ISSN 0485-8972

УДК 621.391.15:519.7 **DOI:10.30837/rt.2026.1.224.04**

А.В. БЕССАЛОВ, д-р техн. наук

АЛГОРИТМ PQC CSIKE НА НЕЦИКЛІЧНИХ КРИВИХ ЕДВАРДСА З ОДНОЧАСНИМ ФОРМУВАННЯМ ДВОХ НЕЗАЛЕЖНИХ КЛЮЧІВ ІНКАПСУЛЯЦІЇ

Вступ

У 2018 р. з'явився алгоритм CSIDH (Commutative Supersingular Isogeny Diffi-Hellman) [1] пост квантової криптографії (PQC). Він відрізняється від інших відомих алгоритмів мінімальною довжиною ключа. На той час найбільш швидкими були криві у формі Едвардса [2, 3], а побудова ланцюжків ізогенних кривих виконувалась за формулами [4]. У роботах [5, 6], вперше розглянуто його імплементації на кривих Едвардса на основі координат Фарашахі–Хосейні $(W:Z)$. Порівняно з традиційній швидкій арифметиці кривих у формі Монтгомері [1], авторам [5, 6] вдалось отримати виграш 20 % у швидкості виконання операцій.

В роботі [7] ми дали огляд наших робіт, присвячених аналізу і модифікаціям алгоритму CSIDH на нециклічних кривих Едвардса. Інтегральна оцінка виграшу в швидкодії CSIDH при реалізації цих модифікацій замість відомих досягає 1500 разів. Наприклад, алгоритм «constant-time CSIDH» [8], який пропонує захист від атак побічного каналу, лише вдвічі гальмує імплементацію алгоритму.

В роботі [9] альтернативою «constant-time CSIDH» ми запропонували метод рандомізації алгоритму. Крім захисту від атак побічного каналу він прискорює алгоритм приблизно у чотири рази.

Формули теореми 2 фундаментальної роботи [4] не дають можливості розраховувати параметри ізогеній скручених кривих Едвардса. Тому ми в роботі [10] вперше довели теорему 1, формули якої включають параметр *a* скрученої кривої Едвардса. Такі криві мають значні переваги при застосуванні в алгоритмі CSIDH.

Оригінальний алгоритм CSIKE (Commutative Supersingular Isogeny Key Encapsulation) запропоновано нами в [11, 12]. Метою цієї роботи є обґрунтування і моделювання одночасного розрахунку Алісою двох ключів інкапсуляції замість одного у класичному алгоритмі. Це дозволяє, по-перше, отримати резервний ключ для симетричної криптосистеми. По-друге, фрагментами додаткового ключа можна нарощувати перший ключ і значно збільшувати рівень безпеки криптосистеми. По-трете, паралельні обчислення двох незалежних ланцюжків ізогеній лишає глузду задачу вимірювання часу розрахунку фрагментів цих ціпочок, атака побічного каналу неможлива. Алгоритм «constant-time CSIDH» стає даремним.

Во всіх наших роботах ми застосовуємо більш коректну, порівняно з [3], класифікацію кривих у формі Едвардса [13]. Це дозволяє не допускати явних помилок, наприклад в роботі [14], які коментуються в роботі [15].

Ідея одночасного розрахунку двох ключів інкапсуляції базується на існуванні в класах квадратичних і скручених кривих Едвардса двох множин ізоморфних суперсингулярних кривих Едвардса (СКЕ). Елементи цих множин пов'язані як $d \leftrightarrow d^{-1}$, тобто кожній нециклічній кривій E_d відповідає ізоморфна крива $E_{d^{-1}}$. Тому на двохпроцесорному комп'ютері з різними програмами можна будувати незалежні ціпочки ізогеній і ключі. На відміну від попередньої роботи [12], в моделі CSIKE трьох ступенів 3, 5, 7 ізогеній цієї роботи ми одразу будуємо всі потрібні ланцюжки ізогеній на їх періоді T. При цьому дві СКЕ з параметрами $d = 2^{\pm 1} mod p$ над полем F_p, $p \equiv 7\, mod\, 8$, вже відомі [16, 17]. Стало зрозуміло, що 3-ізогенія максимального періоду $T = 33$ містить всі елементи першої множини, а їх інверсії дають другу множину ізоморфних кривих (і відповідну 3-ізогенію).

