https://doi.org/10.31891/2219-9365-2025-84-36
УДК 004.056.55+004.738.5+004.75

ШКІТОВ Андрій
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0005-4600-8467
e-mail: opncore@gmail.com
АВДАЛОВ Герман
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0007-7728-6659
Germannavdalov@gmail.com

ОЦІНЮВАННЯ ПРОДУКТИВНОСТІ ГІБРИДНИХ КРИПТОГРАФІЧНИХ СХЕМ ПРИ ВПРОВАДЖЕННІ У СИСТЕМИ З ОБМЕЖЕНИМИ РЕСУРСАМИ В УМОВАХ КВАНТОВОЇ ЗАГРОЗИ

У статті представлено результати дослідження продуктивності гібридної криптографічної схеми, орієнтованої на мікроконтролерні системи з обмеженими ресурсами. Запропонована архітектура поєднує постквантовий алгоритм Kyber512, що використовується для захищеного обміну ключами, з потоковим симетричним шифром ChaCha20-Poly1305, який забезпечує шифрування основного потоку даних. Реалізацію здійснено на апаратній платформі STM32F407VGT6 під керуванням операційної системи FreeRTOS із використанням механізмів DMA та RNG для оптимізації обчислень. У ході експериментів проведено оцінювання часу виконання, енергоспоживання, використання пам'яті, мережевої затримки та навантаження на процесор.

Результати продемонстрували, що гібридна схема забезпечує постквантову стійкість без суттєвої втрати продуктивності: середній час обробки пакета становить 8475 мкс, споживання енергії — 6.89 мДж, що є прийнятними параметрами для пристроїв класу STM32F4. Зростання навантаження на CPU не перевищує 53%, а збільшення мережевої затримки є незначним. Запропоноване рішення підтвердило свою ефективність у контексті застосувань, де важливо досягнути балансу між безпекою та енергетичною ефективністю, зокрема у системах телеметрії, моніторингу довкілля, енергетичних та медичних пристроях.

Отримані результати свідчать про доцільність впровадження гібридних криптографічних схем у реальні вбудовані системи, а також створюють підґрунтя для подальших досліджень адаптивних постквантових протоколів, здатних самостійно регулювати криптографічне навантаження залежно від стану ресурсів пристрою.

Ключові слова: постквантова криптографія, гібридна схема, Kyber512, ChaCha20-Poly1305, STM32, FreeRTOS.

SHKITOV Andrii, AVDALOV German
Open International University of Human Development Ukraine

EVALUATION OF THE PERFORMANCE OF HYBRID CRYPTOGRAPHIC SCHEMES WHEN IMPLEMENTED IN SYSTEMS WITH LIMITED RESOURCES IN CONDITIONS OF QUANTUM THREAT

This paper presents an experimental evaluation of a hybrid cryptographic scheme tailored for resource-constrained embedded systems facing quantum threats. The scheme combines Kyber512, a post-quantum key exchange algorithm, with the ChaCha20-Poly1305 stream cipher for secure, efficient data encryption.

Implementation was carried out on the STM32F407VGT6 microcontroller (ARM Cortex-M4, 168 MHz, 1 MB Flash, 192 KB RAM) using FreeRTOS and the lwIP network stack for UDP transmission. Hardware features such as DMA and RNG were leveraged to offload cryptographic processing and ensure high throughput. During initialization, Kyber512 is used to establish a secure symmetric key, which is then applied in ChaCha20-Poly1305 for encryption and authentication of telemetry packets.

Performance was evaluated across key metrics: execution time, RAM/Flash usage, energy consumption, network delay, and CPU load. Tests were conducted for three configurations: ChaCha20-Poly1305 only, Kyber512 only, and the full hybrid scheme. Results show the hybrid setup achieved 8475 µs average execution time, 6.89 mJ energy per cycle, and moderate memory use (9376 bytes RAM). CPU load did not exceed 53%, and network delay increased only slightly to 0.4 ms – acceptable for real-time applications.

