

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КІЇВСЬКИЙ 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

9 листопада 2025 р.
м. Київ

ЗМІСТ

1 Вступне слово	1
2 Загальне теоретичне дослідження	2
2.1 Постквантова криптографія	2
2.2 Передумови створення TiGER	2
2.3 Участь у КрqC та злиття з SMAUG	3
2.3.1 Злиття TiGER та SMAUG	3
2.3.2 Результати КрqC 2023	4
3 Теоретична база алгоритму TiGER	5
3.1 Алгебраїчні структури	5
3.1.1 Кільця та многочлени	5
3.1.2 Факторкільця многочленів	6
3.1.3 Кільце многочленів у TiGER	6
3.1.4 Операції в кільці R_q	6
3.2 Задачі на решітках	7
3.2.1 Решітки та базові задачі	7
3.2.2 Задача Learning With Errors (LWE)	7
3.2.3 Задача Ring Learning With Errors (RLWE)	8
3.2.4 Задача Learning With Rounding (LWR)	8
3.2.5 Задача Ring Learning With Rounding (RLWR)	9
3.3 "Сімейство" алгоритмів на базі RLWE/RLWR	9
3.3.1 Lizard	9
3.3.2 RLizard	10
3.3.3 CRYSTALS-Kyber	10
3.3.4 Saber	11
3.3.5 Порівняння алгоритмів, і що з них взяв TiGER	12
3.4 Криптографічні примітиви	12
3.4.1 Схема шифрування з відкритим ключем (PKE)	12
3.4.2 Механізм інкапсуляції ключа (KEM)	13
3.4.3 Побудова KEM з PKE	13
3.4.4 Криптографічні геш-функції	14
3.4.5 Зв'язок PKE та KEM у TiGER	14
3.5 Основні поняття безпеки, що стосуються TiGER	14
3.5.1 IND-CPA безпека	14
3.5.2 IND-CCA безпека	15
3.5.3 Ймовірність помилки розшифрування (DFP/R)	16
3.5.4 Квантова безпека a.k.a. QROM	17
3.6 Перетворення Fujisaki-Okamoto	17
3.6.1 Класичне перетворення FO	17
3.6.2 Перетворення FO_m^f з неявним відхиленням	18
3.6.3 Застосування у алгоритмі TiGER	19

4 Повний опис алгоритму TiGER	20
4.1 Загальна структура алгоритму	20
4.1.1 Модульна побудова алгоритму	20
4.1.2 Взаємодія між компонентами TiGER	21
4.2 Публічні параметри	21
4.3 Допоміжні алгоритми	23
4.4 TiGER.PKE	25
4.4.1 KeyGen – генерація ключів	25
4.4.2 Encryption – шифрування	26
4.4.3 Decryption – розшифрування	27
4.5 TiGER.KEM	29
4.5.1 KeyGen – генерація ключів	29
4.5.2 Encapsulation – інкапсуляція	29
4.5.3 Decapsulation – декапсуляція	30
4.6 Аналіз коректності	32
4.7 Особливості реалізації	34
5 Результати досліджень	36
6 Аналіз атак на TiGER	37
7 Порівняльний аналіз	38
8 Перенесення атак та можливі покращення	39

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 (КроС).

Наши 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 привів до появи сімейства алгоритмів, що використовують детермінований 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 числа, 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 (з малою вагою Геммінга)** — зменшення розміру секретного ключа та прискорення множення многочленів;
- **Корекція помилок** — застосування кодів XEf та D2 для зниження ймовірності помилки розшифрування.

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

2.3 Участь у КроС та злиття з SMAUG

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

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

2.3.1 Злиття TiGER та SMAUG

Команди TiGER та SMAUG об'єдналися для створення спільногого 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), розрідженні 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(Internet of Thing)-пристроїв з мінімальним шифротекстом завдяки використанню D2 кодування з TiGER.

2.3.2 Результати КрqС 2023

У січні 2025 року було оголошено фінальні результати конкурсу КрqС. 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

3.1 Алгебраїчні структури

Криптографія на решітках (Lattice-based cryptography) використовує алгебраїчні структури для забезпечення ефективності обчислень та компактності представлення даних. У цьому розділі я розпишу основні алгебраїчні об'єкти, що застосовуються в алгоритмі TiGER.

3.1.1 Кільце та многочлени

Означення 3.1.1 (Кільце).

Кільце ($R, +, \cdot$) – це множина з двома операціями: додавання (+) та множення (\cdot), що задоволяє наступні властивості:

1. $(R, +)$ є абелевою групою за додаванням. Нейтральний елемент 0;
2. Множення є асоціативним: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in R$;
3. Дистрибутивність: $a \cdot (b + c) = a \cdot b + a \cdot c$ та $(b + c) \cdot a = b \cdot a + c \cdot a$, $\forall a, b, c \in R$;
4. Існує нейтральний елемент за множенням: $1 \in R$ такий, що $1 \cdot a = a \cdot 1 = a$, $\forall a \in R$.

Якщо ще $a \cdot b = b \cdot a$, $\forall a, b \in R$, то таке кільце називається комутативним.

Означення 3.1.2 (Кільце многочленів).

Нехай R – комутативне кільце з одиницею. Кільце многочленів $R[x]$ складається з усіх виразів виду

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

де $\forall i : a_i \in R$, $a_n \neq 0$ та $n \in \mathbb{Z}$.

Число n називається степенем многочлена $f(x)$, позначається $\deg(f)$.

Операції додавання та множення многочленів наступним чином:

- $(f + g)(x) = \sum_{i=0}^{\max(\deg(f), \deg(g))} (a_i + b_i)x^i$, де a_i, b_i – коефіцієнти f та g відповідно;
- $(f \cdot g)(x) = \sum_{k=0}^{\deg(f)+\deg(g)} c_k x^k$, де $c_k = \sum_{i=0}^k a_i b_{k-i}$.

3.1.2 Факторкільця многочленів

Означення 3.1.3 (Факторкільце).

Нехай R – кільце та I – його ідеал. Факторкільце R/I складається з класів еквівалентності $a + I = \{a + r : r \in I\}$ для $a \in R$, з операціями:

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = (a \cdot b) + I.$$

У Lattice-based cryptography найчастіше використовується факторкільце многочленів за ідеалом, що породжений циклотомічним многочленом.

Означення 3.1.4 (Циклотомічний многочлен).

n -ий циклотомічний многочлен (Cyclotomic polynomial) $\Phi_n(x)$ визначається як мінімальний многочлен над \mathbb{Q} , коренями якого є примітивні корені n -го степеня з одиницею:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (x - e^{2\pi i k/n}).$$

Лема 3.1.1. Для $n = 2^k$, де $k \in \mathbb{N}$, циклотомічний многочлен має вигляд:

$$\Phi_n(x) = x^{n/2} + 1.$$

Доведення: При $n = 2^k$ примітивними коренями n -го степеня з одиницею є $e^{2\pi i m/n}$ для непарних m . З $(x^{n/2} + 1) = (x^n - 1)/(x^{n/2} - 1)$ випливає твердження леми. \square

3.1.3 Кільце многочленів у TiGER

В алгоритмі TiGER використовується кільце многочленів виду:

$$R_q = \frac{\mathbb{Z}_q[x]}{(x^n + 1)},$$

де n – степінь двійки (зазвичай $n = 512$ або $n = 1024$), а q – модуль, що також є степенем двійки ($q = 256$ у всіх варіаціях алгоритму TiGER).

Елементами R_q є многочлени степеня не вище $n - 1$ з коефіцієнтами з \mathbb{Z}_q :

$$f(x) = \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in \mathbb{Z}_q.$$

Вибір саме такого n та многочлена $x^n + 1$ забезпечує:

- Ефективність множення многочленів (без потреби в NTT);
- Редукцію за модулем $x^n + 1$, що спрощує обчислення;
- Зв'язок з циклотомічними многочленами та решітковими задачами.

3.1.4 Операції в кільці R_q

Для $f(x), g(x) \in R_q$ операції в кільці визначаються наступним чином:

Додавання: покоефіцієнтне за модулем q :

$$(f + g)(x) = \sum_{i=0}^{n-1} ((f_i + g_i) \bmod q) x^i.$$

Множення: спочатку виконується звичайне множення многочленів, потім взяття за модулем $(x^n + 1)$ та q . Оскільки $x^n \equiv -1 \pmod{x^n + 1}$, то маємо:

$$h_i = \left(\sum_{j=0}^i f_j g_{i-j} - \sum_{j=i+1}^{n-1} f_j g_{n+i-j} \right) \pmod{q},$$

де $h(x) = (f \cdot g)(x) = \sum_{i=0}^{n-1} h_i x^i$.

3.2 Задачі на решітках

Безпека TiGER базується на обчислювальній складності певних задач на решітках. У цьому підпункті зазначимо основні решіткові задачі, що лежать в основі постквантової криптографії.

3.2.1 Решітки та базові задачі

Означення 3.2.1 (Решітка).

Нехай $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m \in \mathbb{R}^n$ – лінійно незалежні вектори. Решітка Λ , породжена цими векторами, визначається як:

$$\Lambda = \Lambda(\mathbf{b}_1, \dots, \mathbf{b}_m) = \left\{ \sum_{i=1}^m a_i \mathbf{b}_i : a_i \in \mathbb{Z} \right\}.$$

Вектори $\mathbf{b}_1, \dots, \mathbf{b}_m$ називаються базисом решітки, а m – розмірністю решітки.

Означення 3.2.2 (Мінімальна відстань решітки(shortest vector)).

Мінімальна відстань решітки Λ визначається як:

$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|,$$

де $\|\cdot\|$ – евклідова норма.

Означення 3.2.3 (SVP).

Shortest Vector Problem (SVP): Для заданого базису решітки Λ знайти ненульовий вектор $\mathbf{v} \in \Lambda$ такий, що $\|\mathbf{v}\| = \lambda_1(\Lambda)$.

SVP є NP-складною задачею [13]. Для криптографічних цілей часто використовується наступна версія:

Означення 3.2.4 (Апроксимаційна задача SVP).

γ -approximate SVP (γ -SVP): Для заданого базису решітки Λ та параметра наближення $\gamma \geq 1$, знайти ненульовий вектор $\mathbf{v} \in \Lambda$ такий, що $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda)$.

3.2.2 Задача Learning With Errors (LWE)

Задача Learning With Errors була введена Одедом Регевим у 2005 році [3] і стала основою для багатьох постквантових криптосистем.

Означення 3.2.5 (LWE задача (search version)).

