КІБЕРНЕТИКА

УДК 621.391.15 : 519.7

А.В. БЕССАЛОВ
Київський університет імені Бориса Грінченка, Київ, Україна,
e-mail: *a.bessalov@kubg.edu.ua.*

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

ОСОБЛИВІ ВЛАСТИВОСТІ ЗАКОНУ ДОДАВАННЯ ТОЧОК НЕЦИКЛІЧНИХ КРИВИХ ЕДВАРДСА

Анотація. Проведено аналіз особливих властивостей двох класів квадратичних і скручених кривих Едвардса, що враховують їхню нециклічну структуру, а також неповноту закону додавання точок. Обидва класи кривих містять особливі точки 2-го і 4-го порядків за однією нескінченною координатою, що породжують точки з невизначеністю $0/0$ в одній з координат суми, які названо нечіткими точками. Сформульовано і доведено п'ять теорем, що дають змогу розв'язати ці невизначеності і задати умови, за якими закон додавання точок у таких класах кривих є повним.

Ключові слова: крива в узагальненій формі Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, особлива точка, нечітка точка, колесо точок, квадратичний лишок, квадратичний нелишок.

ВСТУП

Одним із перспективних протоколів постквантової криптографії (Post Quantum Crypthography, PQC) нині є протокол відкритого обміну ключами — алгоритм CSIDH [1] на ізогеніях суперсингулярних еліптичних кривих над полем F_p з мінімальною довжиною ключа. У реалізаціях алгоритму CSIDH раніше використовували швидку арифметику ізогеній кривих Монтгомері. У роботі [2] запропоновано новий ефективний метод обчислення ізогеній непарних ступенів на повних кривих Едвардса на основі w-координат Фарашахи–Хоссейні. У роботах [3, 4] замість повних кривих Едвардса обґрунтовано і проілюстровано на прикладі імплементацію алгоритму CSIDH на квадратичних і скручених кривих Едвардса.

Значними перевагами повних кривих Едвардса з одним параметром d ($\chi(d) = -1$), визначених у роботі [5], є повнота та універсальність закону додавання точок, технологічність, афінні координати нейтрального елемента групи точок. Введення другого параметра a кривої $E_{a,d}$ в роботі [6] дало змогу розширити клас кривих Едвардса і створити згідно з прийнятою в [7–9] класифікацією два нових класи: скручені і квадратичні криві Едвардса. Ці класи утворюють пари квадратичного кручення, які є перспективними для імплементації алгоритму CSIDH [4].

Особливістю таких класів нециклічних кривих Едвардса (з трьома точками 2-го порядку) порівняно з повними кривими Едвардса є втрата властивості повноти закону додавання точок [6]. Це означає, що існують пари точок, сума яких породжує особливі точки, де одна координата є нескінченною (нуль у знаменнику формул додавання), а також за допомогою програмування було виявле-