ВИКОРИСТАННЯ АЛГОРИТМІВ ПРИВЕДЕННЯ БАЗИСУ РЕШІТКИ ПРИ АТАКАХ НА АЛГОРИТМ ЕЦП FALCON

Черниш Д. І., Мельникова О. А.
Харківський національний університет радіоелектроніки, Харків, Україна

Криптосистеми на основі алгебраїчних решіток є перспективним напрямком постквантової криптографії. Перші криптосистеми цього класу були відомі задовго до початку конкурсу NIST PQC. Одною з таких систем був алгоритм електронно цифрового підпису (ЕЦП) NTRUSign. Цей алгоритм не набув популярності через велику кількість успішних атак на цю криптосистему. Алгоритм ЕЦП FALCON[1] який на даний момент є фіналістом третього раунду хоч і побудований на решітках NTRU але він використовує іншу схему побудування ЕЦП відмінну від GGH (що використовується в NTRUSign) а саме структуру GPV[2] запропоновану Джентрі, Пейкертом та Вайкунтонатаном у 2008 році. Автори FALCON затверджують що таке поєднання (решітки NTRU зі структурою GPV) робить алгоритм захищеним від відомих атак на криптосистеми побудовані на базі решіток. Існує декілька видів атак що є можливими для реалізації на цю криптосистему. Найбільш цікавими є атаки типу відновлення ключа та підробка підпису. Більшість з них базується на алгоритмах приведення базису решітки.

Метою доповіді є аналіз відомих алгоритмів приведення базису решітки таких як Slide та різні модифікації алгоритму BKZ. Розгляд можливості використання цих алгоритмів для реалізації атак на ЕЦП FALCON.

В доповіді наводяться характеристики та принцип роботи самих ефективних алгоритмів приведення базису решітки а саме Self-dual BKZ[3] та Slide. Наведені обмеження роботи цих алгоритмів. Дослідження показали, що для повноцінного FALCON існуючі алгоритми приведення базису рештки не підходять, тобто не є ефективними, бо самий ефективний алгоритм DBKZ здатний видавати високоякісний результат при розмірі блоку не більше 80. З розрахунків наведених авторами FALCON можна побачити, що при використанні FALCON зі ступенем поліному 512 цей розмір блоку дорівнює 392 що робить використання алгоритму неефективним для атаки на повно розмірний FALCON.

Список літератури

1. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin. https://falcon-sign.info/falcon.pdf

2. Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction. InMarc Fischlin and Jean-Sébastien Coron, 2016. Springer, Heidelberg,Germany.

3. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. 2008. ACM Press.