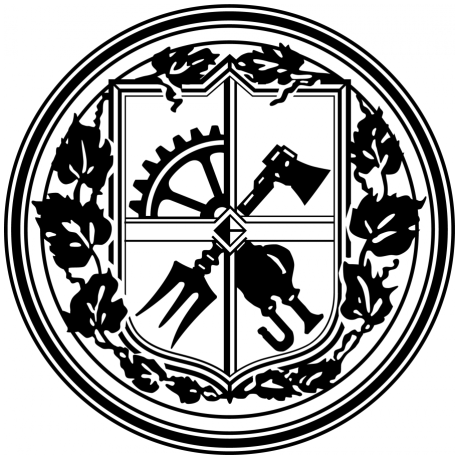
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ



Звіт за темою:

“ДОСЛІДЖЕННЯ СУЧАСНИХ АЛГЕБРАЇЧНИХ КРИПТОСИСТЕМ”

Виконали:
студенти групи ФІ-32мн
Баєвський Констянтин,
Шифрін Денис

Київ — 2023

ЗМІСТ

1 Мета практикуму

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

1. 1 Постановка задачі та варіант завдання

Бригада №4 ***Алгоритм LUOV***

Треба виконати	**Зроблено**
Повний теоретичний опис алгоритму	✓
Повний теоретичний опис реалізації основних алгебраїчних операцій, які використовує обраний алгоритм	✓
Реалізація алгоритму	
Результати проходження тестових даних	

2 Хід роботи та опис труднощів

Для початку було проаналізовано документацію щодо роботи алгоритму LUOV, аналізу проведених атак на даний алгоритм та відомих результататів досліджень. В процесі роботи було детально описано:

– криптографічний алгоритм LUOV та його складові частини;

– реалізації основних алгебраїчних операцій, які використовує даний алгоритм;

– результати порівняльного аналізу швидкодії даного алгоритму зі схожими алгоритмами (або модифікаціями алгоритму за допомогою заміни складових частин);

– наявні результати досліджень даного алгоритму;

– результати порівняльного аналізу стійкості даного алгоритму зі схожими алгоритмами з обґрунтуванням можливості застосування відомих атак.

В результаті було отримано повний теоретичний опис алгоритму та реалізації основних алгебраїчних операцій, які використовує обраний алгоритм. Дані описи будуть використовуватись безпосередньо для подальшої реалізації даного алгоритму.

При виконанні практикуму поки ніяких труднощів не виникло.

3 Результати дослідження

В результаті проробленої роботи було детально проаналізовано та теоретично описано алгоритм LUOV та реалізації основних алгебраїчних операцій, які використовує

даний алгоритм.

3. 1 Опис алгоритму

LUOV Signature Scheme for NIST PQC Project — це пост–квантовий алгоритм цифрового підпису, заснований на використанні еліптичних кривих. Він забезпечує безпеку підпису навіть у випадку, якщо квантові комп'ютери будуть створені.

Алгоритм LUOV Signature Scheme є одним із найперспективніших пост-квантових алгоритмів цифрового підпису. Він є безпечним, ефективним і відносно простим у реалізації.

Розглянемо еліптичну криву E над полем F_p, де p – просте число. Нехай G – точка на кривій E, а n – деяке число, що ділить порядок групи $E(F_p)$.

Алгоритм 0.1. LUOV Signature Scheme працює наступним чином:
– Вибирається пара випадкових чисел a і b, таких що $0 < a < n$ і $0 < b < n$.
– Генерується випадкова точка P на кривій E.
– Обчислюється точка $Q = aP + bG$.
– Ключом алгоритму є пара чисел (a, b).

Формування підпису:

Для формування підпису повідомлення M, яке є випадковим числом з інтервалу $[0, n-1]$, виконується наступна операція: $R = (M + aQ) \bmod n$ $S = (bQ + R) \bmod n$.

Перевірка підпису:

Для перевірки підпису (R, S) повідомлення M виконується наступна операція: $V = (RS) \bmod n$.

Якщо $V = M$, то підпис є дійсним.

Схема підпису може використовуватись в **режимі відновлення повідомлень**. Використання відновлення повідомлення не впливає на алгоритм створення підпису. Ту саму пару ключів можна використовувати для підпису повідомлень у режимі відновлення повідомлень і в режимі доданого підпису, підпис для M у режимі доданого підпису не пов'язаний з підписом для того самого повідомлення в режимі відновлення повідомлення, оскільки інший байт додається до повідомлення в кожному режимі.

Приватний ключ для схеми підпису LUOV – це послідовність із 256 випадкових бітів (які використовуються для заповнення Keccak1600 Sponge) і просто кодується як послідовність із 32 байтів.

Відкритий ключ схеми підпису LUOV – це послідовність із 32 байтів (які використовуються для заповнення Keccak Sponge) і матриці m на $\frac{m(m+1)}{2}$ із двійковими записами. Матриця кодується шляхом об'єднання стовпців і доповнення результату нульовими бітами, щоб отримати послідовність бітів, довжина яких ділиться на 8. Потім

послідовність інтерпретується як послідовність байтів, де перші біти мають найменші значення.

Публічне початкове число, представлене 32 байтами, отримують із губки шляхом стиснення (видавлювання) 32 байтів. Ця операція називається SqueezePublicSeed.

Безпека алгоритму:

Безпека алгоритму LUOV Signature Scheme базується на тому, що важко обчислити точку P, знаючи лише точку Q і пару чисел (a, b). Ця задача є NP–складною, і навіть якщо квантові комп'ютери будуть створені, то її рішення буде вимагати значних ресурсів.

Особливості реалізації алгоритму:

– У реалізації алгоритму використовується еліптична крива над полем F p, де p – число з 128 біт.

– Для генерації випадкових чисел використовується криптографічний генератор псевдовипадкових чисел.

– Для обчислення точки $aP + bG$ використовується алгоритм швидкого множення еліптичних кривих.

Основні алгебраїчні операції, які використовує LUOV, це:

– Додавання еліптичних кривих;

– Множення числа на точку еліптичної кривої.

4 Висновки

В даному практикумі наведено повний теоретичний опис алгоритму з усіма деталями та відомими результатами досліджень. Також проведено теоретичний порівняльний аналіз обраного алгоритму зі схожими алгоритмами та дослідження відомих атак на даний алгоритм.