Нехай $n, q \geq 1$ – цілі числа, χ – розподіл ймовірностей на \mathbb{Z}_q . Пошукова задача $LWE_{n,q,\chi}$ визначається наступним чином:

Для невідомого секрету $\mathbf{s} \in \mathbb{Z}_q^n$ та заданої послідовності пар $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, де

$$b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \pmod{q},$$

з випадково обраними $\mathbf{a}_i \in \mathbb{Z}_q^n$, $\langle \cdot, \cdot \rangle$ – операція векторного добутку та $e_i \xleftarrow{p} \chi$, знайти секрет \mathbf{s} .

Означення 3.2.6 (LWE задача (detection version)).

Розпізнавальна задача $Decision-LWE_{n,q,\chi}$ полягає у розрізненні наступних двох розподілів:

- $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \pmod{q})$, де $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $\mathbf{s} \in \mathbb{Z}_q^n$ фіксоване, $e \xleftarrow{p} \chi$;
- (\mathbf{a}, u) , де \mathbf{a}, u – рівномірно розподілені на \mathbb{Z}_q^n та \mathbb{Z}_q відповідно.

Теорема 3.2.1 (Регева).

Для певних параметрів n, q, χ , розв’язання задачі $Decision-LWE$ за поліноміальний час у середньому випадку еквівалентно розв’язанню наближеної задачі γ -SVP за квантовий поліноміальний час у найгіршому випадку для деякого $\gamma = \tilde{O}(n/\sigma)$.

3.2.3 Задача Ring Learning With Errors (RLWE)

Ring-LWE є алгебраїчною версією LWE, що вже використовує кільця многочленів для більшої ефективності [4].

Означення 3.2.7 (RLWE задача).

Нехай $R = \mathbb{Z}[x]/(x^n + 1)$, $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, та χ – розподіл ймовірностей на R_q . Розпізнавальна задача $Decision-RLWE_{n,q,\chi}$ полягає у розрізненні наступних розподілів:

- $(a, a \cdot s + e)$, де обрано $a \in R_q$ (рівномірний розподіл), $s \in R_q$ фіксоване, $e \xleftarrow{p} \chi$;
- (a, u) , де a, u обрані рівномірно з R_q .

Важливим є те, що RLWE дозволяє представляти n секретів (LWE-зразків) у вигляді одного многочлена в R_q , що значно зменшує розмір ключів та шифротекстів. Для TiGER використовується $n \in \{512, 1024\}$ та $q = 256$.

3.2.4 Задача Learning With Rounding (LWR)

Learning With Rounding є детермінованим варіантом LWE, де замість додавання випадкової помилки використовується округлення [5].

Означення 3.2.8 (LWR задача).

Нехай n, q, p – цілі числа, $p < q$. Визначимо функцію округлення $\lfloor \cdot \rceil_p : \mathbb{Z}_q \rightarrow \mathbb{Z}_p$ як

$$\lfloor x \rceil_p = \left\lfloor \frac{p}{q} \cdot x \right\rfloor \pmod{p},$$

де $\lfloor \cdot \rceil$ позначатиме округлення до найближчого цілого.

Розпізнавальна задача $Decision-LWR_{n,q,p}$ полягає у розрізненні наступних розподілів:

- $(\mathbf{a}, \lfloor \langle \mathbf{a}, \mathbf{s} \rangle \rfloor_p)$, де $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $\mathbf{s} \in \mathbb{Z}_q^n$ – фіксоване;
- (\mathbf{a}, u) , де $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $u \leftarrow \mathbb{Z}_p$.

Теорема 3.2.2 (Редукція (взяття за модулем) LWR до LWE [5]). Для відповідних параметрів n, q, p та достатньо малого розподілу помилок χ , задача $\text{Decision-LWR}_{n,q,p}$ зводиться до задачі $\text{Decision-LWE}_{n,q,\chi}$.

Зауваження. (Ідея теореми) При достатньо великому відношенні q/p , округлення $\lfloor \langle \mathbf{a}, \mathbf{s} \rangle \rfloor_p$ стає еквівалентно до додавання малої помилки округлення, яка розподілена майже рівномірно на інтервалі $(-q/(2p), q/(2p)]$.

3.2.5 Задача Ring Learning With Rounding (RLWR)

RLWR поєднує переваги RLWE (компактність – за рахунок алгебраїчної структури) та LWR (детермінованість, та відсутність потреби у відборі помилок(sampling)).

Означення 3.2.9 (RLWR задача).

Нехай $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, $R_p = \mathbb{Z}_p[x]/(x^n + 1)$, де $p < q$. Функція округлення застосовуються для кожного коефіцієнта окремо:

$$\lfloor f \rceil_p = \sum_{i=0}^{n-1} \left\lfloor \frac{p}{q} \cdot f_i \right\rfloor x^i \bmod p.$$

Розпізнавальна задача $\text{Decision-RLWR}_{n,q,p}$ полягає у розрізненні:

- $(a, \lfloor a \cdot s \rceil_p)$, де $a \in R_q$ обрано рівномірно, $s \in R_q$ фіксоване;
- (a, u) , де $a \in R_q$, $u \in R_p$ обрані рівномірно.

Твердження 3.2.1.

При певних параметрах n, q, p , задача $\text{RLWR}_{n,q,p}$ є не легшою за задачу $\text{RLWE}_{n,q,\chi}$ з розподілом помилок χ , що відповідає помилці округлення.

У TiGER використовується комбінація: RLWR – для генерації відкритого ключа (компактність) та RLWE – для шифрування (гнучкості у контролі помилок). Модулі обираються як степені двійки: $q = 256$, $p \in \{64, 128\}$, що дозволяє реалізувати округлення через побітові зсуви. Про це поговоримо детальніше наступному, 4 розділі.

3.3 “Сімейство” алгоритмів на базі RLWE/RLWR

TiGER належить до сімейства алгоритмів на решітках, які базуються на задачах RLWE та RLWR. Опишемо основні алгоритми цього сімейства, які вплинули на дизайн TiGER (далі). Далі їх буде порівняно у розділі 6 та попередньо у таблиці 3.1.

3.3.1 Lizard

Lizard [6] був одним з перших алгоритмів, що комбінував у собі LWE та LWR для досягнення балансу між безпекою та ефективністю.

Основні характеристики:

- **Структура:** LWE для генерації відкритого ключа, LWR для шифрування;

- **Простір:** Цілочисельні решітки над \mathbb{Z}_q^n без використання кільцевої структури;
- **Модуль:** Малий модуль q для покращення коректності;
- **Розміри:** Великі ключі (через відсутність алгебраїчної структури).

Переваги:

- Консервативна безпека (базується на стандартній LWE);
- Низька ймовірність помилки розшифрування.

Недоліки:

- Великі розміри ключів та шифротекстів;
- Повільніше множення векторів (порівняно з кільцевими варіантами).

3.3.2 RLizard

RLizard [7] є кільцевою версією попереднього алгоритму, оптимізованою для IoT-пристроїв.

Основні характеристики:

- **Структура:** RLWE для генерації ключів, RLWR для шифрування;
- **Простір:** $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, $n = 512$ або $n = 1024$;
- **Модуль:** Малий модуль q (наприклад, $q = 1024$);
- **Помилки:** Дискретний гаусівський розподіл помилок з високою точністю (CDT-sampling).

Переваги:

- Компактні ключі та шифротексти завдяки кільцевій структурі;
- Швидке шифрування/розшифрування;
- Висока коректність;
- Підходить для пристроїв з обмеженим ресурсом.

Недоліки:

- Відносно велика пропускна здатність порівняно з найкомпактнішими схемами;
- Залежність від якісного (справді випадкового) семплювання гаусівських помилок.

3.3.3 CRYSTALS-Kyber

Kyber [14] є одним з фіналістів конкурсу NIST PQC і базується на Module-LWE (MLWE).

Основні характеристики:

- **Структура:** MLWE для обох операцій – генерації ключів та шифрування повідомлення;
- **Простір:** Модульні решітки R_q^k , де $k \in \{2, 3, 4\}$ (залежно від рівня безпеки);

- **Модуль:** $q = 3329$ (просте число для ефективного NTT);
- **Оптимізація:** Number Theoretic Transform (NTT) для швидкого множення многочленів (хах, тут порівнюючи з чим саме і що вважати швидко);
- **Компресія:** Агресивне "стиснення" шифротексту.

Переваги:

- Стандартизовано під NIST (FIPS 203);
- Непоганий баланс між розмірами, швидкістю та безпекою;
- Ефективна реалізація з NTT.

Недоліки:

- Використання простого модуля ускладнює деякі оптимізації;
- Більший шифротекст порівняно з деякими MLWR-схемами.

3.3.4 Saber

Saber [15] є Module-LWR схемою, фіналістом NIST PQC Round 3.

Основні характеристики:

- **Структура:** MLWR для обох операцій;
- **Простір:** Модульні решітки R_q^k , $k \in \{2, 3, 4\}$;
- **Модуль:** $q = 8192 = 2^{13}$;
- **Оптимізація:** Відсутність NTT (округлення завдяки побітовим операціям);
- **Помилки:** Детермініновані (через застосування округлення).

Переваги:

- Компактний шифротекст;
- Простота реалізації (без потреби в NTT чи гаусівському семплюванні);
- Ефективні побітові операції;
- Хороша стійкість до side-channel атак.

Недоліки:

- Більший(за розміром) відкритий ключ порівняно з Kyber;

3.3.5 Порівняння алгоритмів, і що з них взяв TiGER

Характеристика	Lizard	RLizard	Kyber	Saber
Структура	LWE/LWR	RLWE/RLWR	MLWE	MLWR
Розмірність	n	n	$n \times k$	$n \times k$
Модуль q	малий	малий	3329	8192
NTT	Hi	Hi	Так	Hi
Семплювання	Гаусс	Гаусс/CDT	Centered binomial	Округлення
Компресія	Помірна	Помірна	Агресивна	Помірна

Таблиця 3.1: Порівняння підходів у сімействі RLWE/RLWR алгоритмів

TiGER об'єднує в собі найкращі ідеї з попередніх доборок:

Позиція TiGER:

- Базується на **RLWE/RLWR** (як RLizard);
- Використовує **степені двійки** для q, p (як Saber);
- **Розрідженні секрети** для ефективності;
- **Корекція помилок** (XEf, D2) для мінімізації DFP/R;
- **Без NTT** для простоти;
- Фокусування на **мінімальному шифротексті** для легшого впровадження в існуючі протоколи.

3.4 Криптографічні примітиви

У цій частині розділу розглянемо базові криптографічні примітиви, що використовуються для безпосередньо при побудові TiGER: схеми шифрування з відкритим ключем (PKE) та механізми інкапсуляції ключа (KEM).

3.4.1 Схема шифрування з відкритим ключем (PKE)

Означення 3.4.1 (PKE схема).

