Petro Davydov

Рев'ю на тему «Гібридні ключі на практиці: поєднання класичної, квантової та постквантової криптографії»

1. Вступ

Наукова публікація під назвою **«Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography»** представляє дослідження та практичну реалізацію гібридної системи встановлення ключів, яка поєднує три криптографічні парадигми: класичний обмін ключами (KEX), постквантові механізми інкапсуляції ключів (KEM) та квантовий розподіл ключів (QKD). Автори роботи працювали над створенням безпечних комунікаційних систем в умовах зростаючих квантових загроз та переходу до постквантової криптографії.

Центральне дослідницьке питання, яке розглядається у статті: *Як спроєктувати та реалізувати гібридну систему встановлення ключів, яка забезпечує довгострокову безпеку проти класичних, постквантових та квантових атак, залишаючись ефективною та придатною для реального використання?*

Основна мета дослідження - запропонувати, реалізувати та протестувати архітектуру *3-key combiner*, яка безпечно інтегрує ключі з трьох криптографічних джерел. Комбінатор розроблений як гнучкий компонент, що дозволяє використовувати або виключати QKD залежно від потреб розгортання, і має формальний доказ безпеки в *Quantum Standard Model (Q-SM)*. Автори демонструють, що така система може бути реалізована на FPGA-платформах з низьким споживанням ресурсів, високою пропускною здатністю та гарантіями безпеки.

Публікація робить внесок у галузь, поєднуючи теоретичні моделі безпеки з практичними реалізаціями, пропонуючи рішення, яке є одночасно *доказово безпечним та апаратно-ефективним*. Вона також позиціонується як перша відома реалізація гібридного комбінатора KEX+KEM з формальними доказами безпеки та квантовою адаптивністю.

2. Методологія

Методологія дослідження базується на проектуванні, реалізації та формальному аналізі безпеки *гібридного 3-ключового комбінатора*, який об'єднує три криптографічні примітиви: *класичний обмін ключами (KEX), постквантовий механізм інкапсуляції ключів (KEM) та протокол квантового розподілу ключів (QKD)*.

Криптографічна конструкція

Основою системи є *3-ключовий комбінатор на основі dual-PRF*. Він приймає три незалежно згенеровані ключі K1, K2, K3, K_1, K_2, K_3, кожен з яких походить з різного криптографічного джерела:

- ✓ K1K_1: отриманий з постквантового KEM (Kyber) з автентифікованим обміном.
- ✓ K2K_2: отриманий з класичного KEX (ECDH).
- ✓ K3K_3: отриманий з QKD-протоколу (наприклад, 4-станова Coherent One-Way).

Кожен ключ обробляється через функцію $g(K_i)$, утворюючи проміжні значення u_i, які потім комбінуються за допомогою HMAC та SHA3-512 у послідовності конструкцій. Фінальний ключ KK обчислюється як:

$$K=H(U \oplus HMAC(k2,u1 \| u3 \| 2) \oplus HMAC(k3,u1 \| u2 \| 3))$$

Ця конструкція доведена як *IND-CCA безпечна*, за умови, що HMAC - це PRF, g - ін'єктована та одностороння функція, а H - ε-регулярна.

Реалізація на апаратному рівні

Система реалізована на *FPGA Virtex UltraScale+ (xcvu9p-flgb2104-2-i)* з використанням *Vivado*. Комбінатор спроектовано як модульний та ресурсоефективний:

- ✓ Внутрішні операції виконуються з *64-бітними транзакціями*.
- ✓ Один *Keccak-блок* використовується як для SHA3-512, так і для HMAC.
- ✓ FIFO-буфери зберігають u1,u2,u3, u_1, u_2, u_3.
- ✓ Підтримується режим з QKD / без нього через параметр конфігурації.

Валідація та тестування

Коректність реалізації перевірена через:

- ✓ Тисячі симуляцій з Python реалізацією (на основі *hashlib* та *hmac*).
- ✓ Інтеграцію в повну систему шифрування, де комбінатор використовувався для встановлення ключів.

Бенчмарк продуктивності

Автори виміряли:

- ✓ *Кількість тактів* для кожного криптографічного примітива (Kyber, ECDH, QKD).
- ✓ *Максимальну частоту* та *швидкість генерації ключів* з QKD та без.
- ✓ *Використання ресурсів* (LUT, FF) та *споживання енергії* для кожного компонента.

Можемо сказати, що був задіяний подвійний фокус на *формальній безпеці* та *практичній ефективності,* та вказати це як ключову перевагу методології.

3. Результати

* Даний розділ формувався за допомогою AI з певними командами для створення таблиць, перевірки підрахунків та перевірявся у пошукових системах

Результати охоплюють як теоретичні гарантії безпеки, так і практичні показники продуктивності. Автори підтверджують коректність, ефективність та адаптивність 3-ключового комбінатора через симуляції, синтез апаратури та розгортання.

Перевірка коректності

- ✓ Комбінатор протестовано через *багаторазові симуляцій*.
- ✓ Використано Python-реалізацію (hashlib, hmac) для перевірки узгодженості виходів.
- ✓ Компонент інтегровано в повну систему шифрування - підтверджено надійність при встановленні ключів.

Використання ресурсів FPGA

Синтезовано на FPGA Virtex UltraScale+ (xcvu9p-flgb2104-2-i)

*Таблиця створено за допомогою AI

Компонент	**LUTs**	**FFs**	**Потужність [Вт] (макс/очікування)**
ECDH	26,625	24,090	2.505 / 2.022
Kyber	19,839	35,129	2.496 / 1.741
SHA3-512	2,901	1,702	2.514 / 0.643
HMAC	403	659	2.474 / 0.294
Key Combiner	4,471	3,287	2.480 / 0.746
Key Combiner з QKD	4,532	3,363	2.480 / 0.756
Загалом	67,464	79,197	**2.557 / 5.486**

Комбінатор має низьке споживання ресурсів - придатний для малих FPGA (наприклад, Artix-7).

