УДК 004.056.5 д.т.н. Чевардін В. (ВІТІ) ORCID 0000-0002-1070-4568
Пономарьов О. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОСИСТЕМ НА ОСНОВІ ПЕРЕТВОРЕНЬ В ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Проведено аналіз відомих загроз сучасним криптографічним алгоритмам на основі еліптичних кривих. Визначені недоліки найбільш відомих підходів щодо вдосконалення криптографічних алгоритмів на еліптичних кривих. Розглянуті вимоги до криптостійких еліптичних кривих необхідних для розробки криптографічних додатків на основі перетворень в групі точок еліптичної кривої в формі Веєрштраса, які застосовуються в діючих стандартах криптографічного захисту інформації. Проведено аналіз стандартизованих еліптичних кривих, які можуть бути представлені в формі Едвардса. Побудовані криптографічні програмні функції для обчислення точок еліптичних кривих з використанням арифметики великих чисел. Отримані нові параметри еліптичних кривих в формі Веєрштраса та Едвардса для відповідних рівнів безпеки: 256, 384, 512 бітовій характеристики поля. Згенеровані відповідні базові точки кривих для реалізації в існуючих та перспективних криптографічних додатках. Отримані три варианти стандартних кривих, для яких обчислені оцінки середнього часу скалярного множення точок кривої. Розглянуті ізоморфні трансформації для стандартизованих еліптичних кривих. Побудована ізогенія еліптичної кривої третього порядку та отримана ізоморфна трансформація еліптичної кривої. Розроблені необхідні програмні операцій для побудови ізогенії еліптичної кривої на основі бібліотеки програмних функцій Miracl. Побудовані та перевірені операції для обчислення ізогенії заданого порядка еліптичної кривої, параметри якої забезпечують зазначені в стандарті рівні безпеки: 256, 384, 512. Визначені перспективи розвитку криптосистем на еліптичних кривих.

***Чевардин В.Е., Пономарев А.А. Перспективы развития криптосистем на основе преобразований в группе точек эллиптической кривой**. Проведен анализ известных угроз современным криптографическим алгоритмам на основе эллиптических кривых. Определены недостатки наиболее известных подходов по совершенствованию криптографических алгоритмов на эллиптических кривых. Рассмотрены требования к криптостойким эллиптическим кривым, необходимые для разработки криптографических приложений на основе преобразований в группе точек эллиптической кривой в форме Веерштраса, которые применяются в действующих стандартах криптографической защиты информации. Проведен анализ стандартизированных эллиптических кривых, которые могут быть представлены в форме Эдвардса. Построенные криптографические программные функции для вычисления точек эллиптических кривых с использованием арифметики больших чисел. Получены новые параметры эллиптических кривых в форме Веерштраса и Эдвардса для соответствующих уровней безопасности: 256, 384, 512 битной характеристики поля. Сгенерированы соответствующие базовые точки кривых для реализации в существующих и перспективных криптографических приложениях. Получено три варианта стандартизованых кривых, для которых вычислены оценки среднего времени скалярного умножения точек кривой. Рассмотрены изоморфные трансформации для стандартизированных эллиптических кривых. Построена изогения эллиптической кривой третьего порядка и получена изоморфная трансформация эллиптической кривой. Разработаны необходимые программные операций для построения изогении эллиптической кривой на основе библиотеки программных функций Miracl. Построены и проверены операции для вычисления изогении заданного порядка эллиптической кривой, параметры которой обеспечивают указанные в стандарте уровни безопасности: 256, 384, 512. Определенны перспективы развития криптосистем на эллиптических кривых.*

***V.Chevardin, A.Ponomarev Perspective of the development of cryptosystems based on transformations in group of elliptic curve points.** The known threats to modern cryptographic algorithms based on elliptic curves are analyzed. Deficiencies of the most well-known approaches for improving cryptographic algorithms on elliptic curves are determined. The requirements for cryptographic elliptic curves necessary for developing cryptographic applications based on transformations in the group of points of an elliptic curve in the form of Veerstrass, which are used in the current standards of cryptographic information protection, are considered. The analysis of standardized elliptic curves, which can be represented in the form of Edwards. The constructed cryptographic program functions for calculating the points of elliptic curves using arithmetic of large numbers. New parameters of elliptic curves in the form of Veerstrass and Edwards are obtained for the corresponding security levels: 256, 384, 512 bit field characteristics. Corresponding base points of the curves are generated for implementation in existing and perspective cryptographic applications. Three versions of standardized curves are obtained for which estimates of the average time of scalar multiplication of curve points are calculated. Isomorphic transformations for standardized elliptic curves are considered. The isogeny of a third-order elliptic curve for scalar multiplication and isomorphic transformation of an elliptic curve is constructed. The necessary software operations have been developed for constructing the isogeny of an elliptic curve based on the Miracl library of program functions. Operations are constructed and verified for calculating the isogeny of a given order of an elliptic curve, the parameters of which provide the security levels specified in the standard: 256, 384, 512. The prospects for the development of cryptosystems based on elliptic curves.*