Наш аналіз спирається на властивості суперсингулярних квадратичних та скручених кривих Едвардса, пов'язаних як пари квадратичного кручення [13]. Суперсингулярні криві

цих класів з однаковим порядком $N_E = p+1 = 2^m n, m \geq 3,$ (n – непарне) існують лише при $p \equiv 3 \bmod 4$. Мінімальний парний кофактор порядку таких кривих дорівнює 8, тоді для алгоритмів CSIDH, CSIKE з непарним $n = \prod_{i=1}^{K} l_i$ модуль поля F_p слід вибирати як $p = 8n - 1.$

У розд. 1 наведено основні визначення для класів повних, скручених і квадратичних суперсингулярних кривих Едвардса (СКЕ) [12, 13]. У розд. 2 розглядається класичний алгоритм CSIKE з передачею одного ключа. Розд. 3 присвячено обґрунтуванню можливості паралельних обчислень на двопроцесорному комп'ютері одразу двох ключів, розрахунку в полі F_p, p =8 39, всіх ланцюжків ізогеній 3, 5 і 7 ступенів і моделюванню процедур інкапсуляції і декапсуляції двох ключів. Наведено висновки і подальші напрямки досліджень.

1. Основні визначення

Розглянемо деякі специфічні властивості СКЕ. Еліптична крива в узагальненій формі Едвардса [13] визначається рівнянням з двома параметрами *a*,*d*, вперше заданим в фундаментальній роботі [3]:

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

При квадратичному характері $\chi(ad) = -1$ крива (1) ізоморфна *повній кривій* Едвардса [2] з одним параметром d:

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

Такі криві є циклічними, а їх порядок $N_E \equiv 0 \bmod 4$.

У випадку $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ має місце ізоморфізм кривої (1) з *квадратичною кривою Едвардса* [13]

$$E_d: \quad x^2 + y^2 = 1 + dx^2 y^2, \quad \chi(d) = 1, \ d \neq 1. \tag{3}$$

Ці криві є нециклічними з порядком $N_E \equiv 0 \bmod 8$.

На відміну від (2) параметр d кривої (3) визначено як квадрат. Для обох кривих (2) та (3) зазвичай приймають в (1) $a = 1$. У роботі [3] крива (3) разом із кривою (2) названі *кривими Едвардса*. Разом з цим відмінність квадратичних характерів цих кривих веде до кардинально різних їх властивостей, що привело до їх нової класифікації [13].

Скручена крива Едвардса визначена в роботі [13] як окремий випадок кривої (1) при $\chi(a) = \chi(d) = -1.$

Ми визначаємо пару квадратичної і скрученої кривої Едвардса [13] як пару квадратичного кручення з параметрами $\chi(ad) = 1, a' = ca, d' = cd, \chi(c) = -1$). Оскільки СКЕ існують лише при $p \equiv 3 \bmod 4$ [13], можна прийняти $c = -1, a' = -a = -1, d' = -d,$ де $a, d -$ параметри квадратичної кривої, відповідно $a', d' -$ скрученої кривої. Інакше кажучи, перехід від квадратичної до скрученої кривої і назад можна визначити як $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Відповідно рівняння скрученої СКЕ при $p \equiv 3 \bmod 4$ з (1) можна записати

$$E_{-1,-d}: \quad x^2 - y^2 = 1 - dx^2 y^2, \quad d \in F_p^*, \quad d \neq 1., \chi(d) = 1. \tag{4}$$

Порядки нециклічних СКЕ (3) і (4) над простим полем F_p однакові $N_E = p + 1$, однак структури їх відрізняються. Крім двох точок $(0, \pm 1),$ всі їхні точки різні, тому ізогенії однакових ступенів мають різні ядра і обчислюються незалежно. Обидві криві є нециклічними щодо точок парного порядку (мають по три точки другого порядку, дві з яких – особливі точки

$D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$ [13]). Квадратична СКЕ, крім того, містить дві особливі точки четвертого порядку $\pm F_1=\left(\infty,\pm\frac{1}{\sqrt{d}}\right)$. Наявність трьох точок другого порядку обмежує числом 8 мінімальний парний кофактор порядку $N_E=8n,\ (n-\textit{непарне})$ скручених і квадратичних СКЕ [13]. Важливо, що точки парних порядків у обчисленнях алгоритму CSIDH не беруть участь (після першого множення на 4 випадковій точки R).

