ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ КВАНТОВО-СТІЙКИХ КРИПТОСИСТЕМ

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

З розвитком квантових обчислень з'являється потреба в модернізації криптографії. Алгоритми розкладання цілих чисел і дискретних логарифмів, які використовуються в RSA та Elliptic Curve Cryptography (ECC), стають вразливими до квантових атак.

Спірос Магліверас дослідив логарифмічні підписи, які лягли в основу криптосистем MST1 та MST2. MST3 - нова криптосистема, що поєднує MST1 та MST2, ґрунтується на логарифмічних підписах і випадкових покриттях неабелевих груп. Вона використовує Судзукі 2-групи для реалізації. MST3 - квантово-стійка криптосистема, що використовується для створення цифрових підписів.

Серед переваг можна виділити: стійкість до квантових атак, відносно невеликий розмір ключів, можливість використання на мобільних пристроях.

Метою доповіді є розгляд та порівняння пост-квантових алгоритмів, що перемогли у конкурсі NIST у 2022 році.

Переможцями конкурсу є: CRYSTALS-Dilithium - криптосистема на основі ґраток Falcon - криптосистема на основі ґраток, SPHINCS+ - криптосистема на основі хеш-функцій. MST3 не брала участі в конкурсі NIST, але вона має схожі характеристики з CRYSTALS-Dilithium і Falcon, хоч і побудована на логарифмічних підписах.

Актуальним є створення і розвиток нових алгоримів стійких до квантових атак, зниження складності обчислень та розміру ключів, оптимізація для швидшої роботи, розробка планів та методів переходу з доквантових криптосистем на постквантові, створення тестових векторів та інструментів для оцінки стійкості алгоритмів.

Також одним з найактуальніших питань є розробка та прийняття міжнародних стандартів для постквантових криптосистем.

Виконано попередній порівняльний аналіз алгоритмів переможців конкурсу NIST та криптосистеми MST3, який показує що на поточний момент алгоритми CRYSTALS-Dilithium та MST3 лідирують з огляду на розмір ключа, швидкість підпису та швидкість перевірки, у порівнянні з іншими алгоритмами які вибрав за переможців NIST.

Список літератури

1. Hong, Haibo & Li, Jing & Wang, Licheng & Yang, Yixian & Niu, Xinxin. (2014). A Digital Signature Scheme Based on MST3 Cryptosystems. Mathematical Problems in Engineering. 2014. 10.1155/2014/630421.

2. Svaba, Pavol. (2011). Covers and Logarithmic Signatures of Finite Groups in Cryptography.

3. NIST. (2022). First Four Quantum-Resistant Cryptographic Algorithms.