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

1. Постановка проблеми та актуальність дослідження

Сьогодні дуже гостро стають питання обрання криптографічної системи шифрування даних та генерації криптографічних ключів для практичного застосування. Вже посіли своє місце в історії кібервпливів та кіберінцидентів випадок приховування дірки в криптографічном алгоритмі генерації псевдовипадкових послідовностей [1], закладання дірок в програмні реалізації, таких як вплив на систему Siemens SIMATIC на основі підміни SIMATIC STEP 7 частини, що відповідає за прошивку програмованих логічних контролерів [2]. Слід також не забувати шифр DES, вузли замін (S-box) якого уразливі до диференційного аналізу, які ще використовуються сьогодні в деяких операційних системах та програмному забезпеченні. Але головною проблемою цього століття стала поява квантових комп'ютерів [3], потужність яких постійно зростає. Це змінює розвиток класичної асиметричної криптографії. Проблема побудови квантовостійких криптографічних алгоритмів викликала дуже багато суперечок між різними колами дослідників. Основні напрямки досліджень розділилися на частину робіт щодо вдосконалення класичних асиметричних систем, що базуються на складності рішення задач DLP, ECDLP та інших еквівалентних ним. Друга частина робіт присвячена розробці нових криптопримітивів стійких до квантового криптоаналізу [4].

Основними криптосистемами, які стандартизовані та реалізовані в системах електронного цифрового підпису та інших програмно-апаратних додатках, що використовуються для надання довірчих інформаційних послуг в Україна є системи на еліптичних кривих, які достатньо глибоко вивчені [5, 6]. Є роботи наукові роботи, результатами яких є незначне збільшення швидкодії основної криптографічної операції на еліптичних кривих - операції скалярного множення точок кривої за рахунок переходу до нових форм кривих, таких як криві Монтгомері, криві Едвардса [6, 7]. Слід зауважити, що ці підходи цікаві в більшості з наукової точки зору та не знайшли свого практичного застосування. Основна ідея більшості з цих підходів це зведення кривої в нормальній формі (формі Вейєрштраса) чи канонічній формі над полем з характеристикою $p \neq 2,3$ чи над розширенням поля $q \neq 2^m$ до спрощених форм. Це, в свою чергу, надає можливість спростити число примітивних операцій для виконання скалярного множення точок, а з іншого боку накладає додаткові обмеження на параметри кривої та умови виконання операції скалярного множення, наприклад для кривих Едвардса обираються криві, порядок яких не є простим числом і є кратним 4, що вважається уразливістю для криптографічно стійких кривих. Перехід до еліптичних кривих в формі Едвардса дозволяє в середньому підвищити швидкодію операцій скалярного множення в два рази та, як наслідок, при фіксованій швидкодії збільшити довжину модулю в 1,5 – 1,7 разів, тобто перейти від кривих над полем 2^{256} до кривих над полем 2^{384}. Перехід до таких кривих не дасть захисту від квантових комп'ютерів, тому цей шлях дає тільки тимчасовий виграш для існуючих еліптичних кривих.

У зв'язку з цим, актуальним питанням є пошук та розробка нових алгоритмів та криптографічних примітивів підвищеної стійкості з урахуванням сучасних і перспективних можливостей потенційного криптоаналитика.

2. Аналіз останніх публікацій та наукових результатів

Класичні підходи до використання операцій над точками еліптичних кривих зводяться, як правило, до використання широко відомої нормальної форми еліптичної кривої, а саме кривої Вейєрштраса [5]. Більшість останніх результатів щодо вдосконалення відомих алгоритмів на еліптичних кривих та розробки нових базуються на використанні ізоморфних трансформацій нормальної форми кривої до інших скорочених форм кривої [7 – 13]. Розглянемо деякі положення з теорії еліптичних кривих.

