АНАЛІЗ КВАНТОВИХ АЛГОРИТМІВ CRYSTALS-KYBER І CRYSTALS-DILITHIUM

Хівренко Г.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Постквантова криптографія (PQC) стала центром досліджень, оскільки прориви в квантових обчисленнях загрожують безпеці класичних криптографічних систем. У роботі досліджені протоколи CRYSTALS-KYBER і CRYSTALS-Dilithium, призначені для захисту зв'язку від квантових противників [1, 2]. Використовуючи решіткові задачі, які вважаються стійкими до квантових атак, ці протоколи пропонують перспективне рішення для захисту конфіденційних даних від руйнівного потенціалу нових квантових технологій.

Метою роботи є оцінка теоретичних основ, які забезпечують безпеку алгоритмів CRYSTALS-KYBER і CRYSTALS-Dilithium від відомих квантово-здатних опонентів. Також проаналізовані їх характеристики продуктивності, такі як розмір ключа, затримка та накладні витрати на обчислення, під час розгортання на різних платформах, включаючи обмежені середовища, такі як пристрої IoT. Крім того досліджені стратегії безперебійного переходу від поточних стандартів (RSA та ECC) до квантово-стійких протоколів, що забезпечують безперервність захищених комунікацій без шкоди для ефективності та зручності використання.

Квантові комп'ютери можуть скомпрометувати існуючі криптографічні алгоритми протягом найближчих десятиліть. Завдяки систематичному вивченню CRYSTALS-KYBER і CRYSTALS-Dilithium - двох провідних кандидатів у постквантові стандарти NIST - надаються практичні ідеї для практиків безпеки і системних архітекторів, які готуються до майбутнього [3].

У доповіді розглянуті комплексна структура для розуміння та впровадження CRYSTALS-KYBER і CRYSTALS-Dilithium, підкреслюючи їхні криптографічні переваги, практичні міркування щодо розгортання та ширшу актуальність для захисту цифрових комунікацій [4].

Проведено аналіз формування ключових пар, створення цифрового підпису для CRYSTALS-Dilithium та шифрування для CRYSTALS-Dilithium. Проведений аналіз безпеки цих алгоритмів та була проведена оцінка швидкості та ефективність наведених алгоритмів.

Список літератури

1. Khalimov, G. and others. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement Proceedings of the 2021 5th World Conference on Smart Trends in Systems Security and Sustainability, WorldS4 2021, 2021, P. 204–211.

2. Micciancio, D., & Regev, O. (2009). *Lattice-based Cryptography*. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), Post-Quantum Cryptography (pp. 147–191). Springer.

3. NIST. (2022). Post-Quantum Cryptography Standardization Process: Round 3 Submissions. Retrieved from https://csrc.nist.gov/Projects/post-quantum-cryptography.

4. Chen, L., et al. (2016). *Report on Post-Quantum Cryptography*. NISTIR 8105.