

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО”**

Циганкова Оксана Валентинівна

УДК 004.9

**МЕТОДИ ПІДВИЩЕННЯ ШВИДКОДІЇ АСИМЕТРИЧНИХ
КРИПТОСИСТЕМ З ВИКОРИСТАННЯМ ЕЛІПТИЧНИХ
КРИВИХ У ФОРМІ ЕДВАРДСА**

Спеціальність 05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана на кафедрі математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Бессалов Анатолій Володимирович,
Київський університет імені Бориса
Грінченка, професор кафедри інформаційної та
кібернетичної безпеки.

Офіційні опоненти: доктор технічних наук, професор
Яремчук Юрій Євгенович, Вінницький
національний технічний університет Міністерства
освіти і науки України, м. Вінниця, директор
центру інформаційних технологій і захисту
інформації

кандидат технічних наук, професор
Корнейко Олександр Васильович,
Національна академія внутрішніх справ,
Міністерство внутрішніх справ України, м. Київ,
завідувач кафедри інформаційних технологій та
кібербезпеки

Захист відбудеться 28.04.2021 р. о 14 годині на засіданні спеціалізованої вченої ради Д 26.002.29 при КПІ ім. Ігоря Сікорського, 03056 Київ, проспект Перемоги, 37, корпус № 11, аудиторія № 215.

З дисертацією можна ознайомитися в науковій бібліотеці КПІ ім. Ігоря Сікорського за адресою 03056 Київ, проспект Перемоги, 37.

Автореферат розісланий _____ березня 2021 р.

Вчений секретар
спеціалізованої вченої ради Д 26.002.29
доктор технічних наук, професор



Теленик С.Ф.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми

Найважливішим завданням забезпечення інформаційної безпеки держави є створення та підтримання умов, що гарантують захист державних і особистих інформаційних ресурсів, безпечну обробку, зберігання та передачу інформації. На сьогодні неможливо уявити собі забезпечення інформаційної безпеки без застосування криптографічних методів захисту інформації. Більшість сучасних асиметричних криптосистем цифрового підпису (ЦП) побудовано на основі математичного апарату еліптичних кривих, який ґрунтується на складності задачі дискретного логарифмування в групі точок еліптичної кривої. В алгоритмах діючих стандартів ЦП ДСТУ 4145-2002 та ДСТУ ISO/IEC 14888-3:2014 використовуються криптографічні перетворення несуперсингулярних еліптичних кривих у формі Вейєрштрасса. У ДСТУ 4145-2002 використовуються криві у формі Вейєрштрасса над полями характеристики 2. Еліптичні криві, що використовуються в національному стандарті ЦП ДСТУ 4145-2002, наразі відповідають сучасним вимогам безпеки, проте розвиток обчислювальної техніки призвів до постійного зростання об'єму та швидкості передачі інформації, яка потребує захисту і, як наслідок, до можливого зменшення терміну життя існуючих криптосистем.

Значний внесок у розвиток криптосистем на еліптичних кривих зробили такі зарубіжні та вітчизняні вчені: Koblitz N., Menezes A., Edwards H., Washington L., Bernstein D., Lange T., Кочубинський А.І., Бессалов А.В., Ковальчук Л.В., Горбенко І.Д., Чевардін В.Є., Корнейко О.В. та інші, а деякі з них відзначали еліптичні криві у формі Едвардса (далі ЕКФЕ), як оптимальні для використання в асиметричних криптосистемах з точки зору швидкодії та координат подання точок кривих. Завдяки поширеному науковому та практичному інтересу до ЕКФЕ *актуальною* стає задача оновлення існуючих або створення нових методів підвищення швидкодії стійких до криптоатак асиметричних криптосистем саме на кривих у формі Едвардса над простими полями.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася відповідно до планів наукових досліджень кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського в рамках таких науково-дослідних робіт, виконаних на замовлення державних організацій:

- 1) «Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації» (шифр «Мокрель», номер держреєстрації 0115U004118);
- 2) «Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень» (шифр «Кобія», номер держреєстрації 0116U006384);
- 3) «Дослідження, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем» (шифр «Аргус», номер держреєстрації 0117U001817).

Дисертаційна робота також виконувалась в рамках таких науково-дослідних робіт на замовлення Міністерства освіти і науки України:

1) «Дослідження методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціонування» № 2030-п (номер держреєстрації 0117U000500), з 01.01.2017 по 31.12.2019.

2) «Логіко-ймовірнісний підхід в задачах безпеки структурно-складних систем» № 2602-ф (номер держреєстрації 0113U002468), з 01.01.2013 по 31.12.2015.

Тематика роботи включена в науково-технічні плани кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського.

Мета і завдання дисертаційного дослідження.

Метою дисертаційного дослідження є підвищення швидкодії асиметричних криптосистем шляхом розроблення більш швидких за існуючі методів знаходження точок простого порядку та методів зниження складності експоненціювання точки з використанням властивостей еліптичних кривих у формі Едвардса.

Об'єктом дослідження є процеси перетворення інформації за допомогою асиметричних криптосистем, що базуються на складності задачі дискретного логарифмування на еліптичних кривих у формі Едвардса.

Предметом дослідження є властивості еліптичних кривих у формі Едвардса над простими полями та створені на їх основі алгоритми.

Відповідно до поставленої мети у дослідженні вирішувалися такі **основні завдання**:

1. Проаналізувати властивості ЕКФЕ над простими полями з метою знаходження кривих, придатних для застосування у криптоалгоритмах.

2. Розробити методи зниження складності виконання операцій додавання та подвоєння точок ЕКФЕ.

3. Провести порівняльний аналіз складності експоненціювання точки кривих у формі Вейерштрасса та ЕКФЕ.

4. Розробити методи підвищення швидкості знаходження точки простого порядку на ЕКФЕ над простими полями та провести порівняльний аналіз зі стандартними методами знаходження точки простого порядку.

5. Розробити більш швидкі за існуючі алгоритми пошуку генератора криптосистеми та розрахувати загальносистемні параметри кривих, придатних для застосування в асиметричних криптоалгоритмах.

Методи дослідження. Проведені дослідження базуються на використанні основ алгебраїчної геометрії, абстрактної алгебри та теорії чисел (для дослідження властивостей ЕКФЕ, визначення кількості кривих різних класів порядку $4n$, удосконалення класифікації ЕКФЕ, розроблення методів знаходження точки максимального порядку і базової точки, оцінювання складності алгоритмів пошуку генератора криптосистеми), теорії ймовірностей

(для розроблення методів оцінювання швидкодії експоненціювання точки ЕКФЕ і методів її підвищення); теорії алгоритмів (для розроблення алгоритмів знаходження точки простого порядку, оцінювання виграшу роботи алгоритмів).