The hybrid scheme ensures quantum-resistant key exchange with minimal performance loss in the main data flow. Post-quantum operations are performed once per session, while the symmetric cipher handles continuous encryption efficiently. The design proves suitable for low-power systems such as environmental monitoring, medical telemetry, and industrial IoT.

Future work includes testing on other platforms (ESP32-S3, RISC-V), integration with MQTT, LoRa, BLE, and exploration of adaptive cryptographic scheduling and resilience to side-channel threats. The results highlight the feasibility of post-quantum hybrid cryptography for embedded systems operating under strict resource constraints.

Keywords: post-quantum cryptography, hybrid scheme, Kyber512, ChaCha20-Poly1305, STM32, FreeRTOS.

Стаття надійшла до редакції / Received 30.09.2025
Прийнята до друку / Accepted 27.10.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Швидкий розвиток квантових обчислень становить потенційну загрозу для класичних криптографічних алгоритмів, що використовуються для забезпечення конфіденційності, цілісності та автентичності даних у цифрових системах [1]. Особливо вразливими до таких загроз є системи з обмеженими ресурсами, до яких належать вбудовані пристрої, сенсорні вузли IoT-мереж, мобільні платформи, пристрої з енергонезалежною пам'яттю, мікроконтролери тощо [2]. Через обмежену обчислювальну потужність, невелику кількість пам'яті та енергоспоживання вони не здатні ефективно виконувати обчислення, пов'язані з сучасними постквантовими алгоритмами, які зазвичай мають високу складність [3].

У цих умовах гібридні криптографічні схеми, що поєднують постквантові алгоритми з класичними симетричними або полегшеними методами, розглядаються як перспективний напрям, здатний забезпечити збалансоване співвідношення між безпекою та продуктивністю. Проте виникає нагальна потреба в дослідженні ефективності таких гібридних схем саме в контексті обмежених обчислювальних середовищ, оскільки навіть незначне збільшення криптографічного навантаження може призвести до деградації роботи системи, підвищення часу відгуку або надмірного енергоспоживання.

Сучасна наукова спільнота зосереджує увагу на стандартизації постквантових алгоритмів (зокрема, в рамках ініціативи NIST PQC), однак недостатньо уваги приділяється питанням їх практичного впровадження в реальні, ресурсно-обмежені пристрої. Існує також обмежена кількість експериментальних оцінок ефективності гібридних підходів з урахуванням особливостей конкретних апаратних архітектур (наприклад, STM32, ESP32), операційних середовищ (FreeRTOS, Zephyr) та протоколів зв'язку (LoRa, MQTT, BLE).

У зв'язку з цим важливо здійснити проєктування та експериментальну перевірку гібридних криптографічних схем, які поєднують елементи постквантового та симетричного шифрування і є придатними для використання у системах з обмеженими ресурсами. Особливу увагу слід приділити оцінюванню продуктивності таких рішень в умовах реального середовища з урахуванням обмежень щодо пам'яті, обчислювальної потужності та енергоспоживання. Метою дослідження є оцінювання ефективності гібридних криптографічних схем при впровадженні у вбудовані обчислювальні середовища, зокрема на базі STM32, в умовах потенційних квантових загроз.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематика стійкості криптографічних засобів до квантових атак активно досліджується впродовж останнього десятиліття [4]. Із зростанням обчислювальних можливостей квантових комп'ютерів зростає ризик компрометації класичних алгоритмів, таких як RSA, DSA, ECDSA, що базуються на задачах факторизації або обчислення дискретного логарифму [5]. У відповідь на ці виклики Національний інститут стандартів і технологій США (NIST) ініціював багаторічний процес стандартизації постквантових криптографічних алгоритмів, у рамках якого у 2022 році було обрано першу хвилю кандидатів, зокрема алгоритми Kyber (для шифрування) та Dilithium (для цифрового підпису) [6].