Показники продуктивності

- Максимальна частота:
  - Без QKD: 399 МГц
  - З QKD: 388 МГц

- Затримка генерації ключа:
  - Без QKD: 1155 тактів
  - З QKD: 2007 тактів

- Швидкість генерації ключів:
  - Без QKD: 345,454 ключів/сек
  - З QKD: 193,323 ключів/сек

Затримка KEX / KEM

- Kyber (K_1):
  - Клієнт: 21,196 тактів
  - Сервер: 15,920 тактів
- ECDH (K_2): 221,619 тактів
- QKD (K_3): +-9.2 ключів/сек (2365 bps при 256-бітних ключах)

Загальна затримка визначається найповільнішим компонентом - ECDH.
Підсумкова затримка: *222,774 тактів 362 МГц - 1,624 ключів/сек***.**

Швидкість QKD

*Таблиця згенерована AI

Протокол QKD	**Відстань**	**Втрати (дБ)**	**Швидкість**
3-state COW	~7 км	2.1	2684 bps
4-state COW	~7 км	2.1	2365 bps
4-state COW	~2.2 км	6.6	1230 bps

4-станова COW має вищу стійкість, але трохи нижчу швидкість. Рекомендоване затухання: *10–14 дБ***.**

Бенчмарк системи

- ✓ Повна система (ECDH + Kyber + QKD + Combiner + AES) досягла *53.57 Gbps (iPerf3).*
- ✓ Теоретичний максимум: *~100 Gbps*
- ✓ Обмеження - *тестовий сервер*, не криптографічна система.

4. Ключові інсайти

* Для більш поглибленого розуміння теми використовувався AI та Google

Інсайти із публікації, які важливі для криптографічної інженерії, реалізації на FPGA та постквантової безпеки.

1. Конструкція dual-PRF забезпечує IND-CCA безпеку

Безпека комбінатора базується на властивостях dual-PRF, що гарантує нерозрізненість при атаках з вибором шифртексту.

Чому це важливо: Це формальна основа для побудови безпечних гібридних систем.

2. Поєднання KEX, KEM і QKD посилює довгострокову безпеку

Система інтегрує класичні, постквантові та квантові джерела ключів - для компрометації потрібно зламати всі три.

Чому це важливо: Такий тришаровий захист ідеально підходить для середовищ з високими вимогами до безпеки та відповідає цілям у сфері квантової стійкості.

3. Низьке споживання ресурсів на FPGA

Комбінатор використовує ~4500 LUTs та ~3300 FFs - придатний для малих платформ (Artix-7).

Чому це важливо: Можна розгортати на обмеженому обладнанні - корисно для вбудованих систем і бюджетних рішень.

4. Повторне використання Keccak для SHA3-512 і HMAC

Один Keccak-блок використовується для хешування та MAC - оптимізація ресурсів.

Чому це важливо: Відповідає принципам гігієни інфраструктури та модульного дизайну - менше дублювання, більше підтримка.

5. Паралельна генерація ключів з урахуванням вузьких місць

Хоча всі джерела ключів працюють паралельно, найповільніший (ECDH) визначає затримку.

Чому це важливо: Допомагає проектувати системи з урахуванням таймінгу та оптимізувати пропускну здатність.

6. **Інтеграція QKD є опціональною та параметризованою**

Система дозволяє вмикати/вимикати QKD через параметр - гнучке розгортання.

Чому це важливо: Можна адаптувати до середовищ з або без квантової інфраструктури - підвищує практичну цінність.

7. **Валідація через Python-симуляції**

Симуляції з Python (hashlib, hmac) підтвердили коректність апаратної реалізації.

Чому це важливо: Можна застосувати цей підхід для тестування криптомодулів перед синтезом, що може гарантувати коректність.

8. **Безпека зберігається навіть при компрометації одного примітива**

Якщо хоча б одне джерело ключів залишається безпечним - фінальний ключ теж безпечний.

Чому це важливо: Така надмірність критична для гібридних систем - знижує ризики нових вразливостей.

9. **Швидкість QKD достатня для ліній 100 Gbps**

Хоча QKD повільніший за Kyber та ECDH, він підтримує високошвидкісні лінії при буферизації.

Чому це важливо: Після більш поглибленого вивчення цього наукового напрямку, можна спробувати обґрунтувати використання QKD у реальних системах без втрати продуктивності.

10. **Теоретична безпека поєднується з практичною ефективністю**

Система поєднує формальні моделі (Q-SM) з реальним FPGA-розгортанням та AES-інтеграцією.

Чому це важливо: Є можливість створення, поліпшення або поєднання відтворюваних аудиторних систем, які є одночасно безпечними та ефективними (звісно при більш глибокому зануренню у тему)

5. Висновок

Публікація *«Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography»* пропонує новаторський та практичний підхід до гібридного встановлення ключів, інтегруючи три криптографічні парадигми - класичну, постквантову та квантову - в одну безпечну та ефективну систему. Автори успішно демонструють, що така система може бути реалізована на FPGA-платформах з низьким споживанням ресурсів, високою пропускною здатністю та формальними гарантіями безпеки.

Запропонований *3-ключовий комбінатор* вирізняється як перша відома реалізація, яка:

- ✓ Має *доказову безпеку в Quantum Standard Model (Q-SM).*
- ✓ Є *практично придатною* для апаратного розгортання (FPGA Virtex UltraScale+).
- ✓ *Адаптується* до різних сценаріїв розгортання - з QKD або без.
- ✓ *Стійка* до майбутніх квантових загроз та сучасних атак.

Модульна архітектура комбінатора, конструкція dual-PRF та сумісність з будь-якими IND-CCA безпечними KEX/KEM роблять його універсальним інструментом для захищених комунікацій. Його здатність зберігати безпеку навіть при компрометації одного джерела ключів додає критичну надійність для довготривалих криптографічних систем.

З точки зору розгортання, система підходить для середовищ з високими вимогами до безпеки - уряд, фінанси, телекомунікації або у хмарі. Вона підтримує високошвидкісні з'єднання (до 100 Gbps) та може бути масштабована або оптимізована для компактних FPGA-платформ.

Що до перспективи майбутніх досліджень, автори окреслюють кілька відкритих проблем та напрямів розширення:

- *Масштабування до багатовузлових QKD-мереж*, включно з управлінням ключами та довіреними ретрансляторами.
- *Оптимізація FPGA-реалізацій* для компактних платформ (наприклад, мережевих карт).
- *Підвищення швидкості QKD* через покращення оптичних умов та налаштування обладнання.
- *Захист від квантового хакінгу* через автентифіковані квантові пристрої.
- *Адаптація до нових стандартів* через постійний моніторинг криптографічних змін.