Наукова новизна отриманих результатів полягає у наступному:

1. Розроблено *нові* методи знаходження точки простого порядку на повних та скручених ЕКФЕ, на основі *нового* методу знаходження порядків випадкових точок кривої Едвардса, які, за результатами порівняльного аналізу зі стандартними методами, швидші за існуючі.

2. *Вперше* отримана оцінка кількості та визначені умови існування ЕКФЕ з корисними властивостями для криптосистем, які доцільно рекомендувати для створення асиметричних криптосистем.

3. *Вперше* отримана оцінка складності експоненціювання точок на кривих у формі Едвардса, яка, у порівнянні з аналітичними оцінками складності експоненціювання точок кривих у формі Вейєрштрасса менша, завдяки чому імплементація алгоритмів на кривих у формі Едвардса швидша за існуючі.

4. *Удосконалено* класифікацію кривих в узагальненій формі Едвардса, в якій, на відміну від існуючої, множину кривих розподілено на три різних класи з різними за квадратичністю параметрами a і d , що надало можливість виявити класи кривих з корисними властивостями для застосування у криптоалгоритмах.

5. *Дістало подальшого розвитку* обчислення загальносистемних параметрів криптостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем в рекомендованих стандартах FIPS-186-2-2000, FIPS-186-4-2013 та ISO/IECCD 15946 простих полях, які можуть бути рекомендовані для використання в алгоритмах асиметричних криптосистем.

Практичне значення отриманих результатів. У результаті виконання дисертаційної роботи отримано такі практичні результати:

- запропоновано використання ЕКФЕ над простими полями в криптоалгоритмах для підвищення швидкодії асиметричних криптосистем;

- розроблено науково обґрунтовані нові методи генерування загальносистемних параметрів криптосистеми на основі арифметики ЕКФЕ, що зменшує кількість та складність групових операцій у 1,6 рази у порівнянні з методами, які використовуються у чинних стандартах ЦП;

- запропоновано новий метод пошуку генератора криптосистеми на скручених ЕКФЕ, який швидше стандартного у $32 (\log n)$ разів де n – порядок генератора;

- розраховано загальносистемні параметри 25 криптостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем, які можуть бути рекомендовані для використання в сучасних асиметричних криптосистемах.

Отримані результати було використано у наукових розробках на замовлення Служби зовнішньої розвідки України, а також впроваджено в навчальному процесі при викладанні навчальної дисципліни «Криптосистеми на

еліптичних кривих» здобувачам вищої освіти Фізико-технічного інституту КПІ ім. Ігоря Сікорського.

Особистий внесок здобувача. Усі результати, що виносяться на захист, отримані автором особисто. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, здобувачу належать:

- модифікація закону додавання точок на ЕКФЕ над простим полем [1, 2, 3, 4, 5, 6, 11, 13];
- побудова методів знаходження точки простого порядку на ЕКФЕ [2, 9];
- застосування подвійної симетрії координат точок для аналізу їх властивостей [3, 13];
- оцінка складності операції подвоєння точок на ЕКФЕ над простим полем [5];
- ідея проведення порівняльного аналізу кількості операцій при експоненціюванні точки на ЕКФЕ та на кривій у формі Вейерштрасса [5];
- постановка задачі пошуку властивостей ЕКФЕ, які дозволяють знайти випадкову точку максимального порядку [5];
- систематизація ознак кривих в узагальненій формі Едвардса [6, 7, 11];
- аналіз особливих точок 2-го порядку ЕКФЕ [7];
- координація завдань виконавців розрахунків [9];
- опис алгоритмів пошуку генератора криптосистеми на ЕКФЕ [8];
- порівняльний аналіз швидкодії створених алгоритмів пошуку генератора криптосистеми з швидкодією чинних алгоритмів стандарту ЦП [10];
- постановка задачі та участь у роботі групи дослідників щодо розрахунку загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим скінченним полем [12];
- розроблення методу реконструкції усіх точок ЕКФЕ, створення графічної ілюстрації скалярного добутку точок при експоненціюванні ЕКФЕ [13];
- участь в аналізі властивостей суперсингулярних повних кривих Едвардса [14];
- вибір параметрів та участь у розрахунку параметрів a і d , побудова методів знаходження точки простого порядку на ЕКФЕ [9].

Апробація результатів дисертації. Основні положення дисертації розглядалися і обговорювалися на засіданнях кафедри математичних методів захисту інформації ФТІ КПІ ім. Ігоря Сікорського та семінару «Проблеми сучасної криптології», що проводиться під егідою НАН України. Результати доповідалися і обговорювалися на:

- XVII Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (26-28 травня 2015р., м. Київ);
- XVIII Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (25-27 травня 2016р., м. Київ);
- XIX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (25-26 травня 2017р., м. Буча);

- XV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (25-27 травня 2017р., м. Київ);
- XX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (22-24 травня 2018р. м. Буча).

Публікації. За матеріалами дисертації опубліковано 14 друкованих праць, з яких 8 статей у наукових фахових виданнях (з них 2 статті у закордонних виданнях, що входять до WoS або Scopus), 5 публікацій матеріалів науково-технічних конференцій.

Структура та обсяг дисертації. Дисертація викладена на 145 сторінках, складається з вступу, чотирьох розділів, висновків, списку використаних джерел з 68 найменувань та 4 додатків. Загальний обсяг дисертації 145 сторінок, в тому числі 116 сторінок основного тексту та 7 сторінок використаних джерел. Робота містить 6 рисунків і 6 таблиць.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження, визначено об'єкт та предмет, сформульовано мету і завдання роботи, визначено наукову новизну і практичне значення отриманих результатів. Подано відомості про публікації, апробацію й впровадження розробок і результатів досліджень.

У **першому розділі** аналізується сучасний стан технологій криптографічного захисту інформації в галузі використання асиметричної криптографії. В результаті аналізу визначено, що стандарти ЦП, в яких використовуються криві у формі Вейерштрасса, можуть бути оновлені за допомогою більш швидких та крипостійких технологій еліптичної криптографії. Обґрунтована доцільність використання специфічних особливостей ЕКФЕ у побудові сучасних криптоалгоритмів. Сформульована постановка науково-технічної проблеми та задач досліджень.

