ЗАХИСТ ДАНИХ З ВИКОРИСТАННЯМ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ ТА ПОСТКВАНТОВИХ АЛГОРИТМІВ ШИФРУВАННЯ

Гирченко І.Р., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Квантові комп'ютери є однією з найсерйозніших загроз для сучасних систем захисту інформації. Стійкість алгоритмів RSA, схем на ЕК ґрунтується на складності факторизації й дискретного логарифмування, а квантовий алгоритм Шора розв'язує обидві задачі за поліноміальний час. Додатковою небезпекою є стратегія «harvest now, decrypt later», за якою зашифровані дані перехоплюються вже сьогодні для розшифрування в майбутньому [1, 2].

Метою доповіді є визначити склад схеми захисту даних, стійкої до атак із застосуванням квантових комп'ютерів на основі результатів аналізу постквантових алгоритмів та протоколів автентифікації з нульовим розголошенням. **В доповіді** наводяться результати аналізу алгоритмів, що у 2024 році стандартизовані інститутом NIST. Знизити ризики квантових атак можна, замінивши вразливі асиметричні механізми алгоритмами, що не мають відомих ефективних квантових атак, а в поєднанні з ними застосовувати перевірені симетричні шифри. Для цього розглядаються такі складові:

1. Узгодження ключів з використанням алгоритму ML-KEM (Kyber), що ґрунтується на задачах на решітках і замінює класичні механізми обміну ключами [1].
2. Цифровий підпис ML-DSA (Dilithium) [1].
3. Автентифікація за протоколом з нульовим розголошенням, що дозволяє підтвердити знання секрету без його розкриття та без зберігання на сервері. Класична схема Шнорра вразлива до алгоритму Шора, тому розглядаються її решітчасті аналоги [3].
4. Симетричне шифрування AES-256, яке залишається стійким, оскільки алгоритм Гровера лише квадратично прискорює перебір ключів. Ключ для нього виводиться зі спільного секрету, узгодженого за допомогою ML-KEM.

Жодна криптосистема не гарантує абсолютного захисту, але поєднання цих складових дозволяє суттєво знизити ризик компрометації даних у майбутньому. Для цього важливо переходити на стандартизовані алгоритми заздалегідь, не очікуючи появи потужних квантових комп'ютерів, а також ретельно підбирати параметри обраних схем.

Список літератури

1. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204: Module-Lattice-Based Digital Signature Standard. – 2024.
2. Bhadane S., Gupta D., Deshmukh P. V., Mishra N. A hybrid hash framework for post quantum secure zero knowledge identification. Scientific Reports. 2025. Vol. 15. Article 42176. DOI: https://doi.org/10.1038/s41598-025-26117-7
3. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM Journal on Computing. – 1989. – Vol. 18, No. 1. – P. 186–208.