У науковій літературі все частіше з'являються роботи, що присвячені впровадженню постквантових алгоритмів у системи з обмеженими ресурсами. Так, у [7] розглянуто складнощі імплементації алгоритмів сімейства CRYSTALS на мікроконтролерах ARM Cortex-M, зокрема в контексті обмеженого обсягу пам'яті. Інші дослідники [8] акцентують увагу на значному навантаженні на CPU під час реалізації алгоритмів на решті вбудованих систем, що ставить під сумнів можливість їх повноцінного використання у сенсорних мережах.

Одним із підходів до зниження обчислювального навантаження є використання гібридних криптографічних схем, які комбінують постквантові алгоритми (наприклад, Kyber, BIKE, NTRU) із симетричними методами (AES, ChaCha20, Grain) або полегшеними алгоритмами шифрування (наприклад, SPECK, PRESENT, GIFT). У [9] продемонстровано, що поєднання Kyber512 з AES-GCM дозволяє значно зменшити час обробки даних порівняно з виключно постквантовим підходом. Аналогічні результати були отримані у [10], де оцінювалась продуктивність гібридних схем на STM32F4 для IoT-додатків, з акцентом на адаптивне перемикання між шифрувальними блоками залежно від поточних ресурсних умов пристрою.

Публікації останніх років також торкаються впровадження таких схем у контексти реального застосування. Зокрема, у [11] проаналізовано ефективність гібридного шифрування в системах телеметрії для енергомоніторингу, а в [12] досліджено поведінку гібридних криптографічних модулів у розподілених медичних сенсорних системах. У [13] підкреслено потребу в стандартизованих критеріях оцінювання ефективності таких схем – з урахуванням часу виконання, використання пам'яті, стійкості до атак сторонніх каналів та енергоспоживання.

Водночас більшість наявних досліджень зосереджуються або на математичних властивостях алгоритмів, або на загальних архітектурних рішеннях, тоді як питання реального експериментального порівняння гібридних схем у конкретних апаратних середовищах залишається відкритим. У цьому контексті недостатньо вивченими залишаються аспекти інтеграції гібридного захисту в системах з реальними обмеженнями – такими як STM32 або ESP32 – під керуванням FreeRTOS чи Zephyr, із врахуванням обмежень на тактову частоту, обсяг пам'яті й енергоспоживання.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Гібридні криптографічні схеми, що поєднують класичні симетричні та постквантові алгоритми, стають ключовим підходом для захисту даних в умовах очікуваного зростання обчислювальної потужності квантових машин [14]. У запропонованій реалізації використано комбінацію симетричного потокового шифру ChaCha20-Poly1305 та криптографічного алгоритму на основі ґраток Kyber512, який пройшов третій раунд відбору в рамках ініціативи NIST PQC та рекомендований до стандартизації для цілей забезпечення стійкого обміну ключами [15].

Логіка взаємодії складових у цій гібридній схемі передбачає, що Kyber512 використовується на етапі ініціалізації з'єднання для генерації спільного симетричного сеансового ключа, який у подальшому застосовується в ChaCha20-Poly1305 для забезпечення конфіденційності та автентичності основного потоку даних. Така побудова дозволяє суттєво зменшити обчислювальне навантаження на пристрій, оскільки дорогі з обчислювальної точки зору операції Kyber виконуються лише один раз на початку сесії, тоді як високошвидкісний ChaCha20-Poly1305 використовується для потокового шифрування.

У контексті цього дослідження схема реалізована для захисту телеметричних даних у сенсорній системі моніторингу з передачею даних протоколом UDP через стек lwIP. Захист даних здійснюється на транспортному рівні, без втручання в прикладну логіку, шляхом вбудовування блоку шифрування у гілку формування пакета безпосередньо перед його відправленням у мережевий стек. Це дозволяє зберегти прозорість реалізації та зменшити ризики конфліктів з протоколами верхнього рівня. Основна цільова група даних – пакети розміром від 256 до 1024 байт, що є типовим обсягом у системах безперервного збору екологічних, технічних або фізіологічних параметрів.