Вибір пари кривих квадратичного кручення (3), (4) замість повних кривих (2) подвоює кількість всіх СКЕ і прискорює алгоритм CSIDH з оцінкою в 2:[5] разів за рахунок відсутності потреби в інверсії параметра *d* для квадратичного кручення кривої (2) [7].

Для кривої (1) J -інваріант дорівнює [3, 18]

$$J(a,d)=\frac{16(a^2+d^2+14ad)^3}{ad(a-d)^4},\quad ad(a-d)\neq 0,\quad . \tag{5}$$

Цей параметр розрізняє ізогенні (з різними J -інваріантами) і ізоморфні (з рівними J інваріантами) криві. Так як J -інваріант зберігає своє значення для всіх ізоморфних кривих і пар квадратичного кручення [18], він однаковий для пари квадратичних і скручених СКЕ ($a=\pm 1$). Він є корисним інструментом при пошуку суперсингулярних кривих, так і при побудові графів ланцюжків ізогеній. Однією з властивостей J -інваріанту $J(d)$ є

$$J(d)=J(d^{-1}).$$

Важливо, що для нециклічних класів СКЕ (3), (4) заміна $d\to d^{-1}$ дає ізоморфізм, а для повних кривих Едвардса (2) – квадратичне кручення.

2. Алгоритм CSIIKE на нециклічних кривих Едвардса

Алгоритм PQC CSIDH (Commutative SIDH) запропонований авторами [1] для вирішення тієї ж задачі обміну ключами (SIDH-Supersingular Isogeny Diffie-Hellman), але на основі ізогенних відображень еліптичних кривих в цілому як адитивних абелевих груп. Таке відображення над простим полем F_p визначено як клас групової дії (the class group action [1]) і є комутативним. У порівнянні з відомою оригінальною схемою CRS (Couveignes (1997), Rostovtsev, Stolbunov (2004)) на несуперсингулярних кривих використання ізогеній суперсингулярних кривих дозволило кардинально прискорити алгоритм і отримати найменший з відомих розмір ключа (512 біт у роботі [1]) при рівні квантової безпеки 128 біт).

Нехай крива E над простим полем F_p порядку $N_E=p+1\equiv 0 \bmod 8$ містить точки малих непарних порядків $l_k, k=1,2,...,K.$ Тоді існує ізогенна крива E' того ж порядку N_E як відображення ступеня: $l_k: E\to E'=[l_k]*E$. Повторення цієї операції e_k разів позначається як $[l_k{}^{e_k}]*E$. Значення експонент $e_k\in Z$ визначають довжину ланцюжка ізогеній ступеня l_k. У роботі [1] прийнятий інтервал значень експонент $[-m\le e_k\le m], m=5,\ K=74,$ що забезпечує рівень безпеки 128 біт при атаках квантового комп'ютера. Негативні значення експоненти означають перехід до скрученої СКЕ (4).

Імплементація алгоритму CSIDH в [1] використовує швидку арифметику еліптичних кривих Монтгомері $y^2=x^3+Cx^2+x,\ C\neq\pm 2$, що містять дві точки четвертого порядку і, відповідно, мають порядок $N_E=4n\left(n=\prod_{k=1}^{K}l_k\right)$. У роботі [5] алгоритм будується на повних СКЕ того самого порядку. У цій роботі пропонуємо використовувати в алгоритмі CSIDH квадратичні та скручені СКЕ, що мають більш високі показники швидкодії, ніж повні криві

Едвардса (2). Таким чином, для цих класів СКЕ з порядком $N_E = 8n = p + 1$, модуль поля в алгоритмі CSIDH слід вибирати як $p \equiv 7 \bmod 8$ або $p = 8\prod_{k=1}^{K} l_k - 1$.