З метою подальшого формулювання та інтерпретації результатів дисертації у розділі також наведено основні положення математичного апарату еліптичних кривих у різних формах та представлень, їх взаємозв'язок та властивості. Наводяться загальні теоретичні властивості ЕКФЕ. Здійснено трансформацію деяких еліптичних кривих, що використовуються в стандартах ЦП, у форму Едвардса. З метою підтвердження належності ЕКФЕ до еліптичних кривих, як алгебраїчних структур, знайдені та доведені умови ізоморфізму цих кривих і кривих у формі Вейерштрасса, що дозволяє стверджувати, що ЕКФЕ задовольняють аналогічним вимогам щодо забезпечення безпеки стосовно розв'язання задачі дискретного логарифмування (DLP). За аналізом, який підтверджує наявність ізоморфізму між ЕКФЕ та кривими у формі Вейерштрасса, наведено теорему щодо визначення точного числа повних кривих Едвардса, ізоморфних кривим у формі Вейерштрасса з ненульовими параметрами a і b .

У **другому розділі** запропоновано модифікацію закону додавання точок ЕКФЕ із заміною позначення координат та розроблена нова класифікація ЕКФЕ над простим полем.

З метою представлення симетрії точок кривої горизонтально відносно осі x , яка має місце в класичній арифметиці еліптичних кривих, закон додавання точок ЕКФЕ модифіковано шляхом взаємної заміни координат $x \leftrightarrow y$, на підставі чого, криву в узагальненій формі Едвардса, визначено рівнянням:

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

Для форми кривої (1) визначено універсальний модифікований закон додавання точок (2):

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \right), \quad (2)$$

та закон подвоєння точок при збігу координат точок (3):

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2} \right). \quad (3)$$

На основі нової модифікації закону додавання точок (1) ЕКФЕ введена арифметика для групових операцій з особливими точками цих кривих, визначено координати точок малих порядків і їх взаємозв'язок з іншими точками кривої.

Використання апарату скінченних полів та алгебраїчної геометрії дозволило здійснити теоретичне дослідження та аналіз ЕКФЕ над простими скінченними полями характеристики $p > 3$. Із застосуванням модифікації закону додавання точок ЕКФЕ було створено нову повну класифікацію кривих в узагальненій формі Едвардса з використанням методу перебору властивостей параметрів кривої за їх квадратичністю (табл.1, табл. 2).

У порівнянні з існуючою класифікацією, запропонованою у роботі «Twisted Edwards Curves» авторами Bernstein D., Birkner P., Joye M., Lange T., Peters C., за якою криві з різними властивостями належали до одного класу, у новій класифікації криві, в залежності від квадратичності параметрів a і d кривої у рівнянні (1), належать до трьох різних класів, що не перетинаються:

- повні криві Едвардса з умовою C1: $\chi(ad) = -1$;
- скручені криві Едвардса з умовами C2.1: $\chi(a) = \chi(d) = -1$;
- квадратичні криві Едвардса з умовами C2.2: $\chi(a) = \chi(d) = 1$.

де χ – квадратичний характер елементу поля.

Нова класифікація дозволила створити повний опис властивостей кривих у формі Едвардса над простими полями (табл.1 та 2), провести аналіз та виявити і описати переваги та недоліки цих кривих з метою застосування їх в асиметричних криптосистемах.

Таблиця 1

Нова класифікація ЕКФЕ над простими полями. Координати точок ЕКФЕ D - 2-го та F - 4-го порядків з мінімальним кофактором порядку кривої N_E .

	Параметри	Клас кривих	Точки 2-го порядку	Точки 4-го порядку
1	$\chi(ad) = -1$			
a	$\chi(a) = 1$ $\chi(d) = -1$	<u>Complete</u> $N_E = 4n$	$D_0 = (-1,0)$	$\pm F_0 = (0, \pm 1/\sqrt{a})$
b	$\chi(a) = -1$ $\chi(d) = 1$			$\pm F_0 = (0, \pm 1/\sqrt{d})$
	$\chi(a) = \chi(d) = 1$	Нові класи		
2	$\chi(a) = -1$ $\chi(d) = -1$	<u>Twisted</u> $N_E = 4n$	$D_0 = (-1,0)$ $D_{1,2} = (\pm\sqrt{a/d}, \infty)$	$\pm F_{2,3} = \left(\pm\sqrt[4]{a/d}, \pm\sqrt{-1/\sqrt{ad}} \right)$ $(p \equiv 3 \bmod 4)$
3	$\chi(a) = 1$ $\chi(d) = 1$	<u>Quadratic</u> $N_E \geq 8n$	$D_0 = (-1,0)$ $D_{1,2} = (\pm\sqrt{a/d}, \infty)$	$\pm F_0 = (0, \pm 1/\sqrt{d})$ $\pm F_1 = (\infty, \pm 1/\sqrt{d})$ $\pm F_{2,3} = \left(\pm\sqrt[4]{a/d}, \pm\sqrt{-1/\sqrt{ad}} \right)$

Таблиця 2

Нова класифікація кривих у формі Едвардса над простими полями.
Умови та класи ізоморфізму

	Параметри	Клас кривих	Ізоморфізм	Клас ізоморфізму
1	$\chi(ad) = -1$		$X^2 + Y^2 = 1 + d'X^2Y^2$	
a	$\chi(a) = 1$ $\chi(d) = -1$	Complete $N_E = 4n$	$d' = a/d \Rightarrow \chi(d) = -1$ $(x, y) \rightarrow (X, Y/\sqrt{a})$ $X^2 + dY^2 = 1 + aX^2Y^2$	$E_{E,a,d} \sim$ $E_{E,1,d/a}$
b	$\chi(a) = -1$ $\chi(d) = 1$		$d' = cd, a' = ca, \Rightarrow \chi(c') = -1$ $(x, y) \rightarrow (X, Y/\sqrt{d})$ $\bar{x}^2 + \bar{y}^2 = 1 + (a/d)\bar{x}^2\bar{y}^2$	$E'_{E,1,d/a} \sim$ $E_{E,1,a/d}$
	$\chi(a) = \chi(d) = 1$	<i>Нові класи</i>		
2	$\chi(a) = -1$ $\chi(d) = -1$	Twisted $N_E = 4n$	$a \leftrightarrow d$	$E_{E,a,d} \sim$ $E_{E,d,a}$
3	$\chi(a) = 1$ $\chi(d) = 1$	Quadratic $N_E \geq 8n$	$d' = a/d \Rightarrow \chi(d) = 1$ $(x, y) \rightarrow (X, Y/\sqrt{a})$ $X^2 + Y^2 = 1 + d'X^2Y^2$	$E_{E,a,d} \sim$ $E_{E,1,d/a}$

За результатами аналізу нових класів ЕКФЕ було визначено кількість кривих і можливих значень їх порядків, які доцільно рекомендувати для використання в криптосистемах. Також було розраховано кількість кривих, що мають мінімальний кофактор порядку кривої 4 та виявлено, що їх близько половини (приблизно $3/8$) загальної кількості повних та скручених ЕКФЕ (таблиця 3). За результатами певних розрахунків було з'ясовано, що повні і скручені ЕКФЕ мають найвищу швидкість експоненціювання точки у порівнянні з кривими інших форм. Поряд з тим, на відміну від повних, на скручених ЕКФЕ генератор криптосистеми знаходиться у два рази швидше.

