НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

СУЧАСНІ АЛГЕБРАЇЧНІ КРИПТОСИСТЕМИ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ

Дослідження сучасних алгебраїчних криптосистем

Виконали:
Волинець Сергій ФІ-42мн
Сковрон Роман ФІ-42мн

Київ — 2024

Зміст

1 Мета

Дослідження особливостей реалізації сучасних алгебраїчних криптосистем на прикладі учасників першого раунду процесу стандартизації постквантової криптографії (NIST PQC).

2 Постановка задачі

Розробити програмну реалізацію алгоритму цифрового підпису “CRYSTALS-Dilithium”. Знайти схожі алгоритми та провести порівняльний аналіз швидкодії за різних умов та використання модифікацій складових частин. Навести повний теоретичний опис алгоритму з усіма деталями та відомими результатами досліджень. Провести теоретичний порівняльний аналіз обраного алгоритму зі схожими алгоритмами та дослідити можливість перенесення відомих атак на обраний алгоритм.

3 хід виконання роботи та опис труднощів

4 Опис криптографічного алгоритму та його складових частин

Вступ CRYSTALS-Dilithium — це схема цифрового підпису, заснована на складності задачі пошуку коротких векторів у решітці. Безпека цієї схеми ґрунтується на цій складності. Алгоритм спроектований для забезпечення високого рівня захисту від різних атак, включаючи атаки з використанням квантових комп’ютерів. У порівнянні з іншими схемами на решітках, які потребують складної генерації випадкових чисел за допомогою дискретного гауссівського розподілу, Dilithium спрощує свою реалізацію, використовуючи рівномірний розподіл, що мінімізує ризики вразливостей до атак через побічні канали. Крім того, це збільшує простоту реалізації, а тому він має менші ризики зменшення рівня безпеки, через необережну імплементацію. Алгоритм оптимізований для зменшення розміру публічного ключа та підпису, зберігаючи при цьому модульність для варіативних рівнів безпеки. За словами авторів, він має найменшу сумарну довжину ключа та підпису з існуючих схем підпису на решітках з таким же рівнем безпеки.

5 Результати порівняльного аналізу швидкодії обраного алгоритму зі схожими алгоритмами

6 Огляд наявних результатів досліджень обраного алгоритму

7 Результати порівняльного аналізу стійкості обраного алгоритму зі схожими алгоритмами

8 Опис тестів, які проводилися з метою перевірки коректності реалізованої програми

9 Детальний опис особливостей реалізації та приклади застосування

10 Результати аналізу постквантової стійкості за наявними результатами аналізу

11 Висновки до роботи