КІБЕРНЕТИКА

УДК 621.391.15:519.7

А.В. БЕССАЛОВ
Київський університет імені Бориса Грінченка, Київ, Україна, e-mail: *bessalov@ukr.net.*

С.В. АБРАМОВ
Київський університет імені Бориса Грінченка, Київ, Україна,
e-mail: *s.abramov.asp@kubd.edu.ua.*

АЛГОРИТМ PQC CSIKE НА НЕЦИКЛІЧНИХ КРИВИХ ЕДВАРДСА

Анотація. Запропоновано оригінальний алгоритм постквантової криптографії CSIKE як модифікацію CSIDH, але з одним відкритим ключем замість двох. Обґрунтовано умови його імплементації на двох класах нециклічних кривих Едвардса. Розглянуто властивості квадратичних та скручених суперсингулярних кривих Едвардса, що утворюють пари квадратичного кручення порядку $p+1 \equiv 0 \bmod 8$ над простим полем F_p. Наведено модифікацію алгоритму CSIDH і алгоритм CSIKE, які побудовані на ізогеніях цих кривих замість традиційної арифметики кривих у формі Монтгомері. Для ізогеній ступенів 3, 5, 7 розраховано і табульовано параметри ізогенних ланцюжків нециклічних суперсингулярних кривих Едвардса, якщо $p = 839$. Розглянуто імплементацію схеми інкапсуляції ключа за умови, що Аліса шифрує його відкритим ключем Боба. Запропоновано новий рандомізований алгоритм CSIKE з випадковим рівноймовірним вибором кривої з двох класів на кожному кроці ланцюжка ізогеній. Наведено оцінку ймовірності успішної атаки побічного каналу в рандомізованому алгоритмі, у якому запропоновано можливість відмови від обчислення ізогенної функції $\phi(R)$ випадкової точки R, що істотно прискорить алгоритм.

Ключові слова: крива в узагальненій формі Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, ізоморфізм, ізогенія, u-координати, квадратичний лишок, квадратичний нелишок.

ВСТУП

Алгоритм CSIDH (Commutative Supersingular Isogeny Diffi–Hellman) [1] постквантової криптографії (PQC) на відміну від інших відомих алгоритмів має мінімальну довжину ключа, що приблизно дорівнює модулю простого поля F_p, над яким виконуються групові операції. Перші його імплементації базувалися на традиційній швидкій арифметиці кривих у формі Монтгомері. У роботі [2] запропоновано новий ефективний метод обчислення ізогеній непарних ступенів на кривих Едвардса на основі координат Фарашахі–Хосейні [3]. Ця робота базується на методі Монтгомері диференціального додавання точок та адаптує його до кривих Едвардса. Оптимізація арифметики ізогеній на кривих Едвардса в проєктивних координатах $(W:Z)$ [2] значно прискорила алгоритми, розглянуті в [4], і надала можливість отримати виграш 20 % у швидкості виконання операцій порівняно з реалізацією алгоритму CSIDH на кривих у формі Монтгомері. Формули обчислення ізогеній непарних ступенів кривих Едвардса [5] також містять компоненти диференціального додавання точок, що стало основою методу, запропонованого в [2].

Імплементація CSIDH в [2] використовує повні суперсингулярні криві Едвардса порядку $N_E = p+1 \equiv 0 \bmod 4$. Алгоритм CSIDH будується на ізогеніях

суперсингулярних кривих певного класу та їхніх квадратичних крученнях. Для повних кривих Едвардса E_d квадратичне кручення лежить усередині цього класу і досягається заміною параметра $d \to d^{-1}$, $\chi(d) = -1$. Ми пропонуємо вдвічі розширити простір кривих Едвардса в алгоритмі CSIDH, використовуючи два класи нециклічних квадратичних і скручених кривих Едвардса, що утворюють пари квадратичного кручення. З цією метою в роботі [6] доведено дві теореми, що адаптують формули ізогеній [5] до скручених кривих Едвардса та до формул у координатах $(W:Z)$. У роботі [8] і в цій статті розглянуто приклади імплементації алгоритму CSIDH або його блоків на нециклічних класах квадратичних і скручених кривих Едвардса. Однією з їхніх особливих властивостей на відміну від повних кривих є кратність їхнього порядку числу 8: $N_E = p+1 \equiv 0 \bmod 8$. У статті [8] також наведено критичний аналіз теоретичних результатів, отриманих у роботі [7], в якій ця відома умова [9–14] не виконується.

У цій статті запропоновано оригінальну модифікацію алгоритму CSIDH — алгоритм CSIKE (Commutative Supersingular Isogeny: Key Encapsulation). Він суттєво відрізняється від відомого прототипу SIKE [15] і відкритий для модифікації. Тут ми демонструємо його роботу на простій моделі. Найважливішою перевагою CSIKE є використання одного відкритого ключа замість двох.

Відома проблема алгоритму CSIDH — це вразливість до атаки побічного каналу, побудованої на вимірюванні часу обчислення ланцюжка ізогеній кожного ступеня l_k, пропорційного секретній експоненті e_k ключа. У багатьох роботах [17, 18] та ін. цю проблему пропонують розв'язувати нарощуванням експонент e_k фіктивними експонентами до відомого максимуму (Constant time CSIDH). Зрозуміло, що така надмірність знижує швидкість виконання алгоритму. У цій статті ми пропонуємо та обґрунтовуємо альтернативний підхід для протидії згаданій атаці — рандомізацію алгоритму CSIDH (CSIKE). Вона зумовлює неминуче зростання ймовірності помилки аналітика, яка через довготривалий процес вимірювань зриває атаку.

Наш аналіз у цій роботі базується на властивості суперсингулярних квадратичних та скручених кривих Едвардса, які утворюють пари квадратичного кручення [13, 14]. Суперсингулярні криві цих класів, які мають однаковий порядок $N_E = p+1 = 2^m n$, $m \ge 3$ (n — непарне), існують лише за умови $p \equiv 3 \bmod 4$. Мінімальний парний кофактор порядку таких кривих дорівнює 8, тоді для алгоритму CSIDH з непарним $n = \prod_{i=1}^{K} l_i$ модуль поля потрібно вибирати як у випадку $p = 8n - 1$.

У розд. 1 наведено короткий огляд властивостей скручених і квадратичних суперсингулярних кривих Едвардса (СКЕ) [11, 13, 14]. У розд. 2 розглянуто специфічні аспекти імплементації моделі алгоритму CSIDH на квадратичних і скручених СКЕ, наведено модифікацію алгоритму [1], на основі теорем 1, 2 та твердження 1 обґрунтовано властивості ізогенних ланцюжків цих класів СКЕ. У розд. 3 запропоновано алгоритм CSIKE, розраховано та табульовано параметри ізогенних кривих ступенів 3, 5, 7, наведено приклад обчислень Аліси та Боба у схемі інкапсуляції ключа. У розд. 4 обґрунтовано рандомізацію алгоритму CSIKE (CSIDH) зі статистичною оцінкою ймовірності успішної атаки побічного каналу, наведено новий рандомізований алгоритм CSIKE, в якому запропоновано можливість відмови від обчислення ізогенної функції $\phi(R)$ випадкової точки R кривої в алгоритмі CSIKE (CSIDH).