Реалізація розроблена з урахуванням обмежень обчислювальних ресурсів мікроконтролера STM32F407VGT6, зокрема обмеженого обсягу оперативної пам’яті (192 КБ), обмеженого обсягу Flash (1 МБ), відсутності апаратної підтримки постквантових операцій та жорстких вимог до енергоспоживання [16]. У зв’язку з цим в архітектуру впроваджено механізми буферизації з використанням DMA для передачі зашифрованих блоків, а також циклічні черги на базі SRAM для ефективного розподілу завантаження між потоками шифрування та обробки пакетів.

Загальна структура побудованого криптографічного модуля представлена на рисунку 1.

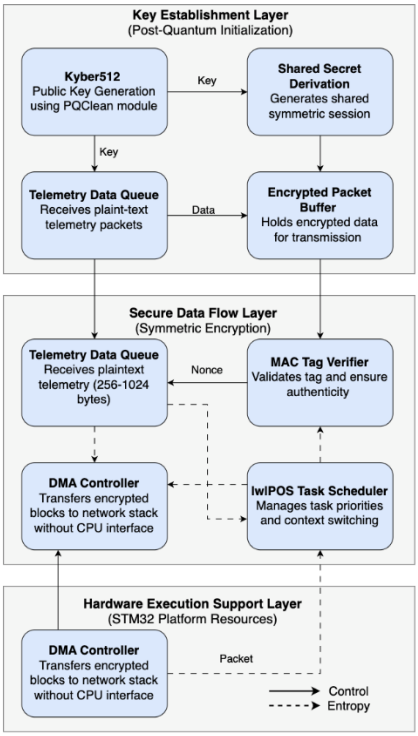

Рис. 1 Архітектура гібридної криптографічної схеми з використанням Kyber512 та ChaCha20-Poly1305

На верхньому рівні реалізовано ініціалізаційний етап, у межах якого відбувається обмін публічними параметрами та формування спільного симетричного ключа за допомогою постквантового алгоритму Kyber512. Далі цей ключ передається у модуль симетричного шифрування ChaCha20-Poly1305, який забезпечує шифрування основного потоку даних та перевірку їхньої автентичності через тег MAC. На нижньому рівні архітектури розміщено апаратні ресурси мікроконтролера STM32, зокрема контролер прямого доступу до пам’яті (DMA), генератор випадкових чисел (RNG) і таймери, які синхронізують процес шифрування з мережею.

Інтеграція цієї архітектури у середовище FreeRTOS дозволяє забезпечити паралельне виконання криптографічних операцій і мережевих задач, що підвищує пропускну здатність системи без істотного зростання споживання енергії. Така організація дає змогу мінімізувати час затримки при передачі телеметричних даних і забезпечити їх захист навіть у разі потенційного компрометування окремих каналів зв'язку в умовах квантової загрози.

Для реалізації гібридної криптографічної схеми використано апаратну платформу STM32F407VGT6, яка побудована на базі ядра ARM Cortex-M4 з тактовою частотою 168 МГц, обсягом 1 МБ Flash-пам'яті та 192 КБ оперативної пам'яті (SRAM). Вибір цієї платформи обумовлений її широким застосуванням у пристроях з обмеженими ресурсами, стабільною підтримкою інструментів розробки, а також наявністю апаратних модулів, таких як DMA-контролер, апаратний RNG, таймери високої точності та периферія для мережевого інтерфейсу. Реалізація проводилася у середовищі STM32CubeIDE, з використанням STM32CubeMX для генерації ініціалізаційного коду.

Програмна реалізація включала інтеграцію з операційною системою FreeRTOS та мережевим стеком lwIP, що дозволило забезпечити багатозадачність та підтримку транспортного протоколу UDP. Система призначена для передачі телеметричних даних (температури, вологості, енергоспоживання тощо) на віддалений вузол або базову станцію через інтерфейс Ethernet. На рівні прикладної логіки використано C/C++, із залученням апаратних регістрів і CMSIS-драйверів для оптимізації продуктивності.

