УДК 004.056

В. Ю. Юра
Ю. Є. Яремчук

РОЗРОБКА СИСТЕМИ АДАПТИВНОГО ПОСТКВАНТОВОГО ЗАХИСТУ НА БАЗІ ГІБРИДНОЇ СХЕМИ AES+ML-KEM ІЗ МЕХАНІЗМАМИ АПАРАТНОЇ ПРИВ'ЯЗКИ ТА АКТИВНОЇ ДЕЗІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі запропоновано систему локального захисту файлів, орієнтовану на постквантову стійкість, прив'язку ключового сховища до пристрою та приховану поведінку в неавторизованому середовищі. Гібридний контур AES-256-GCM + ML-KEM-1024 використовується для поєднання швидкого автентифікованого шифрування даних із постквантовим механізмом інкапсуляції ключового матеріалу. Для зниження ризику перенесення ключів на інший комп'ютер застосовано HWID-прив'язку локального сховища my_keys.pqc. У разі невідповідності апаратного контексту система переходить у Intruder Mode та формує honey output замість прямого повідомлення про відмову.

Ключові слова: постквантова криптографія, ML-KEM, AES-GCM, HWID, апаратна прив'язка, honey output, локальний захист файлів.

Abstract

The paper presents a local file protection system focused on post-quantum readiness, hardware binding of key storage, and stealth behavior in an unauthorized environment. The AES-256-GCM + ML-KEM-1024 hybrid cryptographic scheme combines fast authenticated file encryption with a post-quantum key encapsulation mechanism. To reduce the risk of using copied keys on another device, HWID binding is applied to the my_keys.pqc local key storage. If the hardware context does not match the authorized device, the system switches to Intruder Mode and generates honey output instead of a direct access denial.

Keywords: post-quantum cryptography, ML-KEM, AES-GCM, HWID, hardware binding, honey output, local file protection.

Вступ

Локальні файли користувача часто містять дані, які залишаються цінними протягом тривалого часу: документи, резервні копії, конфігураційні файли, архіви та службові матеріали. Для таких даних недостатньо враховувати лише поточний рівень обчислювальних можливостей зловмисника. Розвиток квантових обчислень посилює актуальність сценарію «збери зараз — розшифруй пізніше», коли зашифровані артефакти можуть бути викрадені до появи практично доступних засобів їх розкриття [1].

Класичні засоби файлового шифрування переважно будуються за схемою «правильний ключ — доступ, неправильний ключ — відмова». Така модель забезпечує базову конфіденційність, однак не усуває ризик перенесення контейнера і ключового матеріалу на інший пристрій та не приховує факт спрацювання захисту. Тому для локального сховища файлів доцільним є поєднання криптографічної стійкості, прив'язки до середовища виконання та поведінкового рівня протидії несанкціонованому запуску.

Метою роботи є розробка системи адаптивного постквантового захисту локальних файлів на основі гібридної схеми AES-256-GCM + ML-KEM-1024 із HWID-прив'язкою ключового сховища та механізмом активної дезінформації у неавторизованому середовищі.

Результати дослідження

У запропонованій системі криптографічний контур поділено на два рівні. ML-KEM-1024 використовується для інкапсуляції ключового матеріалу та отримання спільного секрету, а безпосереднє шифрування вмісту файла виконується алгоритмом AES-256-GCM. Такий розподіл дозволяє не шифрувати великий файл постквантовим механізмом, а застосовувати його лише для захисту ключового матеріалу, тоді як AES-GCM забезпечує швидку обробку даних і перевірку цілісності через тег автентифікації [2].

Під час шифрування формується контейнер .pqc_lock, до якого входять KEM-капсула, параметр nonce, тег автентифікації та зашифрований вміст файла. Локальне сховище ключів my_keys.pqc

захищається окремим device key, що формується на основі апаратного відбитка пристрою. У разі перенесення ключового файла на інший комп'ютер змінюється апаратний контекст, тому коректне відновлення локального сховища ключів стає неможливим.

На відміну від базового підходу, за якого файл захищається лише симетричним ключем або паролем, розроблена система додатково контролює середовище виконання. Якщо звичайний AES-шифратор після перенесення ключа може залишати можливість повторних спроб дешифрування на сторонньому пристрої, то у запропонованій схемі просте копіювання .pqc_lock та my_keys.pqc не забезпечує доступу до реального ключового матеріалу без збігу HWID.

Другий рівень захисту пов'язаний не з математичною стійкістю алгоритмів, а з поведінкою застосунку. У разі невдалого відкриття my_keys.pqc система не видає пряме повідомлення про відмову, а переходить у Intruder Mode. У цьому режимі імітується успішне виконання операції та формується правдоподібний фейковий результат — honey output. Ідея такого підходу узгоджується з концепцією Honey Encryption, у якій некоректна спроба доступу не обов'язково завершується явною помилкою, а може давати правдоподібний хибний результат [3].

