НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Звіт до лабораторної роботи за темою: Дослідження сучасних алгебраїчних криптосистем на прикладі постквантових криптографічних алгоритмів. Алгоритм TiGER

Оформлення звіту:
Юрчук Олексій, ФІ-52мн
Дигас Богдан, ФІ-52мн

5 листопада 2025 р.
м. Київ

ЗМІСТ

Розділ 1

Вступне слово

Мета роботи (власне, для чого ми тут зібралися):

Дослідити особливостей реалізації сучасних алгебраїчних криптосистем на прикладі учасників першого раунду національного конкурсу з постквантової криптографії в Кореї (KpqC).

Наші задачі на комп'ютерний практикум та порядок їх виконання:

1) Роздітися на бригади. Визначили хто за що відповідатиме. Богдан – займається реалізацією алгоритму TiGER, Олексій – теоретичною частиною і звітом загалом.

2) Провести теоретичне дослідження теми, надавши вичерпний та повний опис теоретичної сторони алгоритму з усіма деталями та відомими результатами досліджень; провести аналіз вже існуючих атак на алгоритм TiGER, а також загалом можливих атак; виконати порівняльний аналіз нашого алгоритму зі схожими та дослідити можливість перенесення та застосування відомих атак на нього.

3) Реалізувати алгоритм програмно та всі(нє, ну ми постараємося) можливі варіанти цього алгоритму;

4) Перевірити коректність – підтвердити правильність реалізації за допомогою тестів, використавши тестові дані з офіційної реалізації;

5) Зробити аналіз продуктивності алгоритму та, знову ж таки, провести порівняння та аналіз швидкодії за різних умов, дослідити вплив модифікацій окремих його складових частин на ефективність.

Розділ 2

Загальне теоретичне дослідження

2.1 Постквантова криптографія

Сучасна криптографія з відкритим ключем, зокрема RSA та криптографія на еліптичних кривих – Elliptic Curve Cryptography (ECC), базується на обчислювальній складності задач факторизації великих чисел та дискретного логарифмування. Однак у 1994 році Пітер Шор [1] продемонстрував квантові алгоритми, здатні розв'язувати ці задачі за поліноміальний час на достатньо потужному квантовому комп'ютері. Це створює критичну загрозу для існуючої криптографічної інфраструктури.

Постквантова криптографія (Post-Quantum Cryptography, PQC) – це галузь криптографії, що розробляє алгоритми, стійкі як до класичних, так і до квантових атак. Серед основних напрямків PQC виділяють криптографію на решітках, криптографію на кодах виправлення помилок, багатовимірну поліноміальну(квадратичну) криптографію та криптографію на основі геш-функцій [2].

2.2 Передумови створення TiGER

Механізм інкапсуляції ключа (Key Encapsulation Mechanism, KEM) є одним з найважливіших криптографічних примітивів для захищеного обміну ключами. У контексті заміни класичних протоколів, таких як Diffie-Hellman (DH) або Elliptic Curve Diffie-Hellman ECDH, постквантові KEM повинні забезпечувати не лише високий рівень безпеки, але й бути ефективними за розміром даних та залишатися обчислювано складними для зламу зловмисником.

Криптографія на решітках, зокрема алгоритми на основі задач Learning With Errors (LWE) [3] та Ring Learning With Errors (RLWE) [4], продемонструвала перспективність у створенні ефективних постквантових схем. Розвиток цього напрямку призвів до появи сімейства алгоритмів, що використовують детерміністичний варіант – Learning With Rounding (LWR) [5], який замінює випадкову помилку округленням, що покращує як продуктивність, так і довжину шифротексту.

Серед попередніх розробок слід відзначити алгоритми Lizard [6] та RLizard [7], які комбінували RLWE для генерації ключів з RLWR для шифрування, досягаючи балансу між безпекою та ефективністю. Однак ці схеми мали певні обмеження щодо розміру відкритого ключа та шифротексту, що ускладнювало їх інтеграцію в існуючі протоколи.

TiGER (Tiny bandwidth key encapsulation mechanism for easy miGration based on RLWE(R)) [8] був розроблений командою дослідників з метою створення компактного та ефективного KEM, придатного для легкої інтеграції в існуючі системи безпеки. Основні задачі, які ставили перед собою науковці це:

- **Мінімізація розміру шифротексту та відкритого ключа**
- **Висока обчислювальна ефективність** — використання в якості модуля число, яке є степенем двійки ($q = 2^k$) (для оптимізації операцій округлення через побітові зсуви);
- **Відмова від NTT** — алгоритм не використовує Number Theoretic Transform, що спрощує реалізацію;
- **Використання розріджених секретів** — зменшення розміру секретного ключа та прискорення множення многочленів;
- **Корекція помилок** — застосування кодів XEf та D2 для зниження ймовірності помилки дешифрування.

Конструкція TiGER базується на комбінації RLWR для генерації відкритого ключа та RLWE для шифрування, з подальшим застосуванням перетворення Fujisaki-Okamoto [9, 10] для досягнення IND-CCA безпеки.

