{Z_1Z_2(X_1X_2 - aY_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)}{(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)} \\ \frac{Y_3}{Z_3} &= \frac{Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)} \end{aligned} \tag{2.20}$$

Позначимо:

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

Отримуємо:

$$\begin{aligned} X_3 &= AG(D - C) \\ Y_3 &= AF((X_1 + Y_1)(X_2 + Y_2) - C - D) \\ Z_3 &= FG \end{aligned}$$

Отже, складність додавання двох різних точок: $C(P_1+P_2) = 10M+1S+2U$.

Закон подвоєння точок для скрученої кривої Едвардса у проєктивних координатах представимо у вигляді:

$$2(x_1,y_1) = (\frac{x_1^2 - y_1^2}{2 - x_1^2 - y_1^2}, \frac{2x_1y_1}{x_1^2 - y_1^2}) \tag{2.21}$$

Представимо у проєктивних координатах (2.21):

$$\begin{aligned} \frac{X_3}{Z_3} &= \frac{(X_1^2 - Y_1^2)(X_1^2 + Y_1^2)}{(2Z_1^2 - X_1^2 - Y_1^2)(X_1^2 + Y_1^2)} \\ \frac{Y_3}{Z_3} &= \frac{2X_1Y_1(X_1^2 + Y_1^2)}{(2Z_1^2 - X_1^2 - aY_1^2)(X_1^2 + aY_1^2)} \end{aligned} \tag{2.22}$$

Позначимо:

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

Отримуємо:

$$\begin{aligned} X_3 &= DE \\ Y_3 &= 2XYE \\ Z_3 &= DF \end{aligned}$$

Складність подвоєння точки: $C(2P_1) = 3M + 4S + 1U$.

Отже, ефективність звичайного додавання та подвоєння точок на одному кроці Монтгомері дорівнює $C(P_1 + P_2,2P_1) = 13M + 5S + 3U$.

2.5.2 Складність обчислення диференціальних координат Р. Фарашахі

Якщо $w_1, w_2,\ w_3, w_4$ представлено як дроби, то для $i = 1,2,3,4 : w_i = \frac{W_i}{Z_i}$, то формули (2.21) та (2.12) у проєктивних $(W : Z)$ координатах наступні:

$$\frac{W_3}{Z_3} = \frac{Z_0(W_2Z_1 - W_1Z_2)^2}{W_0(W_1W_2 - Z_1Z_2)^2} \tag{2.23}$$

$$\frac{W_4}{Z_4} = \frac{4W_1Z_1((Z_1 + W_1)^2 - 4\frac{d}{a}W_1Z_1)}{(Z_1^2 - W_1^2)^2} \tag{2.24}$$

$$\tag{2.25}$$

Або:

$$\begin{aligned} W_3 &= Z_0((W_1 - Z_1)(W_2 + Z_2) - (W_1 + Z_1)(W_2 - Z_2))^2 \\ Z_3 &= W_0((W_1 - Z_1)(W_2 + Z_2) + (W_1 + Z_1)(W_2 - Z_2))^2 \\ W_4 &= 4W_1Z_1((W_1 + Z_1)^2 - 4\frac{d}{a}(W_1Z_1)) \\ Z_4 &= (W_1 - Z_1)^2(W_1 + Z_1)^2 \end{aligned} \tag{2.26}$$

Отже, w — координат формули диференціального додавання та подвоєння на одному кроці алгоритму Монтгомері у проєктивних координатах мають загальну складність, яка дорівнює ефективність $C(P_1 + P_2,2P_1) = 6M + 4S + 1U + 1I$, де I — це інверсія у полі F_p. Якщо приймемо, що $Z_0 = 1$, то складність буде $C(P_1 + P_2,2P_1) = 5M + 4S + 1U + 1I$.

2.6 Порівняння ефективності групових операцій

Наведемо усі оцінки складності групових операцій еліптичної кривої Едвардса у вигляді таблиці (2.1).