Гібридна криптографічна схема реалізована у вигляді окремого FreeRTOS-завдання, яке взаємодіє з буферами телеметричних даних через черги і семафори. На першому етапі, під час ініціалізації, викликається функція з бібліотеки PQClean, яка реалізує алгоритм Kyber512. Вона генерує пару ключів (публічний та приватний) і ініціює процедуру обміну ключами з віддаленою стороною. Отриманий сеансовий ключ зберігається у захищеній області пам'яті SRAM.

Після встановлення симетричного ключа викликається модуль ChaCha20-Poly1305, реалізований на основі бібліотеки TinyCrypt. Дані з буфера збираються у блок розміром 512 байт, шифруються з додаванням автентифікаційного тегу MAC, після чого результат зберігається у вихідному буфері. Для кожного блоку виконується валідація довжини, генерація унікального 96-бітного nonce (на основі таймера TIM2) та контроль цілісності за допомогою тега.

Передача зашифрованих даних відбувається через UDP, використовуючи функції netconn_write() з бібліотеки lwIP. Паралельно із процесом шифрування дані передаються до DMA-контролера, що дозволяє мінімізувати навантаження на процесор і збільшити пропускну здатність.

Важливою особливістю є те, що обмін ключами виконується лише один раз при старті сесії або перезавантаженні пристрою. Надалі використовується вже встановлений симетричний ключ, який оновлюється або за таймером, або за кількістю переданих пакетів.

Для об'єктивного оцінювання продуктивності запропонованої гібридної криптографічної схеми було визначено критичні метрики, релевантних для вбудованих систем з обмеженим обсягом пам'яті, низьким енергобюджетом і вимогами до часової чутливості. До таких метрик належать:

1. Час виконання окремих криптографічних операцій.
2. Споживання оперативної пам'яті.
3. Енергоспоживання під час криптографічного циклу.
4. Затримка в мережевій передачі зашифрованих даних.

Усі вимірювання проводилися у реальному часі з використанням осцилографа Tektronix MDO3054 для вимірювання енергоспоживання через шунт на лінії живлення, а також вбудованого таймера TIM2 для високоточного обчислення часу виконання. Споживання пам'яті аналізувалося на етапі компіляції за виводами компілятора GCC, з розбиттям по сегментах .text, .data та .bss. Результати вимірювань узагальнено у таблиці 1. Усі тести проводилися при однакових умовах: живлення 3.3 В, частота 168 МГц, без зовнішнього навантаження на інші периферійні модулі.

Таблиця 1

Результати продуктивності криптографічних схем на STM32F407VGT6

Параметр	ChaCha20-Poly1305	Kyber512 (обмін ключами)	Гібридна схема (Kyber512 + ChaCha20)
Середній час виконання, мкс	144	8347	8475
Максимальний час, мкс	158	8412	8511
Мінімальний час, мкс	139	8281	8432
Споживання RAM, байт	5568	8740	9376
Споживання Flash, байт	9280	14064	17852
Споживання енергії, мДж	0.74	6.21	6.89
Мережева затримка, мс	0.3	0.3	0.4
Навантаження на CPU, % (FreeRTOS)	12	49	53

Вимірювання здійснювалися на трьох конфігураціях криптографічної обробки:

1. ChaCha20-Poly1305 окремо (без обміну ключами).
2. Kyber512 окремо (одноразове встановлення ключа).

3. Гібридна схема Kyber512 + ChaCha20-Poly1305 (повний ланцюг).

Для кожного випадку здійснювалося серійне тестування на 1000 пакетах даних розміром 512 байт з формуванням середнього, мінімального та максимального часу виконання. Було також зафіксовано кількість циклів CPU для кожної криптографічної операції з використанням вбудованих засобів трасування ARM DWT (Data Watchpoint and Trace).