Як підсумок можна сказати, що ця робота поєднує теоретичні моделі криптографії з реальним апаратним втіленням, пропонуючи безпечне, ефективне та перспективне рішення для гібридного встановлення ключів.

**Наступний розділ є опціональним, та пов'язаний з самостійним додатковим навчанням на суміжних платформах з пізнання сфери кібербезпеки.*

6. HackTheBox Модулі

На платформі HackTheBox наразі ***немає окремого модуля***, присвяченого гібридним системам встановлення ключів, які поєднують KEX, KEM та QKD. Проте існують суміжні модулі, що допоможуть розвинути необхідні навички:

Криптографія

- **Crypto Fundamentals**: Основи симетричної/асиметричної криптографії, хешування, обміну ключами.
- **Post-Quantum Cryptography (у розробці)**: Очікується поява модулів, присвячених PQC, після стандартизації NIST.

Зворотна інженерія та аналіз протоколів

- **Hardware Hacking**: Аналіз вбудованих систем і FPGA-дизайнів.
- **Wireshark 101 / Packet Analysis**: Корисно для аналізу трафіку QKD та перевірки протоколів обміну ключами.

Практична користь

- **LS Attacks**: Хоч і не гібридні, ці модулі допомагають зрозуміти вразливості класичних протоколів (RSA, ECDHE).
- **Crypto CTF-челенджі**: Часто включають HMAC, SHA3, PRF - безпосередньо пов'язані з логікою 3-key Combiner.

Зовнішні ресурси

QUBIP Hybridization Module (GitHub): Відкрите рішення, що поєднує QKD і PQC за ETSI GS QKD 004, з інтеграцією TLS і Docker-інфраструктурою.

Практичне середовище для експериментів з гібридним обміном ключами - https://github.com/QUBIP/hybridization-module.git.

Словник

FPGA (Field-Programmable Gate Array) - це інтегральна мікросхема, яку можна програмувати після виробництва для реалізації цифрових логічних функцій. Вона складається з масиву логічних блоків, з'єднаних програмованими міжз'єднаннями, що дозволяє створювати спеціалізовані апаратні рішення. У криптографії FPGA використовується для реалізації алгоритмів шифрування, хешування, обміну ключами з високою продуктивністю. Вона дозволяє паралельну обробку даних, що критично для систем реального часу. FPGA-платформи, як Virtex UltraScale+ або Artix-7, підтримують реалізацію складних схем з низьким енергоспоживанням.

KEX (Key Exchange) - це криптографічний протокол, який дозволяє двом сторонам безпечно обмінятися секретним ключем через незахищений канал. Класичні приклади включають Diffie-Hellman та ECDH, які базуються на складності математичних задач, таких як дискретне логарифмування. KEX не забезпечує автентифікацію, тому часто комбінується з іншими механізмами. У гібридних системах KEX може бути доповнений постквантовими або квантовими методами. Його роль - забезпечити початкову основу для симетричного шифрування.

KEM (Key Encapsulation Mechanism) - це криптографічна конструкція, яка дозволяє безпечно передати симетричний ключ, інкапсулюючи його в шифротекст. Вона складається з трьох функцій: генерації ключів, інкапсуляції та декапсуляції. KEM часто використовується в постквантових алгоритмах, таких як Kyber, оскільки дозволяє ефективну реалізацію на апаратному рівні. На відміну від KEX, KEM може бути легко адаптований до однонаправлених комунікацій. У гібридних системах KEM забезпечує постквантову стійкість.

QKD (Quantum Key Distribution) - це метод розподілу криптографічних ключів, який використовує принципи квантової механіки для забезпечення безумовної безпеки. Найвідоміші протоколи - BB84, E91, COW - використовують фотони для передачі інформації, де будь-яка спроба перехоплення змінює стан системи. QKD дозволяє виявити наявність зловмисника через підвищення QBER (рівня помилок). Хоча QKD має обмеження по відстані та швидкості, він є критичним компонентом для захисту від квантових атак. У гібридних системах QKD додає третій рівень захисту.

IND-CPA (Indistinguishability under Chosen-Plaintext Attack) - це модель безпеки, яка гарантує, що шифротекст не розкриває інформацію про відкритий текст, навіть якщо атакуючий може вибирати тексти для шифрування. Це базовий рівень безпеки для симетричних та асиметричних шифрувальних схем. Якщо схема IND-CPA безпечна, то вона стійка до пасивного спостереження.

Проте вона не захищає від активних атак, де зловмисник може змінювати шифротексти. У сучасних протоколах IND-CPA є необхідною, але недостатньою умовою.

IND-CCA (Indistinguishability under Chosen-Ciphertext Attack) - це розширена модель безпеки, яка гарантує, що шифротекст не розкриває інформацію про відкритий текст, навіть якщо атакуючий може запитувати розшифрування інших шифротекстів. Це критично для захисту протоколів, які використовуються в реальних мережах, таких як TLS. IND-CCA безпека вимагає додаткових механізмів, таких як перевірка автентичності або використання FO-перетворення. У гібридних системах IND-CCA є ключовим критерієм для вибору KEM/KEX. Вона забезпечує стійкість до активних атак.

Dual PRF (Подвійна псевдовипадкова функція) - це конструкція, яка використовує дві незалежні псевдовипадкові функції для комбінування кількох ключів. Вона дозволяє створити фінальний ключ, який залежить від усіх вхідних значень, зберігаючи криптографічну стійкість. У 3-key combiner dual PRF використовується для об'єднання K_1, K_2, K_3 з використанням HMAC та SHA3. Така конструкція дозволяє довести IND-CCA безпеку комбінатора. Dual PRF також забезпечує гнучкість - можна адаптувати до різних схем.

Integer Factorization Problem (IF) - Задача цілочисельної факторизації - це проблема розкладу великого числа на прості множники. Вона лежить в основі безпеки RSA та інших класичних алгоритмів. Складність задачі зростає експоненційно з розміром числа, що робить її стійкою до класичних атак. Проте квантові алгоритми, такі як алгоритм Шора, можуть вирішити IF за поліноміальний час. Тому IF вважається нестійкою в постквантовому контексті.