Таблиця 2.1 – Ефективність групових операцій експоненціювання точок на одному кроці сходів Монтгомері

Координати	Кількість операцій
x	$13M + 5S + 3U$
$w(x,y) = dx^2y^2$	$5M + 4S + 1U$
$w(x,y) = a\frac{y^2}{x^2}$	$5M + 4S + 1U + 1I$

Якщо візьмемо обчислювальну складність зведення в квадрат як $1S = 0.67M$, а множення на параметри еліптичної кривої як $1U = 0.5M$, то отримаємо оцінки складності для звичайних координат та координат Р. Фарашахі.

Нехай, C_1 — оцінка складності для звичайного закону додавання точок, тоді $C_1 = 13M + 5 \cdot 0.67M + 3 \cdot 0.5M = 17{,}85M$.

C_2 — оцінка складності для раціональної функції $w(x,y) = dx^2y^2$, $C_2 = 5M + 4 \cdot 0.67M + 1 \cdot 0.5M = 8{,}18M$.

C_3 — оцінка складності для раціональної функції $w(x,y) = a\frac{y^2}{x^2}$, $C_3 = 5M + 4 \cdot 0.67M + 1 \cdot 0.5M = 8{,}18M$.

Виграш у швидкості обчислень у порівнянні $C_1 = C_2$ до C_3 складає 2,18 раз.

Отже, використання w — координат формули диференціального додавання та подвоєння на одному кроці алгоритму Монтгомері у проєктивних координатах прискорюють експоненціювання точки у 2,18 раз. Якщо порівнювати дві раціональні функції між собою, то $w(x,y) = dx^2y^2$ є швидшою за $w(x,y) = a\frac{y^2}{x^2}$ оскільки раціональна функція при обчисленні диференціальної координати вимагає ще додаткової

інверсії у полі.

Підвищити ефективності диференціального додавання у проєктивних координатах Р. Фарашахі можна шляхом мінімізації константи $4\frac{a}{d}$ при $p \equiv 5 mod 8$ [10]. Якщо взяти $d = 2$ як мінімальний квадратичний нелишок простого поля F_p, то методом нарощування квадратичних нелишків можна знайти криву порядку $4n$. І тоді можна знехтувати константою $4\frac{a}{d}$.

Тоді оцінки складності C_2 та C_3 наступні $C_2 = C_3 = 5M+4S = 7{,}68M$ та є однаковими. Отже, виграш у швидкості обчислень у порівнянні C_1 до $C_2 = C_3$ складає 2,32 раз.

2.7 Приклад застосування нових диференціальних координат Р. Фарашахі

Розглянемо криву Монтгомері над F_{17}, яка задана рівнянням:

$$Bv^2 = u^3 + Au^2 + u, \tag{2.27}$$

де $A = 9, B = 1, a = 11, d = 7$.

Оскільки a та d — квадратичні нелишки за $\pmod{17}$, то відповідно умові для класу скручених кривих Едвардса, можемо отримати скручену криву Едвардса над F_{17}:

$$E_{11,7} : x^2 + 11y^2 = 1 + 7x^2y^2 \tag{2.28}$$

Якщо виразити $x^2 = \frac{y^2-1}{7y^2-11}$ та прирівняти чисельник та знаменник до 0, то крива (2.28) при $y^2 = 1$ має точку другого порядку $D_0 = (-1, 0)$. А при $y^2 = 4$ крива (2.28) дві особливі точки порядку два $D_{1,2} = (\pm 2, \infty)$.

Маємо точку $P = (3, -5)$, яка має порядок 5. Використовуючи звичайний закон подвоєння скрученої кривої Едвардса (1.21) та (1.22) маємо: $2P = (-4; 6)$, $3P = (-4; -6)$, $4P = (3; 5)$, $5P = 0$.

Оцінимо кількість операцій при експоненціюванні точки за алгоритмом Монтгомері: при обчисленні $2P = (-4; 6)$: $2M + 2S + 3U + 2I$, при обчисленні $3P = (-4; -6)$: $5M + 2U + 1I$, при обчисленні $5P = (3; 5)$: $5M + 2U + 2I$.