Таблиця 3

Розподіл кількості існуючих ЕКФЕ з мінімальним кофактором 4 порядку кривої при модулі простого поля $p \equiv 1 \pmod{4}$ і $p \equiv 3 \pmod{4}$ ($N_E = 4n$)

Умова		Клас	Кількість кривих	
A $p \equiv 1 \pmod{4}$	A1 $p \equiv 1 \pmod{4}$	Повні	$M_{A1} = (p-1)/4$	$M_A = M_{A1} + M_{A2} = (p-3)/2$
	A2 $p \equiv 1 \pmod{4}$	Скручені	$M_{A2} = (p-5)/4$	
B $p \equiv 3 \pmod{4}$		Повні		$M_B = (p+1)/4$

За результатами аналізу властивостей квадратичних ЕКФЕ було виявлено, що мінімальний кофактор порядку кривої 8 призводить до надмірної кількості точок та збільшує кількість операцій при пошуку генератора, а наявність у квадратичних кривих чотирьох точок з нескінченними координатами ускладнює програмування. На підставі цього зроблено висновок, що властивості квадратичних ЕКФЕ не дозволяють рекомендувати їх використання в криптосистемах, але завдяки тому, що квадратичні ЕКФЕ утворюють пару квадратичного кручення зі скрученими, має сенс використання їх для теоретичного аналізу.

На підставі проведеного аналізу властивостей ЕКФЕ різних класів, визначено кількість та описано властивості корисних кривих, які доцільно рекомендувати до використанні у криптосистемах.

У другій частині **розділу 2** було зроблено оцінку складності експоненціювання точки на ЕКФЕ та на кривих у формі Вейерштрасса методом підрахунку кількості операцій у полі у групових операціях додавання і подвоєння точок, що надало змогу провести порівняльний аналіз кількості операцій при експоненціюванні точки на ЕКФЕ та на кривих у формі Вейерштрасса.

За результатами аналізу кількості операцій в групі для точок повної та скрученої ЕКФЕ в проєктивних координатах та на кривій Вейерштрасса (табл. 4) визначено, що у загальному випадку найменших обчислювальних витрат вимагають операції на повних ЕКФЕ. Особливо повні ЕКФЕ виграють при

подвоєнні, яке обходиться без операції множення на параметр кривої. Також, з метою зменшення кількості операцій в групі точок ЕКФЕ, був запропонований метод досягнення мінімальної складності операцій, який полягає у фіксації параметру a мінімальним значенням 2 або 3 ($a = 2 \rightarrow$ одне додавання, $a = 3 \rightarrow$ два додавання у групі точок) та вибором мінімального параметру d , який забезпечує порядок $4n$ кривої з мінімальним кофактором 4, де $n \in \mathbb{P}$. При застосуванні запропонованого методу зниження складності операцій, з'являється можливість зменшити складність додавання у групі точок завдяки нехтуванню операцією множення на параметри a та (або) d для точок кривої, як малим числом.

Таблиця 4

Кількість операцій в групі точок ЕКФЕ та Вейерштрасса, де M – множення у полі, S – піднесення до квадрата, U – множення на параметри a та (або) d для точок кривої

Клас кривих	Кількість операцій в полі для однієї групової операції		Оцінка складності при $1S = 2/3M$; $1U = 1/2M$	
	Додавання точок	Подвоєння точок	Додавання точок	Подвоєння точок
Повні ЕКФЕ	$10M + 1S + 1U$	$3M + 4S$	11.17M	5.67M
Скручені ЕКФЕ	$10M + 1S + 2U$	$3M + 4S + 1U$	11.67M	6.17M
Криві у формі Вейерштрасса	$12M + 2S$	$7M + 5S$	13.34M	10.33M
Кількість операцій з використанням запропонованого методу зниження складності операцій				
Повні та скручені ЕКФЕ	$M + 1S$	$M + 4S$	10.67M	5.67M

Виконані дослідження дозволили з'ясувати, що у повних і скручених кривих Едвардса, для експоненціювання точки, використовується менша кількість операцій ніж у кривих у канонічній формі Вейерштрасса, що у результаті значно прискорює швидкість експоненціювання точки.

На наступному кроці було проведено порівняльний аналіз складності експоненціювання точки на скрученій і повній кривій Едвардса у порівнянні з кривою у формі Вейерштрасса. Для цього було застосовано отримані оцінки складності додавання і подвоєння:

на кривій у формі Вейерштрасса: $V_W = 13.33M$, $T_W = 10.33M$,

на повній ЕКФЕ: $V_{Епов} = 11.17M$, $T_{Епов} = 5.67M$,

на скрученій ЕКФЕ: $V_{Ескр} = 11.67M$, $T_{Ескр} = 6.17M$.

За аналізом складності операцій додавання і подвоєння точок на різних кривих визначено коефіцієнт виграшу $\gamma(v)$ у складності експоненціювання точки на повній і скрученій ЕКФЕ у порівнянні з кривою у формі Вейерштрасса:

$$\gamma(v) = \frac{T_W + v \cdot V_W}{T_E + v \cdot V_E}$$

де v – відносна частота знаків «1» в двійковому (трійковому) зображенні числа k у скалярному добутку kP ; $T_{W/E}$ – кількість подвоєння на кривих Вейерштрасса / та на кривих у формі Едвардса та $V_{W/E}$ – кількість додавання на кривих Вейерштрасса / та на кривих у формі Едвардса.

Також знайдено максимальний виграш у складності експоненціювання точки для повної і скрученої ЕКФЕ з застосуванням запропонованого методу досягнення мінімальної складності операцій у групі. Результати розрахунку виграшу у складності експоненціювання точки ЕКФЕ у порівнянні з експоненціюванням точки кривої у формі Вейерштрасса представлено у табл. 5.

