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