УДК 004.4:37 004.421

АНАЛІЗ МОЖЛИВОСТЕЙ АЛГОРИТМУ KYBER CRYSTALS

Циганок Д.А.
Науковий керівник – проф. Качко О.Г.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна
тел.: +38(066) 805-19-47, e-mail: daria.tsyhanok@nure.ua

This work is devoted to the analysis capabilities of the Kyber CRYSTALS algorithm. The structure, level of protection, principle of operation are considered. An analysis of the distinctive qualities and capabilities of the post-quantum algorithm was conducted, which prove that it has a significant advantage over other algorithms of post-quantum cryptography.

Уже на початку 2000-х років криптографи все більше хвилювалися щодо потенційних досягнень квантових обчислень. Оскільки Пітер Шор опублікував свій знаменитий алгоритм Шора, ми знаємо, що достатньо великий квантовий комп’ютер зламав би всі широко використовувані системи відкритих ключів. Це включає конструкцію RSA, кінцевого поля та еліптичної кривої.

Як наслідок, у 2017 році Національний інститут стандартів і технологій закликав створити нові системи відкритих ключів, які можуть протистояти квантовим комп’ютерам. Kyber є такою запропонованою постквантовою схемою. У 2021 році NIST вирішив, що він гідний стандартизації.

Kyber – постквантова система шифрування з відкритим ключем. Його основним варіантом використання є встановлення ключів систем із симетричними ключами в протоколах вищого рівня, таких як TLS, Signal або OpenPGP. це постквантова система, оскільки Kyber спеціально розроблений для забезпечення безпеки навіть за наявності квантових комп’ютерів (Таблиця 1). Компроміси розміру та безпеки наведено в наступній таблиці з RSA як попередньо-квантове порівняння.

Таблиця 1 – Порівняльні характеристики систем шифрування

Версія	Рівень безпеки	Розмір приватного ключа	Розмір публічного ключа	Розмір зашифрованого тексту
Kyber512	AES128	1632	800	768
Kyber768	AES192	2400	1184	1088
Kyber1024	AES256	3168	1568	1568

Хоча ключі RSA все ще менші, розміри ключів Kyber залишаються такими ж. Це не критично, оскільки деякі системи PQC мають ключі в сотні кілобайт, а у випадку класичного McEliece навіть у мегабайтному діапазоні.

За своєю суттю Kyber – це, по суті, система шифрування Любашевського, Пейкерта, Регева (LPR) у налаштуваннях модульного навчання з помилками (MLWE). Оригінальні схеми LPR були визначені в налаштуваннях LWE та Ring LWE.

Різниця між ними проста:

1. LWE працює з векторами цілих чисел;
2. RING LWE працює з поліномами;
3. Модуль LWE працює з векторами поліномів.

Хоча вектори поліномів, безумовно, неінтуїтивно зрозумілі для роботи, вони дозволяють набагато краще поєднувати швидкість/розмір/безпеку. Безпека MLWE (і, отже, Kyber) фактично базується на проблемі решітки, а саме задачі найкоротшого вектора (SVP). Отже, відновлення повідомлення із зашифрованого тексту (або приватного з відкритого ключа) має бути таким же важким, як вирішення великого екземпляра SVP. Це має бути обчислювально нездійсненним навіть для квантового комп'ютера. Зменшення від Kyber до MLWE до SVP є нетривіальним, але добре задокументованим. Якщо вас цікавлять деталі, я рекомендую прочитати публікацію Kyber NIST і слідкувати за цитатами.

Основна перевага схем на основі решітки, таких як Kyber, полягає в тому, що вони дуже швидкі, особливо порівняно з іншими постквантовими системами. Недоліком є те, що не зовсім зрозуміло, чи можна використовувати додаткову структуру решіток основного модуля для формулювання кращих атак на конкретний екземпляр SVP.

Список використаних джерел:

1. CRYSTALS. Cryptographic Suite for Algebraic Lattices (2022). https://pq-crystals.org/kyber/index.shtml

2. Національний інститут стандартів і технології. (2022). Обрані алгоритми: шифрування з відкритим ключем та алгоритми встановлення ключів https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022