Схема шифрування з відкритим ключем (*Public Key Encryption, PKE*) складається з трьох алгоритмів:

- $\text{KeyGen}(1^\lambda) \rightarrow (\text{pk}, \text{sk})$ — ймовірнісний алгоритм генерації ключів, що на вході приймає параметр безпеки λ і повертає пару: відкритий ключ pk та секретний ключ sk ;
- $\text{Enc}(\text{pk}, m; r) \rightarrow c$ — ймовірнісний алгоритм шифрування, що приймає відкритий ключ pk , повідомлення m з простору повідомлень \mathcal{M} та випадкове число r , і повертає шифротекст c ;

- $\text{Dec}(\text{sk}, c) \rightarrow m'$ — детермінінований алгоритм розшифрування, що приймає секретний ключ sk і шифротекст c , та повертає повідомлення m' або помилку \perp .

Означення 3.4.2 (Коректність РКЕ).

РКЕ схема є $(1 - \delta)$ -коректною, якщо для будь-якої пари ключів $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$ та будь-якого повідомлення $m \in \mathcal{M}$ виконується:

$$\mathbb{P}[\text{Dec}(\text{sk}, \text{Enc}(\text{pk}, m)) \neq m] \leq \delta,$$

де ймовірність визначається через випадковість алгоритму Enc . Параметр δ називається ймовірністю помилки розшифрування (Decryption Failure Probability/Rate, DFP/R)

У задачах на решітках, через наявність помилок у RLWE/RLWR, коректність не завжди є ідеальною. Тому для практичних застосувань необхідно, щоб δ було незначним ($\delta \leq 2^{-128}$).

3.4.2 Механізм інкапсуляції ключа (КЕМ)

Означення 3.4.3 (КЕМ схема).

Механізм інкапсуляції ключа (Key Encapsulation Mechanism, КЕМ) складається з трьох кроків:

- $\text{KeyGen}(1^\lambda) \rightarrow (\text{pk}, \text{sk})$ — алгоритм генерації ключів (аналогічно до РКЕ);
- $\text{Encaps}(\text{pk}) \rightarrow (c, K)$ — ймовірнісний алгоритм інкапсуляції, що приймає відкритий ключ pk і повертає шифротекст c та спільний секретний ключ $K \in \mathcal{K}$;
- $\text{Decaps}(\text{sk}, c) \rightarrow K'$ — детермінінований алгоритм декапсуляції, що приймає секретний ключ sk і шифротекст c , та повертає прихований секретний ключ K' або символ помилки \perp .

Означення 3.4.4 (Коректність КЕМ).

КЕМ схема є $(1 - \delta)$ -коректною, якщо для будь-якої пари ключів $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$ справджується таке:

$$\mathbb{P}[\text{Decaps}(\text{sk}, c) \neq K : (c, K) \leftarrow \text{Encaps}(\text{pk})] \leq \delta.$$

3.4.3 Побудова КЕМ з РКЕ

Стандартний спосіб побудови КЕМ з РКЕ полягає у шифруванні випадкового повідомлення та використанні геш-функції для отримання спільногого ключа.

Твердження 3.4.1 (Нативна побудова КЕМ).

Нехай РКЕ = $(\text{KeyGen}, \text{Enc}, \text{Dec})$ — РКЕ це ось така трійка, що містить у собі простір повідомлень \mathcal{M} , та $H : \mathcal{M} \rightarrow \mathcal{K}$ — деяка геш-функція. Тоді можна побудувати КЕМ таким способом:

- Спосіб генерації KeyGen такий же, як у РКЕ;
- $\text{Encaps}(\text{pk})$: обирають $m \in \mathcal{M}$, а далі обчислюють $c \leftarrow \text{Enc}(\text{pk}, m)$ та $K \leftarrow H(m)$. На виході отримано пару: (c, K) ;

- $\text{Decaps}(\text{sk}, c)$: обчислюють $m' \leftarrow \text{Dec}(\text{sk}, c)$ та на виході отримуємо $K' \leftarrow H(m')$.

Така побудова не забезпечує IND-CCA безпеки навіть якщо базова PKE схема є IND-CPA безпечною, але для нас головне щоб було зрозуміло як цей механізм працює). А для досягнення IND-CCA безпеки вже необхідно застосувати перетворення Fujisaki-Okamoto (розділено його у секції 3.6).

3.4.4 Криптографічні геш-функції

Означення 3.4.5 (Криптографічна геш-функція).

Функція $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ називається криптографічною геш-функцією, якщо вона задовільняє наступні умови:

1. **Стійкість до знаходження прообразу:** Для випадкового $y \in \{0, 1\}^n$ обчислювано важко знайти x такий, що $H(x) = y$;
2. **Стійкість до знаходження другого прообразу:** Для заданого x обчислювано важко знайти $x' \neq x$ такий, що $H(x') = H(x)$;
3. **Стійкість до колізій:** Обчислювано важко знайти дві різні величини x, x' такі, що $H(x) = H(x')$.

У TiGER використовуються геш-функції з сімейства SHA-3 – SHAKE256 (або SHA3-256) для генерації випадковості, обчислення спільних ключів та інших криптографічних операцій. SHAKE256 є функцією з розширенним виходом (XOF), що дозволяє генерувати вихід довільної довжини.

3.4.5 Зв'язок PKE та KEM у TiGER

TiGER складається з двох рівнів:

1. **TiGER.PKE** – являє собою базову IND-CPA безпечну схему шифрування, що базується на RLWE(R);
2. **TiGER.KEM** – KEM, отриманий застосуванням перетворення Fujisaki-Okamoto (FO) до TiGER.PKE для досягнення IND-CCA безпеки.

Це дозволяє:

- Окремо аналізувати безпеку PKE (на базі RLWE/RLWR);
- Використовувати загальні результати про перетворення FO для доведення IND-CCA безпеки KEM;

3.5 Основні поняття безпеки, що стосуються TiGER

3.5.1 IND-CPA безпека

Означення 3.5.1 (IND-CPA (Indistinguishability under Chosen-Plaintext Attack) гра для PKE).

Розглянемо наступну "гру" між претендентом (*challenger*) \mathcal{C} та супротивником (*adversary*) \mathcal{A} :

1. \mathcal{C} генерує $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$ і передає pk супротивнику \mathcal{A} ;
2. \mathcal{A} обирає два повідомлення $m_0, m_1 \in \mathcal{M}$ однакової довжини і передає їх \mathcal{C} ;
3. \mathcal{C} Випадковим чином обирає біт $b \xleftarrow{p} \{0, 1\}$, обчислює $c \leftarrow \text{Enc}(\text{pk}, m_b)$ і передає c супротивнику \mathcal{A} ;
4. \mathcal{A} виводить біт b' .

Перевага супротивника визначається наступним чином:

$$\text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A}) = \left| \mathbb{P}[b' = b] - \frac{1}{2} \right| + \varepsilon(\lambda).$$

PKE схема є IND-CPA безпечною, якщо для будь-якого ефективного (PPT) супротивника \mathcal{A} перевага $\text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathcal{A})$ є незначною функцією від λ .

IND-CPA безпечність означає нерозрізnenість шифротекстів: супротивник маючи доступ до відкритого ключа (а отже, має можливість шифрувати будь-які повідомлення), не може визначити, яке з двох повідомень було зашифроване. Це вимагає від шифрування, щоб воно було ймовірнісним.

Означення 3.5.2 (IND-CPA (Indistinguishability under Chosen-Plaintext Attack) безпека для KEM).

Для KEM "гра" IND-CPA визначається аналогічно:

1. \mathcal{C} генерує пару $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$ і передає pk супротивнику \mathcal{A} ;
2. \mathcal{C} обирає $b \xleftarrow{p} \{0, 1\}$. Якщо обрано $b = 0$, то обчислює $(c, K_0) \leftarrow \text{Encaps}(\text{pk})$; а якщо $b = 1$, обчислює $(c, K_0) \leftarrow \text{Encaps}(\text{pk})$ та $K_1 \xleftarrow{p} \mathcal{K}$. Опісля передає пару (c, K_b) супротивнику;
3. \mathcal{A} виводить біт b' .

Перевага супротивника $\text{Adv}_{\text{KEM}}^{\text{IND-CPA}}(\mathcal{A})$ визначається аналогічно як і в PKE.

Безпека KEM тісно пов'язана з:

- IND-CPA безпекою базової PKE схеми;
- Ймовірністю помилки розшифрування ε ;
- Параметрами випадкових оракулів (про трохи далі).

Важливим є те, що навіть за наявності помилок розшифрування (що неминуче для схем на решітках), можна довести IND-CCA безпеку за умови достатньо малого $\varepsilon(\lambda)$.

3.5.2 IND-CCA безпека

Означення 3.5.3 (IND-CCA для PKE).

"Гра" IND-CCA відрізняється від IND-CPA тим, що противник \mathcal{A} має додатково доступ до оракула десифратора (decryption oracle) $\text{Dec}(\text{sk}, \cdot)$:

1. \mathcal{C} генерує $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$ і передає pk супротивнику \mathcal{A} ;

2. \mathcal{A} робить запити до оракула дешифрування, подаючи на вхід довільні шифротексти c_i і отримувати $m_i = \text{Dec}(\text{sk}, c_i)$;
3. \mathcal{A} обирає m_0, m_1 і отримує challenge шифротекст $c^* \leftarrow \text{Enc}(\text{pk}, m_b)$ для випадкового b ;
4. \mathcal{A} продовжує робити запити до оракула дешифрування, але не може запитувати c^* – випадок **IND-CCA2** (а якщо запити заборонені вже після отримання c^* – це **IND-CCA1**);
5. \mathcal{A} виводить біт b' .

Перевага $\text{Adv}_{\text{PKE}}^{\text{IND-CCA}}(\mathcal{A})$ визначається аналогічно.

Означення 3.5.4 (IND-CCA безпека для KEM).

Для KEM схеми противник має доступ до оракула декапсуляції $\text{Decaps}(\text{sk}, \cdot)$ і **не може** запитувати challenge шифротекст c^* після його отримання.

IND-CCA (Indistinguishability under Chosen Ciphertext Attack) безпека є значно сильнішою, ніж IND-CPA, оскільки моделює активного противника, який може маніпулювати шифротекстами та спостерігати результати дешифрування. Для практичних застосувань зазвичай потрібна IND-CCA2 безпека.

3.5.3 Ймовірність помилки розшифрування (DFP/R)

Означення 3.5.5 (Decryption Failure Probability/Rate).