Як демонструють результати, наведені у таблиці 1, гібридна криптографічна схема Kyber512 + ChaCha20-Poly1305 характеризується вищими показниками використання ресурсів порівняно з класичним симетричним шифруванням, проте вона забезпечує стійкість до квантових атак на етапі обміну ключами, зберігаючи при цьому прийнятну продуктивність на етапі потокового шифрування. Середній час виконання повного циклу криптографічної обробки у гібридному варіанті становить 8475 мкс, що лише на 1.5% перевищує аналогічний показник для ізольованого використання Kyber512, і на порядок вищий за час, необхідний для шифрування тільки за допомогою ChaCha20-Poly1305. Проте варто зазначити, що операції Kyber512 виконуються лише одноразово – під час ініціалізації – тоді як основний обсяг переданих даних обробляється симетричним алгоритмом із високою швидкодією.

Що стосується використання оперативної пам’яті, то гібридна схема потребує 9376 байт, що на 1808 байт більше за Kyber512 і на 3808 байт більше порівняно з ChaCha20-Poly1305. Збільшення пам’яті пояснюється одночасним зберіганням ключових структур двох криптографічних алгоритмів, а також додатковими буферами для потокового шифрування та автентифікації. Попри це, загальне споживання пам’яті не перевищує 10 КБ, що є допустимим для мікроконтролерів класу STM32F4.

Особливу увагу варто звернути на показники енергоспоживання. Вимірювання за допомогою осцилографа продемонстрували, що гібридна схема споживає 6.89 міліджоулів на цикл обробки, що лише на 0.68 мДж перевищує ізольований випадок Kyber512. Водночас класичне симетричне шифрування потребує у 9 разів менше енергії (0.74 мДж), проте не забезпечує жодного захисту від квантових атак. Таким чином, енергетичні витрати гібридного підходу цілком виправдані у критичних застосуваннях, де безпека стоїть на першому місці.

Мережева затримка, яка вимірювалась як різниця між моментом ініціалізації відправки пакета та моментом завершення його формування, зросла з 0.3 мс (у класичних реалізаціях) до 0.4 мс у гібридному варіанті. Таке збільшення є несуттєвим для більшості систем телеметрії, де прийнятним вважається діапазон до 1 мс. Аналогічно, пікове навантаження на CPU в середовищі FreeRTOS зросло до 53%, що все ще залишає ресурс для виконання паралельних завдань, таких як обробка сенсорних даних, логування чи передача пакетів у високопріоритетному контексті.

Аналіз навантаження на процесор показав, що при серійному шифруванні 1000 пакетів гібридна схема забезпечує стабільну продуктивність, без деградації системної реакції або перевищення тайм-аутів задач. Цьому сприяє ефективне розподілення обробки за допомогою механізмів планування FreeRTOS, а також використання DMA для вивільнення ядра від рутинної передачі байтів у мережевий стек.

Окремо варто підкреслити, що наявність Kyber512 у складі системи жодним чином не впливає на критичні ділянки потоку даних після ініціалізації. Отриманий симетричний ключ зберігається в SRAM та використовується протягом усієї сесії, а оновлення ключів виконується лише за подією – таймером, рестартом пристрою або перевищенням встановленого порогу кількості пакетів. Це дозволяє мінімізувати витрати на постквантові обчислення та водночас гарантувати захищеність від квантових загроз при збереженні високої пропускної здатності.

Таким чином, результати експериментального дослідження свідчать про практичну придатність запропонованої гібридної криптографічної схеми для впровадження у реальні системи з обмеженими ресурсами. За умов правильної інтеграції у середовище FreeRTOS та грамотної організації буферів пам’яті, така схема дозволяє забезпечити сучасний рівень безпеки без критичного погіршення продуктивності, затримок чи енергетичного профілю системи. Вона є особливо актуальною для застосування в галузях екологічного моніторингу, енергетики, медицини, індустрії 4.0, де безперервний обмін чутливими даними має відбуватися в умовах невисокого енергобюджету та обмежених апаратних ресурсів.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті запропоновано та експериментально досліджено гібридну криптографічну схему, яка поєднує постквантовий алгоритм Kyber512 для обміну ключами та симетричний потоковий шифр ChaCha20-Poly1305 для шифрування основного трафіку. Реалізація орієнтована на мікроконтролери з обмеженими ресурсами, зокрема STM32F407VGT6, і враховує обмеження щодо обсягу пам’яті, обчислювальної потужності та енергоспоживання.