Класичний неінтерактивний алгоритм Діффі–Хелмана ґрунтується на використанні двох відкритих ключів. Те ж завдання формування загального секрету може бути вирішено в інтерактивному протоколі з одним сеансом передачі та одним відкритим ключем одержувача, що є більш безпечним. Для цього Аліса генерує загальний секрет κ, шифрує його відкритим ключем Боба та відправляє йому зашифрований ключ. Після отримання Боб розшифровує його своїм секретним ключем. Цей протокол називається інкапсуляцією ключа.

На основі CSIDH ми пропонуємо його модифікацію як алгоритм CSIKE (Commutative Supersingular Isogeny Key Encapsulation). Він включає три етапи:

1**. Генерація ключа** κ. Аліса за допомогою датчика випадкових чисел знаходить секретний вектор $\Omega_\kappa = (e_1, e_2, .., e_K)$, будує функцію класу групової дії $\Theta_\kappa = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ і обчислює ізогенну криву$E_\kappa = \Theta_\kappa * E_0$, де $E_0 -$ стартова крива, параметр d_κ кривої E_κ вона приймає як секретний ключ $d_\kappa = \kappa$.

2. **Інкапсуляція ключа**. Це процедура шифрування Алісою ключа κ відкритим ключем Боба E_B Для цього Аліса обчислює ізогенну криву $\Theta_\kappa * E_B = E_{\kappa B}$. Параметр $d_{\kappa B}$ цієї кривої як шифрований ключ інкапсуляції вона надсилає Бобу.

3. **Декапсуляція ключа**. Дешифрування Бобом кривої $E_{\kappa B}$ своїм секретним ключем Ω_B зводиться до обчислення ним ізогенної кривої $\overline{\Theta_B} * E_{\kappa B} = E_\kappa$, де відображення $\overline{\Theta_B}$ будується за допомогою адитивна-оберненого секретного ключа Боба: $\Omega_B \to (-\Omega_B)$.

По суті ми пропонуємо оригінальний алгоритм CSIKE як модифікацію CSIDH, замінюючи секретний ключ Аліси секретним вектором Ω_κ, за допомогою якого вона обчислює криву $E_\kappa = \Theta_\kappa * E_0$ та загальний секретний ключ $d_\kappa = \kappa$. Далі Аліса шифрує його відкритим ключем Боба E_B і обчислює криву $E_{\kappa B} = \Theta_\kappa * E_B = \Theta_\kappa * \Theta_B * E_0$. Боб при декапсуляції знімає свій шифр за допомогою мультиплікативно зворотної функції $\overline{\Theta_B}$ (такої що $\Theta_B * \overline{\Theta_B} = \mathrm{I}$), тим самим він реставрує криву$E_\kappa = \Theta_\kappa * E_0$. Як ключ інкапсуляції обома сторонами можна прийняти J -інваріант кривої E_κ.

Слід зазначити, що додатковим секретним параметром двох сторін є також стартова крива E_0, яку одноразово можна обирати з відомого масиву або обчислювати згідно з секретною функцією Θ_s. Це нарощує рівень безпеки алгоритму.

3. Моделювання процедур інкапсуляції та декапсуляції двох незалежних ключів

Розглянемо просту модель імплементації алгоритму CSIKE на квадратичних та скручених СКЕ, що утворюють пари квадратичного крутіння кривих з порядком $p+1$. Такі криві існують лише за умови $p \equiv -1 \bmod 8$ і мають порядок $N_E = cn$ ($n - непарне$), $c \equiv 0 \bmod 8$. Нехай така пара кривих містить ядра третього, п’ятого і сьомого порядків. При значенні $n = 105$ мінімальне просте $p = 8n - 1 = 839$, тоді порядок цих кривих $N_E = 8n = 840$.

У попередній роботі [12] ми розраховували множину всіх 66 квадратичних СКЕ E_d перебором параметрів $d \neq 1$, які є квадратами в полі F_p. Тут зручніше одразу розраховувати ланцюжки 3-ізогеній на періоді T = 33. Це і визначає множину всіх елементів d СКЕ, яка шукається.