Для PKE схеми ймовірність помилки розшифрування (DFP/R) визначається як:

$$\delta = \max_{m \in \mathcal{M}} \mathbb{P}_{(\text{pk}, \text{sk}), r} [\text{Dec}(\text{sk}, \text{Enc}(\text{pk}, m; r)) \neq m],$$

де ймовірність береться за випадковістю генерації ключів та шифрування.

Для KEM схеми:

$$\delta = \mathbb{P}_{(\text{pk}, \text{sk}), (c, K)} [\text{Decaps}(\text{sk}, c) \neq K].$$

У решіткових схемах помилки розшифрування виникають природнім шляхом (наявність шуму у RLWE/RLWR), тому параметри схеми (розміри модулів, розподіл помилок, коефіцієнт стиснення) мають бути підібрані так, щоб забезпечити мале δ . (!) Висока ймовірність помилки розшифрування може привести до наступних атак:

- **Failure boosting attacks [16]:** Супротивник може ітеративно створювати шифротексти, що мають високу ймовірність помилки, щоб витягувати поступово інформацію про секретний ключ;
- **Multi-target attacks [17]:** При наявності багатьох публічних ключів або сесій, навіть відносно мала DFP/R може стати проблемою.

Для реалізацій TiGER цільова DFP/R становить:

- TiGER128: $\delta \approx 2^{-120}$;
- TiGER192: $\delta \approx 2^{-136}$;
- TiGER256: $\delta \approx 2^{-167}$.

P.S. Ці значення вважаються достатньо малими для практичного застосування.

3.5.4 Квантова безпека а.к.а. QROM

Означення 3.5.6 (Quantum Random Oracle Model).

Модель квантового випадкового оракула (скорочено *QROM*) – це розширення класичної моделі випадкового оракула (*ROM*), де противник має квантовий доступ до геш-функцій, тобто може ще робити запити у суперпозиції.

Для TiGER необхідно, щоб перетворення Fujisaki-Okamoto забезпечувало IND-CCA безпеку у *QROM*, це гарантуватиме стійкість проти квантових атак.

3.6 Перетворення Fujisaki-Okamoto

Перетворення Fujisaki-Okamoto (скорочено *FO*) [9, 10] є загальним методом перетворення IND-CPA безпечної PKE схеми у IND-CCA безпечну KEM схему. В цьому підпункті наведемо просте класичне *FO* перетворення та його модифікацію – варіант з неявним відхиленням, що використовується в TiGER.

3.6.1 Класичне перетворення *FO*

Теорема 3.6.1 (Fujisaki-Okamoto).

Нехай $\text{PKE} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ – IND-CPA безпечна PKE схема з однозначним детермінованим розшифруванням. Нехай $G : \mathcal{M} \rightarrow \mathcal{R} \times \mathcal{K}$ та $H : \mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}$ – випадкові оракули. Тоді наступна конструкція є IND-CCA безпечною KEM у моделі випадкового оракула [9]:

Algorithm 1 $\text{KeyGen}()$

- 1: Generate $(pk, sk) \leftarrow \text{PKE.KeyGen}(1^\lambda)$
- 2: **return** (pk, sk)

Algorithm 2 $\text{Encaps}(pk)$

- 1: Choose $m \xleftarrow{p} \mathcal{M}$
- 2: Calculate $(r, K) \leftarrow G(m)$
- 3: Calculate $c \leftarrow \text{PKE.Enc}(pk, m; r)$
- 4: **return** (c, K)

Algorithm 3 $\text{Decaps}(sk, c)$

- 1: Calculate $m' \leftarrow \text{PKE.Dec}(sk, c)$
- 2: Calculate $(r', K') \leftarrow G(m')$
- 3: Calculate $c' \leftarrow \text{PKE.Enc}(pk, m'; r')$
- 4: **if** $c = c'$ **then**
- 5: **return** K'
- 6: **else**
- 7: **return** \perp
- 8: **end if**

Ключова ідея перетворення FO полягає у **повторному шифруванні** (re-encryption): після розшифрування повідомлення m' воно повторно шифрується з тією ж випадковістю, і результат порівнюється з отриманим шифротекстом. Це дозволяє виявити модифікації шифротексту.

3.6.2 Перетворення FO_m^{\perp} з неявним відхиленням

Для схем на решітках з ненульовою ймовірністю помилки розшифрування було розроблено модифікацію – варіант FO з **неявним відхиленням** (implicit rejection) [18].

Означення 3.6.1 (Перетворення FO_m^{\perp}).

Нехай PKE – IND-CPA безпечна PKE схема. Конструкція FO_m^{\perp} відрізняється від класичного FO у додатковій декапсуляції:

Algorithm 4 KeyGen()

- 1: Generate $(pk, sk') \leftarrow \text{PKE.KeyGen}(1^\lambda)$
- 2: Choose $z \xleftarrow{p} \mathcal{Z}$ \triangleright Додатковий випадковий ключ
- 3: **return** $(pk, sk = (sk', z))$

Algorithm 5 Encaps(pk)

- 1: Choose $m \xleftarrow{p} \mathcal{M}$
- 2: Calculate $r \leftarrow G(m, pk)$
- 3: Calculate $c \leftarrow \text{PKE.Enc}(pk, m; r)$
- 4: Calculate $K \leftarrow H(m, c)$
- 5: **return** (c, K)

Algorithm 6 Decaps(sk, c)

- 1: Split $sk = (sk', z)$
- 2: Calculate $m' \leftarrow \text{PKE.Dec}(sk', c)$
- 3: Calculate $r' \leftarrow G(m', pk)$
- 4: Calculate $c' \leftarrow \text{PKE.Enc}(pk, m'; r')$
- 5: **if** $c = c'$ **then**
- 6: **return** $K' \leftarrow H(m', c)$
- 7: **else**
- 8: **return** $\bar{K} \leftarrow H(z, c)$ \triangleright Неявне відхилення
- 9: **end if**

Ключова відмінність: замість повернення \perp при невдалій перевірці, алгоритм повертає псевдовипадковий ключ $\bar{K} = H(z, c)$, де z – секретний випадковий ключ. Це має дві переваги:

- **Захист від side-channel атак:** Оскільки зовнішньому спостерігачу стає важче визначити, чи відбулася помилка при декапсуляції;
- **Постійний час виконання:** Обидва варіанти (успіх/невдача) тепер виконують однакові операції гешування.

3.6.3 Застосування у алгоритмі TiGER

TiGER.KEM побудовано із застосуванням варіанту перетворення FO_m^{\perp} до TiGER.PKE:

- **TiGER.PKE:** Базується на RLWR (для відкритого ключа) та RLWE (для шифрування), забезпечує IND-CPA безпеку;
- **Геш-функції:** Використовуються $G = H = \text{SHAKE256}$ (функція з розширенним виходом) для генерації випадковості та спільних ключів;
- **Додаткове гешування:** Відкритий ключ pk гешується разом з повідомленням: $r \leftarrow G(m, H(\text{pk}))$, що забезпечує захист від multi-target атак;
- **Неявне відхилення:** При невдалій декапсуляції повертається $\bar{K} = H(z, c)$, що захищає від витоку інформації про помилки та розкритті хоч і мізерної, та інформації, про ключ.

Розділ 4

Повний опис алгоритму TiGER

4.1 Загальна структура алгоритму

TiGER має модульну архітектуру, що складається з двох рівнів: базової схеми шифрування з відкритим ключем (TiGER.PKE) та механізму інкапсуляції ключа (TiGER.KEM), отриманого застосуванням перетворення Fujisaki-Okamoto до PKE схеми.

4.1.1 Модульна побудова алгоритму

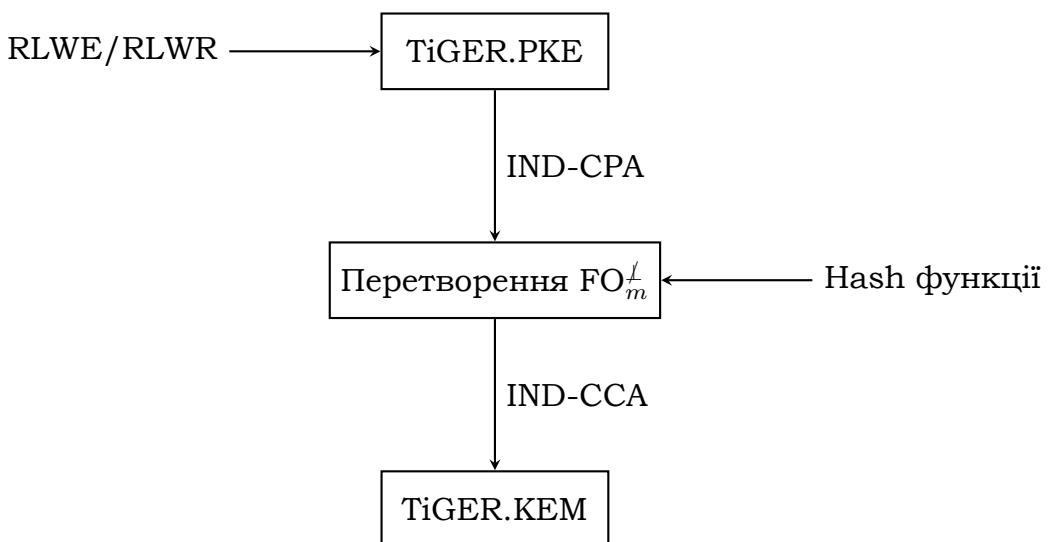


Рис. 4.1: Модульна структура TiGER

Конструкція TiGER базується на трьох наступних принципах:

- Перший крок – TiGER.PKE:** Схема шифрування з відкритим ключем, що використовує комбінацію RLWR для генерації відкритого ключа та RLWE для шифрування повідомень. На припущення складності RLWE та RLWR задача маємо IND-CPA безпеку.
- Перетворення FO_m^f :** Варіант перетворення Fujisaki-Okamoto з неявним відхиленням, що перетворює IND-CPA безпечну PKE схему в IND-CCA безпечну KEM схему використовує геш-функції SHAKE256 та SHA3-256 як випадкові оракули $H : \mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}$.

3. **Вихід – TiGER.KEM:** Повний механізм інкапсуляції ключа з IND-CCA безпекою у моделі квантового випадкового оракула (QROM), придатний для практичного використання у постквантових протоколах.

4.1.2 Взаємодія між компонентами TiGER

Взаємодія між компонентами відбувається наступним чином:

Генерація ключів:

- TiGER.PKE генерує пару (pk, sk') використовуючи RLWR;
- TiGER.KEM додає випадковий ключ z до секретного ключа: $\text{sk} = (\text{sk}', z)$;
- Відкритий ключ pk гешується для захисту від multi-target атак.

