КВАНТОВО-СТІЙКИЙ ЦИФРОВИЙ ПІДПИС ДЛЯ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНИХ ГРУП

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

Сучасний розвиток квантових обчислень створює нові ризики для безпеки традиційних криптографічних систем, що використовуються у захисті телекомунікаційних мереж. Квантові комп'ютери можуть ефективно розв'язувати задачі, які є основою класичних алгоритмів шифрування, ставлячи під загрозу цілісність і конфіденційність даних у таких мережах. Основною небезпекою є здатність квантових комп'ютерів до ефективного розв'язання математичних задач, які лежать в основі сучасних криптографічних алгоритмів, таких як RSA чи ECC. З огляду на це, дослідження у сфері постквантової криптографії стають дедалі актуальнішими, що вимагає розробки нових моделей, стійких до квантового криптоаналізу.

Метою доповіді є представлення архітектури цифрового підпису, яка базується на некомутативних багатопараметричних групах, для забезпечення стійкості до атак з боку квантових обчислювальних систем. У даній роботі описуються математичні структури та алгоритми, що дозволяють досягти високого рівня захисту шляхом використання складних обчислень у некомутативних просторах Така структура дозволяє досягнути криптографічної стійкості завдяки складності обчислення групових операцій у некомутативному середовищі, що на сьогодні залишається поза можливостями квантових алгоритмів, таких як алгоритм Шора.

Актуальним є застосування квантово-стійких підписів у телекомунікаційних мережах, оскільки зростання потужності квантових комп'ютерів створює ризики для безпеки даних, які передаються та обробляються у цих мережах. Особливу значущість такі підписи мають для критично важливих інфраструктур, де порушення захисту може призвести до серйозних наслідків.

Проведено аналіз існуючих моделей цифрових підписів та їх можливостей до опору квантовому криптоаналізу. Проведено моделювання обчислювальних процесів із застосуванням багатопараметричних груп та оцінено їхню ефективність у контексті телекомунікаційних систем.

Список літератури

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*.

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

3. Wang, Y., Liu, X., & Lee, B. (2021). Quantum-resistant digital signature schemes based on non-commutative algebra. *Advances in Post-Quantum Cryptography*.