Згідно з теоремою 1 роботи [17] при $p \equiv -1 \bmod 8$ квадратична крива (3) з параметром $d = 2^{\pm 1}$ є суперсінгулрною. Ми можемо завжди побудувати циклічний ланцюжок 3-ізогенії такої СКЕ, яка має при стартовому елементі d = 2 вигляд вектору довжиною 33 3-розрядних числа:

$I3_d$ = (002, 028, 259, 752, 773, 015, 243, 021, 433, 180, 514, 578, 293, 666, 038, 112, 172, 683, 258, 772, 488, 636, 286, 508, 076, 236, 043, 788, 061, 289, 144, 414, 405) (6)

Зауважимо, що серед всіх 33 елементів на множині (6) нема ізоморфних кривих (див. (5)).

Нехай $\delta = d^{-1}$, тоді відповідний ланцюжок параметрів δ 3-ізогеній ізоморфних СКЕ може бути записано як

$I3_\delta$ = (420, 030, 230, 135, 750, 056, 511, 040, 808, 564, 475, 045, 063, 742, 052, 427, 200, 640, 413, 288, 098, 777, 795, 365, 276, 032, 800, 329,784 090, 705, 610,810). (7)

Для множин параметрів (5) і (6) виділяємо першу жирним шрифтом. Ланцюжки 5- та 7-ізогеній мають періоди T = 11, тому всі параметри попадають в три вектори для кожного ступеня:

$$I5_{d1} = (002, 788{,}636, 112{,}180, 752, 144, 076, 258, 293, 243),$$

$$I5_{d2} = (028, 061, 286, 172, 514, 773, 414, 236, 772, 666, 021),$$

$$I5_{d3} = (259, 289, 508, 683, 578{,}015, 405, 043, 488, 038, 433),$$

$$I7_{d1} = (002, 112, 144, 293, 788, 180, 076, 243, 636, 752, 258),$$

$$I7_{d2} = (028, 172, 414, 666, 061, 514, 236, 021, 286, 773, 772),$$

$$I7_{d3} = (259, 683, 405, 038, 289, 278, 043, 433, 508, 015, 488).$$

Якщо обчислення виконуються на множині (7), всі елементи приведених вище ланцюжків інвертуються.

Слід зауважити, що всі три підмножини 11 параметрів 5- та 7-ізогеній співпадають, хоча порядок їх чергування в ланцюжках різний. Наведена вище інформація є достатньою для шифрування будь яких секретних ключів у нашої моделі. Розглянемо приклад обчислень Аліси і Боба у процедурі інкапсуляції ключів.

Нехай відправник Аліса створює два секретних вектори $\Omega_1 = (-5{,}5{,}6)$ і $\Omega_2 = (7{,}2{,}-6)$, а секретний ключ отримувача Боба $\Omega_B = (6, -4{,}5)$. Боб розраховує свій відкритий ключ за допомогою стартової квадратичної СКЕ з параметром d = 2 і отримує за 15 кроків ізогенну криву з параметром:

$$\frac{d_0 = 2}{(3)} \xrightarrow{6} \frac{243}{(5)} \xrightarrow{-4} \frac{144}{(7)} \xrightarrow{5} 243, \quad d_B = 243.$$

Тут, як і в роботах [11, 12 та ін.], ступінь ізогеній пишемо внизу, параметр d – вгорі, а над стрілкою – число кроків ланцюжка («+» для квадратичної кривої, «–» для скрученої). В першому випадку в послідовності елементів векторів ізогеній ми йдемо зліва – направо, в другому випадку – справа – ліворуч.

Для розрахунку одночасно двох ключів інкапсуляції Аліса застосовує двопроцесорний комп'ютер, де один процесор працює з 33 елементами $I3_d$ (5), а другий – з ізоморфними СКЕ (6). Параметри їх стартових кривих $d_0 = 2^{\pm 1} \bmod p$ взаємно зворотні в полі F_p .