Криві Вейєрштраса

Гладкою (неособливою) еліптичною кривою порядка n над полем F_p називається множина точок , які задовольняють рівнянню (1), де багаточлен ступені[1] m з коефіцієнтами з

[1] Ступінь багаточлена є максимальна степінь одночленів, з яких він складається.

F_p. Така крива не повинна мати особливих точок, в яких часткові похідні дорівнюють одночасно нулю. Множина точок еліптичної кривої разом з точкою на нескінченності з операцією додавання[2] є абелевою групою. Для криптографічних цілей для кожної еліптичної кривої повинні виконуватись вимоги: дисрімінант кривої $\Delta(\mathrm{E}) \neq 0$ та j-інваріант кривої $j \neq \{0, 12^3\}$. Остання вимога обмежує використання суперсингулярних кривих. Крива (1) називається кривою Веэрштраса або нормальною формою еліптичної кривої над полем F_p.

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \qquad (1)$$

Коли коефіцієнти a_1, a_2, a_3 в виразі (1) дорівнюють нулю, крива може бути представлена в канонічній формі (або скороченій формі Веєрштрасса):

$$y^2 = x^3 + a_4 x + a_6,\ a_4, a_6 \in F_p \qquad (2)$$

Крива (2) є більш розповсюдженою для застосування в криптографічних додатках та системах електронного цифрового підпису. Основною криптографічною операцією яка використовується для цього це операція скалярного множення точок кривої.

Еліптичні криві отримали своє поширення на заміну відомих операцій в скінченних полях, на основі яких було побудовано криптосистеми RSA, ElGamal, DH та багато інших. Сутність операцій над точками кривої заключається в використанні групової операції додавання елементів групи точок кривої, $R = P + Q$, причому, сама операція додавання є складною операцією, яка реалізована багатогратним виконанням операцій над елементами скінченного поля F_p. Операції додавання точок кривої можна замінити еквівалентними операціями над елементами скінченного поля за рахунок ізоморфізма операцій в мультиплікативних групах, але порядок еквівалентної групи цілих чисел в такому випадку буде за довжиною перебільшувати для деяких кривих в 30 і більше разів. Для кривих уразливих до MOV-атаки цей параметр може бути значно менший, що позбавлює можливості використовувати такі криві на практиці.

Криптографічно стійкими кривими вважаються криві для яких $\Delta = 4A^3 + 27B^2 \neq 0$, а також j-інваріант кривої дорівнює $j(E)=1728(4A^3/(4A^3 + 27B^2))$. Якщо $j(E)$ еліптичних кривих дорівнюють один одному, то такі криві вважаються ізоморфними.

Розглянемо еліптичну криву над скінченним полем (таблиця 1).

Таблиця 1

Параметри кривої Вейєрштраса в скороченій формі E512

p	134078079299425970995740249982058461274793658205923 933777235614437217640300735469768018742981669034276 900318581864860508537538828119465699464336490060775 17	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE64D
n	335195198248564927489350624955146153186984145514809 834443089036093044100751839757485911534210550442196 835811514229286893314430518103105578013406983588466 7	40000000000000000000000000000000000000000000000 0000000000000000017F1EF80AF949ECB3AC390D869E51A CD0E05576A5B2F6A96416B8365C69B687B
A	543035432213890671838226655127588753445616279276615 308053645411472119173687692551334047124101494237132 110951324552557030568484518643777146923055068974138	A5E4D496D6632D5AA2972FF09BA88E9CD374E0C6C27 B3226E391A148E29DF79BDED5826B4B849F900106D0E CDF2819133DFE99241FE393EA5A029B71B178C3A
B	475680624011518723670254189330346265735309579366786 863842383626166630401267180726783731461998258495239 333776565383470549120809603707498413842632272312324 7	5AD2C8D9A9D30A1013556086C13B7EE911A267E5D9F0 00442AF650AD0EABADA25E81CF96AC661C456B89D0E 766BAD9394717EB216C72C5FB6B457380D919B02F

Для еліптичної кривої згенеровані випадкові параметри A, B та p за допомогою алгоритма SEA з використаням бібліотеки програмних функцій Miracl. Отримані параметри криптографічно стійких кривих в формі Вейєрштраса та Едвардса можуть бути застосованні для розробки та дослідження нових алгоритмів криптографічного захисту інформації. Для практичних цілей були згенеровані п’ять кривих для простих характеристик скінченного поля. В таблиці 1 наведено один з результатів генерації параметрів еліптичної кривої над

[2] Скалярне множення точок кривої: kP={P+P+P+...+P}k разів.