1. ВЛАСТИВОСТІ КВАДРАТИЧНИХ І СКРУЧЕНИХ СУПЕРСИНГУЛЯРНИХ КРИВИХ ЕДВАРДСА

Розглянемо деякі специфічні властивості суперсингулярних кривих Едвардса [13, 14]. Еліптичну криву в узагальненій формі Едвардса [11] можна визначити рівнянням

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

За умови квадратичності $\chi(ad) = -1$ крива (1) є ізоморфною повній кривій Едвардса [9, 10] з одним параметром d

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

Такі криві є циклічними, а їхній 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 [11]

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

Ці криві є нециклічними і мають порядок $N_E \equiv 0 \bmod 8$.

На відміну від (2) параметр d кривої (3) визначено як квадрат. Для кривих (2) та (3) зазвичай вважають $a = 1$. У роботі [10] криву (3) і криву (2) названо кривими Едвардса. Водночас відмінність квадратичних характерів цих кривих визначає і кардинально різні їхні властивості [11, 12].

Скручену криву Едвардса описано в роботі [11] як окремий випадок кривої (1) для $\chi(ad) = 1, \chi(a) = \chi(d) = -1$. Ми визначаємо пару квадратичної і скрученої кривої Едвардса [11] як пару квадратичного кручення з параметрами $\chi(ad) = 1$, $a' = ca$, $d' = cd$, $\chi(c) = -1$ (розд. 2, теорема 2). Оскільки СКЕ існують лише за умови $p \equiv 3 \bmod 4$ [13], можна вважати $c = -1$, $a' = -a = -1$, $d' = -d$, де a, d — параметри квадратичної кривої, відповідно a', d' — параметри скрученої кривої. Інакше кажучи, перехід від квадратичної до скрученої кривої і зворотно можна визначити, як $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Відповідно рівняння скрученої СКЕ за умови $p \equiv 3 \bmod 4$ з (1) можна записати у вигляді

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

Порядок еліптичної кривої N_E над простим полем F_p визначається на основі сліду t характеристичного рівняння ендоморфізму Фробеніуса $\pi^2 - t\pi + p = 0$ як $N_E = p + 1 - t$. Для кривої квадратичного кручення E^t відповідний порядок становить $N_E^t = p + 1 + t$. Еліптична крива є суперсингулярною тоді і тільки тоді, якщо над будь-яким розширенням простого поля F_p слід рівняння Фробеніуса становить $t \equiv 0 \bmod p$, при цьому $\pi^2 = -p, \pi = \pm\sqrt{-p}$ [13, 14, 16]. Інакше кажучи, в алгебраїчному замиканні $\overline{F}_p$ суперсингулярна крива не містить точок порядку p. Над простим полем F_p така крива завжди має порядок $N_E = p + 1$.

Отже, квадратичні і скручені СКЕ як пара квадратичного кручення мають однаковий порядок $N_E = p + 1$, $p \equiv 7 \bmod 8$, але різну структуру. Крім двох точок $(0, \pm 1)$, всі їхні точки різні, тому ізогенії однакових ступенів мають різні ядра і обчислюються незалежно. Ці криві є нециклічними щодо точок парного порядку (мають по три точки 2-го порядку, дві з них — особливі $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty \right)$ [11]). Квад-

ратична СКЕ, крім того, містить дві особливі точки 4-го порядку $\pm F_1 = \left(\infty, \pm \frac{1}{\sqrt{d}} \right)$.

Наявність трьох точок 2-го порядку обмежує числом 8 мінімальний парний кофактор порядку $N_E = 8n$ (n — непарне) скручених і квадратичних СКЕ [11]. Зауважимо, що точки парних порядків у обчисленнях алгоритму CSIDH не використовують (після першого множення на 4 випадкової точки R).

Для кривої (1) J-інваріант має вигляд [10, 16]

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

Цей параметр розрізняє ізогенні (з різними J-інваріантами) та ізоморфні (з однаковими J-інваріантами) криві. Оскільки J-інваріант зберігає своє значення для всіх ізоморфних кривих і пар квадратичного кручення [16], він є однаковим для пари квадратичних і скручених СКЕ ($a = \pm 1$), тому ми будемо послуговуватися J-інваріантом $J(d)$. Він є корисним інструментом для пошуку суперсингулярних кривих і для побудови графів ланцюжків ізогеній. Однією з властивостей J-інваріанту $J(d)$ є

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

Для аналізованих класів СКЕ заміна $d \to d^{-1}$ дає ізоморфізм, а для повних кривих Едвардса — квадратичне кручення.

2. АЛГОРИТМ CSIDH НА КВАДРАТИЧНИХ І СКРУЧЕНИХ КРИВИХ ЕДВАРДСА

Алгоритм PQC CSIDH запропоновано в [1] для розв'язання задачі обміну ключами (SIDH — Supersingular Isogeny Diffie–Hellman), але на основі ізогенних відображень еліптичних кривих у 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 дає змогу прискорити алгоритм і отримати найменший із відомих розмір ключа (512 біт у роботі [1] за умови квантової безпеки 128 біт).

Нехай крива E порядку $N_E = p + 1 \equiv 0 \bmod 8$ над простим полем F_p містить точки малих непарних порядків l_k, $k = 1, 2, \ldots, K$. Тоді існує ізогенна крива E' того самого порядку N_E як відображення ступеня: $l_k : E \to E' = [l_k] * E$. Повторення цієї операції e_k разів позначається як $[l_k^{e_k}] * E$. Показники експонент $e_k \in Z$ визначають довжину ланцюжка ізогеній ступеня l_k. У роботі [1] прийнято інтервал значень експонент $[-m \le e_k \le m]$, $m = 5$, $K = 74$, що забезпечує рівень безпеки 128 біт у разі атак квантового комп'ютера. Від'ємні значення експоненти означають перехід до суперсингулярної кривої квадратичного кручення.

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 4-го порядку і відповідно мають порядок $N_E = 4n$ ($n = \prod_{k=1}^{K} l_k$). У роботі [2] алгоритм побудовано на повних СКЕ того самого порядку. У цій роботі в алгоритмі CSIDH ми пропонуємо використовувати квадратичні та скручені СКЕ, що мають ті самі рекордні показники швидкодії, що й повні криві Едвардса [2]. Така можливість виникає з урахуванням доведених нами в роботі [6] теорем.

Отже, для цих класів СКЕ порядку $N_E = 8n = p+1$ модуль поля в алгоритмі CSIDH слід вибирати за умови $p \equiv 7 \bmod 8$ або $p = 8\prod_{k=1}^{K} l_k - 1$. Характеристичне рівняння ендоморфізму Фробеніуса має вигляд $\pi^2 = -p = 1 \bmod l_k \Rightarrow$ $\Rightarrow (\pi - 1)(\pi + 1) = 0$. Суперсингулярні пари квадратичного кручення як два розв'язки рівняння ендоморфізму Фробеніуса часто позначають $E[\pi - 1]$ і $E[\pi + 1]$. Зазначимо, що заміна одного класу повних СКЕ двома класами квадратичних і скручених СКЕ подвоює кількість кривих, що використовують в алгоритмі CSIDH, і, як наслідок, посилює його безпеку. Це подвоєння зумовлене тим, що параметр d всіх повних кривих Едвардса «пробігає» всі $\dfrac{p-1}{2}$ значень квадратичних нелишків, тоді як для двох інших класів використовуються всі значення $d \neq 0.1$.

В основі побудови ізогеній непарних простих ступенів для квадратичних кривих Едвардса лежить теорема 2 з роботи [5], а для скручених кривих Едвардса — теорема 1 з [6]. У роботі [6] вперше наведено формули відображень для кривої (1), що залежать від двох параметрів (теорему наведено далі).