Проведені експерименти засвідчили, що запропоноване рішення забезпечує постквантову стійкість на етапі встановлення з’єднання, не призводячи до істотної деградації швидкодії або зростання навантаження на системні ресурси. Гібридна схема продемонструвала прийнятні показники часу виконання, споживання енергії та затримки в мережевій передачі даних, що дозволяє її інтеграцію у реальні сенсорні системи

моніторингу. Застосування FreeRTOS та апаратних механізмів DMA і RNG забезпечило ефективну організацію обчислень і розподіл навантаження в умовах багатозадачності.

Перспективи подальших досліджень полягають у розширенні експериментальної бази шляхом тестування схеми на інших платформах (наприклад, ESP32-S3, RISC-V), адаптації до інших протоколів передачі даних (MQTT, LoRa, BLE), дослідженні поведінки системи в умовах атак сторонніх каналів та оцінці стійкості до різних сценаріїв компрометації ключів. Також доцільно вивчити можливості адаптивного керування криптографічним навантаженням залежно від поточних ресурсних умов пристрою та розробити механізми відновлення ключів у разі збоїв з урахуванням вимог до безпеки.

З урахуванням результатів роботи запропонований підхід може бути основою для формування універсального криптографічного модуля для захисту чутливих даних в embedded-системах нового покоління, що працюють в умовах постійно зростаючого рівня загроз, включаючи квантові виклики.

Література

1. Tom, J. J., Anebo, N. P., Onyekwelu, B. A., Wilfred, A., & Eyo, R. E. (2023). Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol, 12(5), 25-38.
2. Goyal, S. B., Islam, S. M., Rajawat, A. S., & Singh, J. (2024). Quantum computing in the era of IoT: Revolutionizing data processing and security in connected devices. In Applied Data Science and Smart Systems (pp. 552-559). CRC Press.
3. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Innovative resource-saving security strategies for IoT devices. Journal of Edge Computing, 4(1), 35-56.
4. Лісовський П.М., Лісовська Ю.П., Шкітов А.А. Феноменологія кібербезпеки: воєнно-правовий стан захищеності інформаційного капіталу в обороноздатній інфраструктурі України: монографія. Київ: Ліра-К, 2025, 860 с.
5. Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. (2020, August). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In Annual International Cryptology Conference (pp. 62-91). Cham: Springer International Publishing.
6. Dziechciarz, D., & Niemiec, M. (2024). Efficiency analysis of NIST-standardized post-quantum cryptographic algorithms for digital signatures in various environments. Electronics, 14(1), 70.
7. Żyliński, M., Nassibi, A., & Mandic, D. P. (2023). Design and implementation of an atrial fibrillation detection algorithm on the ARM cortex-M4 microcontroller. Sensors, 23(17), 7521.
8. Paulino, N., Ferreira, J. C., & Cardoso, J. M. (2020). Improving performance and energy consumption in embedded systems via binary acceleration: A survey. ACM Computing Surveys (CSUR), 53(1), 1-36.
9. Lin, M. B., & Chuang, J. H. (2023). The design of a high-throughput hardware architecture for the AES-GCM algorithm. IEEE Transactions on Consumer Electronics, 70(1), 425-432.
10. Rzepka, K., Szary, P., Cabaj, K., & Mazurczyk, W. (2024). Performance evaluation of Raspberry Pi 4 and STM32 Nucleo boards for security-related operations in IoT environments. Computer Networks, 242, 110252.
11. Almihyawi, A. Y. T. (2025). A secure smart monitoring network for hybrid energy systems using IoT, AI. Discover Computing, 28(1), 1-19.
12. Rozlomii I., Yarmilko A., Naumenko S. Resource-Efficient Solutions for Data Security at the Network Level of the Medical Internet of Things. In: Proceedings of the 7th International Conference on Informatics & Data-Driven Medicine (IDDM'2024). P. 171–182, 2024.
13. Subramanian, A., & Donta, L. S. (2024, May). Assessing the strength of hybrid cryptographic algorithms: A comparative study. In 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-6). IEEE.
14. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. IEEE Access, 12, 23206-23219.
15. Escribano Pablos, J. I., & González Vasco, M. I. (2023). Secure post-quantum group key exchange: Implementing a solution based on Kyber. IET Communications, 17(6), 758-773.
16. Shen, Y. (2024, May). Design and construction of computer laboratory security monitoring system based on STM32 microcontroller. In Fourth International Conference on Telecommunications, Optics, and Computer Science (TOCS 2023) (Vol. 13161, pp. 105-116). SPIE.