полем характеристики довжиною 512 біт. Також в таблиці наведено порядок n базової точки кривої. Однак слід зауважити, що порядок даної кривої дорівнює $NP = 4*n$. За стандартом NIST такі криві вважаються припустимі в криптографії. Від основної форми кривих форми Вейєрштраса отримуються інші форми еліптичної кривої шляхом ізоморфних трансформацій кривої. Найбільш популярними стали трансформації до форм кривих Монтгомері та Едвардса. З усіх спроб збільшити швидкодію операції скалярного множення точок кривої криві Едвардса дозволили це зробити практично в два рази.

Криві Едвардса

Криві Едвардса є ізоморфними кривими звичайних кривих Вейєрштраса, порядок яких кратний степені 2, в більшості останніх робіт розглядаються криві Едвардса, порядок яких кратний 4, як можливість замінити існуючі стандартизовані криві з метою покращення обчислювальної складності. Але для підвищення стійкості до квантового криптоаналізу заміна кривих Вейєрштраса на криві Едвардса не дає суттєвого виграша. Як заначалось раніше [7 – 8] основним напрямком розвитку криптографії на еліптичних кривих, в тому числі і кривих Едвардса, є використання множини ізоморфних кривих, що дозволить підвищити стійкість асиметричних алгоритмів до квантового криптоаналізу. Розглянемо сутність алгоритмів генерації параметрів еліптичних кривих та кривих Едварсдса.

Для генерації кривої Едвардса використовуються також алгоритми Schoof та SEA, але спочатку параметри кривої Едвардса після чого здійснюється ізоморна трансформація кривої в форму Вейєрштраса, після чого за алгоритмом за алгоритмом SEA визначається порядок кривої, а у разі відповідності параметрів здійснюється висновок що крива може використовуватись в криптографічних додатках. Криві Едвардса бувають звичайні, скручені та скручені в інверсних координатах. Враховуючи, результати робіт [6, 7] будемо використовувати скручені криві в інверсних координатах. Згенеруємо параметри скрученої кривої Едвардса над полем характеристики довжиною 512 біт, яка є ізоморфною кривій в таблиці 1.

Таблиця 2

Параметри кривої Едвардса Edw512

p	134078079299425970995740249982058461274793658205923 933777235614437217640300735469768018742981669034276 900318581864860508537538828119465699464336490060775 17	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE64D
n	335195198248564927489350624955146153186984145514809 834443089036093044100751839757485911534210550442196 835811514229286893314430518103105578013406983588466 7	40000000000000000000000000000000000000000000000 0000000000000000017F1EF80AF949ECB3AC390D869E51A CD0E05576A5B2F6A96416B8365C69B687B
A	2	2
B	85	55

До перспективних алгоритмів генерації криптографічних псевдовипадкових послідовностей на основі еліптичних кривих можна віднести запропонований в роботах [7 – 8] підхід щодо застосування ізоморфних трансформацій еліптичних кривих. Зазначений в роботі підхід дозволив покращити показники стійкості алгоритмів генерації ПВП до відтворення та передбачення. В роботах [7 – 8] наведені результати дослідження та вдосконалення генераторів ПВП на основі ізоморфних трансформацій еліптичних кривих, також розглянуті способи вдосконалення стандартизованого генератору Dual_EC_DRBG. Використання ізоморфних трансформацій еліптичної кривої було першою спробою побудувати новий криптографічний примітив, який дозволить підвищити стійкість криптографічних алгоритмів до квантового криптоаналізу. Це надало змогу збільшити число внутрішніх станів генератору без суттєвих втрат часу. Як наслідок, це дозволить продовжити використання генераторів ПВП цього классу до переходу на постквантову криптографію.

У зв’язку з цим, використання ізоморфних трансформацій еліптичної кривої є одним з можливих шляхів подальшого розвитку методів криптографічного захисту інформації.

Метою даної роботи є проведення аналізу основних положень теорії еліптичних кривих, а саме гомоморфних трансформацій еліптичної кривої – ізогенії еліптичної кривої для побудови квантовостійких алгоритмів криптографічного захисту інформації.

3. Викладення основного матеріалу.