Теорема 1 [6]. Нехай $G = \{(1, 0), \pm Q_1, \pm Q_2, \ldots, \pm Q_s\}$ — підгрупа непарного простого порядку $l = 2s + 1$ точок $\pm Q_i = (\alpha_i, \pm\beta_i)$ кривої $E_{a,d}$ (1) над полем F_p.

Визначимо

$$\phi(P) = (x', y') = \left(\prod_{Q \in G} \frac{x_{P+Q}}{x_Q} \frac{x_{P-Q}}{x_{Q,}}, \prod_{Q \in G} \frac{y_{P+Q}}{x_Q} \frac{y_{P-Q}}{x_{-Q,}} \right).$$

Тоді $\phi(x, y)$ — це l-ізогенія з ядром G кривої $E_{a,d}$ у криву $E_{a',d''}$ з параметрами

$$a' = a^l, \; d' = d^l A^8, \; A = \prod_{i=1}^{s} \alpha_i, \tag{6}$$

і з відображуваною функцією

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i x)^2 - (a\beta_i y)^2}{1 - (d\alpha_i \beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i \beta_i xy)^2} \right) \tag{7}$$

або

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{x^2 - a\beta_i^2}{1 - d\beta_i^2 x^2}, \frac{-y}{A^2} \prod_{i=1}^{s} \frac{x^2 - \alpha_i^2}{a - d\alpha_i^2 x^2} \right). \tag{8}$$

Її доведення наведено у [6]. Тут параметр a фігурує у формулах (6), (7) та (8) на відміну від [5].

З темою нашої статті перетинається робота [7]. Оскільки термін «криві Едвардса», вперше визначений у роботі [10] для всіх кривих E_d з одним параметром d, є неоднозначним (не враховує значення квадратичного характеру $\chi(d)$), виникає питання: про які криві Едвардса ((2) або (3)) йдеться у роботі [7]? Автори [7] зняли це питання новим терміном «purely Edwards curves», маючи на увазі всі криві E_d з одним параметром, крім повних. За нашою класифікацією [11, 12], це квадратичні криві Едвардса (3). Але всередині цього класу кривих не існує пар квадратичного кручення, на яких будується алгоритм CSIDH. Це доведемо у такій теоремі.

Теорема 2. Для кривої $E_{a,d}$ (1) в узагальненій формі Едвардса $x^2 + ay^2 = 1 + dx^2y^2$, яку задано над простим полем F_p, існує єдина (з точністю до ізоморфізму) крива квадратичного кручення $E^t_{a,d} = E_{\bar{a},\bar{d}}$ з параметрами $\bar{a} = ca$, $\bar{d} = cd$, $c \in F_p^*$.

Доведення. З рівняння (1) маємо

$$y^2 = \frac{1-x^2}{a-dx^2}. \tag{9}$$

Нехай $\chi(d) = -1,\ \chi(a) = 1,\ a = d^2 = c^{-1}$. Квадратичне кручення (9) можна задати перетворенням квадрата y^2 в квадратичний нелишок

$$dy^2 = \frac{1-x^2}{d^2-dx^2}\cdot d = \frac{1-x^2}{1-d^{-1}x^2}\cdot d^{-1} \Rightarrow \chi\left(\frac{1-x^2}{1-d^{-1}x^2}\right) = 1.$$

Тоді для кривої квадратичного кручення можна записати рівняння

$$E^t_{\bar{a},\bar{d}} = E_{d^{-1}}:\ x^2 + y^2 = 1 + d^{-1}x^2y^2,\ \chi(d) = -1.$$

Задані вище умови справедливі для класу повних кривих Едвардса з одним параметром, якщо $a = d^2 = c^{-1}$, $\bar{a} = 1$, $\bar{d} = d^{-1}$. Цей результат добре відомий з роботи [9].

Нехай тепер $\chi(a) = \chi(d) = 1, \chi(c) = -1$. Тоді квадратичне кручення (9) можна записати у вигляді

$$c^{-1}y^2 = \frac{1-x^2}{a-dx^2} \Rightarrow y^2 = \frac{1-x^2}{ca-cdx^2} = \frac{1-x^2}{\bar{a}-\bar{d}x^2}.$$

Звідси випливає, що квадратичне кручення кривої $E_{a,d}$ з параметрами, що задовольняють умові $\chi(a) = \chi(d) = 1$ (квадратична крива, яка ізоморфна (3)) визначає криву класу скручених кривих Едвардса (1) після підстановки $\bar{a} = ca$, $\bar{d} = cd$, $\chi(c) = -1$. Інакше кажучи, квадратичним крученням кривої E_d (3) є скручена крива Едвардса $E^t_d = E_{c,cd}$, $\chi(d) = 1, \chi(c) = -1$. Різні параметри c утворюють ізоморфні криві. Обернене відображення задають множенням обох параметрів на c^{-1}: $E^t_{c,cd'} = E_d,\ \chi(d) = 1,\ \chi(c) = -1$. Теорему доведено.

Наслідок 1. Для квадратичних кривих Едвардса E_d ($\chi(d) = 1$, $d \neq 1$) не існує кривих квадратичного кручення всередині цього класу. Квадратичним крученням кривої (3) є скручена крива Едвардса $E_{c,cd}$, $\chi(d) = 1, \chi(c) = -1$.

Наслідок 2. Для повних кривих Едвардса E_d ($\chi(d) = -1$) існують криві квадратичного кручення $E_{d^{-1}}$ лише всередині цього класу.

Наслідок 1 випливає з унікальності відображення квадратичного кручення як бієкції. Воно дає змогу вилучити з розгляду криві $E_d[\pi - 1]$ з одним параметром [7]. Детальну критику теорем з роботи [7] наведено в [8].

Зауважимо, що твердження теореми 2 відомі з піонерських робіт [9, 10]. Однак у теоремі 2 ми даємо оригінальну і більш загальну схему доведення для всіх класів кривих Едвардса у вигляді (1).

Отже, у класі повних кривих Едвардса (2) пара квадратичного кручення $E_d \leftrightarrow E^t_d = E_{d^{-1}}$ лежить усередині цього класу і має мультиплікативні зворотні параметри $d^{\pm 1}$. Навпаки, для класу квадратичних кривих Едвардса (3) для $p \equiv 3 \bmod 4$ і $c = -1$ квадратичне кручення $E^t_d \to E_{-1,-d}$ утворює криву з класу скручених кривих Едвардса з адитивними зворотними параметрами a (ca) і d (cd).

Неінтерактивний обмін ключами за схемою Діффі–Хеллмана включає такі етапи [1].

1. Вибір параметрів. Для малих простих непарних l_k обчислюють $n = \prod_{k=1}^{K} l_k$, де K визначається рівнем безпеки, і вибирають відповідний модуль поля $p = 2^m \prod_{k=1}^{K} l_k - 1$, $m \geq 2$, а також стартову еліптичну криву E_0.

2. Обчислення відкритих ключів. Аліса за допомогою свого секретного ключа $\Omega_A = (e_1, e_2, \ldots, e_K)$ будує функцію класу групової дії як ізогенні відображення $\Theta_A = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ та обчислює ізогенну криву $E_A = \Theta_A * E_0$ як свій відкритий ключ. Боб на основі секретного ключа Ω_B та функції Θ_B виконує ті самі обчислення та отримує свій відкритий ключ $E_B = \Theta_B * E_0$. Ці криві визначаються їхніми параметрами з точністю до ізоморфізму.

