ПОСТКВАНТОВІ АЛГОРИТМИ НА АЛГЕБРАГІЧНИХ РЕШІТКАХ. АЛГОРИТМ CRYSTALS-KYBER

Скибенко М.С., Долинський В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасному світі швидкістю та ефективністю обчислювання традиційних криптографічних алгоритмів, квантові комп'ютери значно перевищують класичні комп'ютерні архітектури, в результаті чого, криптографічні системи стають потенційно вразливими для криптографічних атак. Постквантові конструкції здатні врятувати криптографічний світ від квантових нападів.

Метою доповіді є розгляд алгоритму Crystals-Kyber, його властивостей та постквантових алгоритмів на алгебраїчних решітках в цілому, аналіз Kyber, як механізму захисту CPS (Cyber-Physical Systems) [1].

Kyber - це захищений є від IND-CCA2 (негнучкості для адаптивних атак на основі підібраного шифротексту) механізм інкапсуляції ключів, захист якого базується на складності вирішення проблеми навчання з помилками (LWE - Learning With Errors) над решітчастими модулями. Kyber є кандидатом на стандартизацію Національним інститутом стандартів і технологій (NIST).

В роботі проведені дослідження алгебрагічних решіток [2]. Решітка складається з набору точок у n-вимірному просторі з періодичною структурою. За допомогою n-лінійно незалежних векторів будь-яка точка цієї структури може бути відтворена. Безпека криптографічних примітивів на основі решітки базуються на NP-складних проблемах високовимірних решіток, наприклад, проблема найкоротшого вектора (SVP).

В ході досліджень як механізму захисту CPS Kyber показав дуже високу продуктивність на всіх оцінених рівнях безпеки CPS [2, 3]. Оскільки промислові кіберфізичні системи (CPS) зазвичай розгортаються десятиліттями, захист від довгострокових загроз є необхідністю [4].

Таким чином, Crystals-Kyber – побудований за допомогою алгебраїчних решіток механізм інкапсуляції ключів, що демонструє себе як ефективний механізм захисту CPS.

Список літератури

1. Roberto Avanzi, Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schank, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber. NIST PQC Standardization: Round 2., 2019

2. Sebastian Paul, Patrik Scheible, Friedrich Wiemer. Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication. Paul, Scheible, and Wiemer, 2021.

3. Petrenko, O. E., Petrenko, O. S., Sievierinov, O. V., Fiediushyn, O. I., Zubrych, A. V., & Shcherbina, D. V. (2021). Аналіз шляхів підвищення стійкості криптоалгоритмів на алгебраїчних решітках щодо часових атак. Radiotekhnika, (207), 59-65.

4. Edward A. Lee, Sanjit A. Seshia. An Introductory Textbook on Cyber-Physical Systems. University of California, Berkeley, USA. 2010.