ПОСТКВАНТОВА КРИПТОГРАФІЯ З ВИКОРИСТАННЯМ LWE ТА AES

Куліш О.В., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток квантових обчислень актуалізує питання довгострокового захисту інформації, оскільки поява достатньо потужних квантових комп'ютерів може поставити під загрозу криптографічні механізми, стійкість яких ґрунтується на факторизації великих чисел і дискретному логарифмуванні. Одним із напрямів протидії таким загрозам є постквантова криптографія, що використовує математичні задачі, для яких наразі не відомо ефективних квантових алгоритмів розв'язання. Серед перспективних підходів виокремлюється решіткова криптографія, зокрема задача Learning With Errors (LWE) [1].

Метою роботи є дослідження принципів побудови гібридної постквантової криптосистеми та розроблення її навчальної програмної реалізації, у якій механізм на основі LWE використовується для формування секретного значення, а алгоритм Advanced Encryption Standard (AES) у режимі Galois/Counter Mode (GCM) – для захисту повідомлень. Такий поділ функцій дає змогу поєднати асиметричний механізм узгодження секрету з ефективним симетричним шифруванням даних.

Задача LWE полягає у відновленні секретного вектора за системою лінійних співвідношень, у яких до результатів додано випадковий шум. У спрощеному поданні публічно доступні матриця A та вектор b, пов'язаний із секретним вектором s співвідношенням $b = A \cdot s + e$ (за модулем q), де e – вектор шуму. Саме наявність шуму ускладнює відновлення секрету та робить LWE важливою математичною основою для низки решіткових криптографічних конструкцій [1]. Водночас властивості конкретної програмної схеми залежать від вибраних параметрів і способу реалізації, тому сам факт використання LWE не є достатнім доказом її практичної криптографічної стійкості.

У запропонованій архітектурі отримувач формує пару ключів, після чого відправник використовує відкритий ключ для інкапсуляції випадкового секретного значення. На основі отриманого секрету формується ключ для AES-GCM, яким шифрується повідомлення. Через канал передаються зашифровані дані та результат інкапсуляції секрету. Отримувач застосовує закритий ключ для відновлення секретного значення, формує симетричний ключ і виконує дешифрування. Режим GCM забезпечує не лише конфіденційність, а й перевірку цілісності за допомогою тегу автентифікації; це дає змогу виявити шифротексту за умови коректного використання режиму.

Практичну частину реалізовано мовою Python. Програмна модель демонструє взаємодію двох криптографічних компонентів: LWE-подібного механізму для захищеного формування секретного значення та AES-GCM для шифрування текстових даних. Такий прототип корисний для дослідження послідовності криптографічних операцій, перевірки циклу

шифрування/дешифрування та аналізу обмежень навчальних реалізацій. При цьому реалізацію необхідно відрізняти від стандартизованого механізму ML-KEM, визначеного NIST у FIPS 203 [2]. ML-KEM використовує Module-LWE та стандартизовані набори параметрів, тоді як навчальна схема на основі базової LWE не є його еквівалентом.

Важливим результатом аналізу є визначення меж застосовності прототипу. Для використання в реальних системах недостатньо продемонструвати успішне шифрування й відновлення повідомлення: необхідні формальна оцінка стійкості параметрів, коректна обробка помилок, перевірка вхідних даних, безпечне керування ключами та криптоаналітичне тестування. Якщо схема не реалізує механізми, потрібні для стійкості до атак з обраним шифротекстом, її не слід розглядати як повноцінну заміну стандартизованому KEM. Для симетричного компонента також важливо дотримуватися вимог стандарту AES та правил використання режиму GCM [3].

Умовою безпечного використання AES-GCM є забезпечення унікальності значення nonce для кожного шифрування з одним і тим самим симетричним ключем. Повторне використання nonce може призвести до порушення конфіденційності повідомлень і компрометації механізму автентифікації. Крім того, отримувач повинен перевіряти тег автентифікації до використання розшифрованих даних.

У разі невідповідності тегу повідомлення має відхилятися, оскільки його цілісність та автентичність не підтверджені.

Отже, гібридний підхід демонструє практичний принцип розподілу криптографічних функцій: постквантовий механізм використовується для узгодження секретного значення, а AES-GCM – для захисту основного потоку даних.

Розроблена програмна модель має навчально-дослідницьке призначення та може слугувати основою для подальшого порівняння з ML-KEM, вимірювання продуктивності й розширення тестів безпеки. Подальша робота має бути зосереджена на формальній оцінці параметрів, перевірці стійкості до активних атак і наближенні реалізації до вимог актуальних криптографічних стандартів.

Список літератури

1. Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. Journal of the ACM. 2009. Vol. 56, No. 6. Article 34. DOI: https://doi.org/10.1145/1568318.1568324.

2. National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203. 2024. DOI: https://doi.org/10.6028/NIST.FIPS.203.

3. National Institute of Standards and Technology. Advanced Encryption Standard (AES). FIPS 197. Updated edition, 2023. DOI: https://doi.org/10.6028/NIST.FIPS.197.