Discrete Logarithm Problem (DLP) - це задача знаходження показника x у рівнянні $g^x=h \bmod p$, g - генератор, h - елемент групи. Вона лежить в основі безпеки протоколів Diffie-Hellman, ElGamal, ECDH. DLP вважається складною для класичних комп'ютерів, але вразливою до квантових атак. У еліптичних кривих (EC) DLP має аналог - ECDLP, який є ще складнішим. DLP - фундаментальна задача для класичної криптографії.

EC (Elliptic Curve) - Еліптичні криві - це математичні об'єкти, які використовуються в криптографії для побудови ефективних та безпечних алгоритмів. Криптографія на основі еліптичних кривих (ECC) забезпечує той самий рівень безпеки, що й RSA, але з меншими розмірами ключів. Це дозволяє зменшити обчислювальні витрати та енергоспоживання, що критично для мобільних та вбудованих пристроїв. ECC базується на складності задачі

дискретного логарифмування в групі точок на кривій. Протоколи, такі як ECDH та ECDSA, широко використовуються в TLS, SSH та блокчейн-системах.

EC DSA (Elliptic Curve Digital Signature Algorithm) - це алгоритм цифрового підпису, який базується на еліптичних кривих. Він дозволяє перевірити автентичність повідомлення та його автора, не розкриваючи приватний ключ. ECDSA широко використовується в протоколах безпеки, таких як TLS, SSH, Bitcoin. Його перевага - висока безпека при малих розмірах ключів. Проте він вразливий до квантових атак, тому в майбутньому його можуть замінити постквантові схеми підпису.

ANSSI (Agence nationale de la sécurité des systèmes d'information) - це національне агентство Франції з кібербезпеки, яке займається стандартизацією, сертифікацією та рекомендаціями щодо захисту інформаційних систем. Воно публікує технічні документи, включно з позицією щодо переходу до постквантової криптографії. ANSSI підтримує використання гібридних схем для поступового переходу до PQC. Їх рекомендації враховуються при розробці європейських стандартів. Організація також бере участь у міжнародних криптографічних дослідженнях.

BSI (Bundesamt für Sicherheit in der Informationstechnik) - Федеральне відомство з безпеки інформаційних технологій Німеччини. Воно відповідає за розробку стандартів, сертифікацію продуктів та оцінку ризиків у сфері кібербезпеки. BSI активно досліджує постквантову криптографію та публікує рекомендації щодо її інтеграції. Відомство підтримує використання гібридних схем для забезпечення перехідної безпеки. BSI також співпрацює з ENISA та іншими європейськими органами.

ENISA (European Union Agency for Cybersecurity) - агентство Європейського Союзу, яке займається кібербезпекою, включно з криптографічними стандартами, сертифікацією та дослідженнями. ENISA публікує звіти про інтеграцію постквантової криптографії, включно з аналізом ризиків та сценаріями розгортання. Агентство підтримує використання гібридних схем, які поєднують класичні та PQC-примітиви. ENISA також координує європейські ініціативи щодо квантової безпеки. Її документи використовуються для формування політик у країнах-членах ЄС.

AES-256-GCM - це симетричний алгоритм шифрування, який використовує 256-бітний ключ та режим Galois/Counter Mode (GCM). GCM забезпечує як конфіденційність, так і автентичність даних через вбудовану MAC-функцію. AES-256-GCM є стандартом у TLS 1.3, IPsec, SSH та інших протоколах. Його

перевага - висока продуктивність на апаратному рівні та стійкість до відомих атак. У гібридних системах AES використовується для шифрування даних після встановлення ключа через KEX/KEM/QKD.

ECDH (Elliptic Curve Diffie-Hellman) - варіант протоколу Diffie-Hellman, який використовує еліптичні криві для обміну ключами. Він дозволяє двом сторонам створити спільний секрет, не передаючи його напряму. ECDH забезпечує менші розміри ключів та вищу продуктивність порівняно з класичним DH. Протокол широко використовується в TLS, Signal, SSH. У гібридних системах ECDH може бути доповнений постквантовими або квантовими методами для підвищення стійкості.

IETF (Internet Engineering Task Force) - міжнародна організація, яка розробляє та стандартизує інтернет-протоколи, включно з TLS, IPsec, DNSSEC. Вона публікує RFC-документи, які описують технічні специфікації та рекомендації. IETF активно працює над інтеграцією постквантової криптографії в існуючі протоколи, зокрема TLS 1.3. Організація підтримує гібридні моделі обміну ключами для забезпечення перехідної безпеки. Її стандарти є основою для реалізації криптографії в інтернеті.

Hybrid Key Exchange in TLS 1.3 - Гібридний обмін ключами в TLS 1.3 - це механізм, який поєднує класичні та постквантові примітиви для встановлення спільного секрету. Наприклад, одночасно використовуються ECDH та Kyber, а фінальний ключ формується через комбінування обох. Такий підхід дозволяє зберегти сумісність з існуючими системами та забезпечити стійкість до квантових атак. Гібридні моделі підтримуються в IETF-драфтах та експериментальних реалізаціях. Вони є перехідним рішенням до повної інтеграції PQC.

LUT (Look-Up Table) - базовий логічний елемент у FPGA, який реалізує довільну логічну функцію шляхом зберігання всіх можливих результатів у таблиці. Кожен LUT має фіксовану кількість входів (зазвичай 4 або 6) і може бути сконфігурований для реалізації будь-якої булевої функції цих входів. У контексті криптографії LUT використовується для реалізації логіки шифрування, хешування або обміну ключами. Кількість LUT вказує на складність або обсяг логіки, необхідної для реалізації певного модуля.

FF (Flip-Flop) - це базовий елемент пам’яті в цифрових схемах, який зберігає один біт інформації. У FPGA Flip-Flops використовуються для зберігання станів, реалізації регістрів, лічильників і синхронізації сигналів. Вони критичні для реалізації послідовних логічних схем, таких як FSM або криптографічні

протоколи з внутрішнім станом. Кількість FF вказує на обсяг необхідної пам'яті або кількість регістрів у модулі.

