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

ДОДАТКОВЕ ЗАВДАННЯ

Виконала студентка
групи ФІ-52мн
Балацька Вікторія

Київ — 2025

1 AIGIS

Aigis — це схема на основі Module-LWE, розроблена Zhang et al. Вона містить KEM Aigis-enc і схему підпису Aigis-sig [4].

Aigis-Enc — це алгоритм шифрування, заснований на асиметричній LWE. Він використовує структуру MLWE (Module-LWE) і спеціальні матриці, згенеровані з 9 ротаційних підматриць 256×256. Модуль $q = 7681$. Процес стиснення використовується як під час генерації ключа, так і під час шифрування, що еквівалентно додаванню LWR-шуму (Learning With Rounding). У рекомендованій конфігурації Aigis-Enc використовуються параметри вибірки $\{\eta_1, \eta_2\} = \{1, 4\}$. Симетрична LWE-схема для порівняння використовує $\{\eta_1, \eta_2\} = \{2, 2\}$.

У статі [3], [1]проводиться порівняльний аналіз криптографічного алгоритму Aigis-Enc та симетричної LWE (Learning With Errors) схеми шифрування в тому ж масштабі, використовуючи рекомендовані параметри. Аналіз зосереджений на трьох ключових показниках: безпека CPA (стійкість до атак з вибраним відкритим текстом), обчислювальна складність та ймовірність помилки розшифрування.

Також, судячи з того що багато сайтів та статей посилаються на [5], то там також є інформація про Aigis (але я не можу його відкрити).

2 LAC.PKE

Пейпер [2] вводить та детально аналізує схему шифрування LAC – практичну постквантову схему відкритого ключа на основі Ring-LWE, у якій модуль – байтового розміру, а шум – "бітового"рівня.

Схема LAC є схемою шифрування з відкритим ключем, побудованою на задачі Ring-LWE.

Параметри.

– Нехай n — ступінь полінома (як правило, $n \in \{512, 1024\}$).

– q — невеликий модуль байтового розміру (наприклад, $q = 251$ або $q = 256$).

– Кільце:

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

– χ_s, χ_e — розподіли для секрету та шуму (розподіли з малими коефіцієнтами).

– ECC — код з виправленням помилок (комбінація D_2-коду та BCH-коду) для кодування/декодування бітових повідомлень.

Генерація ключів KeyGen.

1) Випадково обираємо $a \leftarrow R_q$.

2) Вибираємо секретний вектор (поліном) $s \leftarrow \chi_s^n$ та шум $e \leftarrow \chi_e^n$.

3) Обчислюємо

$$b = a \cdot s + e \bmod q.$$

4) Публічний ключ: $\mathsf{pk} = (a, b)$, секретний ключ: $\mathsf{sk} = s$.

Шифрування $\mathsf{Enc}(\mathsf{pk}, m)$.

1) Бітове повідомлення m кодується помилкостійким кодом:

$$\mu = \mathsf{ECC\_Enc}(m).$$

2) Випадково обираємо $r \leftarrow \chi_s^n$, $e_1, e_2 \leftarrow \chi_e^n$.

3) Обчислюємо

$$c_1 = a \cdot r + e_1 \bmod q,$$

$$c_2 = b \cdot r + e_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mu \bmod q.$$

4) Шифротекст:

$$\mathsf{ct} = (c_1, c_2).$$

Розшифрування $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$.

1) Обчислюємо

$$u = c_1 \cdot s \bmod q.$$

2) Віднімаємо вклад секрету зі c_2:

$$v = c_2 - u \bmod q.$$

3) З вектора v отримуємо "зашумлене"кодове слово $\tilde{\mu}$, відновлюючи біти за пороговим правилом (коефіцієнти, близькі до 0, відповідають біту 0, близькі до $\frac{q}{2}$ — біту 1).

4) Застосовуємо декодування коду з виправленням помилок:

$$m = \mathsf{ECC\_Dec}(\tilde{\mu}).$$

Таким чином, LAC реалізує стандартну RLWE-схему шифрування з малим модулем q та сильним блоком корекції помилок для досягнення дуже малої ймовірності помилки розшифрування.

Аналіз безпеки

Безпека схеми LAC ґрунтується на складності задачі Ring-LWE та додатково підтверджується аналізом стійкості до спеціалізованих атак, які враховують особливості малого модуля q та структуру шумів. Нижче наведено огляд основних класів атак і відповідних контрзаходів відповідно до статті.

1. Атаки типу primal, dual та hybrid.

– **Primal-атаки:** полягають у відновленні секретного полінома шляхом побудови відповідної ґратки та запуску алгоритму BKZ. Складність визначається параметрами n, q та дисперсією шуму.

– **Dual-атаки:** намагаються знайти короткий вектор у дуальній ґратці для розрізнення справжніх та випадкових вибірок.

– **Hybrid-атаки:** комбінують частковий перебір секрету з редукцією ґраток (BKZ з sieving).

Для параметрів LAC автори оцінюють складність цих атак, використовуючи моделі core-SVP та (Q)sieving, що відповідають сучасному стану криптоаналізу.