3. Обмін ключами. Тут протокол такий самий, як у п. 2 із заміною $E_0 \to E_B$ для Аліси та $E_0 \to E_A$ для Боба. Знаючи відкритий ключ Боба, Аліса обчислює $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$. Аналогічні дії Боба визначають результат $E_{AB} = \Theta_B * E_A = \Theta_B * \Theta_A * E_0$, що збігається з першим ключем унаслідок комутативності групової операції. Як розділений секрет береться J-інваріант кривої $E_{AB}\,(E_{BA})$.

Для кожної Θ_A існує мультиплікативна обернена функція $\overline{\Theta_A}$ така, що $\Theta_A * \overline{\Theta_A} = \mathrm{I}$, де $\mathrm{I} = [1, 1, \ldots, 1]^K$ — нейтральний елемент класу групової дії (K-вимірний вектор з одиниць). Відображення $\overline{\Theta_A}$ будується шляхом інверсії знаків усіх експонент e_k відображення Θ_A. Ми використовуємо його як $\overline{\Theta_B}$ у нашому алгоритмі декапсуляції ключа.

Важливою властивістю ізогенних ланцюжків пари квадратичного кручення СКЕ (3) та $E_{-1,-d}$ (4) суперсингулярних еліптичних кривих є таке твердження.

Твердження 1. Послідовність параметрів $\{d^{(i)}\}$, $i = 0, 1, 2, \ldots, T$, у періоді T l-ізогенних СКЕ $E_d^{(i)}$ (3) над простим полем F_p має реверсний порядок $i = T, T-1, T-2, \ldots, 1, 0$ для СКЕ квадратичного кручення $E_{-1,-d}^{(i)}$ (4).

Доведення. Компоненти функції Θ класу групової дії мають властивості мультиплікативної групи і тому комутативні та можуть бути зворотними. На одному кроці ланцюжка ізогенії $[l_k^1]$ крива $E_d^{(0)}$ відображається в ізогенну криву $E_d^{(1)} = E_d^{(0)} * [l_k^1]$, а її параметр $d^{(0)} \to d^{(1)}$. Функція діє і на квадратичне кручення кривої E_d — криву $E_{-1,-d}$. Долучимо до попереднього результату наступний крок ізогенії $[l_k^{-1}]$, тоді $E_d^{(2)} = E_d^{(0)} * [l_k^1] * [l_k^{-1}] = E_d^{(0)}$ унаслідок $[l_k^1] * [l_k^{-1}] = 1$. Отже, два ізогенні переходи для кривих пари квадратичного кручення повертають нас до стартової кривої $E_d^{(0)}$. Для параметра кривої на другому етапі це означає перехід $d^{(1)} \to d^{(0)}$. Очевидною є справедливість обернення порядку параметрів кривих $\{d^{(i)}\}$ пари квадратичного кручення для довільного значення e_k експоненти ізогенії з урахуванням $[l_k^{e_k}] * [l_k^{-e_k}] = 1$. Доведення завершено.

Граф ізогеній на підставі твердження 1 є неорієнтованим у тому сенсі, що будь-яка його вершина може бути як виходом, так саме і входом.

Наведемо модифікацію алгоритму обчислень Аліси відповідно до п. 2 [2] з використанням ізогеній квадратичних та скручених СКЕ.

Algorithm 1: Evaluating the class-group action on twisted and quadratic SEC.

Input: $d_A \in E_A$, $\chi(d)=1$ *and a list of integers* $\Omega_A=(e_1,e_2,\dots,e_K)$.

Output: d_B *such that* $[l_1^{e_1},l_2^{e_2},\dots,l_K^{e_K}]*E_A=E_B$, *where* $E_{A,B}: x^2+y^2=$

$=1+d_{A,B}x^2y^2$,

1. **While** *some* $e_i\neq 0$ **do**
2. *Sample a random* $x\in F_p$,
3. Set $a\leftarrow 1$, $E_A: x^2+y^2=1+d_Ax^2y^2$ **if** $(1-x^2)/(1-dy^2)$ *is a square in* F_p,
4. **else** $a\leftarrow -1$, $E_A: x^2-y^2=1-d_Ax^2y^2$,
5. *Let* $S=\{i\mid ae_i>0\}$. **If** $G=\varnothing$ *then start over to line 2 while* $a\leftarrow -a$,
6. *Let* $n=\prod_{i\in S}l_i$, *and compute* $R\leftarrow[(p+1)/2n]P$, $P\leftarrow P(x,y)$,
7. **For** *each* $i\in S$ **do**
   8. *Compute* $Q\leftarrow[k/l_i]R$,
   9. **If** $Q\neq(1,0)$ *Compute an isogeny* $\phi: E_A\to E_B$ *with* $\ker\phi=Q$,
   10. *Set* $d_A\leftarrow d_B$, $R\leftarrow\phi(R)$, $e_i\leftarrow e_i-a$,
   11. *Skip* i *in* S *and* $n\leftarrow n/l_i$ **if** $e_i=0$,
12. **Return** d_A.

У порівнянні з алгоритмом 2 з роботи [1] в алгоритмі 1, адаптованому до квадратичних і скручених СКЕ, зроблено деякі корекції.

1. Перевірку квадратичного характеру у правій частині y^2 п. 3 виконують для рівняння квадратичної кривої Едвардса (3).

2. Скориговано п. 9 (не можна вилучати індекс до обнулення в п. 10).

3. Оновлення числа $n\leftarrow n/l_i$ разом із вилученням i в п. 11 потрібно робити після обнулення e_i.

Відповідно до п. 10 для кожного l_i обчислюють тільки e_i ізогеній до обнулення експоненти e_i. Залежно від знака ізогенії обчислюють в класі квадратичних ($e_i>0$) або скручених СКЕ ($e_i<0$).

3. АЛГОРИТМ CSIKE НА КВАДРАТИЧНИХ І СКРУЧЕНИХ КРИВИХ ЕДВАРДСА

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

На основі CSIDH ми пропонуємо алгоритм CSIKE (Commutative Supersingular Isogeny: Key Encapsulation), який аналогічно [15] складається з трьох етапів.

1. Генерація ключа κ. Аліса за допомогою датчика випадкових чисел знаходить секретний вектор $\Omega_\kappa=(e_1,e_2,\dots,e_K)$, будує функцію класу групової дії $\Theta_\kappa=[l_1^{e_1},l_2^{e_2},\dots,l_K^{e_K}]$ і обчислює ізогенну криву $E_\kappa=\Theta_\kappa*E_0$, параметр d_κ якої вважає секретним 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 вона надсилає Бобу.

3. Декапсуляція ключа. Щоб дешифрувати криву $E_{\kappa B}$ своїм секретним ключем Ω_B, Боб обчислює ізогенну криву $\overline{\Theta_B} * E_{\kappa B} = E_\kappa$, де відображення $\overline{\Theta_B}$ будується з інверсією всіх знаків експонент секретного ключа Боба: $\Omega_B \to (-\Omega_B)$.

Власне, 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 $d_\kappa = \kappa$. Потім 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 під час декапсуляції скасовує свій шифр, використовуючи мультиплікативну обернену функцію $\overline{\Theta_B}$ (таку, що $\Theta_B * \overline{\Theta_B} = I$), тим самим він відновлює криву $E_\kappa = \Theta_\kappa * E_0$. Як ключ інкапсуляції обидві сторони використовують J-інваріант кривої E_κ.