ε-регулятор / ε-регулярна функція - Епсилон-регулярна функція - це функція, яка гарантує, що її вихід розподілений майже рівномірно незалежно від розподілу вхідних даних. Формально, вона є ε-регулярною, якщо її вихід не відрізняється від рівномірного розподілу більш ніж на ε у статистичній відстані. У криптографії такі функції використовуються як екстрактори випадковості або хеш-функції. Вони забезпечують, що навіть частково випадкові входи дають майже ідеально випадкові виходи. Це критично для безпеки схем, які комбінують кілька джерел ключів.

IND-CCA KEM - це механізм інкапсуляції ключів, який є стійким до атак з вибором шифротексту (Chosen-Ciphertext Attack). Це означає, що навіть якщо атакуючий може запитувати розшифрування довільних шифротекстів (крім цільового), він не зможе дізнатися нічого про інкапсульований ключ. IND-CCA є найвищим стандартом безпеки для KEM і є обов'язковим для використання в TLS, VPN та інших протоколах. У гібридних схемах важливо, щоб кожен компонент мав IND-CCA безпеку. Це дозволяє довести безпеку комбінатора в цілому.

KEM-комбінатори - це криптографічні конструкції, які поєднують кілька KEM-схем для створення одного спільного секрету. Вони можуть бути побудовані через XOR, PRF або інші механізми. Мета - забезпечити стійкість до компрометації одного з KEM, зберігаючи безпеку фінального ключа. Деякі комбінатори мають формальні докази безпеки (наприклад, у моделі ROM або SM), інші - лише емпіричну стійкість. У гібридних системах KEM-комбінатори дозволяють поєднувати класичні та постквантові алгоритми.

SIKE (Supersingular Isogeny Key Encapsulation) - постквантовий алгоритм інкапсуляції ключів, який базується на складності знаходження ізогеній між суперсингулярними еліптичними кривими. Його перевага - дуже малі розміри ключів та шифротекстів, що робить його привабливим для обмежених середовищ. Проте SIKE має високу обчислювальну складність але був зламаний у 2022 році за допомогою нових алгоритмів. Незважаючи на це, SIKE залишається важливим для досліджень у сфері ізогеній. У гібридних схемах його іноді поєднували з ECDH.

Перетворення Фудзісакі-Окамото (FO) - це криптографічна техніка, яка перетворює IND-CPA безпечну KEM у IND-CCA безпечну. Вона використовує хешування відкритого тексту та шифротексту для генерації ключа, який потім перевіряється при розшифруванні. FO-перетворення є стандартним способом

побудови стійких до активних атак KEM. Воно використовується в багатьох постквантових алгоритмах, включно з Kyber. Без FO-перетворення KEM не може бути безпечно використаний у TLS або VPN.

Q-ROM (Quantum Random Oracle Model) - модель безпеки, яка розширює класичну модель випадкового оракула (ROM) для квантових атак. У цій моделі атакуючий має доступ до хеш-функції як до квантового оракула, тобто може робити суперпозиційні запити. Це ускладнює доведення безпеки, оскільки класичні техніки не працюють у квантовому контексті. Q-ROM використовується для аналізу постквантових схем, щоб гарантувати їхню стійкість до квантових атак. Це важливо для доведення безпеки гібридних комбінаторів у квантовому світі.

Store Now Decrypt Later (SNDL) Attack - це стратегія атак, при якій зловмисник перехоплює зашифровані дані сьогодні, зберігає їх, а потім розшифровує в майбутньому, коли з'являться потужніші обчислювальні ресурси (наприклад, квантові комп'ютери). Такий підхід особливо небезпечний для даних з довгим терміном життя, як-от державні документи, медичні записи або фінансові транзакції. Навіть якщо сьогоднішні алгоритми є безпечними, вони можуть бути зламані в майбутньому. Гібридні системи з QKD та PQC дозволяють захиститися від SNDL, оскільки забезпечують довготривалу безпеку. Це одна з головних мотивацій для переходу до постквантової криптографії.

QBER (Quantum Bit Error Rate) - це показник кількості помилок у переданих квантових бітах (квбітів) у системах QKD. Він визначається як відсоток невідповідностей між бітами, отриманими двома сторонами, і є критичним параметром для оцінки безпеки каналу. Високий QBER може свідчити про наявність зловмисника або проблеми з оптичним обладнанням. У практиці QKD системи мають порогові значення QBER, після яких ключі вважаються небезпечними. Контроль QBER дозволяє виявляти атаки типу «прослуховування» та забезпечує безумовну безпеку.

GCM (Galois Counter Mode) - це режим роботи симетричного шифрування, який поєднує лічильник (CTR) для шифрування та аутентифікацію через MAC на основі поля Галуа. Він забезпечує одночасно конфіденційність і цілісність даних, що робить його ідеальним для мережевих протоколів. GCM має високу продуктивність на апаратному рівні, особливо на платформах з апаратною підтримкою множення в полях Галуа. У TLS 1.3 GCM є стандартним режимом для AES. Його використання в гібридних системах дозволяє захищати дані після встановлення ключа.

SHAKE / SHAKE-512 - це розширювана хеш-функція, яка є частиною стандарту SHA-3. SHAKE-512 дозволяє генерувати хеші довільної довжини з 512-бітною безпекою. Вона базується на алгоритмі Keccak і має високу стійкість до колізій та атак типу preimage. SHAKE використовується для генерації ключів, сертифікатів, ідентифікаторів сеансів у квантових протоколах. У QKD системах, таких як CLAVIS 3, SHAKE застосовується для обробки метаданих, включно з keyID та логами. Її гнучкість робить її придатною для гібридних криптографічних систем.

Keccak - це алгоритм хешування, який лежить в основі стандарту SHA-3. Він використовує sponge-конструкцію, де вхідні дані «вбираються» в стан, а потім «вичавлюються» у вихід. Keccak має високу стійкість до атак, включно з диференціальними та алгебраїчними. Його архітектура дозволяє ефективну реалізацію на FPGA, з можливістю повторного використання ядра для різних функцій (SHA3, HMAC, SHAKE). У 3-key combiner Keccak використовується для побудови PRF та хешування ключів. Це один із найнадійніших хеш-алгоритмів сучасності.