Таблиця 5

Результати оцінок виграшу у кількості операцій складності експоненціювання точки для повної і скрученої ЕКФЕ у порівнянні з кривою у формі Вейерштрасса (в дужках - значення максимального виграшу при мінімальній складності операцій у групі)

Клас кривих	Виграш $\gamma(v)$ де k – скалярний множник генератора криптосистеми	
	$(v=0.5)$ – двійкове k	$(v = 0.33)$ – трійкове k
Повні ЕКФЕ	1.51 (max 1.544)	1.574 (max 1.603)
Скручені ЕКФЕ	1.416 (max 1.544)	1.47 (max 1.603)

Порівняльний аналіз кількості операцій, які необхідно здійснити при експоненціюванні точки на скрученій і на повній кривій Едвардса і кривій у формі Вейерштрасса показав, що експоненціювання точки на кривих Едвардса швидше, ніж на кривих у формі Вейерштрасса, більш ніж у 1,5 рази. Особливо ЕКФЕ виграють при трійковому представленні числа скалярного множника генератора криптосистеми.

Третій розділ присвячено розробленню більш швидких за існуючі методів знаходження точки простого порядку кривих, що належать до класу повних та скручених ЕКФЕ над простими полями, з метою застосування їх в алгоритмах пошуку генератора криптосистеми, створення відповідних алгоритмів та порівняльного аналізу кількості операцій, які потрібно виконати при виконанні алгоритмів знаходження точки простого порядку на ЕКФЕ та на кривих у формі Вейерштрасса.

На *першому етапі* дослідження проведено аналіз циклічних повних кривих у формі Едвардса, який дозволив виявити низку нових властивостей повної ЕКФЕ над простим полем. Введенням операції, оберненої до подвоєння точки кривої – операції ділення точки на 2, знайдено умови подільності на 2 для точок повної ЕКФЕ більше 4-го порядку та описано умови, при яких координати цих точок взаємопов'язані. Для створення метода пошуку генератора криптосистеми (точки простого порядку), яка з'являється при подвоєнні точки максимального порядку, сформульовано та доведено 3 теореми про властивості точок повної ЕКФЕ:

1. Для будь-якої точки (x, y) повної кривої Едвардса, що не належить колу радіуса 1, існують 2 точки ділення на 2 $\{P, P+D\}$ тоді і тільки тоді, коли $\chi(1 - y^2) = 1$;

2. Необхідною і достатньою умовою існування 4-х точок 8-го порядку повної кривої Едвардса є $\chi(1 - d) = 1$.

3. Для будь-якої точки (x, y) повної кривої Едвардса, що не належить колу радіуса 1, справедлива рівність $\chi(1 - x^2) \cdot \chi(1 - y^2) = \chi(1 - d)$.

На підставі доведень цих 3 теорем створено новий метод знаходження точки максимального порядку, який полягає у тестуванні значення квадратичного характеру виразу з координатою випадкової точки $(1 - y^2)$. Тобто якщо $\chi(1 - y^2) = -1$, то $\chi(1 - x^2) = 1$ і навпаки, що дає можливість знайти точку максимального порядку одним тестуванням координати випадкової точки кривої, квадратичний характер виразу $(1 - y_1^2)$ має значення -1 . За властивістю точки ЕКФЕ, при додатковому подвоєнні точки максимального порядку $4n$ отримуємо точку простого порядку n , яка і є генератором криптосистеми.

За результатами виконаних досліджень у *другій частині третього розділу* було розроблено три алгоритми пошуку генератора криптосистеми на повних та скручених ЕКФЕ.

Із застосуванням розробленого методу знаходження точки максимального порядку та використанням властивостей точок ЕКФЕ, розроблено метод знаходження точки простого порядку n на повній ЕКФЕ, на основі якого розроблено і описано Алгоритм 1 пошуку генератора криптосистеми.

Алгоритм 1

Умови:

ЕКФЕ має вигляд (1), де $\chi(ad) = -1$, $N_E = 4n$, $n \in \mathbb{P}$, $p \equiv 1 \pmod{4}$.

1. Знаходиться випадкова координата x точки $P = (x, y)$;

2. Якщо $x = 0$, або ± 1 , або $\pm \frac{1}{\sqrt{d}}$, то перейти до кроку 1;

3. Обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} \pmod{p}$;

4. Якщо $\chi(z) \neq 1$, то перейти до кроку 1;

5. Обчислюється $y = \sqrt{z} \pmod{p}$;

6. Якщо $\chi(1 - y^2) \neq 1$, то $x \leftrightarrow y$; $P \leftarrow (y, x)$;

7. Обчислюється $G = 2P$;

Вихід: точка $G = (x_G, y_G)$ така, що $\text{Ord}(G) = n$.

На підставі властивості порядків точок повної ЕКФЕ над полями F_p , де $p \equiv 1 \pmod{4}$, за якою подвоєння точки максимального порядку $4n$ створює точку, порядок якої дорівнює $2n$ та подвоєння точки порядку $2n$ створює точку простого порядку n , розроблено і описано Алгоритм 2 пошуку генератора криптосистеми.

Алгоритм 2

Умови:

ЕКФЕ має вигляд (1), де $\chi(ad) = -1$, $N_E = 4n$, $n \in \mathbb{P}$, $p \equiv 1 \pmod{4}$.

1. Знаходиться випадкова координата x точки $P = (x, y)$;

2. Якщо $x = 0$, або ± 1 , або $\pm \frac{1}{\sqrt{d}}$, то перейти до кроку 1;

3. Обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} \pmod{p}$;

4. Якщо $\chi(z) \neq 1$, то перейти до кроку 1;

5. Обчислюється $y = \sqrt{z} \pmod{p}$;

6. Обчислюється $G = 4P$;

Вихід: точка $G = (x_G, y_G)$ така, що $\text{Ord}(G) = n$.

На підставі того, що для скрученої ЕКФЕ при $(p \equiv 1 \pmod{4})$ точка простого порядку знаходиться одним подвоєнням випадкової точки, розроблено і описано найшвидший, з запропонованих, Алгоритм 3 пошуку генератора криптосистеми.

Алгоритм 3

Умови:

ЕКФЕ має вигляд (1), де $\chi(a) = \chi(d) = -1$, $N_E = 4n$, $n \in \mathbb{P}$, $p \equiv 1 \pmod{4}$.