Використовуючи диференціальні координати Р. Фарахаші оцінимо кількість операцій необхідних для експоненціювання точки $P = (3, -5)$ у афінних координатах для різних раціональних функцій.

Щоб обчислити скалярний добуток для точки P у диференціальних координатах з використанням $w = dx^2y^2$ за допомогою алгоритму Монтгомері на кожному кроці алгоритму отримуємо такі пари при $k = (5)_10 = (101)_2$: $\{w_4,w_1\}, \{w_3,w_6\},\{w_8,w_5\}$.

Отже, $w_1 = w(P) = 11$; $w_4 = w(2P) = 3$; $w_3 = w(3P) = 3$; $w_6 = w(4P) = 11$; $w(5P) = 0$

Для експоненціювання точки з диференціальними координатами використовуючи сходи Монтгомері необхідно на першому кроці: $4M + 2S + 2U + 2I$; на другому — $4M + 3S + 1U + 3I$; на третьому — $4M + 4S + 1U + 3I$. Для того, щоб отримати координати точки на останньому кроці алгоритму Монтгомері необхідно $57M + 1S + 2U + 1I$

Щоб обчислити скалярний добуток для точки P у диференціальних координатах з використанням $w = a\frac{ay^2}{x^2}$ на кожному кроці алгоритму Монтгомері отримуємо такі пари $k = (5)_10 = (101)_2$: $\{w_2,w_1\}, \{w_3,w_4\},\{w_6,w_5\}$.

Отже, $w_1 = w(P) = 6$; $w_4 = w(2P) = 12$; $w_3 = w(3P) = 12$; $w_6 = w(4P) = 6$; $w(5P) = 0$.

Для експоненціювання точки з диференціальними координатами використовуючи сходи Монтгомері необхідно на першому кроці: $4M + 2S + 2U + 3I$; на другому — $4M + 3S + 1U + 3I$; на третьому — $4M + 4S + 1U + 3I$. Для того, щоб отримати координати точки $P = (x,y)$ з відповідного значення $w(P)$ для $w = a\frac{ay^2}{x^2}$ необхідно: $58M + 1S + 1U + 1I$.

Висновки до розділу 2

У даному розділі застосовано нові диференціальні координати Р. Фарашахі до формули додавання та подвоєння точок еліптичної кривої Едвардса згідно з формою кривої у ДСТУ 9041:2020. Наведено алгоритми знаходження координат точки на останньому кроці алгоритму Монтгомері з диференціальними координатами. З використанням сходів Монтгомері, оскільки вони забезпечують захист від атак сторонніми каналами, підраховано кількість операцій, у проєктивних координатах необхідних для експоненціювання точки, для звичайного алгоритму додавання та подвоєння точки та алгоритму з диференціальними координатами Р. Фарашахі. Звичайний алгоритм додавання точок вимагає 13 операцій множення точок, 5 піднесень до квадрату та тричі множення на параметри кривої. Дві раціональні функції для експоненціювання точки вимагають 5 операцій множення, 4 піднесення до квадрату та один раз множення на константу, але раціональна функція $w = \frac{ay^2}{x^2}$ вимагає додаткову інверсію у полі. Виграш у швидкості обчислень експоненціювання точки з використанням диференціальних координат Р. Фарашахі до класичного закону додавання у проєктивних координатах складає 2,18 раза. Якщо мінімізувати константу методом описаним у пункті 2.6, то виграш у швидкості складе 2,32 рази.

ВИСНОВКИ

У ході даної роботи проведений аналіз опублікованих джерел за тематикою досліджень еліптичних кривих, які використовуються у сучасних криптосистемах. Проаналізовано форми еліптичні кривих, що використовуються у сучасних криптосистемах: їх властивості, ефективність закону множення точки на скаляр (експоненціювання точки). Розглянуто міжнародні стандарти, що використовують еліптичні криві Едвардса. Проаналізовано вибір та оптимізацію параметрів скрученої кривої Едвардса для криптографічних додатків та стандартів. Аналіз опублікованих джерел показав, що у зв'язку зі швидким розвитком технологій питання безпеки та покращення швидкості обчислення експоненціювання точки в криптосистемах на еліптичних кривих та стандартах, які використовують еліптичні криві залишається відкритим.

