

УДК 003.26:004.056.53

Пономаренко Є. О.¹, Неласа Г. В.²

¹асп. каф. ІБтаН НУ «Запорізька політехніка»

²доц. каф. ІБтаН НУ «Запорізька політехніка»

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ІЗОГЕНІЙ ГІПЕРЕЛІПТИЧНІ КРИВИХ ДРУГОГО РОДУ У КРИПТОГРАФІЧНИХ ПРОТОКОЛАХ

Гіпереліптичні криві другого роду[1] стали важливим компонентом сучасної криптографії, надаючи можливість ефективного захисту в умовах зростаючих загроз з боку квантових обчислень. Ізогенії гіпереліптичні кривих другого роду визначають відображення між гіпереліптичними кривими зі збереженням їхньої математичної структури, що має важливе значення в криптографічних системах. Порівняно з еліптичними кривими,

криві другого роду дозволяють використовувати основне поле зменшеного пропорційно роду кривої розміру зі збереженням розміру ключа. Ця властивість є важливою в умовах, де потрібно проводити обчислення на пристроях з обмеженими ресурсами, наприклад, в мобільних чи вбудованих системах. Ізогенії на гіпереліптичних кривих можуть використовуватись у протоколах обміну ключами, генерації цифрових підписів та шифруванні даних, забезпечуючи захист від атак, які використовують квантові обчислення, адже складність оберненого обчислення ізогеній значно перевищує можливості сучасних алгоритмів, навіть квантових.

Гіпереліптичні криві роду g визначаються рівнянням виду:

$$y^2 + h(x)y = f(x), \quad (1)$$

де $h(x)$ — многочлен степеня не більше ніж g ;

$f(x)$ — многочлен степеня $(2g+1)$, що не має кратних коренів.

Такі криві мають додаткові особливості, які виділяють їх серед інших алгебраїчних кривих. Криві другого роду мають складнішу структуру ніж еліптичні криві, що призводить до підвищеної складності обчислень. Головну роль у цих обчисленнях відіграє яacobіан кривої роду 2, що є аналогом групового закону еліптичних кривих. Яacobіан має вдвічі більшу розмірність, що ускладнює криптографічні операції, але водночас забезпечує більший запас стійкості проти квантових атак. Яacobіан кривої роду 2 є двовимірним абелевим многовидом, що відіграє ключову роль у розумінні структури кривої. Яacobіан можна розглядати як певний узагальнений об'єкт, що кодує інформацію про криву, зокрема про її дільники та раціональні точки. Група дільників на кривій є формальною групою, утвореною сумою точок на кривій, і саме через аналіз цієї групи можна отримати важливі властивості кривої.

Ключовим класом ізогеній для кривих роду 2 є ізогенії Рішело[2]. Вони передбачають складні обчислення дивізорів та їх взаємодій, що значно перевищує простоту точкових операцій на еліптичних кривих. Ізогенії Рішело є спеціальним типом ізогеній, які виникають у випадку, коли многочлен, що визначає гіпереліптичну криву, можна розкласти на три квадратні множники. Цей розклад дозволяє явно побудувати нову гіпереліптичну криву роду 2 і визначити ізогенію між яacobіанами початкової кривої та нової кривої. Алгоритми для обчислення таких ізогеній потребують більше ресурсів та складних структур даних, що ускладнює їх практичну реалізацію. Крім того, велика кількість ізогеній у гіпереліптичних кривих створює і переваги, і виклики з точки зору криптографії. Така різноманітність ізогеній пов'язана з більш складною геометрією кривих і розширеними математичними структурами.

Гіпереліптичні криві роду 2 або вище мають значно більше ендоморфізмів порівняно з еліптичними кривими. Геометрія таких кривих сприяє побудові більш складних відображень між кривими. Збільшена кількість ізогеній підвищує міцність протоколів, в контексті стійкості як до класичних, так і до квантових атак.

Водночас, обчислювальна складність знаходження ізогеній у контексті гіпереліптичних кривих значно перевищує аналогічні процеси на еліптичних кривих. Такі обчислення потребують розкладання поліномів на множники і складної арифметики дивізорів, що суттєво збільшує витрати на обчислення.

Використання гіпереліптичних ізогеній у криптографії відкриває нові шляхи для інноваційних протоколів. Зокрема, їх складність може бути використана для побудови більш безпечних протоколів обміну ключами або цифрових підписів. Завдяки підвищеній стійкості проти квантових загроз, такі протоколи можуть забезпечити надійний захист у майбутніх системах. Окрім того, математичні особливості гіпереліптичних кривих дозволяють створювати нові криптографічні конструкції, наприклад хеш-функції на основі ізогеній. Взаємодія між ізогеніями роду 2 та іншими постквантовими методами, такими як криптографія на основі решіток, відкриває додаткові можливості для розробки нових криптографічних протоколів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. E. V. Flynn and Yan Bo Ti, Genus Two Isogeny Cryptography, Cryptology {ePrint} Archive, Paper 2019/177. Режим доступу: <https://eprint.iacr.org/2019/177>.
2. E. Florit and B. Smith, An atlas of the Richelot isogeny graph, Cryptology {ePrint} Archive, Paper 2021/013. Режим доступу: <https://eprint.iacr.org/2021/013>.