УДК 004.056

Товма О. М.

АНАЛІЗ ПРОДУКТИВНОСТІ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ RSA, ECDSA ТА DILITHIUM В КОНТЕКСТІ ПЕРЕХОДУ ДО ПОСТ-КВАНТОВОЇ КРИПТОГРАФІЇ

Розвиток квантових обчислень створює суттєві виклики для сучасної криптографічної інфраструктури, оскільки алгоритм Шора здатний ефективно розв’язувати задачі факторизації великих чисел та обчислення дискретного логарифму, на яких базуються алгоритми RSA та ECDSA. Застосування потужних квантових комп’ютерів потенційно може зробити ці криптографічні механізми вразливими для використання у довгостроковій перспективі, що ставить під загрозу існуючі системи захисту інформації.

Сучасна цифрова інфраструктура критично залежить від алгоритмів цифрового підпису, які забезпечують автентифікацію, цілісність даних та невідмовність у широкому спектрі застосувань – від електронної комерції та фінансових транзакцій до систем державного управління, військових інформаційних мереж та захищених каналів зв’язку. Протягом останніх десятиліть алгоритми RSA та ECDSA домінували у сфері асиметричної криптографії завдяки їх математичній обґрунтованості, перевіреній криптостійкості у класичній моделі обчислень та достатній практичній ефективності.

Разом з тим поява квантових обчислювальних технологій кардинально змінює криптографічний ландшафт. Алгоритм Шора, запропонований у 1994 році, теоретично дозволяє виконувати факторизацію великих чисел та обчислення дискретних логарифмів за поліноміальний час на квантовому комп’ютері. Незважаючи на те, що сучасні квантові комп’ютери залишаються експериментальними системами з обмеженою кількістю кубітів та значними технічними обмеженнями, криптографічна спільнота усвідомлює необхідність завчасної підготовки до переходу на квантово-стійкі криптографічні алгоритми.

У відповідь на цю проблему Національний інститут стандартів і технологій США (NIST) у 2016 році ініціював міжнародний конкурс із стандартизації пост-квантових криптографічних алгоритмів. Процес відбору тривав понад шість років і включав кілька етапів відкритого криптоаналізу. У конкурсі розглядалося 82 початкові алгоритмічні пропозиції, які піддавалися інтенсивному аналізу на предмет криптографічної стійкості, продуктивності та практичної реалізованості.

У результаті цього процесу в липні 2022 року було обрано алгоритм CRYSTALS-Dilithium як один із базових стандартів для реалізації пост-квантових цифрових підписів. Даний алгоритм базується на задачах теорії решіток, зокрема на проблемі Module Learning With Errors (M-LWE), яка на сьогодні вважається стійкою до атак як класичних, так і квантових комп’ютерів. Решіткові криптографічні конструкції демонструють прийнятний баланс між криптографічною стійкістю та обчислювальною ефективністю.

Таким чином, дослідження продуктивності алгоритмів RSA, ECDSA та Dilithium обумовлене необхідністю практичного переходу криптографічної інфраструктури до пост-квантових стандартів. Організації повинні враховувати не лише криптографічну стійкість нових алгоритмів, але й їх обчислювальну ефективність, розмір ключів та підписів, вимоги до пам’яті і енергоспоживання. Особливо актуальним це є для ресурсообмежених систем, зокрема пристроїв Інтернету речей, мобільних платформ, вбудованих систем та телекомунікаційних вузлів, де вибір криптографічного алгоритму безпосередньо впливає на продуктивність і надійність функціонування інформаційних систем.