Інкапсуляція:

- Генерується випадкове повідомлення m ;
- геш-функція G обчислює детерміновану випадковість r з m та гешу pk ;
- TiGER.PKE шифрує m з випадковістю r і видає шифротекст c ;
- Спільний ключ K обчислюється як $H(m, c)$.

Декапсуляція:

- TiGER.PKE розшифровує шифротекст c та повертає повідомлення m' ;
- Виконується повторне шифрування (re-encryption) m' для перевірки цілісності;
- Якщо перевірка успішна, повертається $K' = H(m', c)$;
- Якщо перевірка невдала, повертається псевдовипадковий ключ $\bar{K} = H(z, c)$ (невідхилення).

4.2 Публічні параметри

TiGER визначає три набори параметрів, що відповідають трьом рівням безпеки згідно з класифікацією NIST: TiGER128 (рівень 1), TiGER192 (рівень 3) та TiGER256 (рівень 5). Розглянемо детальніше значення кожного параметра та обґрунтування їх вибору.

Параметр	TiGER128	TiGER192	TiGER256
n	512	1024	1024
q	2^{14}	2^{15}	2^{16}
p	2^{10}	2^{11}	2^{11}
k_1 (бітів для \mathbf{b})	10	11	11
k_2 (бітів для \mathbf{c}_1)	4	4	5
h_s	274	284	274
h_r	274	284	274
h_e	274	284	274
d (для XEf)	8	8	9
f (для D2)	2	2	2
$ \mathbf{pk} $ (кількість байт)	804	1568	1568
$ \mathbf{sk} $ (кількість байт)	1876	3680	3680
$ \mathbf{ct} $ (кількість байт)	804	1408	1600
Рівень безпеки NIST	1	3	5
Класична безпека (кількість біт)	143	207	272
Квантова безпека (кількість біт)	128	192	256
DFP	2^{-120}	2^{-136}	2^{-167}

Таблиця 4.1: Параметри TiGER для різних рівнів безпеки

Структурні параметри:

- n — степінь многочлена, що визначає розмірність поліноміального кільця $R = \mathbb{Z}[x]/(x^n + 1)$. Більше n забезпечує вищу безпеку, але і водночас збільшує обчислювальну складність та розміри ключів;
- q — основний модуль, що визначає кільце $R_q = R/qR$. В даному алгоритмі обрано як степінь двійки для оптимізації операцій модульної арифметики.
- p — модуль для RLWR округлення при генерації відкритого ключа. Задовільняє $p < q$ та також є степенем двійки. Відношення q/p визначає рівень "шуму" від округлення.

Параметри для стиснення:

- k_1 — кількість біт для представлення компонент вектора \mathbf{b} у відкритому ключі. Стиснення з $\log_2 q$ до k_1 біт зменшує розмір відкритого ключа;
- k_2 — кількість біт для представлення першої частини шифротексту \mathbf{c}_1 . Агресивніша компресія зменшує розмір шифротексту, але збільшує ймовірність помилки розшифрування(!).

Параметри розподілів помилок:

- h_s — вага Геммінга (Hamming weight) секретного ключа \mathbf{s} . TiGER використовує розрідженні тернарні многочлени з коефіцієнтами $\{-1, 0, 1\}$, де рівно h_s коефіцієнтів є ненульовими;
- h_r — вага Геммінга помилки \mathbf{r} при генерації відкритого ключа (RLWR);
- h_e — вага Геммінга для помилок $\mathbf{e}_1, \mathbf{e}_2$ при шифруванні (RLWE).

Параметри кодів корекції помилок:

- d — параметр коду XEf (extended XOR-based error correction). Визначає кількість біт повідомлення, які кодуються разом. Чим більше d , тим краща корекція помилок, але при цьому збільшуються обчислення;
- f — параметр коду D2 (duplication code). Визначає частоту дублювання бітів повідомлення для додаткового захисту від помилок DFP/R.

Фактичні бітові розміри криптографічних об'єктів обчислюються наступним чином:

Відкритий ключ $\text{pk} = (\rho, \mathbf{b})$:

$$|\text{pk}| = 32 + n \cdot k_1 / 8 \text{ байт},$$

де 32 байти – розмір seed ρ , який використовується для генерації випадкового многочлена $\mathbf{a} \in R_q$. Замість зберігання повного многочлена \mathbf{a} (що займало б $n \log_2 q$ біт) пам'яті, зберігається лише seed, з якого \mathbf{a} відновлюється за потреби. Компонента \mathbf{b} – це результат RLWR обчислення $\mathbf{b} = [\mathbf{a} \cdot \mathbf{s} + \mathbf{r}]_p$, стиснута до k_1 біта на кожен коефіцієнт.

Секретний ключ $\text{sk} = (\text{sk}', z, h, \text{pk})$:

$$|\text{sk}| = |\text{sk}'| + 32 + 32 + |\text{pk}| \text{ байт},$$

де sk' – зжате представлення розрідженої секратного ключа \mathbf{s} , z та h – 32-байтові значення для FO перетворення.

Шифротекст $\text{ct} = (\mathbf{c}_1, \mathbf{c}_2)$:

$$|\text{ct}| = n \cdot k_2 / 8 + n / 8 \text{ байт}.$$

Параметри TiGER були підібрані розробниками з урахуванням наступних критеріїв:

1. **Безпека:** Забезпечують стійкість до відомих атак на RLWE/RLWR, включаючи атаки з використанням решіткових алгоритмів (BKZ, LatticeSieve) на класичних та квантових комп'ютерах. Запас безпеки становить 10-15 біт понад нормово;
2. **Коректність:** Ймовірність помилки розшифрування (DFP/R) не перевищує 2^{-120} для всіх наборів параметрів, що є достатнім для практичного використання;
3. **Ефективність:** Вибір степенів двійки для модулів дозволяє використовувати швидкі побітові операції, а розрідженні секрети прискорюють множення многочленів;
4. **Компактність:** Параметри компресії (k_1, k_2) обрані так, щоб мінімізувати розміри при збереженні прийнятного рівня DFP/R. Коди корекції помилок дозволяють застосовувати агресивнішу компресію без погіршення коректності.

4.3 Допоміжні алгоритми

TiGER використовує набір допоміжних алгоритмів для генерації випадкових величин, розширення seed-значень та корекції помилок.

1. **Алгоритм HWT_h** відповідає за генерацію розрідженої тернарного многочлена з фіксованою вагою Геммінга.

Algorithm 7 HWT_h

- 1: Input: Seed $\sigma \in \{0, 1\}^{256}$, weight $h \leq n$.
- 2: Output: Поліном $\mathbf{s} \in R$ з коефіцієнтами $\{-1, 0, 1\}$ та рівно h ненульовими коефіцієнтами.

Алгоритм використовує SHAKE256 для генерації послідовності випадкових індексів та знаків. Спочатку обираються h різних позицій в діапазоні $[0, n - 1]$, потім дляожної позиції генерується випадковий знак ± 1 . Використовується метод rejection sampling для забезпечення рівномірного розподілу індексів. Виконується за константний час (з точністю до rejection sampling).

2. **Алгоритм** expandA — генерація псевдовипадкового многочлена \mathbf{a} з seed.

Algorithm 8 HWT_h

- 1: Input: Seed $\rho \in \{0, 1\}^{256}$.
- 2: Output: Многочлен $\mathbf{a} \in R_q$ з рівномірно розподіленими коефіцієнтами.

Тут також використовується SHAKE256 як додаткова псевдовипадковості (PRG). Seed ρ розширяється до послідовності байтів, які інтерпретуються як коефіцієнти многочлена в \mathbb{Z}_q . Застосовується rejection sampling для забезпечення рівномірності: якщо згенероване значення $\geq q$, воно відкидається і генерується нове. Многочлен \mathbf{a} використовується у RLWR для обчислення відкритого ключа: \mathbf{b} та у RLWE при шифруванні.

Цей підхід дозволяє зберігати у відкритому ключі лише 32 байти seed замість повного многочлена, що займає $n \log_2 q$ біт — для TiGER256 це $1024 \times 16 = 16384$ біт = 2048 байт). Обидві сторони (відправник і отримувач) можуть незалежно відновити \mathbf{a} з ρ .

3. **Алгоритми корекції помилок** eccENC та eccDEC — кодування та декодування повідомлення для зниження DFP/R.

- Код XEf (XOR-based error correction with extension): Повідомлення розбивається на блоки по d біт. Для кожного блоку обчислюється біт парності як ксор (XOR) усіх біт блоку та додається до закодованого повідомлення. Це дозволяє виявити та виправити одиночні помилки в кожному блоці. При декодуванні для кожного блоку перевіряється цей біт парності. Якщо він не збігається, алгоритм намагається виправити помилку перебором всіх d позицій у блоці.
- Код D2 (Duplication code): Додатковий рівень захисту, що дублює кожен біт повідомлення f разів. При декодуванні використовується мажоритарне голосування (majority voting): якщо більшість копій біта мають значення 1, результат буде 1, інакше – 0.

TiGER застосовує спочатку код XEf, потім код D2, що дає двоетапну систему корекції помилок. Це дозволяє використовувати агресивнішу компресію шифротексту при збереженні низької DFP/R.

4. **Геш-функції** — використовуються для генерації випадковостей та обчислення спільних ключів у перетворенні FO.

- **SHAKE256**: Функція з розширенним виходом (XOF) зі стандарту SHA-3. Використовується першочергово як генератор псевдовипадковості (PRG) у expandA та HWT_h , функція G у перетворенні FO для отримання детермінованої випадковості з повідомлення та для генерації довгих послідовностей псевдовипадкових байтів.
- **SHA3-256**: Криптографічна геш-функція зі стандарту SHA-3. Використовується як функція H у перетворенні Fujisaki-Okamoto для обчислення спільного ключа $K = H(m, c)$, гешуванні відкритого ключа для захисту від multi-target атак та для генерації фінального спільного ключа фіксованого розміру (256 біт).

Обидві ці функції є частиною стандарту FIPS 202 (2015 р) та мають формальний аналіз безпеки. У моделі квантового випадкового оракула (QROM) вони моделюються як ідеальні випадкові функції та доступними супротивнику.

4.4 TiGER.PKE

TiGER.PKE це базова схема шифрування з відкритим ключем, що забезпечує IND-CPA безпеку. Схема використовує комбінацію RLWR для генерації відкритого ключа та RLWE для шифрування повідомень.

4.4.1 KeyGen – генерація ключів

Алгоритм генерації ключів створює пару відкритий&секретний ключ на основі RLWR.