Vivado - це програмне середовище для розробки цифрових схем на FPGA, створене компанією Xilinx. Воно дозволяє синтез, моделювання, трасування та аналіз продуктивності апаратних модулів. Vivado підтримує мови опису апаратури (HDL), такі як Verilog та VHDL, а також високорівневі інструменти для оптимізації. У контексті криптографії Vivado використовується для реалізації та тестування алгоритмів шифрування, хешування, обміну ключами.

iPerf3 - це інструмент для вимірювання пропускної здатності мережі, який дозволяє тестувати TCP, UDP та SCTP з’єднання. Він використовується для оцінки реальної швидкості передачі даних між двома вузлами. У криптографічних системах iPerf3 дозволяє перевірити, чи не є шифрування вузьким місцем у продуктивності. Це стандартний інструмент для мережевих бенчмарків.

FPGA Virtex UltraScale+ (xcvu9p-flgb2104-2-i) - високопродуктивна FPGA-платформа від Xilinx, яка підтримує мільйони логічних елементів, DSP-блоки, високошвидкісні інтерфейси. Вона призначена для реалізації складних цифрових систем, включно з криптографією, машинним навчанням, обробкою сигналів. Virtex UltraScale+ є еталоном для промислових криптографічних реалізацій.

Artix-7 - це серія FPGA-платформ від Xilinx, орієнтована на енергоефективні та компактні рішення. Вона має меншу кількість LUT та FF порівняно з Virtex, але достатню для реалізації базових криптографічних модулів. Система доступна для вбудованих пристроїв, IoT та мережевих карт. Artix-7 - оптимальний вибір для бюджетних апаратних реалізацій.

DSP (Digital Signal Processor) - DSP-блоки - це спеціалізовані елементи в FPGA, призначені для обробки чисел з плаваючою комою, множення, фільтрації. У криптографії DSP використовується для реалізації математичних операцій, таких як множення в полях Галуа (GCM), обробка решіток (Kyber), ізогеній (SIKE). У публікації зазначено, що повна система використовує 182 DSP-блоки. Це показник складності та обчислювальної інтенсивності криптографічної реалізації.

Атенюатори (Attenuators) - це оптичні або електронні пристрої, які зменшують потужність сигналу без значного спотворення його форми. У системах QKD атенюатори використовуються для контролю інтенсивності лазерного імпульсу, щоб забезпечити однофотонний режим передачі. Це критично для безпеки, оскільки багатофотонні імпульси можуть бути вразливими до атак типу Photon Number Splitting. Атенюатори також допомагають адаптувати систему до різних довжин оптичного волокна та втрат. Їх правильне налаштування впливає на QBER та загальну ефективність QKD.

Раманівський шум (Raman Noise) - тип оптичного шуму, який виникає в волоконно-оптичних каналах через нелінійні ефекти розсіювання світла. У контексті QKD він може призводити до помилок у детекції фотонів, підвищуючи QBER. Особливо небезпечний при одночасній передачі класичних і квантових сигналів в одному волокні. Для зменшення Raman шуму використовують фільтри, часову ізоляцію та окремі канали. Його контроль є важливим для забезпечення безпеки та стабільності квантового каналу.

QKD-система - ID Quantique CLAVIS 3 - комерційна система квантового розподілу ключів, розроблена компанією ID Quantique. Вона підтримує протоколи BB84, COW та DPS, має вбудовані механізми автентифікації та управління ключами. Система включає лазерні джерела, детектори, атенюатори, та програмне забезпечення для управління сеансами. CLAVIS 3 інтегрується з класичними криптографічними системами через API та сертифікати. Вона використовується в урядових, фінансових та дослідницьких установах для захисту критичних даних.

ID Quantique - це швейцарська компанія, яка є світовим лідером у сфері квантової криптографії та квантових технологій. Вона розробляє QKD-системи, квантові генератори випадкових чисел (QRNG), та рішення для захисту даних. Її продукти використовуються в критичній інфраструктурі, телекомунікаціях, урядових структурах. Компанія активно співпрацює з академічними установами та бере участь у стандартизації ETSI та ISO. ID Quantique є ключовим гравцем у впровадженні квантової безпеки в реальні системи.

CRYSTALS-Kyber - постквантовий алгоритм інкапсуляції ключів, який базується на задачі Learning With Errors (LWE) над решітками. Він був обраний NIST як стандарт для постквантового шифрування. Kyber має високу продуктивність, невеликі розміри ключів та шифротекстів, і підтримує FO-перетворення для IND-CCA безпеки. Реалізація Kyber можлива як на програмному, так і на апаратному рівні (FPGA, ASIC). У гібридних системах Kyber часто комбінується з класичними KEX, такими як ECDH.

Kyber.AKE - це варіант протоколу Kyber, адаптований для автентифікованого обміну ключами (Authenticated Key Exchange). Він включає додаткові етапи перевірки автентичності сторін, що дозволяє використовувати його в протоколах типу TLS. Kyber.AKE забезпечує forward secrecy та стійкість до активних атак. У публікації 3-key combiner Kyber.AKE використовується як джерело одного з ключів (K_1). Це дозволяє інтегрувати постквантову безпеку в реальні комунікаційні системи.

Encaps - це процес інкапсуляції симетричного ключа в шифротекст за допомогою KEM.

Decaps - це процес витягування ключа з шифротексту на стороні отримувача.

Операції Encaps/ Decaps - є основою роботи KEM і використовуються для безпечного обміну ключами. У постквантових алгоритмах, таких як Kyber, Encaps/Decaps реалізуються через матричні операції над решітками. У гібридних системах ці операції комбінуються з класичними та квантовими джерелами ключів.

SHA-3 - це стандарт хеш-функцій, розроблений NIST як альтернатива SHA-2. Він базується на алгоритмі Keccak і має високу стійкість до колізій, preimage та інверсій. SHA-3 включає варіанти з різною довжиною виходу: SHA3-224, SHA3-256, SHA3-384, SHA3-512. У криптографії SHA-3 використовується для хешування повідомлень, генерації ключів, побудови PRF. Його архітектура дозволяє ефективну реалізацію на FPGA та ASIC.

