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

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

Сучасні телекомунікаційні системи і мережі (5G/IMS, IoT, ядро операторських мереж, сервісно-орієнтована архітектура SBA) покладаються на цифрові підписи для автентифікації мережевих функцій, міждоменної сигналізації, керування конфігурацією та журналювання дій [1]. Наближення епохи практичних квантових обчислень зумовлює перегляд криптографічних примітивів у критичних контурах: класичні RSA/ECC стають вразливими до поліноміальних квантових алгоритмів, а життєвий цикл обладнання в ТКС (роки й десятиліття) створює «вікно ураження», якщо міграцію відкладати.

Отже, операторам і постачальникам мережевих рішень потрібні підходи, що поєднують квантову стійкість, криптографічну гнучкість (agility) та придатність до розгортання на граничних і ресурсно-обмежених вузлах. Переважна частина стандартизаційного ландшафту постквантових підписів спирається на ґраткові та геш-орієнтовані конструкції.

Водночас для підвищення криптографічної різноманітності й стійкості екосистеми перспективним є сімейство схем на основі некомутативних багатопараметричних груп (НБГ). Такі підходи використовують задачі в некомутаційних структурах (спряження, декомпозиції, представлення в добутках підгруп тощо), для яких не відомо ефективних квантових алгоритмів загального призначення, а багатопараметричність дозволяє тонко налаштовувати простір безпекових і продуктивних параметрів під конкретні мережеві сценарії [2-4]. Для ТКС це означає можливість зменшити затримку перевірки підпису на контрольній площині, утримати помірні розміри ключів/підписів у транспорті, забезпечити ізоляцію доменів довіри та сумісність із чинними протоколами (TLS 1.3/QUIC, SIP/HTTP-based SBA, O-RAN інтерфейси).

Метою доповіді є розробка та обґрунтування квантово-стійкої схеми цифрового підпису на основі некомутативних багатопараметричних груп для застосування в телекомунікаційних мережах (5G/IMS/IoT) із визначенням класів груп, нормальних форм і простору параметрів.

В роботі сформульовані чіткі припущення безпеки (зокрема варіанти задач спряження/деконструкції) та показана відсутність відомих ефективних класичних і квантових атак, спроєктовані алгоритми KeyGen/Sign/Verify з доказом коректності та аргументами стійкості. В результаті оптимізовані параметри під граничні умови мережевих вузлів (затримка перевірки, пропускна здатність, довжини ключів і підписів) та розроблені профілі інтеграції у PKI/AKI та мережеві протоколи (TLS 1.3/QUIC, сигнальні канали

5G/IMS, сценарії network slicing) у гібридному режимі разом зі стандартизованими PQC-підписами. Також забезпечена сумісність із життєвим циклом ключів, політиками відкликання (CRL/OCSP) і можливістю апаратного захисту (HSM/TEE); проведена порівняльна оцінка з наявними PQC-рішеннями за метриками безпеки й продуктивності та підготовлена дорожня карта міграції для операторських мереж із вимогами до впровадження й експлуатації.

Запропонована схема інтегрується в телекомунікаційну інфраструктуру як компонент PKI/AKI для 5G/IMS/IoT-сегментів (автентифікація функцій ядра, вузлів RAN, мережевих з'єднань у slicing-сценаріях, захист сигналізації між доменами). Ми обговорюємо гібридний режим розгортання: НБГ-підпис як основний примітив у парі з стандартизованими PQC-підписами (наприклад, Dilithium або SPHINCS+) [5, 6] для поетапної міграції та взаємної страховки. Обґрунтовуються вимоги до продуктивності (перевірка на граничних вузлах), політик життєвого циклу ключів, а також варіанти апаратного прискорення. Розгортання узгоджується з відомими моделями загроз у 5G-мережах

Сформульовано дизайн підпису на НБГ з чітким інтерфейсом ключових операцій (KeyGen/Sign/Verify) та керуванням параметрами (розмірність, довжина слова, породжувачі), надано аргументацію безпеки відносно відомих атак (у т.ч. довжин-орієнтованих і лінійного розкладання в поліциклічних групах), визначено профілі інтеграції в мережеві протоколи (TLS для внутрішньомережевих каналів, SUPI/AKA-подібні процеси в 5G). Сформовано дорожню карту переходу до повного PQC із можливістю поступової заміни гібридів після стандартизації відповідних некомутативних підписів.

Список літератури

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*. DOI: https://doi.org/10.1137/S0097539795293172

2. Kotukh, E. V., Severinov, O. V., Vlasov, A. V., Kozina, L. S., Tenytska, A. O., & Zarudna, E. O. (2021). Методи побудови та властивості логарифмічних підписів. Radiotekhnika, (205), 94-99.

3. Alagic, G., et al.(2022) *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST IR 8413. DOI: https://doi.org/10.6028/NIST.IR.8413

4. Khalimov, G., Kotukh, Y., Kolisnyk, M., Khalimova, S., & Sievierinov, O. (2024). LINE: Cryptosystem based on linear equations for logarithmic signatures. Cryptology ePrint Archive.

5. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D. (2018) *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*, TCHES:238–268. DOI: https://doi.org/10.13154/tches.v2018.i1.238-268

6. Kahrobaei, D., Koupparis, C. (2012) *Non-commutative Digital Signatures, Groups Complexity Cryptology*. DOI: https://doi.org/10.1515/gcc-2012-0019