Черговим кроком розвитку криптографії на еліптичних кривих стало застосування ізогенії еліптичної кривої. Розглянемо деякі положення загальної алгебри та теорії еліптичних кривих, необхідних для аналізу алгоритмів на основі перетворень в ізогеніях еліптичних кривих [5].

Визначення 1. Нехай F – скінченне поле [5], яке складається зі скінченного числа елементів. Число елементів поля визначає порядок поля ord(F).

Визначення 2. Нехай E_1 та E_2 гладкі еліптичні криві над полем F, які визначаються рівнянням (2) з відповідними коефіцієнтами. Кожна крива визначена значеннями: ord(E), Δ, $j(E)$.

Визначення 3. Ізогенія еліптичної кривої є неконстатним раціональним відображенням кривої E_1 над скінченним полем F в криву E_2, яке також називається груповим гомоморфізмом та подається в вигляді: $(x; y) \rightarrow (f1(x; y)/f2(x; y), g1(x; y)/g2(x; y))$, де $f1$, $f2$, $g1$, $g2$ – поліноми.

Визначення 4. Степінь ізогенії – є степенем раціонального відображення.

Теорема Tate [14]. Нехай E_1 та E_2 – криві над скінченним полем F. Тоді криві E_1 та E_2 є ізогенними кривими тоді і тільки тоді, коли порядки їх груп дорівнюють, ord(E_1) = ord(E_2).

Приклад. Нехай скінченне поле буде F_{19}, а криві над цим полем E_1: $y^2 = x^3+x+1$ та E_2: $y^2 = x^3 + 4x + 13$.

Порядок кривих E_1 та E_2 дорівнює ord(E_1) = ord(E_2) = 21, інваріанти кривих дорівнють один одному, j(E_1) = j(E_2).

Для заданої кривої була обчислена гоморфна трансформація, а саме вирази для обчислення $f1(x; y)$, $f2(x; y)$, $g1(x; y)$, $g2(x; y)$.

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

Степінь знайденої ізогенії дорівнює 3.

Оберемо точки кривої E_1 та перевіремо правильність ізоморфної трансформації точок кривої. Нехай випадкові точки кривої будуть $P_1 = (9; 6)$ та $P_2 = (14; 2)$. Здобуток точок P_1 та P_2 дорівнює: $P_3 = (5; 6)$. Ізоморфною трансформацією точки P_1 на кривій E_2 буде точка $Q_1 = (14; 1)$, для точки P_2 відповідно точка $Q_2 = (17; 4)$. Здобуток точок Q_1 та Q_2 буде точка $Q_3 = (8; 5)$. Трансформація точки $P_3 = (5; 6)$ на криву E_2 дає точку (8; 5), що підтверджує правильність ізоморфної трансформації точок кривої E_1 в точки кривої E_2. Таким чином, ізогенія кривої знайдена та відповідає вимогам, що надає можливість її застосовувати в алгоритмах криптогарфічного захисту інформації. Для реалізації зазначених операцій на основі ізогенії еліптичної кривої била використана бібліотека програмних функцій Miracl, на базі якої побудовані та перевірені криптографічні функції необхідні для реалізації операцій на ізогеніях еліптичної кривої. Для експерименту були обрані криві для простих полів з бітовою довжиною характеристики поля 256, 384, 512 біт. Були побудовані та реалізовані операції скалярного множення точок кривої, результати обчислення яких наведені нижче. Для кожного випадку пораховані значення часу для скалярного множення точок кривої. В ході проведених досліджень були розроблені програмні функції для реалізації операцій над ізогеніями еліптичних кривих різного порядка, які забезпечують зазначені в стандарті рівні безпеки: 256, 384, 512.

Таким чином, при широкому розповсюдженні квантових комп’ютерів рішення задачі ECDLP буде можливо за 51 рік, коли існуючі можливості дозволяють її вирішити приблизно за 10^{15} років.

modul	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE4D
ord(P)	4000000000000000000000000000000029E26087789BC2815BDFF97093543CCF
koef a, d	2, 18
P (x,y)	91F5D0E7E2D417E3108B13B075CDC7756045F8424479FCFE8F23D27250A0883F, 742F27A268641C9D7DDF69892BE3DF3D8F9CC52260B89A4953C8379C7C0A212B
Випад. число k	25
Q=k*P	19EB06BEA98AC21EFC739590179433B9B68DEDF3CE2F1571755616A4B3E4932F, AB2DFB4ECB2A536BE738FD47BCDBC181B4D792C0BB7B12E7664FA669B6097851
t сер. (сек)	0.01