Згідно з алгоритмом інкапсуляції Аліса на базі двох функцій групових дій $\Theta_1 = (3^{-5}, 5^5, 7^6)$ та $\Theta_2 = (3^7, 5^2, 7^{-6})$ і двох взаємно зворотних стартових СКЕ з параметрами d_0 = 2 і d_0 = 420 розраховує одночасно два ключі інкапсуляції:

$$\frac{d_0=2}{(3)} \xrightarrow{-5} \frac{061}{(5)} \xrightarrow{5} \frac{414}{(7)} \xrightarrow{6} 286, \quad d_{k1} = 286. \tag{8}$$

$$\frac{d_0=420}{(3)} \xrightarrow{7} \frac{040}{(5)} \xrightarrow{2} \frac{784}{(7)} \xrightarrow{-6} 750, \quad d_{k2} = 750. \tag{9}$$

Перевіркою правильности цих результатів є зміна порядків чергування ступенів ізогеній, наприклад:

$$\frac{d_0 = 2}{(5)} \xrightarrow{5} \frac{752}{(7)} \xrightarrow{6} \frac{788}{(3)} \xrightarrow{-5} 286, \quad d_{k1} = 286.$$

$$\frac{d_0{=}420}{(7)} \xrightarrow{-6} \frac{564}{(3)} \xrightarrow{7} \frac{200}{(5)} \xrightarrow{2} 750, \quad d_{k2} = 750.$$

Результати теж самі, властивість комутативності виконується.

Далі Аліса шифрує відкритий ключ Боба $d_B = 243$ на першому процесорі за допомогою функції $\Theta_1 = (3^{-5}, 5^5, 7^6)$ і отримує зашифрований перший ключ інкапсуляції

$$\frac{d_B = 243}{(3)} \xrightarrow{-5} \frac{028}{(5)} \xrightarrow{5} \frac{773}{(7)} \xrightarrow{6} 061, \quad d_{Bk1} = 061.$$

Одночасно другий процесор інвертує відкритий ключ Боба $d_B^{-1} = 511$ і розраховує зашифрований другий ключ $d_B^{-1} * \Theta_2$, $\Theta_2 = (3^7, 5^2, 7^{-6})$

$$\frac{d_B^{-1} = 511}{(\mathbf{3})} \xrightarrow{7} \frac{742}{(5)} \xrightarrow{2} \frac{30}{(7)} \xrightarrow{-6} 475 \quad d_{Bk2} = 475.$$

Передача Алісою останніх двох ключів послідовно завершує етап інкапсуляції. Далі на етапі декапсуляції Бобу вже не потрібен двопроцесорний комп'ютер. Він спочатку за допомогою свого секретного ключа $\Omega_B = (6, -4{,}5)$ і його обернення на $-\Omega_B$ розшифровує перший ключ d_{Bk1}, потім другий:

$$\frac{d_{Bk1}{=}061}{(3)} \xrightarrow{-6} \frac{286}{(5)} \xrightarrow{4} \frac{414}{(7)} \xrightarrow{-5} 286 \quad d_{k1} = 286.$$

$$\frac{d_{Bk2} = 475}{(3)} \xrightarrow{-6} \frac{750}{(5)} \xrightarrow{4} \frac{742}{(7)} \xrightarrow{-5} 750, \quad d_{k2} = 750.$$

Таким чином, Боб отримав два незалежні ключі інкапсуляції (8), (9) замість одного в класичному алгоритмі. Додатковий ключ можна застосовувати як резервний при зміні ключа, або нарощувати його фрагментами перший ключ з метою підвищення рівня безпеки симетричної криптосистеми.

Важливою перевагою алгоритму, який пропонується, є практично ідеальна безпека у відношенні атак побічного каналу по вимірюванню часу розрахунку елементів e_i секретного ключа Аліси. При одночасному розрахунку двома процесорами з випадковими виборами шляхів ізогенних ціпочок в кожному розділити ці процедури неможливо, як і взагалі поставити задачу атаки.