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

Розглянемо просту модель імплементації алгоритму CSIKE на квадратичних та скручених СКЕ, що утворюють пари квадратичного кручення кривих порядку $p+1$. 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 3-го, 5-го і 7-го порядків. Якщо $n = 105$, мінімальне просте $p = 8n - 1 = 839$, то порядок цих кривих становить $N_E = 8n = 840$. Параметр d усієї сім'ї 418 квадратичних кривих Едвардса E_d можна прийняти як квадрати $d = r^2 \bmod p$, $r = 2\ldots419$. З цієї послідовності знайдено 66 пар квадратичних і скручених СКЕ з параметрами $a = \pm 1$ і $\chi(ad) = 1$. У табл. 1 наведено масив значень параметрів d для пар квадратичних E_d та скручених $E_{-1,-d}$ СКЕ. Вони записані як квадрати $d = r^2 \bmod p$, $r = 2\ldots419$, у порядку зростання r. У цьому прикладі відносна частка СКЕ приблизно дорівнює 16 %. Зауважимо, що для кожної кривої з табл. 1 існує щонайменше одна ізоморфна крива з параметром d^{-1} і однаковим J-інваріантом (5).

Для першої квадратичної кривої $E_d^{(0)} = E_{144}$ з табл. 1 можна побудувати 3-, 5- і 7-ізогенії і знайти параметри $d^{(i)}$ ланцюжка ізогенних кривих $E_d^{(i)}$, $i = 0, 1, 2, \ldots$, таких, що $d^{(T)} = d^{(0)}$. Період T ланцюжка ізогеній ділить число $66 = 2 * 3 * 11$ всіх СКЕ. У табл. 2–4 наведено результати розрахунків параметрів $d^{(i)}$ ланцюжків відповідно 3-ізогеній, 5-ізогеній та 7-ізогеній квадратичних СКЕ. На кожному кроці $i = 0, 1, 2, \ldots, T$ ізогенії ступеня $l = 2s + 1$ обчислюють координати $\alpha_1, \ldots, \alpha_s$, $s = (l-1)/2$, точок ядра, потім за формулою (6) розраховують параметр $d^{(i+1)}$ ізогенної кривої $E_d^{(i+1)}$. У табл. 2–4 у першому рядку записано номери i ізогенних кривих, у наступних s рядках — координати точок

Таблиця 1. Масив значень 66 параметрів d квадратичних та скручених СКЕ ($a = \pm 1$) для $p = 839$ і $N_E = 840$

144	289	784	2	61	258	508	365	488	30	705
742	56	259	180	329	135	640	32	38	28	90
564	772	286	40	610	98	475	63	511	43	795
414	76	752	800	405	666	112	413	200	236	433
15	683	293	750	808	578	288	636	514	276	773
243	45	788	172	777	427	21	810	552	420	230

Таблиця 2. Значення параметрів ланцюжка 3-ізогенних квадратичних СКЕ ($a=1$) для $p=839$ (період $T=33$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha^{(i)}$	518	558	768	178	502	44	372	136	258	75	487
$d^{(i)}$	**144**	**414**	**405**	**2**	**28**	**259**	**752**	**773**	**15**	**243**	**21**
i	11	12	13	14	15	16	17	18	19	20	21
$\alpha^{(i)}$	697	481	333	248	613	378	663	404	20	377	99
$d^{(i)}$	**433**	**180**	**514**	**578**	**293**	**666**	**38**	**112**	**172**	**683**	**258**
i	22	23	24	25	26	27	28	29	30	31	32
$\alpha^{(i)}$	718	379	327	139	781	41	601	344	561	230	477
$d^{(i)}$	**772**	**488**	**636**	**286**	**508**	**76**	**236**	**43**	**788**	**61**	**289**

Таблиця 3. Значення параметрів двох ланцюжків 5-ізогенних квадратичних СКЕ ($a=1$) для $p=839$ (період $T=11$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha_1^{(i)}$	78	343	152	337	318	344	588	222	151	352	390
$\alpha_2^{(i)}$	537	655	632	720	545	837	790	832	748	372	790
$d^{(i)}$	**144**	**76**	**258**	**293**	**243**	**2**	**788**	**636**	**112**	**180**	**752**
$\alpha_1^{(i)}$	327	390	91	125	653	17	251	744	409	586	103
$\alpha_2^{(i)}$	726	552	609	583	655	682	393	764	577	692	531
$d^{(i)}$	**289**	**508**	**683**	**578**	**15**	**405**	**43**	**488**	**38**	**433**	**259**

Таблиця 4. Значення параметрів двох ланцюжків 7-ізогенних квадратичних СКЕ ($a=1$) для $p=839$ (період $T=11$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha_1^{(i)}$	9	485	99	161	255	103	367	73	41	422	362
$\alpha_2^{(i)}$	718	700	319	248	705	131	828	258	731	582	820
$\alpha_3^{(i)}$	17	826	678	465	322	324	700	99	229	689	591
$d^{(i)}$	**144**	**293**	**788**	**180**	**76**	**243**	**636**	**752**	**258**	**2**	**112**
$\alpha_1^{(i)}$	314	204	30	86	86	74	324	37	281	284	251
$\alpha_2^{(i)}$	563	416	337	222	489	314	530	164	513	741	544
$\alpha_3^{(i)}$	678	207	313	720	571	430	595	496	418	828	342
$d^{(i)}$	**289**	**578**	**43**	**433**	**508**	**15**	**488**	**259**	**683**	**405**	**38**

ядра, потім — рядок із параметрами $d^{(i)}$ ізогенних кривих. Рядки розташовано один за одним з періодом $s+2$ або $s+1$. Для 3-ізогеній з періодом $T=33$ для повноти не вистачає ще однієї таблиці, подібної до табл. 2, з другою половиною параметрів $d^{(i)}$ з табл. 1. Для 5-ізогеній і 7-ізогеній з періодом $T=11$ табл. 3 і 4 містять лише $1/3$ всіх ізогеній (параметри $d^{(i)}$ ізогеній кривих зображено напівжирним шрифтом).

Далі ми покажемо, що комутативність функції $\Theta_A = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ дає змогу отримувати підсумкові результати за умов неповних даних. Неповнота зумовлена потребою у скороченні обсягу табульованих даних у статті. З цієї ж причини не наведено даних для ізогеній скручених СКЕ $E^{(i)}_{-1,-d}$, $i = 0, 1, 2, \ldots, T-1$. Натомість використано просту властивість твердження 1 про реверсні порядки параметрів $d^{(i)}$ СКЕ ланцюжків $E^{(i)}_d$ і $E^{(i)}_{-1,-d}$.

Приклад 1. Нехай Аліса згенерувала секретний вектор $\Omega_\kappa = (6, -4, 7)$, який відображенням $\Theta_\kappa = [3^6, 5^{-4}, 7^7]$ на першому етапі трансформує у загальний секретний ключ κ, тобто обчислює криву $E_\kappa = \Theta_\kappa * E_0$. На другому етапі вона шифрує цей ключ відкритим ключем Боба d_B. Вважатимемо, що секрет Боба $\Omega_B = (-7, 5, -4)$, відповідно його функція класу групової дії матиме вигляд $\Theta_B = [3^{-7}, 5^5, 7^{-4}]$. Виконаємо обчислення ключів κ, d_B. Нехай стартовою кривою ланцюжка ізогеній є крива $E^{(0)}_d = E_{144}$. Тоді $E_\kappa = E_0 * \Theta_\kappa$, $E_B = E_0 * \Theta_B$.