384

modul	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFF79D
ord(P)	4000000000000000000000000000000000000000000000000AF905B73674AC7D4AF38C53331DC208A51 7DCB3F340EECF
koef a, d	2, 214
P (x,y)	F5FC151B6264CB53A4B879AA9A1F4A5156BBF063B56AAA912617C0E4CEFF15D2DF497D9AEF123 74A22D22C3B402B2C71, A9027207E88074F4AFA3D44D4590DD04BAFBF6AE3D321091F500C783F4707940B7F5EBDD93325C 5391843F9A78526BB1
Випад. число k	25
Q=k*P	A1CEAAC37594B34668E9EB6990099048A60FEF7EE85A9629F4AC3F613201D2A14DE2F755199DA9 CCB11BE0EC4985D752, 1FA6D7AD65274DE5BD21B95FD5662EC9FC6C33CE5FEAB7FA644CF06E352E2389A0939F956DD10 E23DB30CDA43548EB43
t сер. (сек)	0.015

512

modul	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFc95
ord(P)	400000000000000000000000000000000000000000000000000000000000000028A3CE52209E2BD495288 2D5574165192C46C0D0311FEA6BF9FECE70EE63B59F
koef a, d	2, 10D
P (x,y)	5230A1EE747050A072BD7319741586EA520388B6B53094571C821A2FC9A9E83D56665346B5DB04C4 3E75261DBDA512728FAAFAC48AE9260A5A184E2933E3A400, 53A0D50CC63C9219762F451978AEF214DBCFCC3A5CB5EF27124991A86B42B3A1A832724A0E6B93 0FDD1DA2E27A540D6B675E4422C444F529C508F0BAE7D0A85
Випад. число k	25
Q=k*P	E98A73BD0D40C22597796F9D20FDC4C14C7CD73814856E7E6A000605A7AC69A9815C503A457873 AC974F65C2EE5713609F59A33CDC3E817E82E71B90C4E11635, 52DB4C4B91414C2D4ABE10DE55054BDC58C4B1B5ACA469119C48FDF10ED1280F5D0E90017F6C8 93FCA619BBC07BE79E504B23F7CF9AEEDC00A11BA579BDF314A
t сер. (сек)	0.026

Слід врахувати, що одна з складнощів використання квантового комп’ютеру це проведення аналізу та вимірів різних квантових станів, що накладає суттєві обмеження на таку криптоаналітичну систему. В таких умовах, одним з варіантів обрання одного з перспективних напрямків розвитку криптографічних систем на еліптичних кривих,

зазначених в стандартах, є використання ізоморфних та гомоморфних трансформацій еліптичних кривих з метою збільшення стійкості до квантових атак перспективних криптосистем на еліптичних кривих. В ході досліджень були отримані нові параметри еліптичних кривих в формі Веєрштраса та Едвардса для рівнів безпеки: 256, 384, 512. Згенеровані базові точки кривих для реалізації в перспективних криптографічних додатках. Отримані три варианти стандартних кривих, для яких обчислені оцінки середнього часу скалярного множення точок кривої. Побудована ізогенія еліптичної кривої третього порядку та отримана ізоморфна трансформація еліптичної кривої. Розроблені необхідні програмні операцій для побудови ізогенії еліптичної кривої на основі бібліотеки програмних функцій Miracl. Побудовані та перевірені операції для обчислення ізогенії заданого порядка еліптичної кривої, параметри якої забезпечують зазначені в стандарті рівні безпеки.

В подальшому підхід до використання гомоморфних перетворень (ізогенії еліптичної кривої) може бути застосований для побудови алгоритмів генерації криптографічних ключів в легковагової криптографії, в криптографічних системах, які використовуються в інформаційно-телекомунікаційних системах критичної інфраструктури.

ЛІТЕРАТУРА

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

2. Web: https://aroundcyber.files.wordpress.com/2012/11/stuxnet_under_the_microscope.pdf.

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

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

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

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

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

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

9. A. Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. Adv. in Math. of Comm., 4(2):215–235, 2010.

10. S. Galbraith and A. Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. Applicable Algebra in Engineering, Communication and Computing, 24(2):107 – 131, 2013.

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

12. Craig Costello, Patrick Longa, Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. CRYPTO 2016. https://eprint.iacr.org/2016/413.pdf

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

14. J. Tate. Endomoprhisms of abelian varieties over finite fields. Inventiones Mathematica, 2:134–144, 1966.