2. Атаки на підкільцях (subfield attacks). Малий модуль q може призводити до факторизації полінома $x^n + 1$ над $\mathbb{Z}_q$, що дає можливість криптоаналітику працювати в менших підкільцях. Ідея атаки полягає в тому, що якщо RLWE-приклад обмежити підкільцем меншої розмірності, задача може стати легшою.

У пейпері показано, що у відповідних підкільцях вектор, який потрібно знайти, має довжину, несумісну з евристичною оцінкою Гауса для коротких векторів. Таким чином, застосування BKZ не приводить до успішної атаки. LAC залишається стійким до цього типу криптоаналізу.

3. Атаки на аномально великі або структуровані шуми (High-Hamming-Weight та Pattern attacks). Деякі атаки орієнтуються на випадки, коли:

– коефіцієнти шуму мають надто *велику вагу Хеммінга* (high-hamming-weight attack),

– або утворюють *виражені патерни*, що істотно збільшують ймовірність помилок при розшифруванні (pattern attack).

Ці атаки потенційно дають реакційний канал за ознакою успіху/помилки декодування. У LAC-v3 для захисту передбачено:

– використання розподілів з фіксованою вагою для секретів і шумів, що унеможливлює появу аномально великих коефіцієнтів;

– зменшення ймовірності помилки декодування через застосування

BCH-кодів з великим радіусом корекції;

– прив'язку генератора випадкових чисел до публічного ключа (multi-target countermeasure), що унеможливлює дешеву попередню обробку адверсара.

4. Стійкість у моделі IND-CCA2. Схема LAC перетворюється на схему, захищену від атак повного активного зловмисника, за допомогою перетворення Фудзісакі–Окамото (Fujisaki–Okamoto) у класичній та квантовій моделі випадкового оракула. Коректність після FO гарантується надзвичайно низькою ймовірністю помилки декодування (значно меншою за 2^{-128}), яка досягається завдяки комбінації D_2-коду та BCH-коду.

3 SCLOUD

Документ [6] представляє нове сімейство PKE та KEM, назване SCloud, що ґрунтується на неструктурованому LWE (plain LWE), а не RLWE/NTRU. Схеми включають: SCloudCPAPKE – IND-CPA PKE; SCloudCCAPKE – IND-CCA PKE; SCloudKEM – IND-CCA KEM (через трансформацію Fujisaki–Okamoto).

SCloud — це постквантова криптосистема, яка реалізує шифрування з відкритим ключем (PKE) та механізм капсулювання ключів (KEM) на основі задачі LWE (Learning With Errors). На відміну від багатьох сучасних схем, вона не використовує структуровані решітки (як-от RLWE чи NTRU), а працює з plain LWE, що забезпечує більш високий рівень стійкості проти майбутніх квантових атак.

У схемі застосовано два ключові нововведення:

1. Mixed-sampler: Він поєднує центральний біноміальний та обмежений рівномірний розподіли. Це дає: гнучкі параметри шуму, вищу ефективність, кращу стійкість проти dual-атак.

2. Новий механізм узгодження помилки (error reconciliation): Використовує: бінарні лінійні коди, Gray-коди. Цей механізм дозволяє коректно відновлювати повідомлення навіть при значному шумі, зменшує розмір параметрів і покращує швидкість шифрування/розшифрування.

SCloud забезпечує: IND-CPA та IND-CCA безпеку (через Fujisaki–Okamoto трансформацію), параметри для 128/192/256 біт безпеки, високу ефективність для систем без структурованих решіток, низьку ймовірність помилки дешифрування завдяки новій схемі корекції.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Yupu Hu, Siyue Dong та Xingting Dong. «Analysis on Aigis-Enc: asymmetrical and symmetrical». Англ. В: *IET Information Security* (2021). DOI: 10 . 1049 / ise2 . 12009. URL: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2.12009.

[2] Xianhui Lu та ін. *LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus*. Англ. Тех. звіт. 2018/1009. IACR Cryptology ePrint Archive, 2018, с. 36. URL: https://eprint.iacr.org/2018/1009.pdf.

[3] Xidian University та Shaanxi Xi'an. «Analysis on Aigis-Enc: asymmetrical and symmetrical». Англ. В: (2020). URL: https://eprint.iacr.org/2020/036.pdf.

[4] A. Wang, D. Xiao та Y. Yu. «Lattice-based cryptosystems in standardisation processes: A survey». Англ. В: *IET Information Security* 17.2 (2023), с. 227—243. DOI: 10 . 1049 / ise2 . 12101. URL: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ise2.12101.

[5] Fu Yu та Xiufeng Zhao. «Research on Two-Party Cooperative Aigis-sig Digital Signature Protocol». Англ. В: *Security and Privacy in New Computing Environments (SPNCE 2021)*. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Cham, 2022, с. 53—63. DOI: 10 . 1007 / 978 - 3 - 030 - 96791 - 8 _ 4. URL: https://link.springer.com/chapter/10.1007/978-3-030-96791-8_4.

[6] Z. Zheng та ін. *SCloud: Public Key Encryption and Key Encapsulation Mechanism Based on Learning With Errors*. Тех. звіт. 2020/095. IACR Cryptology ePrint Archive, ??