Для спрощення запису в алгоритмі обчислення ізогенної кривої користуватимемося лише параметрами $d^{(i)}$, які повністю визначають криві $E^{(i)}_{-1,-d}(e_k < 0)$ і $E^{(i)}_d(e_k > 0)$ як пари квадратичного кручення. Властивість комутативності функції Θ_κ в нашому прикладі означає, що існує $3! = 6$ варіантів вибору порядку розташування ступенів ізогеній. Якщо дані табл. 2–4 неповні, цей вибір може бути невдалим. У разі успішного вибору ступенів ізогеній обчислення Аліси згідно з $E_\kappa = E_0 * \Theta_\kappa$ можна виконати двома способами:

$$\frac{d_0 = 144}{(7)} \xrightarrow{7} \frac{752}{(5)} \xrightarrow{-4} \frac{788}{(3)} \xrightarrow{6} 2,\ d_\kappa = \kappa = 2,$$

$$\frac{d_0 = 144}{(5)} \xrightarrow{-4} \frac{636}{(7)} \xrightarrow{7} \frac{788}{(3)} \xrightarrow{6} 2.$$

Отже, загальний секретний ключ $\kappa = 2$. Аналогічно одним із цих способів визначаємо відкритий ключ Боба на основі кривої $E^{(0)}_d = E_{144}$ та функції $\Theta_B = [3^{-7}, 5^5, 7^{-4}]$:

$$\frac{d_0 = 144}{(5)} \xrightarrow{5} \frac{2}{(7)} \xrightarrow{-4} \frac{243}{(3)} \xrightarrow{-7} 405,$$

$$\frac{d_0 = 144}{(7)} \xrightarrow{-4} \frac{752}{(5)} \xrightarrow{5} \frac{243}{(3)} \xrightarrow{-7} 405.$$

Отже, відкритий ключ Боба $d_B = 405$. Потім на другому етапі інкапсуляції Аліса шифрує відкритим ключем Боба секретний ключ $\kappa = 2$ і обчислює $E_{B\kappa} = E_B * \Theta_\kappa$. У нашому прикладі обчислення Аліси для $\Theta_\kappa = [3^6, 5^{-4}, 7^7]$ та вибір ступенів 3-, 5-, 7-ізогеній формують зашифрований ключ інкапсуляції:

$$\frac{d_B = 405}{(3)} \xrightarrow{6} \frac{15}{(5)} \xrightarrow{-4} \frac{289}{(7)} \xrightarrow{7} 259 \Rightarrow d_{B\kappa} = 259.$$

Нарешті, на третьому етапі декапсуляції Боб з кривої E_{259} отримує свій секретний ключ за допомогою оберненої функції $\overline{\Theta_B} = [3^7, 5^{-5}, 7^4]$:

$$\frac{d_0 = 259}{(7)} \xrightarrow{4} \frac{289}{(5)} \xrightarrow{-5} \frac{43}{(3)} \xrightarrow{7} 2 \Rightarrow d_\kappa = 2.$$

У результаті він отримує загальний секретний ключ $\kappa = 2$, який для нього обчислила Аліса. Щоб уникнути неоднозначності у разі отримання ізоморфних кривих, ключем інкапсуляції обидві сторони вважають J-інваріант (5) $J(d_\kappa) = 558$ кривої E_2.

4. РАНДОМІЗАЦІЯ АЛГОРИТМУ CSIKE (CSIDH)

Запропонований авторами роботи [1] алгоритм CSIDH побудований так, що обчислення ізогенних ланцюжків згідно з функціями $\Theta_{A,B} = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ виконують у два етапи: спочатку формують множину S з експонентами ключа e_k одного знака, потім іншого. На кожному етапі послідовно обчислюють ядра і параметри $|e_k|$ ізогенних кривих ступеня l_k, побудованих на кривих одного класу (E_d або $E_{-1,-d}$). Це очевидним чином породжує загрозу атаки побічного каналу на основі впорядкованого вимірювання часу цих обчислень, пропорційних довжині $|e_k|$ і ступеню l_k кожної компоненти $\Theta[l_k^{e_k}]$. Тому в більшості статей на цю тему розглядають різні варіанти «Constant time CSIDH» [17, 18], у яких секретні експоненти e_k нарощуються до верхньої межі m фіктивними ланцюжками ізогеній. Зрозуміло, що такий захист досягається значною надмірністю та уповільненням алгоритму.

Ми пропонуємо інший метод розв'язання проблеми — рандомізацію шляху ізогенних ланцюжків. Ідея полягає в тому, що будь-яка випадкова координата x еліптичної кривої завжди породжує випадкову точку $P = (x, y)$ однієї з двох кривих пари квадратичного кручення. На початку алгоритму секрет Аліси розбивається на дві множини: S_0 та S_1 (аналоги S), в які потрапляють значення e_k з різними знаками. На першому кроці вибір випадкової точки $P = (x, y)$ з ймовірністю $1/2$ визначає клас кривих (E_d або $E_{-1,-d}$), одній з яких належить точка P. Далі в цьому класі обчислюють ядро та першу ізогенну криву $E^{(1)} = [l_k] * E^{(0)}$ ступеня l_k, що відповідає знаку експоненти e_k. Вибір l_k рандомізується, а значення $|e_k|$ зменшується на 1. На наступному кроці з новим значенням параметра $d^{(1)}$ цю процедуру повторюють і обчислюють параметр $d^{(2)}$. Процес триває до обнулення всіх e_k. Вочевидь, що такий метод вдвічі прискорює процедуру випадкового вибору точок P і суттєво знижує ймовірність успішної атаки побічного каналу.

Слід зазначити, що у класичному CSIDH вже є гарантований рівень захисту від розглянутого вище типу атаки побічного каналу. Він визначається знаком секретної експоненти e_k ключа. Оскільки для кожної складової $[l_k]$ функції Θ час обчислення $[l_k^{+1}]$ і $[l_k^{-1}]$ однаковий, ймовірність успіху аналітика навіть в умовах безпомилково знайдених значень l_k становить $2^{-K} = 2^{-74}$ (для даних з [1]). Для середньої довжини $\frac{m+1}{2} = 3$ ланцюжка ізогеній кожного ступеня l_k загальна середня довжина ланцюжка ізогеній функцій $\Theta_{A,B} = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ становить $3 \cdot 74 = 222$ кроки. Нехай p_1 — ймовірність безпомилкового визначення ступеня l_k аналітиком на одному кроці рандомізованого протоколу CSIDH, тоді ймовірність його успіху можна оцінити величиною $2^{-74} p_1^{222}$, $p_1 < 1$. Наприклад, для $p_1 = \frac{3}{4}$ ймовірність успіху аналітика дорівнює 2^{-166}, а для $p_1 = 0.9$ значення цієї ймовірності наближається до 2^{-108}. Можливі різні модифікації запропонованого методу рандомізації зі вставками одиночних фіктивних експонент у вибіркові

складові $[l_k]$ функції Θ, що зменшить p_1 і не додасть надмірності в обчислення. Нагадуємо, що одна помилка аналітика руйнує всю його трудомістку роботу.