1. Знаходиться випадкова координата x точки $P = (x, y)$;

2. Якщо $x = 0$, або ± 1 , або $\pm \frac{1}{\sqrt{d}}$, то перейти до кроку 1;

3. Обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} \pmod{p}$;

4. Якщо $\chi(z) \neq 1$, то перейти до кроку 1;

5. Обчислюється $y = \sqrt{z} \pmod{p}$;

6. Обчислюється $G = 2P$;

Вихід: точка $G = (x_G, y_G)$, така, що $\text{Ord}(G) = n$.

У 4 розділі проведено порівняльний аналіз кількості операцій, які потрібно виконати в роботі алгоритмів пошуку генератора криптосистеми на ЕКФЕ та на кривих у формі Вейерштрасса. За розрахунком загальної кількості операцій у полі з урахуванням кількості кроків до успішного результату при

пошуку генератора криптосистеми у стандартному алгоритмі та запропонованих алгоритмах 1, 2 та 3 були отримані результати, які занесені в таблицю 6:

Таблиця 6

Кількість операцій при пошуку генератора криптосистеми

Алгоритми	Кількість операцій у полі, де M – кількість множень у полі
Стандартний алгоритм	$S = 360M \cdot \log(n)$
Алгоритм 1	$S_1 = (12,68 + 2 \log(n))M$
Алгоритм 2	$S_2 = 22,68M$
Алгоритм 3	$S_3 = 11,34M$

За результатом порівняльного аналізу складності обчислень операцій у полі при пошуку генератора криптосистеми у запропонованих алгоритмах до стандартного, було отримані значення, які показали значний вииграш у складності обчислень створених нових алгоритмів пошуку генератора криптосистеми на ЕКФЕ над стандартним алгоритмом на кривих у формі Вейерштрасса. А саме:

- вииграш у складності обчислень Алгоритму 1 порівняно зі стандартним алгоритмом у 180 разів;
- вииграш у складності обчислень Алгоритму 2 порівняно зі стандартним алгоритмом у $16\log(n)$ разів.
- вииграш у складності обчислень Алгоритму 3 порівняно зі стандартним алгоритмом у $32\log(n)$ разів.

Результати обчислень дають змогу зробити обґрунтовані висновки, що знаходження генератора на ЕКФЕ із застосуванням запропонованих методів порівняно зі стандартним алгоритмом, істотно більш швидше і відповідно ефективніше.

У другій частині **четвертого** розділу, у відповідності до поставленої у дисертації задачі, проведені дослідження набули подальшого розвитку стосовно розрахунку загальносистемних параметрів криптостійких ЕКФЕ із застосуванням розроблених алгоритмів пошуку генератора криптосистеми та розробленого методу зниження складності виконання операцій додавання та подвоєння точок ЕКФЕ. У розділі наводяться результати обчислень загальносистемних параметрів криптостійких повних ЕКФЕ, придатних для використання у полях простого порядку, що рекомендовані стандартами FIPS-186-2-2000, FIPS-186-4-2013 та ISO/IECCD 15946. Наведені табульовані результати розрахунків загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим полем у всьому діапазоні стандартних значень

модуля поля довжиною 192, 224, 256, 384 і 521 біт. Усі криві пройшли тестування до MOV-атаки. Розраховані загальносистемні параметри крипостійких ЕКФЕ наведені у **додатках А.1 та А.2.**

Визначено перспективи подальшого дослідження.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі розв'язано актуальну науково-практичну задачу, яка полягає у розробленні нових методів підвищення швидкодії асиметричних криптосистем з використанням властивостей крипостійких ЕКФЕ над простими полями, які дозволяють підвищити швидкість експоненціювання точки та швидкість знаходження генератора криптосистеми. Проведені дослідження дозволили отримати нові наукові результати, які мають переваги перед існуючими та перелічені нижче.

1. Аналіз існуючих досліджень показав, що при описанні властивостей ЕКФЕ виникають суперечності щодо їх належності до певних класів, через некоректність існуючої класифікації. Із застосуванням методу перебору властивостей параметрів кривої існуючу класифікацію ЕКФЕ було удосконалено, що надало можливість описати властивості та умови існування трьох класів ЕКФЕ, що не перетинаються: повних, скручених та квадратичних та визначити кількість ЕКФЕ з мінімальним кофактором порядку кривої $N_E = 4n$, які мають більш високу швидкість експоненціювання точки, завдяки чому їх доцільно рекомендувати до використання для розроблення методів підвищення швидкодії алгоритмів криптосистеми.

2. Розроблено новий метод зниження складності виконання операцій додавання та подвоєння точок ЕКФЕ, який базується на виборі мінімальних параметрів кривої, що надає можливість зменшити складність додавання та прискорити швидкість експоненціювання точки.

3. Вперше проведено порівняльний аналіз швидкості експоненціювання точки кривих у формі Вейерштрасса та ЕКФЕ методом розрахунку кількості операцій при скалярному добутку точок кривої за результатами якого було визначено, що найменших обчислювальних витрат вимагають операції на ЕКФЕ, особливо при подвоєнні, яке обходиться без операції множення на параметр кривої, завдяки чому імплементація алгоритмів на ЕКФЕ швидше ніж на кривих у формі Вейерштрасса більш ніж у 1,5 рази.

4. Розроблено нові методи знаходження точки простого порядку на ЕКФЕ над простими полями, розроблені на основі методу знаходження максимального порядку випадкових точок ЕКФЕ, які, за результатами порівняльного аналізу, швидші від існуючих стандартних методів у $32(\log n)$ разів (де n – порядок генератора).

5. Розроблено три нових алгоритми пошуку генератора криптосистеми на підставі розроблених методів знаходження точки простого порядку та методу зниження складності виконання операцій, з використанням яких розраховано загальносистемні параметри 25 крипостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем в рекомендованих

стандартами FIPS-186-2-2000, FIPS-186-4-2013 та ISO/IECCD 15946 простих полях з довжиною модуля 192, 224, 256, 384 і 521 біт, які можуть бути рекомендовані для використання в асиметричних криптоалгоритмах.