Режим GCM 232 - варіант режиму Galois/Counter Mode, який використовує 232-бітний лічильник або обмеження на довжину повідомлення. Такий режим може бути застосований для специфічних апаратних реалізацій або протоколів з обмеженим простором адресації. Він зберігає властивості GCM: конфіденційність та автентичність. Його використання залежить від вимог до продуктивності та безпеки.

keyID || SHAKE(сертифікат) - конструкція, яка використовується для генерації унікального ідентифікатора ключа (keyID) на основі сертифіката, з використанням хеш-функції SHAKE. Сертифікат містить публічну інформацію про учасника QKD або криптографічного протоколу. Хешування через SHAKE забезпечує компактний, унікальний та криптографічно стійкий ідентифікатор. Такий keyID може використовуватись для автентифікації, логування або узгодження ключів. У системах QKD це дозволяє зв'язати ключі з конкретними сертифікатами без розкриття їх змісту.

keyID || SHAKE(інформація про налаштування сеансу) - конструкція використовується для генерації ідентифікатора ключа на основі параметрів сеансу, таких як довжина ключа, протокол, час, ідентифікатори сторін. Хешування через SHAKE забезпечує унікальність та стійкість до колізій. Це дозволяє системі QKD або TLS відстежувати ключі, пов'язані з конкретними сеансами, без збереження повної конфігурації. Такий підхід важливий для аудиту, відновлення та виявлення аномалій. Він також дозволяє інтегрувати QKD у класичні системи керування ключами.

keyID || SHAKE(повідомлення каналу обслуговування / "Logtail QKD") - хешування службових повідомлень QKD-системи, таких як лог-файли, сигнали синхронізації, повідомлення про помилки. SHAKE забезпечує компактне представлення цих повідомлень для подальшого аналізу або автентифікації. Конструкція дозволяє зв'язати службові події з конкретними ключами або сеансами. У системах типу CLAVIS 3 це використовується для моніторингу та аудиту. Такий підхід підвищує прозорість та безпеку квантового каналу.

SHAKE-512 - це варіант хеш-функції SHAKE з безпекою 512 біт. Вона дозволяє генерувати хеші довільної довжини, що робить її гнучкою для різних криптографічних задач. SHAKE-512 базується на алгоритмі Keccak і має високу стійкість до атак. Вона використовується для генерації ключів, ідентифікаторів, сертифікатів, а також у схемах цифрового підпису. У гібридних системах SHAKE-512 дозволяє інтегрувати QKD з класичними протоколами через узгоджені хеші.

ECDH-512 (крива sect571k1) - варіант протоколу Elliptic Curve Diffie-Hellman, який використовує криву sect571k1 з 571-бітною довжиною. Це одна з найбільш стійких класичних кривих, рекомендована для високозахищених систем. Вона забезпечує forward secrecy та стійкість до класичних атак. Проте вона вразлива до квантових атак, тому її часто комбінують з PQC-примітивами. У гібридних системах ECDH-512 використовується як класичний компонент для сумісності з існуючими інфраструктурами.

KYBER-768 - це параметризація алгоритму Kyber, яка забезпечує NIST Security Strength Category 3 (192-бітну безпеку). Вона балансує між продуктивністю та стійкістю до атак. KYBER-768 використовується в системах, де потрібна підвищена безпека, наприклад, у фінансових або урядових структурах. Вона підтримує FO-перетворення для IND-CCA безпеки. У гібридних системах KYBER-768 може комбінуватись з ECDH або QKD для багаторівневої безпеки.

Протокол Coherent One Way (COW) - протокол квантового розподілу ключів, який використовує когерентні імпульси світла, передані в одному напрямку. Він забезпечує високу швидкість передачі та стійкість до деяких типів атак. COW може працювати на великих відстанях з низьким QBER. У системах типу CLAVIS 3 реалізовано 3-станову та 4-станову версію COW. Протокол підтримує автентифікацію та інтеграцію з класичними криптографічними системами.

NIST Security Strength Category 3 - категорія безпеки, визначена NIST, яка відповідає 192-бітній симетричній безпеці. Вона використовується для оцінки стійкості криптографічних алгоритмів до атак. Категорія 3 рекомендована для захисту довготривалих або критичних даних. Алгоритми, які відповідають цій категорії, включають KYBER-768, ECDH-512, AES-192. У гібридних системах вибір категорії залежить від вимог до безпеки та продуктивності.

PQ-PQ об’єднувачі - це комбінатори, які поєднують два або більше постквантових алгоритмів (наприклад, Kyber + HRSS). Мета - забезпечити стійкість до майбутніх атак на один із примітивів. Такі об’єднувачі можуть використовувати XOR, PRF або інші механізми. Вони дозволяють створити фінальний ключ, який зберігає безпеку при компрометації одного з компонентів. PQ-PQ об’єднувачі є важливим напрямом досліджень у постквантовій криптографії.

Cloudflare - це глобальна компанія, яка надає послуги з кібербезпеки, CDN, DNS та захисту веб-додатків. Вона активно досліджує та впроваджує постквантову криптографію в свої сервіси, зокрема в TLS. Cloudflare брала участь у тестуванні гібридних схем обміну ключами (Kyber + X25519) у реальних умовах. Її публікації є джерелом практичних даних про продуктивність, сумісність та безпеку PQC. Компанія також підтримує відкриті стандарти та співпрацює з IETF.

Постквантові докази безпеки для Signal та TLS - протоколи, які використовуються для захищеної комунікації. Постквантові докази безпеки - це формальні моделі, які показують, що ці протоколи залишаються безпечними навіть при наявності квантового противника. Для TLS це включає гібридні моделі обміну ключами, FO-перетворення, та Q-ROM аналіз. Для Signal - використання PQC-підписів та KEM. Такі докази важливі для довготривалого захисту конфіденційної інформації.

Concatenate-then-Hashing - криптографічна техніка, яка об’єднує кілька вхідних даних (наприклад, ключі, шифротексти) через конкатенацію, а потім хешує результат. Вона використовується для побудови PRF, генерації фінального ключа, або автентифікації. Для безпеки важливо, щоб вхідні дані були незалежними та випадковими.

Quantum Standard Model (Q-SM) - це модель безпеки, яка враховує квантові можливості атакуючого, але не надає йому доступ до квантового оракула. Вона є розширенням класичної моделі SM і використовується для доведення безпеки гібридних схем. У Q-SM атакуючий має квантовий комп’ютер, але обмежений у доступі до хеш-функцій. Це дозволяє аналізувати стійкість схем, таких як 3-key combiner, до реалістичних квантових атак. Q-SM є компромісом між класичною та повною квантовою моделлю.