Algorithm 9 TiGER.PKE.KeyGen()

```

1: Input: Параметри  $(n, q, p, h_s, h_r, k_1)$ 
2: Output: Відкритий ключ  $pk$ , секретний ключ  $sk$ 
3:
4: Generate seed  $\rho \xleftarrow{p} \{0, 1\}^{256}$ 
5: Generate seed  $\sigma_s \xleftarrow{p} \{0, 1\}^{256}$ 
6: Generate seed  $\sigma_r \xleftarrow{p} \{0, 1\}^{256}$ 
7:
8: a  $\leftarrow \text{expandA}(\rho)$                                 ▷ Expand seed в многочлен
9: s  $\leftarrow \text{HWT}_{h_s}(\sigma_s)$                       ▷ Sparse секретний ключ
10: r  $\leftarrow \text{HWT}_{h_r}(\sigma_r)$                       ▷ Sparse error
11:
12: b'  $\leftarrow \mathbf{a} \cdot \mathbf{s} + \mathbf{r} \in R_q$           ▷ RLWR обчислення
13: b'  $\leftarrow \lfloor \mathbf{b}' \cdot (p/q) \rfloor \in R_p$     ▷ Округлення за mod p
14: b  $\leftarrow \text{Compress}(\mathbf{b}', k_1)$                   ▷ Компресія до  $k_1$  біт
15:
16:  $pk \leftarrow (\rho, \mathbf{b})$                            ▷ Save secret seed(!)
17:  $sk \leftarrow \sigma_s$ 
18: return  $(pk, sk)$ 
```

Кроки алгоритму (якщо словами):

1. **Генерація seeds:** Спершу створюються три незалежні 256-бітні seeds:

- ρ — для генерації публічного многочлена \mathbf{a} ;
 - σ_s — для генерації секретного ключа \mathbf{s} ;
 - σ_r — для генерації помилки \mathbf{r} .
2. **Expand a:** Використовується алгоритм `expandA` для детермінованої генерації рівномірно випадкового многочлена $\mathbf{a} \in R_q$ з seed ρ .
3. **Генерація розріджених многочленів:**
- Секретний ключ \mathbf{s} генерується як тернарний многочлен з вагою Геммінга h_s ;
 - Помилка \mathbf{r} аналогічно генерується з вагою h_r .
4. **RLWR:** Обчислюється $\mathbf{b}' = \mathbf{a} \cdot \mathbf{s} + \mathbf{r} \in R_q$, після чого виконується округлення до найближчого цілого модуля p : $\lfloor \mathbf{b}' \cdot (p/q) \rfloor$. Операція округлення вводить детермінований "шум", що замінює явну помилку в класичному RLWE.
5. **Компресія:** Многочлен \mathbf{b}' стискається з $\log_2 p$ біт до k_1 біт на коефіцієнт для зменшення розміру відкритого ключа.
6. **Формування ключів:** Відкритий ключ містить seed ρ та стиснений \mathbf{b}' , а секретний ключ зберігається у вигляді seed σ_s , з якого можна відновити \mathbf{s} за потреби.

4.4.2 Encryption – шифрування

Алгоритм шифрування перетворює повідомлення в шифротекст використовуючи RLWE.

Algorithm 10 TiGER.PKE.Enc($pk, m; r$)

- 1: **Input:** Відкритий ключ $pk = (\rho, \mathbf{b})$, повідомлення $m \in \{0, 1\}^{256}$, випадковість r
- 2: **Output:** Шифротекст $ct = (\mathbf{c}_1, \mathbf{c}_2)$
- 3:
- 4: Parse seeds from r : $(\sigma_{e_1}, \sigma_{e_2}) \leftarrow r$
- 5:
- 6: $\mathbf{a} \leftarrow \text{expandA}(\rho)$ ▷ Відновлення \mathbf{a} з seed
- 7: $\mathbf{b}' \leftarrow \text{Decompress}(\mathbf{b}, k_1)$ ▷ Декомпресія відкритого ключа
- 8:
- 9: $\mathbf{e}_1 \leftarrow \text{HWT}_{h_e}(\sigma_{e_1})$ ▷ Генерація "помилок"
- 10: $\mathbf{e}_2 \leftarrow \text{HWT}_{h_e}(\sigma_{e_2})$
- 11:
- 12: $m' \leftarrow \text{eccENC}(m)$ ▷ Кодування з корекцією помилок
- 13: $\mathbf{m} \leftarrow \text{Encode}(m')$ ▷ Перетворення біт в многочлен
- 14:
- 15: $\mathbf{c}'_1 \leftarrow \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{e}_2 \in R_q$ ▷ RLWE компонента
- 16: $\mathbf{c}_1 \leftarrow \text{Compress}(\mathbf{c}'_1, k_2)$ ▷ Агресивна компресія
- 17:
- 18: $\mathbf{c}'_2 \leftarrow \mathbf{b}' \cdot \mathbf{e}_1 + \mathbf{m} \cdot \lfloor q/2 \rfloor \in R_q$ ▷ Повідомлення + шум
- 19: $\mathbf{c}_2 \leftarrow \text{Compress}(\mathbf{c}'_2, 1)$ ▷ Компресія до 1 біт
- 20:
- 21: **return** $ct = (\mathbf{c}_1, \mathbf{c}_2)$

Кроки алгоритму:

1. **Парсинг випадковості:** З детермінованої випадковості r (згенерованої через геш-функцію G у FO) отримуємо seeds для генерації помилок $\mathbf{e}_1, \mathbf{e}_2$.
2. **Відновлення відкритого ключа:**
 - Многочлен \mathbf{a} відновлюється з ρ seed;
 - Компресований \mathbf{b} декомпресується до $\mathbf{b}' \in R_p$.
3. **Генерація "помилок":** Створюються два розріджених тернарних многочлена $\mathbf{e}_1, \mathbf{e}_2$ з вагою Геммінга h_e кожен.
4. **Підготовка повідомлення:**
 - Повідомлення m кодується через eccENC (коди XEf та D2) для захисту від помилок;
 - Закодоване повідомлення перетворюється в многочлен $\mathbf{m} \in R$ з коефіцієнтами з $\{0, 1\}$;
 - Множиться на $\lfloor q/2 \rfloor$ для розміщення в "середині" модуля q .
5. **RLWE шифрування:**
 - $\mathbf{c}'_1 = \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{e}_2$ — "маскування" помилки \mathbf{e}_1 ;
 - $\mathbf{c}'_2 = \mathbf{b}' \cdot \mathbf{e}_1 + \mathbf{m} \cdot \lfloor q/2 \rfloor$ — зашифроване повідомлення.
6. **Компресія шифротексту:**
 - \mathbf{c}_1 стискається до k_2 біт на коефіцієнт (агресивна компресія);
 - \mathbf{c}_2 стискається до 1 біт на коефіцієнт (зберігається лише знак).

4.4.3 Decryption – розшифрування

Алгоритм розшифрування відновлює повідомлення з шифротексту використовуючи секретний ключ.

Algorithm 11 TiGER.PKE.Dec(sk, ct)

```

1: Input: Секретний ключ  $sk = \sigma_s$ , шифротекст  $ct = (\mathbf{c}_1, \mathbf{c}_2)$ 
2: Output: Повідомлення  $m \in \{0, 1\}^{256}$  або  $\perp$ 
3:
4:  $\mathbf{s} \leftarrow \text{HWT}_{h_s}(\sigma_s)$   $\triangleright$  Відновлення sk з seed
5:
6:  $\mathbf{c}'_1 \leftarrow \text{Decompress}(\mathbf{c}_1, k_2)$   $\triangleright$  Декомпресія шифротексту
7:  $\mathbf{c}'_2 \leftarrow \text{Decompress}(\mathbf{c}_2, 1)$ 
8:
9:  $\mathbf{v} \leftarrow \mathbf{c}'_2 - \mathbf{c}'_1 \cdot \mathbf{s} \in R_q$   $\triangleright$  Видалення маски
10:
11:  $\mathbf{m}' \leftarrow \text{Round}(\mathbf{v})$   $\triangleright$  Округлення до  $\{0, 1\}$ 
12:  $m' \leftarrow \text{Decode}(\mathbf{m}')$   $\triangleright$  Розбиття многочлена на біти
13:
14:  $m \leftarrow \text{eccDEC}(m')$   $\triangleright$  Декодування з корекцією помилок
15:
16: if  $m = \perp$  then
17:   return  $\perp$   $\triangleright$  Помилка розшифрування
18: else
19:   return  $m$ 
20: end if

```

Покроково маємо:

- Відновлення секретного ключа:** З seed σ_s відновлюється розріджений многочлен \mathbf{s} .
- Декомпресія шифротексту:** Обидві компоненти $\mathbf{c}_1, \mathbf{c}_2$ декомпресуються до повного розміру в R_q .
- Видалення маски:** Обчислюється $\mathbf{v} = \mathbf{c}'_2 - \mathbf{c}'_1 \cdot \mathbf{s}$, що має бути близьким до $\mathbf{m} \cdot \lfloor q/2 \rfloor$ (за наявності малої помилки).
- Округлення:** Функція Round округлює кожен коефіцієнт \mathbf{v} до найближчого з чисел: 0 або $\lfloor q/2 \rfloor$, потім нормалізує до $\{0, 1\}$:

$$\text{Round}(v_i) = \begin{cases} 0, & \text{якщо } |v_i| < q/4 \\ 1, & \text{якщо } |v_i - \lfloor q/2 \rfloor| < q/4 \\ \text{error}, & \text{інакше} \end{cases}$$

- Декодування:** Многочлен \mathbf{m}' перетворюється в послідовність біт m' , після чого застосовується eccDEC для виправлення помилок та отримання повідомлення m .
- Перевірка коректності:** Якщо eccDEC виявляє unexpect error, повертається \perp .

Джерела помилок розшифрування можуть виникнути завдяки:

- Помилка \mathbf{r} від RLWR при генерації \mathbf{b} ;
- Помилки $\mathbf{e}_1, \mathbf{e}_2$ від RLWE при шифруванні;

- Помилки від компресії/декомпресії $\mathbf{b}, \mathbf{c}_1, \mathbf{c}_2$ відповідно;

Параметри TiGER підібрані так, щоб сумарна помилка залишалась в межах $\pm q/4$ з високою ймовірністю, забезпечуючи коректне розшифрування. Коди корекції помилок XEf та D2 додатково підвищують надійність.

4.5 TiGER.KEM

TiGER.KEM – механізм інкапсуляції ключа, отриманий застосуванням перетворення Fujisaki-Okamoto з неявним відхиленням до TiGER.PKE. Забезпечує IND-CCA безпеку у моделі квантового випадкового оракула.

4.5.1 KeyGen – генерація ключів

Алгоритм генерації ключів розширює TiGER.PKE.KeyGen додатковою компонентою – FO перетворенням.