Приклад 2. Для ілюстрації методу рандомізації на основі табл. 2–4 наведемо приклад обчислення Алісою секретного ключа κ на основі секретного вектора $\Omega_\kappa = (6, -4, 7)$. Нехай у послідовності ізогеній символ $\lambda = 0$ відповідає випадковому вибору кривої E_d, а символ $\lambda = 1$ — вибору $E_{-1,-d}$. У достатньо довгій послідовності ці символи вважатимуться рівноймовірними. У цьому прикладі довжина ланцюжка ізогеній дорівнює $6 + 4 + 7 = 17$ з розподілом частот $\left\{\frac{13}{17}, \frac{4}{17}\right\}$. Тоді можна змоделювати коротку псевдовипадкову послідовність $\Lambda = 00100100001000100$ довжиною 17 ізогенних кривих протягом обчислення Алісою секретного ключа κ. Як і в розд. 3, розпочнемо зі стартової кривої E_{144} і використовуватимемо дані табл. 2 або табл. 4 для серій символів 0 послідовності Λ і даними табл. 3 — для серій символів 1. У першому випадку рядками таблиць ми рухаємося вправо, в другому — вліво. Кількість кроків визначається довжиною серії однакових символів в Λ (цю кількість записано поруч зі знаками експонент над стрілками ізогенних переходів). Отже, на шляху Λ за 17 кроків Аліса обчислює ключ у такий спосіб:

$$\underset{(3)}{d_0 = 144} \xrightarrow{2} \underset{(5)}{405} \xrightarrow{-1} \underset{(7)}{15} \xrightarrow{2} \underset{(5)}{259} \xrightarrow{-1} \underset{(7)}{433} \xrightarrow{4} \underset{(5)}{259} \xrightarrow{-1} \underset{(3)}{433} \xrightarrow{3} \underset{(5)}{578}$$

$$\underset{(5)}{578} \xrightarrow{-1} \underset{(7)}{683} \xrightarrow{1} \underset{(3)}{405} \xrightarrow{1} 2 \Rightarrow d_\kappa = \kappa = 2.$$

Цей результат збігається з результатом, отриманим у розд. 3. Рандомізація вибору кривих, по суті, випадковим чином дробить експоненти ключа Ω_A і додає значної невизначеності в завдання аналітика.

Розглянемо деякі властивості кривих E_d і $E_{-1,-d}$, які доцільно використати для вибору випадкової точки однієї з них. Для кривих порядку $N_E = 8n$ точок максимального порядку $4n$ у 8 разів більше, ніж точок непарного порядку n. Для останніх, у свою чергу, дуже малоймовірним є вибір точки порядку, що поділяє n.

Рівняння (3) і (4) запишемо у вигляді

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

Вилучаючи точки малих порядків і особливі точки ($(xy \neq 0)$, $(dx^2 \neq 1)$, $(dy^2 \neq 1)$), під час вибору випадкового елемента $x \in F_p$ отримуємо випадкову точку $P(x, y) \in F_d$ чи $P(x, y) \in E_{-1,-d}$. У першому випадку виконується рівність $\chi((dx^2 - 1)(x^2 - 1)) = 1$, у другому — рівність $\chi((dx^2 - 1)(x^2 - 1)) = -1$. За наведеними вище формулами обчислюють y-координату випадкової точки $P(x, y)$. Побудуємо алгоритм 2 рандомізованої імплементації першого етапу алгоритму CSIKE.

Randomized algorithm 2: Evaluating the class-group action on quadratic and twisted SEC.

Input: $d_A \in E_A$, $\chi(d) = 1$ *and a list of integers* $\Omega_\kappa = (e_1, e_2, \ldots, e_K)$.

Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}] * E_A = E_B$, *where* $E_{A,B} : x^2 + y^2 = 1 + d_{A,B} x^2 y^2$,

1. *Let* $S_0 = \{k \mid e_k > 0\}$, $S_1 = \{k \mid e_k < 0\}$, $n_0 = \prod_{k \in S_0} l_k$, $n_1 = \prod_{k \in S_1} l_k$,

2. **While** *some* $e_k \neq 0$ **do**

3. *Sample a random* $x \in F_p$,

4. Set $a \leftarrow 1, \lambda \leftarrow 0,\ E_A: x^2 + y^2 = 1 + d_A x^2 y^2$ **If** $\chi((x^2-1)/(dx^2-1)) = 1$,

5. **Else** $a \leftarrow -1,\ \lambda \leftarrow 1,\ E_A: x^2 - y^2 = 1 - d_A x^2 y^2$,

6. *Compute y-coordinate of the point* $P = (x, y) \in E_A$,

7. *Compute* $R \leftarrow [(p+1)/2n_\lambda]P$,

8. *Sample a random* $l_k \mid k \in S_\lambda$,

9. *Compute* $Q \leftarrow [n_\lambda / l_k]R$,

10. **If** $Q \neq (1, 0)$ *compute kernel G of* l_k*-isogeny* $\phi: E_A \to E_B$,

11. **Else** start over to line 3,

12. *Compute* d_B *of curve* E_B, $d_A \leftarrow d_B$, $e_k \leftarrow e_k - \lambda$,

13. *Skip k in* S_λ *and* set $n_\lambda \leftarrow (n_\lambda / l_k)$ **If** $e_k = 0$,

14. **Return** d_A.

Цей алгоритм має дві важливі відмінності від алгоритму 1.

По-перше, ми не розбиваємо обчислення ізогеній на два етапи з кривими одного класу і потім іншого ($a \leftarrow -a$), а будуємо випадкову послідовність $\{\lambda\}$ з рівноймовірним вибором кривих E_d або $E_{-1,-d}$ на кожному кроці. Цей факт разом з прискоренням вдвічі процедури вибору кривих позбавляє аналітика можливості впорядкованої побудови підмножин S_0, S_1 ступенів ізогеній. Крім того, для кожної складової $[l_k^{e_k}]$ функції Θ ланцюжок ізогеній довжиною $|e_k|$ розбивається на фрагменти загального ланцюжка випадковим чином. Це ускладнює завдання вимірювання часу обчислень відповідно до функції $[l_k^{e_k}]$.

По-друге, в алгоритмі 2 (п. 12) ми відмовляємося від обчислення ізогенної функції $\phi(R)$, що також значно прискорює алгоритм. Кінцевою метою алгоритму розподілу секретів CSIDH є знаходження загального параметра d_{AB} кривої E_{AB}. Для кожного кроку в ланцюжку ізогеній $E \to E'$ необхідним є лише розрахунок параметра $d' = \psi(d, Q)$ на основі параметрів d і ядра $\langle Q \rangle$ домену E. Для цього розрахунку потрібні тільки два скалярні множення (SM) випадкових точок R непарного порядку n_λ та $(l_k - 1)/2$ рекурентні подвоєння точок з $\langle Q \rangle$. Отже, побудова та обчислення достатньо складної функції $\phi(R)$ не є необхідним для реалізації алгоритму CSIDH (CSIKE). Водночас як порядок точки R завжди містить співмножник l_k, порядок її образу $\phi(R)$ такого множника не має, і точка $\phi(R) \in E'$ марна для знаходження ядра кривої E'. Її використовують лише в кінці ланцюжка ізогеній, якщо $R = Q, \phi(Q) = (1, 0)$. Проте ця відома властивість не вимагає перевірки. Частину обчислень в алгоритмі 1, потрібних для розрахунку функції $\phi(R)$, можна випустити.

На початку алгоритму 2 формуються дві підмножини S_λ, $\lambda = 0, 1$, з номерами ступенів l_k разом із двома співмножниками n_0 та n_1 числа $n = n_0 n_1$. Оскільки порядок кривої $p + 1 = 8n$, то в п. 7 алгоритму для кривої E_d обчислюють точку $R = 4n_1 P$ непарного порядку n_0, а для кривої $E_{-1,-d}$ — точку непарного порядку n_1. Так само як і в алгоритмі 1, це мінімізує витрати на обчислення наступного скалярного добутку, що визначає точку Q ядра ізогенії ступеня l_k (п. 9). Далі в п. 10 алгоритму методом подвоєння точок розраховують $(l_k - 1)/2$ координат точок ядра G.

