УДК 003.26 Пономаренко Є.О.[1], Неласа Г.В.[2]

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІЗОГЕНІЙ ЕЛІПТИЧНИХ КРИВИХ В КРИПТОГРАФІЧНИХ ПРОТОКОЛАХ

Арифметика в групі точок еліптичних кривих, визначених над полями Галуа, є одним з найперспективніших інструментів для побудови криптографічних алгоритмів. Криптографічні примітиви, стійкість яких базується на великій обчислювальній складності задачі обчислення дискретного логарифму на еліптичній кривій (ECDLP) є основою більшості сучасних стандартів електронного цифрового підпису. Однак поява квантових комп'ютерів та стрімкий розвиток методів квантових обчислень ставить під загрозу стійкість криптографічних перетворень. Такий комп'ютер здатний утримати в зв'язаному стані порядку декількох тисяч кубітів, що дозволяє знаходити закриті ключі по відкритих ключах для всіх існуючих на даний час асиметричних криптосистем, основаних на використанні абелевих груп. Тому актуальною є задача дослідження нових типів перетворень, стійких у постквантовий період.

Досить новою є ідея побудови криптографічних на алгоритмів відображеннях еліптичних кривих. На цей час відомо, що криптосистеми, засновані на обчисленні алгебраїчних відображень (ізогеній) суперсингулярних еліптичних кривих, є стійкими по відношенню до квантового комп'ютера[1].

В роботі досліджено особливості використання ізогеній суперсингулярних еліптичних кривих в криптографічних протоколах, зокрема в протоколі розділення ключа Діффі-Хеллмана. Виконано розрахунковий приклад проведення обчислень за загальною схемою алгоритму Вєлу в спеціалізованому математичному пакеті.

Висновки. Результати роботи можуть бути використані фахівцями з кібербезпеки для розробки криптографічних протоколів асиметричної криптографії, стійких до атак на квантовому комп'ютері.

ПЕРЕЛІК ПОСИЛАНЬ

1. Luca De Feo, David Jao, Jérôme Plût Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[Електронний ресурс], Cryptology ePrint Archive: Report 2011/506, – Режим доступу: https://eprint.iacr.org/2011/506

[1] студент групи РТ-810м, НУ «Запорізька політехніка»
[2] професор кафедри ЗІ, НУ «Запорізька політехніка», к.т.н., доцент