У роботі застосовано диференціальні координати Р. Фарашахі до законів додавання та подвоєння точок еліптичної кривої у формі Едвардса, яка використовується у стандарті України ДСТУ 9041:2020. З використанням алгоритму Монтгомері обчислено кількість операцій, необхідних для експоненціювання точки у проєктивних координатах, для звичайного закону додавання точок та для закону додавання з диференціальними координатами Р. Фарашахі. Порівняння ефективності методів експоненціювання точки у проєктивних координатах показало, що використання диференціальних координат Р. Фарашахі дозволяє підвищити швидкість експоненціювання точки еліптичної кривої Едвардса у 2,32 рази у порівнянні зі звичайним законом додавання. На сьогодні алгоритм диференціального додавання точок Монтгомері з використанням проєктивних координат Р. Фарахаші на еліптичних кривих Едвардса є найбільш швидким. Нові диференціальні координати можна рекомендувати до застосування

у стандарті України ДСТУ 9041:2020.

ПЕРЕЛІК ПОСИЛАНЬ

1. Farashahi R.R., Hosseini S.G. Differential addition on twisted Edwards curves // Pieprzyk J., Suriadi S. (eds.) Information Security and Privacy. pp. 366-378. Springer International Publishing, Cham (2017)

2. Montgomery, P.L. Speeding the Pollard and elliptic curve methods of factorization // Math. Comp. 48(177). P. 243–264 (1987).

3. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). doi:10.1007/3-540-39799-X 31

4. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. 48(177), 203–209 (1987)

5. D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves, Lect. Notes Comput. Sci. 4833 (2007) 29–50.

6. Бессалов А. В. Еліптичні криві та криптографія Едвардса, 2017. [Публікація російською мовою].

7. D. J. Bernstein, et al., Twisted Edwards curves, Lect. Notes Comput. Sci. 5023 (2008) 389–405.

8. Edwards,H.M.:A normal form for elliptic curves.Bull.Am.Math. Soc. New Ser. 44(3), 393–422 (2007)

9. Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоэлектроника, 2015 Том 14 No 3, , С.197-203.

10. А.В. БЕССАЛОВ, д-р техн. наук, Л.В. КОВАЛЬЧУК, д-р техн. наук, Н.В. КУЧИНСКАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ДИФФЕРЕНЦИАЛЬНОГО СЛОЖЕНИЯ ТОЧЕК КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА, ISSN 0485-8972 Радіотехніка. 2020. Вип. 203

11. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, and Dawson Ed. Twisted Edwards Curves Revisited. ASIACRYPT 2008, LNCS 5350. – Pp.

326 – 343.

12. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем // Сучасний захист інформації. 2011. No4. С.33-36.

13. Costello, C., Smith, B.: Montgomery curves and their arithmetic: The case of large characteristic fields. IACR Cryptology ePrint Archive, Report 2017/212. Available at http://eprint.iacr.org/2017/212 (2017)

14. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем.//Проблемы передачи информации, - Том 51, вып 4, 2015. С.103-109.

15. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых:// Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

16. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. //Кибернетика и системный анализ, т.51, No2, 2015. С.3-12.

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

18. Simon Josefsson and Ilari Liusvaara: Edwards-Curve Digital Signature Algorithm (EdDSA), 2017, RFC 8032, 1-60

19. Р 1323565.1.024–2019 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов»

20. DonJohnson,AlfredMenezes,andScottVanstone.Theellipticcurve digital signature algorithm (ecdsa). International Journal of Information Security, 1(1):36–63, 2001.

21. Song Y.Yan. NumberTheoryforcomputing.Springer-Verlag,Berlin, 2nd edition, 2002.