На рис. 1 показано логіку вибору режиму роботи системи. Ключовою умовою є можливість розкрити локальне сховище my_keys.pqc за допомогою device key. Якщо це вдається, система переходить у Owner Mode і працює з реальними ключами. Якщо розшифрування сховища неможливе, активується Intruder Mode, у якому замість справжнього дешифрування формується honey output.

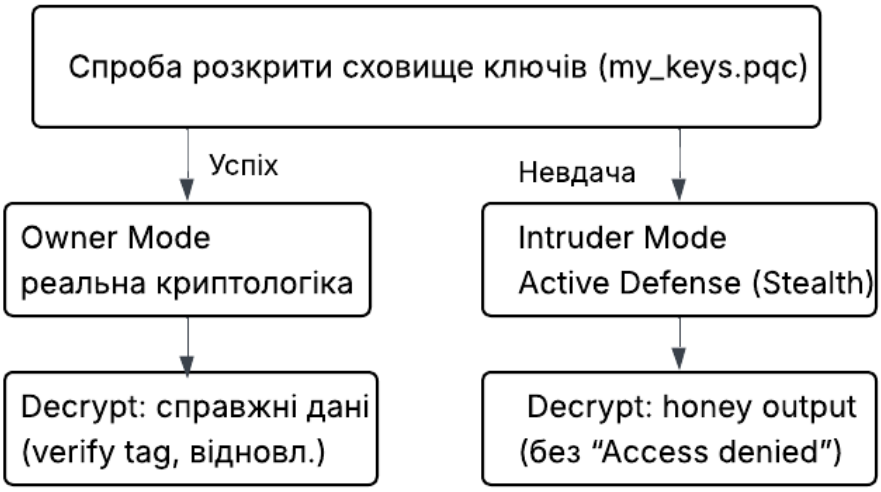

Рисунок 1 – Логіка переходу між Owner Mode та Intruder Mode у розробленій системі

Практична реалізація включає модулі ML-KEM-1024, AES-256-GCM, керування ключами, HWID-прив'язки, генерації honey output, графічного інтерфейсу, журналювання та фонового виконання криптографічних операцій. Виконання шифрування і дешифрування у фоновому потоці дає змогу зберегти доступність інтерфейсу під час роботи з файлами більшого розміру.

Перевірка роботи прототипу охоплювала штатне шифрування і дешифрування на авторизованому пристрої, реакцію на пошкодження контейнера, запуск у неавторизованому середовищі та формування honey output. У штатному режимі система відновлює початковий вміст файла. При зміні або пошкодженні контейнера перевірка тега AES-GCM не проходить, тому відкритий текст не видається. Якщо система запускається в іншому апаратному контексті, ключове сховище не розкривається, а користувач отримує фейковий результат без явного повідомлення про відмову.

Отримані результати показують, що запропоноване удосконалення розширює можливості звичайного файлового шифрування. Гібридний контур забезпечує постквантову готовність керування ключовим матеріалом, HWID-прив'язка обмежує перенесення ключового сховища на інший пристрій, а механізм honey output зменшує інформативність реакції системи для потенційного зловмисника.

Висновки

У роботі запропоновано систему адаптивного постквантового захисту локальних файлів, яка поєднує ML-KEM-1024, AES-256-GCM, HWID-прив'язку та механізм активної дезінформації.

Обґрунтовано, що ML-KEM доцільно використовувати для захисту ключового матеріалу, а AES-GCM — для швидкого автентифікованого шифрування вмісту файлів.

Розроблено структуру контейнера .pqc_lock, локальне сховище ключів my_keys.pqc і логіку роботи у режимах Owner Mode та Intruder Mode. Під час перевірки підтверджено працездатність основних сценаріїв: шифрування і відновлення файлів на авторизованому пристрої, невидачу відкритого тексту при порушенні цілісності контейнера та формування honey output у неавторизованому середовищі. Подальше вдосконалення системи доцільно пов’язати з інтеграцією TPM або Windows DPAPI, розширенням набору honey-шаблонів і кількісним порівнянням продуктивності базового AES-шифрування та гібридної схеми.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology, 2024. [Електронний ресурс]. Режим доступу до ресурсу: https://csrc.nist.gov/pubs/fips/203/final

2. NIST SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology, 2007. [Електронний ресурс]. Режим доступу до ресурсу: https://csrc.nist.gov/pubs/sp/800/38/d/final

3. Juels A., Ristenpart T. Honey Encryption: Security Beyond the Brute-Force Bound. Advances in Cryptology – EUROCRYPT 2014. Springer, 2014.

4. Microsoft. BitLocker overview. Microsoft Learn. [Електронний ресурс]. Режим доступу до ресурсу: https://learn.microsoft.com/windows/security/operating-system-security/data-protection/bitlocker/

Юра Владислав Юрійович – студент групи 1КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vladyuravnt@gmail.com

Яремчук Юрій Євгенович – доктор технічних наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Yura Vladyslav Yuriyovych. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: vladyuravnt@gmail.com

Yaremchuk Yurii Yevhenovych – Doctor of Technical Sciences, Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, Ukraine.