Algorithm 12 TiGER.KEM.KeyGen()

```

1: Input: Параметри  $(n, q, p, h_s, h_r, k_1)$ 
2: Output: Відкритий ключ  $pk$ , секретний ключ  $sk$ 
3:
4:  $(pk', sk') \leftarrow \text{TiGER.PKE.KeyGen}()$                                 ▷ Базова генерація ключів
5:
6:  $z \xleftarrow{p} \{0, 1\}^{256}$                                               ▷ Випадковий ключ для implicit rejection
7:  $h \leftarrow \text{SHA3-256}(pk')$                                          ▷ Геш відкритого ключа
8:
9:  $pk \leftarrow pk'$ 
10:  $sk \leftarrow (sk', z, h, pk')$                                          ▷ Розширений секретний ключ
11:
12: return  $(pk, sk)$ 
```

Компоненти секретного ключа:

- sk' — секретний ключ TiGER.PKE (правду кажучи це seed σ_s);
- z — випадковий 256-бітний ключ для обчислення псевдовипадкового спільногоключа при невдалій декапсуляції (неявне відхилення);
- h — геш відкритого ключа, використовується геш-функцією G для генерації випадковості шифрування;
- pk' — копія відкритого ключа (для можливості повторного шифрування при декапсуляції).

4.5.2 Encapsulation – інкапсуляція

Алгоритм інкапсуляції генерує спільний ключ та його зашифровану форму.

Algorithm 13 TiGER.KEM.Encaps(pk)

```
1: Input: Відкритий ключ  $pk$ 
2: Output: Шифротекст  $ct$  та спільний ключ  $K \in \{0, 1\}^{256}$ 
3:
4:  $m \xleftarrow{p} \{0, 1\}^{256}$  ▷ Вибираємо випадкове повідомлення
5:
6:  $h \leftarrow \text{SHA3-256}(pk)$  ▷ Гешування відкритого ключа
7:  $r \leftarrow \text{SHAKE256}(m \| h)$  ▷ Детермінована випадковість
8:
9:  $ct \leftarrow \text{TiGER.PKE.Enc}(pk, m; r)$  ▷ Шифрування повідомлення
10:
11:  $K \leftarrow \text{SHA3-256}(m \| ct)$  ▷ Спільний ключ обчислюється через геш
12:
13: return  $(ct, K)$ 
```

Ключові аспекти:

1. **Випадкове повідомлення:** Генерується рівномірно (розподілене) випадкове $m \in \{0, 1\}^{256}$, яке буде зашифроване.
2. **Детермінована випадковість:** Замість використання нової випадковості для шифрування, r обчислюється детермінована як $r = \text{SHAKE256}(m \| h)$. Це критично для можливості повторного шифрування при декапсуляції.
3. **Гешування відкритого ключа:** Включення $h = \text{SHA3-256}(pk)$ в обчислення r забезпечує взаємозв'язок шифротексту до конкретного відкритого ключа, що захищає від multi-target атак.
4. **Спільний ключ:** Обчислюється як $K = \text{SHA3-256}(m \| ct)$, як можна бачити є залежність як від повідомлення так і від шифротексту. Це є важливим для безпеки алгоритму загалом: противник не може обчислити K без знання m , навіть якщо перехопив шифротекст ct .

4.5.3 Decapsulation – декапсуляція

Декапсуляція застосовується для відновлення спільногого ключа з шифротексту, виконуючи перевірку цілісності через повторне шифрування.

Algorithm 14 TiGER.KEM.Decaps(sk, ct)

```

1: Input: Секретний ключ  $sk = (sk', z, h, pk)$ , шифротекст  $ct$ 
2: Output: Спільний ключ  $K \in \{0, 1\}^{256}$ 
3:
4:  $m' \leftarrow \text{TiGER.PKE.Dec}(sk', ct)$  ▷ Розшифрування
5:
6: if  $m' = \perp$  then
7:   return  $\bar{K} \leftarrow \text{SHA3-256}(z \| ct)$  ▷ Implicit rejection
8: end if
9:
10:  $r' \leftarrow \text{SHAKE256}(m' \| h)$  ▷ Створення "випадковості"
11:  $ct' \leftarrow \text{TiGER.PKE.Enc}(pk, m'; r')$  ▷ Повторне шифрування
12:
13: if  $ct' = ct$  then
14:   return  $K \leftarrow \text{SHA3-256}(m' \| ct)$  ▷ Успішна декапсуляція
15: else
16:   return  $\bar{K} \leftarrow \text{SHA3-256}(z \| ct)$  ▷ Implicit rejection
17: end if

```

- Розшифрування:** Спершу – звичайне розшифрування через TiGER.PKE.Dec. Якщо розшифрування видало помилку ($m' = \perp$), одразу повертається псевдовипадковий ключ.
- Re-encryption:** Розшифроване повідомлення m' повторно шифрується з тією ж визначеню випадковістю $r' = \text{SHAKE256}(m' \| h)$ (є критичном кроком для забезпечення IND-CCA безпеки).
- Перевірка цілісності:** Отриманий ct' порівнюється з оригінальним ct :
 - Якщо $ct' = ct$, це означає, що шифротекст не був модифікований противником, і тоді повертається справжній спільний ключ $K = \text{SHA3-256}(m' \| ct)$;
 - Якщо $ct' \neq ct$, це сигналізує про атаку або помилку, і повертається псевдовипадковий ключ, щоб заплути словмисника.
- Неявне відхилення (implicit rejection):** Замість явного повернення помилки \perp , алгоритм повертає псевдовипадковий ключ $\bar{K} = \text{SHA3-256}(z \| ct)$. Це має дві такі переваги:
 - Захист від side-channel атак:** Зовнішньому спостерігачу важко визначити, чи відбулась успішна декапсуляція чи ні, оскільки в обох випадках повертається деякий 256-бітний ключ;
 - Константний час:** Що при успішному output, що пои failed виконується однакова кількість геш-операцій.
- Роль секретного ключа z :** Випадковий ключ z є унікальним для кожної пари ключів та невідомим противнику. Це гарантує, що \bar{K} буде непередбачуваним для противника навіть за наявності багатьох невдалих декапсуляцій.

Ключові моменти безпеки або ж чому це безпечно

Перетворення FO_m^L з повторним шифруванням перетворює будь-яку IND-CPA безпечну PKE схему в IND-CCA безпечну KEM.

- **Детермінована випадковість:** Використання $r = \text{SHAKE256}(m\|h)$ замість нової випадковості робить шифрування детермінованим для даного m та rk , що дозволяє виконати перевірку через повторне шифрування;
- **Гешування спільного ключа:** $K = \text{SHA3-256}(m\|ct)$ робить спільний ключ неперебачуваним без знання m , навіть якщо ct скомпроментовано супротивником;
- **Захист від атак вибраного шифротексту:** Противник може подавати довільні модифіковані шифротексти ct^* до оракула декапсуляції, але:
 - Якщо ct^* не є валідним шифруванням деякого m^* , перевірка умови $ct' \neq ct^*$ виявить це;
 - Противник отримає лише $\bar{K} = \text{SHA3-256}(z\|ct^*)$, що не надає жодної інформації про справжній спільний ключ через випадковість z та властивості геш-функції.

4.6 Аналіз коректності

Коректність вимагає від TiGER, того щоб розшифрування майже завжди повертало правильне повідомлення. У цій секції проаналізуємо джерела помилок та обчислимо ймовірність помилки розшифрування.

Математичний аналіз помилок

При розшифруванні повідомлення обчислюється величина:

$$\mathbf{v} = \mathbf{c}'_2 - \mathbf{c}'_1 \cdot \mathbf{s} = \mathbf{m} \cdot \lfloor q/2 \rfloor + \mathbf{err},$$

де \mathbf{err} – сумарна помилка з декількох джерел.

Джерела помилок є наступними:

1. **Помилка від RLWR:** При генерації відкритого ключа:

$$\mathbf{b} = \lfloor (\mathbf{a} \cdot \mathbf{s} + \mathbf{r}) \cdot (p/q) \rfloor,$$

що вносить помилку округлення $\mathbf{err}_{\text{RLWR}}$, де $\mathbf{err}_{\text{RLWR}} \approx \mathbf{r} \cdot (p/q)$.

2. **Помилка від RLWE:** При шифруванні:

$$\mathbf{c}'_1 = \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{e}_2, \quad \mathbf{c}'_2 = \mathbf{b}' \cdot \mathbf{e}_1 + \mathbf{m} \cdot \lfloor q/2 \rfloor,$$

що вносить помилку $\mathbf{err}_{\text{RLWE}} = -\mathbf{e}_2 \cdot \mathbf{s} + \mathbf{err}_{\text{RLWR}} \cdot \mathbf{e}_1$.

3. **Помилка від компресії відкритого ключа:** Компресія \mathbf{b} ($\log_2 p \rightarrow k_1$) біт вносить наступну помилку округлення:

$$\mathbf{err}_{\text{comp}, \mathbf{b}} \approx \mathbf{U}([-p/2^{k_1+1}, p/2^{k_1+1}]).$$

4. **Помилка від компресії шифротексту:** Компресія \mathbf{c}_1 до k_2 біт та \mathbf{c}_2 до 1 біт:

$$\mathbf{err}_{\text{comp}, \mathbf{c}_1} \approx \mathbf{U}([-q/2^{k_2+1}, q/2^{k_2+1}]), \quad \mathbf{err}_{\text{comp}, \mathbf{c}_2} \approx \mathbf{U}([-q/4, q/4]).$$

Сумарна помилка складатиме: помилку в кожному коефіцієнті многочлена \mathbf{v} :

$$\begin{aligned} \mathbf{err} &= \mathbf{err}_{\text{comp}, \mathbf{c}_2} + \mathbf{err}_{\text{comp}, \mathbf{c}_1} \cdot \mathbf{s} \\ &\quad + (\mathbf{err}_{\text{comp}, \mathbf{b}} \cdot \mathbf{e}_1 - \mathbf{e}_2 \cdot \mathbf{s} + \mathbf{r} \cdot \mathbf{e}_1 \cdot (p/q)). \end{aligned}$$

Помилка розшифрування виникає, коли $|\mathbf{err}_i| \geq q/4$ для якогось коефіцієнта i , і це призводить до неправильного округлення.

Оцінка ймовірності помилки

Для оцінки DFP/R необхідно обчислити ймовірність того, що хоча б один коефіцієнт має помилку $\geq q/4$.

Статистичний аналіз:

- Розподіл помилок:** Кожна компонента помилки має рівномірний розподіл в заданих межах.
- Дисперсія:** Для розрідженої тернарного многочлена \mathbf{s} з вагою h_s :

$$\text{Var}(\mathbf{s}) \approx h_s, \quad \text{Var}(\mathbf{s} \cdot \mathbf{e}) \approx h_s \cdot h_e / 3,$$

де ділення враховує коефіцієнти $\{-1, 0, 1\}$.