6. Отримані результати були впроваджені та використовуються у Службі зовнішньої розвідки України, а також в навчальному процесі кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського при викладанні дисципліни «Криптосистеми на еліптичних кривих».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Bessalov, A.V., Tsygankova, O.V. «Interrelation of families of points of high order on the Edwards curve over a primefield» // English translation of Problems of Information Transmission, 2015, Vol. 51, № 4, pp. 391-397. (іноземне видання, проіндексовано в міжнародних наукометричних базах Scopus, Web of science) *Здобувачу належить модифікація закону додавання точок на ЕКФЕ над простим полем.*

2. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. // Проблемы передачи информации. Москва – Том 53, Вып. 1, март 2017, С. 101-111. *Transmission: Bessalov A.V., Tsygankova O.V. «Number of curves in the generalized Edwards form with minima leven cofactor of the curve order» // English translation of Problems of Information 2017. (іноземне видання, проіндексовано в міжнародних наукометричних базах Scopus, Web of science) Здобувачу належить побудови методів знаходження точки простого порядку на ЕКФЕ, модифікація закону додавання точок на ЕКФЕ над простим полем.*

3. Бессалов А.В., Цыганкова О.В. Новые свойства эллиптической кривой в форме Эдвардса над простым полем. // Радиотехника №180, 2015. – С.137-143., Bessalov, A.V., Tsygankova, O.V. «New properties of the Edwards form elliptic curve over a primefield» // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) 2015. (проіндексовано в міжнародних наукометричних базах Scopus, Web of science). *Здобувачу належить застосування подвійної симетрії координат точок для аналізу їх властивостей, модифікація закону додавання точок на ЕКФЕ над простим полем.*

4. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015.– С.58-63. *Здобувачу належить оцінка складності операції подвоєння точок на ЕКФЕ над простим полем, модифікація закону додавання точок на ЕКФЕ над простим полем.*

5. Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2 (26), 2014. С.18-21. *Здобувачу належить постановка задачі пошуку властивостей ЕКФЕ, які*

дозволяють знайти випадкову точку максимального порядку, модифікація закону додавання точок на ЕКФЕ над простим полем, оцінка складності операції подвоєння точок на ЕКФЕ над простим полем, ідея проведення порівняльного аналізу кількості операцій при експоненціюванні точки на ЕКФЕ та на кривій у формі Вейєрштраса.

6. Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. // Прикладная радиоэлектроника, 2015 Том 14 № 3, , С.197-203. *Здобувачу належить систематизація ознак класифікації кривих в узагальненій формі Едвардса, модифікація закону додавання точок на ЕКФЕ над простим полем.*

7. Бессалов А. В., Третьяков Д. Б., Цыганкова О. В. Свойства точек малых порядков кривых в обобщенной форме Эдвардса // Сучасний захист інформації № 2, 2016, С.46-54. *Здобувачу належить аналіз особливих точок 2-го порядку ЕКФЕ, систематизація ознак класифікації кривих в узагальненій формі Едвардса, модифікація закону додавання точок на ЕКФЕ над простим полем.*

8. Цыганкова О.В. Нові алгоритми знаходження базової точки на еліптичних кривих у формі Едвардса // «Інформаційні технології та комп'ютерна інженерія» № 1 (47) 2020. –С. 39-47. *Здобувачу належить опис алгоритмів пошуку генератора криптосистеми на ЕКФЕ, порівняльний аналіз кількості операцій при експоненціюванні точки на ЕКФЕ та на кривій у формі Вейєрштраса*

В інших виданнях

9. Bessalov A., Dykyi V., Malyshko A., Tsygankova O., Yadukha D. Parameters of the Fastest Cryptographically Strong Twisted Edwards Curves . // Theoretical and Applied Cybersecurity 2019. 1. с.7-11. *Здобувачу належить координація завдань виконавців розрахунків, вибір параметрів та участь у розрахунку параметрів a і d , побудова методів знаходження точки простого порядку на ЕКФЕ.*

Матеріали науково-технічних конференцій:

10. Бессалов А.В., Цыганкова О.В. Свойства точек больших порядков кривой Эдвардса // матеріали XVII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2015 р. – С. 30-31. *Здобувачу належить порівняльний аналіз швидкодії розроблених алгоритмів знаходження генератора криптосистеми з чинними алгоритмами стандарту ЦП.*

11. Бессалов А.В., Цыганкова О.В. Классификация кривых в обобщенной форме Эдвардса. // матеріали XVIII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2016 р. – С. 30-31. *Здобувачу належить систематизація ознак класифікації кривих в узагальненій формі Едвардса, модифікація закону додавання точок на ЕКФЕ над простим полем.*

12. Бессалов А.В., Олешко К.А., Поречна Д.Н., Цыганкова О.В., Чорний О.Н. «Криптостійкі скручені криві Едвардса з мінімальною складністю групових

операцій» // матеріали XIX міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах» Київ. – К.: НДЦ «Тезис», 2017 р. – С. 260. *Здобувачу належить постановка задачі та участь у роботі групи дослідників щодо розрахунку загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим скінченним полем.*

13. Цыганкова О.В., Цыганков Р.И. Анимация точек экспоненцирования кривой Эдвардса // матеріали XV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017 р., м. Київ. Том II.– С. 114. *Здобувачу належить графічна ілюстрація скалярного добутку точок експоненціювання ЕКФЕ, модифікація закону додавання точок на ЕКФЕ над простим полем, застосування подвійної симетрії координат точок для аналізу їх властивостей.*

14. Бессалов А.В., Цыганкова О.В. Умови існування суперсингулярних повних кривих Едвардса над простим полем // матеріали XX Ювілейної міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2018 р., – С. 119-120. *Здобувачу належить участь в аналізі властивостей суперсингулярних повних кривих Едвардса, аналіз властивостей суперсингулярних повних ЕКФЕ над простим полем, формулювання теорем про умови існування суперсингулярних ЕКФЕ з j -інваріантами, що дорівнюють 0 та 12^3 .*

АНОТАЦІЯ

Цыганкова О.В. Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», – Київ, 2021.

Роботу присвячено дослідженню криптографічних властивостей еліптичних кривих у формі Едвардса (ЕКФЕ) з метою використання їх в алгоритмах асиметричних криптосистем для підвищення їх швидкодії. Основну увагу зосереджено на ЕКФЕ над полями з модулем p , де $p \in \mathbb{P}$. У роботі представлена удосконалена класифікація кривих в узагальненій формі Едвардса, яка поділяє множину цих кривих на три класи, що не перетинаються. Отримано результати аналізу властивостей ЕКФЕ різних класів. Дано оцінку кількості та визначено умови існування ЕКФЕ з мінімальним кофактором порядку кривої. Отримано аналітичні оцінки швидкості експоненціювання точки на ЕКФЕ та на кривих у формі Вейерштрасса та отримано результати порівняльного аналізу кількості операцій експоненціювання точок на цих кривих. Доведено, що експоненціювання точки класів повних і скручених ЕКФЕ швидше в 1,6 разів ніж експоненціювання точки кривих у формі Вейерштрасса. Розроблено новий

метод знаходження точки простого порядку на повних та скручених, за новою класифікацією, ЕКФЕ, на основі якого створено нові алгоритми пошуку генератора криптосистеми на ЕКФЕ. За допомогою розроблених алгоритмів пошуку генератора криптосистеми та з застосуванням запропонованого методу зниження складності операцій розраховано загальносистемні параметри 25 криптостійких скручених кривих Едвардса над простими полями з довжиною модулів, які рекомендовані стандартами FIPS-186-2-2000, FIPS-186-4-2013 та ISO/IECCD 15946.