Quantum IND-CCA - модель безпеки, яка гарантує, що шифротекст не розкриває інформацію про відкритий текст, навіть якщо атакуючий має квантові обчислювальні ресурси та доступ до розшифрування. Вона є найвищим стандартом безпеки для постквантових KEM. Quantum IND-CCA вимагає FO-перетворення, ε-регулярних функцій та стійких PRF. У гібридних системах ця модель дозволяє довести, що фінальний ключ залишається безпечним навіть при компрометації одного з компонентів. Це критично для захисту від SNDL.

NCSC (National Cyber Security Centre) - британське агентство з кібербезпеки, яке займається захистом урядових, корпоративних та приватних систем. Воно публікує рекомендації щодо криптографії, включно з переходом до PQC. NCSC підтримує гібридні моделі, TLS 1.3, та QKD для критичних систем. Агентство співпрацює з ENISA, BSI, ANSSI. Його документи використовуються для оцінки ризиків та впровадження безпечних протоколів.

Екстрактор - функція, яка перетворює джерело з частковою випадковістю у майже рівномірно випадковий вихід. У криптографії екстрактори використовуються для генерації ключів, хешування, побудови PRF. Вони можуть бути детермінованими або з додатковим випадковим входом (seed). Екстрактори важливі для побудови ε-регулярних функцій. У гібридних схемах вони забезпечують, що фінальний ключ є криптографічно стійким.

RO (Random Oracle) - Модель випадкового оракула - це теоретична модель, в якій хеш-функція розглядається як ідеальна випадкова функція. Вона використовується для доведення безпеки криптографічних схем, таких як FO-перетворення, KEM, PRF. У моделі RO атакуючий може робити запити до оракула, але не має доступу до його внутрішньої логіки. RO дозволяє спростити аналіз та отримати формальні гарантії. У квантовому контексті RO розширюється до Q-ROM.

Атаки APOP (Authenticated Post Office Protocol) - протокол автентифікації в електронній пошті, який використовує хешування пароля з випадковим викликом. Атаки на APOP включають перехоплення хешу та відтворення автентифікації. Вони показали, що просте хешування не забезпечує достатню безпеку. У сучасних системах APOP замінено на TLS або SASL. Аналіз APOP важливий для розуміння слабких місць старих протоколів та переходу до PQC.

FO-перетворення (Fujisaki-Okamoto Transformation) - це криптографічна техніка, яка перетворює схему інкапсуляції ключів (KEM), що є безпечною лише в моделі IND-CPA, у схему, стійку до атак з вибором шифротексту (IND-CCA). Вона працює шляхом повторного хешування відкритого тексту та шифротексту, щоб перевірити їхню узгодженість під час розшифрування. Це дозволяє виявити підроблені або змінені шифротексти. FO-перетворення є стандартним компонентом у багатьох постквантових алгоритмах, зокрема Kyber. Його безпека доведена в моделі випадкового оракула (ROM), а також у квантовому її варіанті (Q-ROM).

Алгоритм Шора (Shor's Algorithm) - це квантовий алгоритм, який дозволяє ефективно розв'язувати задачі факторизації цілих чисел та дискретного логарифмування. Він працює за поліноміальний час, що робить його здатним зламати класичні криптографічні схеми, такі як RSA, DSA, ECDSA та Diffie-Hellman. Алгоритм використовує квантове перетворення Фур'є для пошуку періодів функцій, пов'язаних із криптографічними задачами. Його існування є головною причиною розвитку постквантової криптографії. У моделі безпеки Q-SM вважається, що атакуючий має доступ до алгоритму Шора.

IETF-драфт - це технічний документ, який публікується в рамках Internet Engineering Task Force (IETF) як частина процесу розробки інтернет-стандартів. Драфти описують нові протоколи, розширення до існуючих, або рекомендації щодо безпеки. Вони проходять публічне обговорення, перегляд та можуть стати RFC (Request for Comments), які є офіційними стандартами. У контексті TLS 1.3 існують IETF-драфти, що описують гібридні моделі обміну ключами з PQC. Вони є основою для впровадження постквантової криптографії в інтернет-протоколи.

Поле Галуа (Galois Field) - це скінченне поле, яке містить обмежену кількість елементів і в якому визначені операції додавання, множення, віднімання та ділення (крім ділення на нуль). У криптографії поля Галуа використовуються в алгоритмах шифрування (AES), автентифікації (GCM), кодуванні (Reed-Solomon) та хешуванні. Наприклад, у режимі AES-GCM MAC обчислюється як множення в полі GF(2^128). Поля Галуа забезпечують математичну основу для побудови ефективних та стійких криптографічних примітивів.

Атака типу preimage - Preimage-attack - це криптоаналітична атака, метою якої є знаходження вхідного повідомлення, яке відповідає заданому хешу. У першій preimage-атаці шукається будь-який вхід, що дає заданий хеш. У другій preimage-атаці шукається інший вхід, який дає той самий хеш, що й відомий вхід. Стійкість до таких атак є критичною для хеш-функцій, які використовуються в цифрових підписах, автентифікації та генерації ключів. SHA-3 та SHAKE мають високу стійкість до preimage-атак.

Sponge-конструкція - це загальна схема побудови хеш-функцій, яка складається з двох фаз: поглинання (absorb) та видачі (squeeze). Вхідні дані "вбираються" в стан фіксованого розміру, після чого з нього "вичавлюється" вихід довільної довжини. Ця конструкція використовується в алгоритмі Keccak (SHA-3, SHAKE) і забезпечує гнучкість, паралельність та високу стійкість до атак. Sponge-конструкції також можуть бути використані для побудови PRF, MAC та генераторів випадкових чисел.

Атака типу Photon Number Splitting (PNS) - це атака на системи QKD, яка використовує багатофотонні імпульси, що іноді виникають у реальних джерелах. Зловмисник може “відщепити” один фотон для себе, а інші передати далі, не порушуючи квантовий стан. Це дозволяє йому отримати частину ключа без виявлення. Для захисту від PNS використовують однофотонні джерела, атенюатори, протоколи з детекцією багатофотонних імпульсів (наприклад, decoy states). PNS є однією з головних практичних загроз для QKD.