- Максимальна помилка складає:**

$$\sigma_{\text{err}}^2 \approx h_s \cdot h_e / 3 + h_r \cdot h_e \cdot (p/q)^2 + (q/2^{k_2+1})^2 + (q/2)^2 + \dots$$

- DFP/R для одного коефіцієнта:** Ймовірність помилки в одному з коефіцієнтів:

$$P(\text{помилка в } i\text{-му коефіцієнти}) \approx 2 \cdot Q(q/4/\sigma_{\text{err}}),$$

де $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ – функція розподілу помилок для нормального розподілу.

- Тоді DFP/R для всього повідомлення:**

$$\text{DFP/R} \leq n \cdot P(\text{помилка в одному коефіцієнти}) = n \cdot 2 \cdot Q(q/4/\sigma_{\text{err}}).$$

Різні параметри мають різний вплив на DFP/R:

- Модулі q та p :**

- Більше q збільшує інтервал ($q/4$ стає більшим), зменшуючи DFP/R;
- Менше відношення q/p зменшує помилку від RLWR, але при цьому збільшує розмір відкритого ключа.

- Ваги Геммінга h_s, h_r, h_e :**

- Більші ваги збільшують дисперсію помилки, підвищуючи DFP/R;
- Менші ваги зменшують безпеку (легше атакувати розрідженні ключі);

- Параметри компресії k_1, k_2 :**

- Менші k_1, k_2 краще зменшують розміри ключів/шифротексту, збільшуючи помилку компресії;

- Коди корекції помилок (XEf, D2):**

- Коди XEf можуть виправити одиночні помилки в блоках по d біт, знижуючи доволі DFP/R доволі добре (у d разів) для таких помилок;
- Код D2 з $f = 2$ дублює кожен біт, дозволяючи виправляти помилки через мажоритарне голосування.

Експериментальні результати

Автори TiGER провели обчислювальні експерименти для верифікації теоретичних оцінок DFP/R і отримали:

- **TiGER128:** $\text{DFP}/\text{R} \approx 2^{-120}$ (теоретична), $< 2^{-128}$ (експериментальна після 2^{40} тестів);
- **TiGER192:** $\text{DFP}/\text{R} \approx 2^{-136}$ (теоретична), не виявлено помилок після 2^{45} тестів;
- **TiGER256:** $\text{DFP}/\text{R} \approx 2^{-167}$ (теоретична), не виявлено помилок після 2^{48} тестів.

Експерименти підтверджують, що практична DFP/R не перевищує теоретичних оцінок і є достатньо малою для будь-яких реалістичних сценаріїв використання.

4.7 Особливості реалізації

TiGER розробляється з ухилом на ефективність та безпеку.

Конструкція TiGER має наступні риси, що забезпечують компактність, ефективність та безпеку реалізації.

Компактність досягається через використання RLWR та агресивної компресії, що дозволяє отримати малі розміри відкритого ключа та шифротексту порівняно з аналогами. Наприклад, TiGER128 має відкритий ключ розміром лише 804 байти та шифротекст 804 байти, що менше ніж у Kyber512 ($800 + 768$ байт) та Saber ($672 + 736$ байт). Економія місця особливо важлива для протоколів з обмеженою пропускною здатністю, таких як TLS, де кожен байт має значення. Також зберігання seed замість повних многочленів (як у a) економить до 2 КБ для TiGER256.

Висока обчислювальна ефективність забезпечується через використання модулів які є степенями двійки ($q = 2^k$), що дозволяє виконувати операції модульної арифметики через прості побітові зсуви:

- Округлення $\lfloor x \cdot (p/q) \rfloor$ виконується як побітовий зсув вправо: оскільки $q = 2^{14}$ та $p = 2^{10}$ для TiGER128, ділення на $q/p = 2^4$ еквівалентне зсуву на 4 біти;
- Операції за $\text{mod } q$ виконуються через побітовий AND з числом $q - 1$. Це значно швидше ніж модульні операції, що використовуються в деяких інших схемах.
- Розрідженні секрети ($h_s \ll n$) прискорюють множення многочленів: замість $O(n^2)$ операцій для множення, потрібно лише $O(h_s \cdot n)$ операцій, що дає прискорення приблизно в $n/h_s \approx 2$ рази.

Простота в реалізації є важливою перевагою TiGER. Відмова від використання Number Theoretic Transform (NTT) спрощує імплементацію, оскільки NTT вимагає специфічних модулів виду $q = 1 \bmod 2n$ та bit-reversal permutation (якийсь жах, я таки не вдуплів що це). TiGER використовує множення многочленів, яке, хоч і має вищу асимптотичну складність $O(n^2)$ порівняно з $O(n \log n)$ для NTT, але є простішим для людського сприйняття та реалізації. Для розріджених многочленів складність знижується до $O(h \cdot n)$, що робить це множення конкурентоспроможним. При реалізації важливо уникати умовних переходів та операцій індексації масивів, які залежать від секретних значень, оскільки це може привести до витоку інформації через timing або cache атаки.

Захист від атак забезпечується кількома механізмами:

- Неявне відхилення (*implicit rejection*) у TiGER.KEM захищає від витоку інформації через помилки розшифрування. Це протидіє failure boosting attacks, де противник ітеративним підходом підбирає шифротексти з високою ймовірністю помилки для витягування інформації про секретний ключ. (адаптивна атака на основі вибраного шифротекста)
- Гешування відкритого ключа ($r = G(m, H(pk))$) забезпечує стійкість до multi-target атак, прив'язуючи кожен шифротекст до конкретного відкритого ключа.
- Детермінована випадковість шифрування через G дозволяє виконати перевірку цілісності через повторне шифрування, що є основою IND-CCA безпеки.

Коди корекції помилок є ключовою інновацією вTiGER. Застосування кодів ХЕf та D2 значно знижує ймовірність помилки розшифрування без збільшення розміру шифротексту. Код ХЕf може виправити одиночні помилки в блоках по d біт та відповідно підвищує стійкість у стільки ж разів. Без кодів корекції довелося або використовувати менш агресивне стиснення (більший шифротекст), або змиритися з вищим DFP/R, що неприйнятно для практичних застосувань.

Константний час виконання є критичним для захисту від атак через побічні канали (side-channel attacks). Генерація розріджених многочленів через HWT_h використовує rejection sampling, при цьому загальна кількість ітерацій обмежена та не залежить від секретних даних. Операції з многочленами виконуються за фіксований час незалежно від значень коефіцієнтів. Плюс неявне відхилення гарантує, що (не)успішна декапсуляція виконуються з використанням однакової кількості геш-операцій.

Практичні переваги Модульна структура (PKE + FO) дозволяє окремо тестувати та оптимізувати різні компоненти. Відсутність складних математичних операцій (як pairing у криптографії на еліптичних кривих) робить TiGER перспективним для впровадження на пристроях з обмеженим ресурсом (embedded systems, IoT).

Розділ 5

Результати досліджень

Розділ 6

Аналіз атак на TiGER

Розділ 7

Порівняльний аналіз

Розділ 8

Перенесення атак та можливі покращення

Розділ 5: Результати досліджень

Параметри безпеки (TiGER128, TiGER192, TiGER256) Оцінка безпеки (core-SVP hardness) Ймовірність помилки розшифрування (DFP/R) Розміри ключів та шифротексту Порівняння з Kyber, Saber, NewHope

Розділ 7: Порівняльний аналіз

Порівняння з Kyber (MLWE) Порівняння з Saber (MLWR) Порівняння з RLizard (RLWE/RLWR предок) Порівняння з SMAUG (партнер по злиттю) Таблиці характеристик (безпека, розміри, швидкість)

Розділ 6: Аналіз атак на TiGER

Meet-LWE атака (Alexander May) CCA атаки на PKE (з роботи von Berg)

Атака з доступом до проміжного виводу декодування Атака з урахуванням XEf корекції помилок

Атаки на side-channel Можливі вразливості через DFP/R

Розділ 8: Перенесення атак та можливі покращення

Застосовність атак з інших RLWE/RLWR схем до TiGER Аналіз слабких місць (sparse secrets, error correction, rounding) Можливі напрямки покращення:

Оптимізація параметрів для зменшення DFP/R Альтернативні коди корекції помилок Покращення HWT sampling Контрзаходи проти side-channel атак

Порівняльна таблиця покращень

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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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.

- [13] Miklós Ajtai. «The shortest vector problem in L_2 is NP-hard for randomized reductions». In: *Proceedings of the thirtieth annual ACM symposium on Theory of computing*. 1998, pp. 10–19. DOI: [10.1145/276698.276705](https://doi.org/10.1145/276698.276705).
- [14] Joppe Bos et al. «CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM». In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2018, pp. 353–367. DOI: [10.1109/EuroSP.2018.00032](https://doi.org/10.1109/EuroSP.2018.00032).
- [15] Jan-Pieter D’Anvers et al. «Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM». In: *Progress in Cryptology – AFRICACRYPT 2018*. 2018, pp. 282–305. DOI: [10.1007/978-3-319-89339-6_16](https://doi.org/10.1007/978-3-319-89339-6_16).
- [16] Siemen Dhooghe and Svetla Nikova. «My Gadget Just Cares For Me - How NINA Can Prove Security Against Combined Attacks». In: *Progress in Cryptology – INDOCRYPT 2018*. 2018, pp. 35–55. DOI: [10.1007/978-3-030-05378-9_3](https://doi.org/10.1007/978-3-030-05378-9_3).
- [17] Jan-Pieter D’Anvers, Siemen Dhooghe, and Frederik Vercauteren. «On the Impact of Decryption Failures on the Security of NTRU Encryption». In: *Advances in Cryptology – ASIACRYPT 2019*. 2019, pp. 565–598. DOI: [10.1007/978-3-030-34621-8_20](https://doi.org/10.1007/978-3-030-34621-8_20).
- [18] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. «A Modular Analysis of the Fujisaki-Okamoto Transformation». In: *Theory of Cryptography – TCC 2017*. 2017, pp. 341–371. DOI: [10.1007/978-3-319-70500-2_12](https://doi.org/10.1007/978-3-319-70500-2_12).
- [19] Kathrin Hövelmanns et al. «Generic Authenticated Key Exchange in the Quantum Random Oracle Model». In: *Public-Key Cryptography – PKC 2020*. 2020, pp. 389–422. DOI: [10.1007/978-3-030-45388-6_14](https://doi.org/10.1007/978-3-030-45388-6_14).