Ключові слова: еліптична крива у формі Едвардса, параметри кривої, порядок точки, експоненціювання точок, повна крива Едвардса, скручена крива Едвардса, генератор криптосистеми, криптосистеми на еліптичних кривих, квадратичний характер, квадратичний лишок, квадратичний не лишок.

АННОТАЦИЯ

Цыганкова О.В. Методы повышения быстродействия асимметричных криптосистем с использованием эллиптических кривых в форме Эдвардса. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. - Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», – Киев, 2021.

Работа посвящена исследованию криптографических свойств эллиптических кривых в форме Эдвардса (ЭКФЭ) с целью использования их в алгоритмах асимметричных криптосистем для повышения их быстродействия. Основное внимание сосредоточено на ЭКФЭ над полями с модулем p , где $p \in \mathbb{P}$. В работе представлена усовершенствованная классификация кривых в обобщенной форме Эдвардса, которая разделяет множество этих кривых на три непересекающихся класса. Получены результаты анализа свойств ЭКФЭ разных классов, дана оценка их количества и определены условия существования ЭКФЭ с минимальным кофактором порядка кривой. Получены аналитические оценки скорости экспоненцирования точки на ЭКФЭ и на кривых в форме Вейерштрасса и получены результаты сравнительного анализа количества операций экспоненцирования точек на этих кривых. Доказано, что экспоненцирования точки для классов полных и скрученных ЭКФЭ в 1,6 раз чем кривых у форме Вейерштрасса. Разработан новый метод нахождения точки простого порядка на полных и скрученных, по новой классификации, ЭКФЭ на основании которого созданы новые алгоритмы поиска генератора криптосистемы на ЭКФЭ. С помощью созданных алгоритмов поиска генератора криптосистемы и с применением нового созданного метода минимизации сложности операций рассчитаны общесистемные параметры 25 криптостойких скрученных кривых Эдвардса над простым полем с длиной модуля, рекомендованных стандартами ЦП.

Ключевые слова: эллиптическая кривая в форме Эдвардса, параметры кривой, порядок точки, экспоненцирование точек, полная кривая Эдвардса, скрученная кривая Эдвардса, генератор криптосистемы, криптосистемы на эллиптических кривых, квадратичный характер, квадратичный вычет, квадратичный невычет.

ABSTRACT

Tsygankova O.V. Methods for increasing the speed of asymmetric cryptosystems using elliptic curves in Edwards form. – Manuscript.

This work is dedicated to studying the cryptographic properties of elliptic curves in Edwards form (ECEF) and to the subsequent use of those in the asymmetric cryptosystems in order to increase their speed. The main focus is on the elliptic curves in the Edwards form over fields modulo p , where p is prime. An improved classification of elliptic curves in generalized Edwards form is presented, which splits the set of these curves into three non-intersecting classes. New analytical results about properties of newly introduced ECEF classes are obtained. The existence conditions are determined and a cardinality are evaluated for elliptic curves in Edwards form with the minimum cofactor that can be used in the cryptographic algorithms.

Analytical estimates of the point exponentiation efficiency on the elliptic curves in Edwards form and on curves in Weierstrass form are obtained. Comparative performance analysis are provided in terms of the number of scalar products. It is proved that the point exponentiation in complete and twisted ECEF classes is many times faster than the exponentiation of a point on the Weierstrass curves.

Analysis of published works has shown that some inaccuracies arise in the ECEF properties describing because of the incorrect classification of curves proposed by D. Bernstein and co-authors. However, known results about the properties of the Edwards curves have not been sufficiently mathematically researched for the purpose to find the fastest and easiest-to-implement curves for use in cryptosystems.

Based on the new proposed classification, conditions were obtained for the existence of ECEF with a minimum order coefficient of the curve, which allowed to calculate the number of curves that can be used to find crypto-resistant ECEF for use in the asymmetric cryptosystems. As a result of the calculations, it was obtained that over a prime finite field there are about $3/8$ of the total number of elliptic curves in the generalized Edwards form which have order $4n$, where n is prime, which can be used to find cryptographically strong curves for use in the asymmetric cryptosystems.

A comparative analysis of the point exponentiation on the Edwards curves and the Weierstrass curves was performed, using the method of calculating the number of operations for the scalar product of the curve points, which allowed to estimate analytically the efficiency of point exponentiation on different curves. The results of the analysis show that the point exponentiation of classes of complete and twisted ECEF (by new classification) is 1.6 times faster than the point exponentiation on the

Weierstrass curves used in the modern digital signature algorithms. In particular, the Edwards curves win with the ternary representation of k .

A new method for determining the order of random points of the ECEF has been developed on the base of three theorems about properties of points and curve parameters, which makes it possible to simplify the finding of a prime order point by testing the coordinate of a random point. A new algorithm for finding a cryptosystem generator using the proposed method of determining the order of the random points is formulated, which allows to find the cryptosystem generator on the Edwards curves in $O(\log n)$ times faster than on the Weierstrass curves (here n is the order of the group of points of the elliptic curve).

Using the new algorithms of cryptosystem generator search and the method of minimization of complexity of operations, parameters of 25 twisted and 39 complete cryptographically strong elliptic curves in Edwards form over the prime fields with a modulo length $p = 192, 224, 256, 384$ i 521 bit (recommended by standards FIPS-186-2-2000, FIPS-186-4-2013 and ISO/IECCD 15946) are found, that allows to use them in asymmetric cryptoalgorithms.

A new, simpler and faster than known, method of finding the ECEF order and reconstructions of all points of the complete Edwards curve is proposed. It can be used for teaching disciplines related to elliptic mathematics.

The dissertation consists of an introduction, four sections, conclusions, a list of sources used, five appendices.

The introduction substantiates the relevance of the topic of the dissertation, formulates the purpose and objectives of the research, scientific novelty and practical significance of the obtained results. The information about implementation of work results, their validation, publications and personal contribution of the applicant are given.

Keywords: elliptic curve in Edwards form, curve parameters, point order, point exponentiation, complete Edwards curve, twisted Edwards curve, group generator, elliptic curve cryptosystems, quadratic residue, quadratic non-residue.