2.3 Участь у KpqC та злиття з SMAUG

У 2022 році Національна служба розвідки Республіки Корея ініціювала Korean Post-Quantum Cryptography Competition скорочено – KpqC [11]. Це національний конкурс для стандартизації постквантових криптографічних алгоритмів.

Обраний нами для аналізу алгоритм TiGER був поданий на перший раунд конкурсу KpqC у категорії механізмів інкапсуляції ключа (KEM) і був одним з чотирьох алгоритмів, які пройшли до другого раунду.

Злиття TiGER та SMAUG

Команди TiGER та SMAUG об'єдналися для створення спільного алгоритму SMAUG-T [12]. Метою злиття було поєднання переваг обох підходів:

- Від **TiGER**: Компактність шифротексту, використання RLWE/RLWR на кільцевому рівні, корекція помилок через D2 кодування (для параметра TiMER);
- Від **SMAUG**: Модульна структура (MLWE/MLWR), розріджені секрети через використання гаусівського шуму, покращена безпека за рахунок збільшення розмірності.

Результатом злиття став алгоритм SMAUG-T версії 3.0 (лютий 2024), який включає в себе:

- Три основні набори параметрів: **SMAUG-T128**, **SMAUG-T192**, **SMAUG-T256** (відповідають рівням безпеки NIST 1, 3, 5);
- Додатковий набір параметрів **TiMER** (Tiny SMAUG using Error Reconciliation) – оптимізований для IoT-пристроїв з мінімальним шифротекстом завдяки використанню D2 кодування з TiGER.

Результати KpqC 2023

У січні 2025 року було оголошено фінальні результаті конкурсу KpqC. Переможцями стали:

- У категорії KEM: **SMAUG-T** та **NTRU+**;
- У категорії цифрового підпису: **HAETAE** (до речі, також від команди SMAUG).

Таким чином, ідеї та технології TiGER увійшли до складу національного стандарту постквантової криптографії Кореї через алгоритм SMAUG-T.

Розділ 3

Теоретична база алгоритму TiGER

Розділ 4

Повний опис алгоритму TiGER

Розділ 5

Результати досліджень

Розділ 6

Аналіз атак на TiGER

Розділ 7

Порівняльний аналіз

Розділ 8

Перенесення атак та можливі покращення

Bibliography

[1] Peter W. Shor. «Algorithms for quantum computation: discrete logarithms and factoring». In: *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[2] Wikipedia. *Post-quantum cryptography — Wikipedia, The Free Encyclopedia*. [Online; accessed 7-October-2025]. URL: https://en.wikipedia.org/wiki/Post-quantum_cryptography.

[3] Oded Regev. «On lattices, learning with errors, random linear codes, and cryptography». In: *Journal of the ACM* 56.6 (2009), pp. 1–40. DOI: 10.1145/1568318.1568324.

[4] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. «On Ideal Lattices and Learning with Errors over Rings». In: *Advances in Cryptology – EUROCRYPT 2010*. 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[5] Abhishek Banerjee, Chris Peikert, and Alon Rosen. «Pseudorandom Functions and Lattices». In: *Advances in Cryptology – EUROCRYPT 2012*. 2012, pp. 719–737. DOI: 10.1007/978-3-642-29011-4_42.

[6] Jung Hee Cheon et al. «Lizard: Cut off the Tail! A Practical Post-Quantum Public-Key Encryption from LWE and LWR». In: *Security and Cryptography for Networks – SCN 2018*. 2018, pp. 160–177. DOI: 10.1007/978-3-319-98113-0_9.

[7] Joohee Lee et al. «RLizard: Post-quantum Key Encapsulation Mechanism for IoT Devices». In: *IEEE Access* 7 (2019), pp. 2080–2091. DOI: 10.1109/ACCESS.2018.2886964.

[8] Seunghwan Park et al. *TiGER: Tiny bandwidth key encapsulation mechanism for easy miGration based on RLWE(R)*. Cryptology ePrint Archive, Paper 2022/1651. https://eprint.iacr.org/2022/1651. 2022.

[9] Eiichiro Fujisaki and Tatsuaki Okamoto. «Secure Integration of Asymmetric and Symmetric Encryption Schemes». In: *Advances in Cryptology – CRYPTO '99*. 1999, pp. 537–554. DOI: 10.1007/3-540-48405-1_34.

[10] Eiichiro Fujisaki and Tatsuaki Okamoto. «Secure Integration of Asymmetric and Symmetric Encryption Schemes». In: *Journal of Cryptology* 26.1 (2013), pp. 80–101. DOI: 10.1007/s00145-011-9114-1.

[11] KpqC Team. *Korean Post-Quantum Cryptography Competition*. https://www.kpqc.or.kr. 2023.

[12] Jung Hee Cheon et al. *SMAUG-T: the Key Exchange Algorithm based on Module-LWE and Module-LWR*. KpqC Round 2 Submission. Version 3.0. 2024.