Висновки

Запропонована імплементація оригінального алгоритму CSIKE [12] з паралельним обчисленням одразу двох ключів інкапсуляції, на наш погляд, цікава у перспективі для завдань стандартизації алгоритмів PQC. Сама ідея використання двопроцесорного комп'ютера і раніше не застосованого резерву двох класів нециклічних кривих Едвардса – ізоморфних кривих з двократним розміром цих двох класів, ця ідея є новою і перспективною. Важливою перевагою алгоритму, який пропонується, є практично ідеальна безпека в відношенні атак побічного каналу по вимірюванню часу розрахунку елементів $e_{i,k}$ секретних ключів Аліси. При одночасному розрахунку двома процесорами з випадковими виборами шляхів ізогенних ланцюжків в кожному розділити ці процедури неможливо, як і взагалі поставити задачу атаки. Зрозуміло, що при однакових резервах ефективніше рішити дві задачі, ніж одну. А ще краще – три. Додатковий ключ корисний як резервній, також і для нарощування його фрагментами першого для росту рівня безпеки. Варіантів багато. Не менш перспективним є застосування несуперсингулярних кривих Едвардса [18], які поширюють множини корисних

кривих вже не в два, а в чотири рази. Відповідний розглянутому алгоритм інкапсуляції чотирьох ключів потребує чотирьохпроцесорного комп'ютера. Ми плануємо провести дослідження цієї задачі у наступному.

Список літератури:

1. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: An efficient post-quantum commutative group action // Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology {ASIACRYPT 2018. P. 395{427. Springer I nternational Publishing, Cham (2018).
2. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology–ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833, Berlin: Springer, 2007. P. 29.
3. Bernstein D.J., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards curves // AFRICACRYPT 2008. Vol. 5023 of LNCS. Springer, 2008. P.389–405.
4. Moody D., Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves // Mathematics of Computation. 2016. Vol. 85, no. 300. P. 1929–1951.
5. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves // Security and Communication Networks, 2019.
6. Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong, and Young-Ho Park Efficient Isogeny Computations on Twisted Edwards Curves Hindawi // Security and Communication Networks. 2019. Vol. 2018. Article ID 5747642.
7. Bessalov A., Sokolov V., Abramov S., Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves // MDPI, Cryptography, 2024. P.2–17.
8. Onuki H., Aikawa Y., Yamazaki T., Takagi T. A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.
9. Bessalov A.V., Kovalchuk L.V., Abramov S.V Randomization of CSIDH algorithm on quadratic and twisted Edwards curves // Кібербезпека: освіта, наука, техніка. 2022. Т.1, №17. С.128–144.
10. Bessalov A., Sokolov V., Skladannyi P., Zhyltsov O. Computing of odd degree isogenies on supersingular twisted Edwards curves // CEUR Workshop Proceedings. 2021. Vol. 2923 P. 1–11.
11. Bessalov A., Sokolov V., Skladannyi P. Abramov S., Zhyltsov O. Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves // CEUR Workshop Proceedings. 2022. Vol. 3288. P. 1–10.
12. Бессалов А.В., Абрамов С.В. Алгоритм PQC CSIKE на нециклічних кривих Едвардса // Кібернетика та системний аналіз. 2023.Т. 59, №6. С.3–18.
13. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография : моногр. Киев : Политехника, 2017. 272 с.
14. Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. How to construct CSIDH on Edwards curves // Cryptographers' Track at the RSA Conference–CT-RSA 2020. Springer, 2020. P. 512–537.
15. Bessalov A. V. On correctness of implementation conditions CSIDH algorithm on Edwards curves // Радіотехніка. 2022. Вип. 208. С.16–27.
16. Bessalov A.V., Kovalchuk L.V. Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3. // Cybernetics and Systems Analysis. 2019. Vol. 55(3). P. 347–353.
17. Bessalov A.V., Kovalchuk L.V. Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3 // Cybernetics and Systems Analysis. 2019. Vol. 55(5). P. 731–741.
18. Bessalov A., Abramov S., Sokolov V., Skladannyi P., & Zhyltsov, O. (2023). Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves // Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC). 2023. Vol. 3504. P. 12–25. (Scopus Q4).
19. Washington L. C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

Надійшла до редколегії 02.01.2026
Прийнята до друку після рецензування 23.04.2026
Публікація (оприлюднення) 30.04.2026

Відомості про автора:
Бессалов Анатолій Володимирович – д-р техн. наук, професор, Київський університет імені Бориса Грінченка, професор кафедри інформаційної та кібернетичної безпеки, факультет інформаційних технологій та управління, Україна; email: bessalov@ukr.net; ORCID: https://orcid.org/0000-0002-6967-5001