За результатами імплементації моделі Едвардс-CSIDH [2] у проєктивних координатах $(W : Z)$ стверджують, що вона швидша за модель Монтгомері-CSIDH у координатах $(X : Z)$ на 20 %. Зауважимо, що ця модель у [2] побудована на

повних кривих Едвардса порядку $N_E = p+1 = 4n$. На основі теорем 1 і 2 [6] у цій статті показано, як реалізувати таку модель на квадратичних і скручених СКЕ порядку $N_E = p+1 = 8n$, що утворюють пари квадратичного кручення. Головна перевага цих класів кривих Едвардса над повними полягає у подвоєнні кількості кривих в алгоритмі з відповідним підвищенням безпеки. До того ж непотрібною є трудомістка інверсія параметра $d \to d^{-1}$, яку слід виконувати у разі переходу до повної кривої квадратичного кручення. Це також прискорює виконання алгоритму.

ВИСНОВКИ

Запропонований у цій роботі оригінальний алгоритм CSIKE як модифікацію CSIDH можна вважати переважним у задачі розподілу ключів, оскільки він використовує один відкритий ключ замість двох. Алгоритм може бути цікавим у перспективі для задач стандартизації алгоритмів PQC [15]. Обчислення ізогеній непарних ступенів на СКЕ в координатах $(W:Z)$ [2] дає змогу реалізувати найбільш швидкі на сьогодні обчислення для побудови протоколів CSIKE, CSIDH та подібних. У цій статті обґрунтовано вибір квадратичних і скручених СКЕ замість повних СКЕ [2], що вдвічі розширює простір еліптичних кривих алгоритму. Наведено приклади імплементації простої моделі алгоритму CSIKE. Запропоновано рандомізацію алгоритму CSIKE з випадковим вибором однієї з кривих пари квадратичного кручення на кожному кроці ланцюжка ізогеній. Водночас із прискоренням удвічі процедури вибору метод рандомізації алгоритму дає змогу протистояти атакам побічного каналу. Обґрунтовано можливість відмови від обчислення ізогенної функції $\phi(R)$ випадкової точки R, що суттєво прискорює виконання алгоритму. Найбільші обчислювальні витрати в алгоритмі CSIKE пов'язані зі скалярними множеннями SM випадкових точок, а також з визначенням координат точок ядра ізогеній. У подальших дослідженнях заплановано отримати експериментальні оцінки характеристик імплементації рандомізованого алгоритму CSIKE.

СПИСОК ЛІТЕРАТУРИ

1. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: An efficient post-quantum commutative group action. In: Advances in Cryptology — ASIACRYPT 2018. Peyrin T., Galbraith S. (Eds.). *Lecture Notes in Computer Science*. Cham: Springer, 2018. Vol. 11274. P. 395–427. https://doi.org/10.1007/978-3-030-03332-3_15.
2. Kim S., Yoon K., Park Y.-H., Hong S. Optimized method for computing odd-degree isogenies on Edwards curves. In: Security and Communication Networks, 2019.
3. Farashahi R.R., Hosseini S.G. Differential addition on twisted Edwards curves. In: Information Security and Privacy. ACISP 2017. Pieprzyk J., Suriadi S. (Eds.). *Lecture Notes in Computer Science*. Cham: Springer, 2017. Vol. 10343. P. 366–378. https://doi.org/10.1007/978-3-319-59870-3_21.
4. Kim S., Yoon K., Kwon J., Hong S., Park Y.-H. Efficient isogeny computations on twisted Edwards curves. *Security and Communication Networks*. 2018. Vol. 2018. Article ID 5747642. https://doi.org/10.1155/2018/5747642.
5. Moody D., Shumow D. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*. 2016. Vol. 85, N 300. P. 1929–1951.
6. 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.
7. Moriya T., Onuki H., Takagi T. How to construct CSIDH on Edwards curves. In: Topics in Cryptology — CT-RSA 2020. Jarecki S. (Ed.). *Lecture Notes in Computer Science*. Cham: Springer, 2020. Vol. 12006. P. 512–537. https://doi.org/10.1007/978-3-030-40186-3_22.

8. Bessalov A.V. On correctness of implementation conditions CSIDH algorithm on Edwards curves. *Радиотехника*. 2022. Вып. 208. С. 16–27.

9. Bernstein D.J., Lange T. Faster addition and doubling on elliptic curves. In: Advances in Cryptology — ASIACRYPT 2007. Kurosawa K. (Eds.). *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer, 2007. Vol. 4833. P. 29–50. https://doi.org/10.1007/978-3-540-76900-2_3.

10. Bernstein D.J., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards curves. In: Progress in Cryptology — AFRICACRYPT 2008. Vaudenay S. (Eds.). *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer, 2008. Vol. 5023. P. 389–405. https://doi.org/10.1007/978-3-540-68164-9_26.

11. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев: Политехника, 2017. 272 с.

12. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. *Problems of Information Transmission*. 2017. Vol. 53, N 1. P. 92–101. https://doi.org/10.1134/S0032946017010082.

13. 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, No. 3. P. 347–353. https://doi.org/10.1007/s10559-019-00140-9.

14. 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, N 5. P. 731–741. https://doi.org/10.1007/s10559-019-00183-y.

15. Azarderakhsh R., Campagna M., Costello C., Feo L.D., Hess B., Jalali A., Jao D., Koziel B., LaMacchia B., Longa P., Naehrig M., Renes J., Soukharev V., and Urbanik D. Supersingular isogeny key encapsulation — Submission to the NIST's post-quantum cryptography standardization process. 2017. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/SIKE.zip.

16. Washington L.C. Elliptic curves. Number theory and cryptography. 2nd ed. CRC Press, 2008. 513 p.

17. Onuki, H., Aikawa, Y., Yamazaki, T., Takagi, T. (2019). (Short paper) A faster constant-time algorithm of CSIDH keeping two points. In: Attrapadung, N., Yagi, T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. P. 23–33. Springer, Cham. https://doi.org/10.1007/978-3-030-26834-3_2.

18. Jalali A., Azarderakhsh R., Kermani M.M., Jao D. Towards optimized and constant-time CSIDH on embedded devices. IACR Cryptology ePrint Archive 2019/297. URL: https://eprint.iacr.org/2019/297. (to apper at COSADE 2019).

A.V. Bessalov, S.V. Abramov

PQC CSIKE ALGORITHM IN NON-CYCLIC EDWARDS CURVES

Abstract. The original post-quantum cryptography algorithm CSIKE is proposed as a modification of CSIDH but with one public key instead of two. The conditions for its implementation on two classes of non-cyclic Edwards curves are substantiated. The properties of quadratic and twisted supersingular Edwards curves that form pairs of quadratic twist of order $p+1 \equiv 0 \bmod 8$ over a prime field F_p are considered. A modification of the CSIDH algorithm and the CSIKE algorithm are presented, which are generated on the isogenies of these curves instead of the traditional arithmetic of curves in the Montgomery form. For isogenies of degrees 3, 5, and 7, the parameters of isogenic chains of non-cyclic supersingular Edwards curves are calculated and tabulated for $p = 839$. The implementation of the key encapsulation scheme with its encryption by Alice with Bob's public key is considered. A new randomized CSIKE algorithm with random equiprobable selection of a curve from two classes at each step of the isogeny chain is proposed. An estimate of the probability of a successful side-channel attack in a randomized algorithm is given. It is proposed to abandon the calculation of the isogenic function $\phi(R)$ of a random point R, which significantly speeds up the algorithm.

Keywords: curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, *w*-coordinates, quadratic residue, quadratic nonresidue.

Надійшла до редакції 25.08.2022