References

1. Tom, J. J., Anebo, N. P., Onyekwelu, B. A., Wilfred, A., & Eyo, R. E. (2023). Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol, 12(5), 25-38.
2. Goyal, S. B., Islam, S. M., Rajawat, A. S., & Singh, J. (2024). Quantum computing in the era of IoT: Revolutionizing data processing and security in connected devices. In Applied Data Science and Smart Systems (pp. 552-559). CRC Press.
3. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Innovative resource-saving security strategies for IoT devices. Journal of Edge Computing, 4(1), 35-56.
4. Lisovsky P.M., Lisovska Yu.P., Shkitov A.A. Phenomenology of cybersecurity: military-legal state of information capital security in the defense infrastructure of Ukraine: monograph. Kyiv: Lira-K, 2025, 860 p.
5. Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. (2020, August). Comparing the difficulty of

factorization and discrete logarithm: a 240-digit experiment. In Annual International Cryptology Conference (pp. 62-91). Cham: Springer International Publishing.

6. Dziechciarz, D., & Niemiec, M. (2024). Efficiency analysis of NIST-standardized post-quantum cryptographic algorithms for digital signatures in various environments. Electronics, 14(1), 70.

7. Żyliński, M., Nassibi, A., & Mandic, D. P. (2023). Design and implementation of an atrial fibrillation detection algorithm on the ARM cortex-M4 microcontroller. Sensors, 23(17), 7521.

8. Paulino, N., Ferreira, J. C., & Cardoso, J. M. (2020). Improving performance and energy consumption in embedded systems via binary acceleration: A survey. ACM Computing Surveys (CSUR), 53(1), 1-36.

9. Lin, M. B., & Chuang, J. H. (2023). The design of a high-throughput hardware architecture for the AES-GCM algorithm. IEEE Transactions on Consumer Electronics, 70(1), 425-432.

10. Rzepka, K., Szary, P., Cabaj, K., & Mazurczyk, W. (2024). Performance evaluation of Raspberry Pi 4 and STM32 Nucleo boards for security-related operations in IoT environments. Computer Networks, 242, 110252.

11. Almihyawi, A. Y. T. (2025). A secure smart monitoring network for hybrid energy systems using IoT, AI. Discover Computing, 28(1), 1-19.

12. Rozlomii I., Yarmilko A., Naumenko S. Resource-Efficient Solutions for Data Security at the Network Level of the Medical Internet of Things. In: Proceedings of the 7th International Conference on Informatics & Data-Driven Medicine (IDDM'2024). P. 171–182, 2024.

13. Subramanian, A., & Donta, L. S. (2024, May). Assessing the strength of hybrid cryptographic algorithms: A comparative study. In 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-6). IEEE.

14. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. IEEE Access, 12, 23206-23219.

15. Escribano Pablos, J. I., & González Vasco, M. I. (2023). Secure post-quantum group key exchange: Implementing a solution based on Kyber. IET Communications, 17(6), 758-773.

16. Shen, Y. (2024, May). Design and construction of computer laboratory security monitoring system based on STM32 microcontroller. In Fourth International Conference on Telecommunications, Optics, and Computer Science (TOCS 2023) (Vol. 13161, pp. 105-116). SPIE.