УДК 004.056.55
DOI: 10.31673/2409-7292.2025.041217

Удовик І. М., Гнатушенко В. В., Лактіонов І. С.

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ ДЛЯ РЕАЛІЗАЦІЇ ПОСТКВАНТОВИХ АЛГОРИТМІВ У ВБУДОВАНИХ СИСТЕМАХ

У статті розглядаються теоретичні, структурні та алгоритмічні основи впровадження постквантових криптографічних методів у програмно-апаратні комплекси (ПАК) вбудованих систем безпеки. Обґрунтовано необхідність переходу до криптографічних рішень, стійких до квантових атак, а також наведено аналіз ефективності основних алгоритмів, стандартизованих NIST. Розроблено концептуальну ієрархічну архітектуру ПАК, що забезпечує реалізацію криптографічних операцій у режимі реального часу за умов обмежених ресурсів. Запропоновано математичні моделі процесів шифрування, верифікації та обміну ключами, а також представлено аналітичні метрики часової та енергетичної ефективності.

Окрему увагу приділено аналізу апаратних прискорювачів та їх впливу на продуктивність криптографічних операцій, що дозволяє значно зменшити часові затримки у порівнянні з програмними реалізаціями. Визначено, що використання спеціалізованих NTT-модулів та оптимізованих механізмів модульної арифметики формує основу для ефективної інтеграції постквантових алгоритмів у мікроконтролерні платформи. Здійснено оцінювання стійкості ПАК до атак на побічні канали та експлуатаційних збурень, що дає змогу сформувати комплексні вимоги до безпеки таких систем. У роботі також розглянуто особливості адаптації криптографічних протоколів до різних класів вбудованих процесорів, включно з RISC-V та ARM-архітектурами. Це забезпечує універсальність запропонованого підходу. Наведені результати демонструють можливість побудови масштабованих та енергоефективних ПАК, здатних забезпечувати надійний захист інформації в умовах зростаючих вимог до стійкості та продуктивності.

Ключові слова: постквантова криптографія; вбудовані системи; програмно-апаратний комплекс; енергетична ефективність; криптографічне прискорення; апаратна архітектура.

Вступ

Поява квантових обчислювальних технологій є одним із найглибших викликів для сучасної криптографії та систем державної та інформаційної безпеки. Квантові алгоритми Шора і Гровера продемонстрували принципову можливість радикального прискорення розв’язання задач, що лежать в основі класичних криптографічних механізмів, насамперед RSA, Диффі–Гелмана та еліптичних кривих. Для цих систем у разі появи квантових комп’ютерів середнього масштабу перестає існувати фундаментальна складність факторизації чи обчислення дискретного логарифма, а отже зникає формальна криптографічна стійкість, що забезпечувала їхню безпеку протягом останніх десятиліть. Це означає, що державні системи зв’язку, військові комунікації, критична інфраструктура, потенційно можуть бути уразливими в будь-який момент, коли квантові обчислення досягнуть практичної масштабності.

Таким чином, потреба переходу до постквантових криптографічних алгоритмів стає не перспективним завданням, а нагальною вимогою безпеки. Однак реальне впровадження цих рішень у промислові, відомчі та спеціалізовані системи стикається з принциповими труднощами.

По-перше, апаратна обмеженість вбудованих систем.

По-друге, інша математична природа постквантових алгоритмів на відміну від класичних.

По-третє, навіть за успішної програмної реалізації постквантової криптографії (PQC), виникає потреба у системній архітектурі, здатній забезпечити:

– контроль криптографічної стабільності;

– адаптивний вибір алгоритму залежно від стану системи;

– стійкість до сторонніх впливів, включаючи атаки на побічні канали.

Таким чином, завдання переходу до постквантових алгоритмів неможливо розглядати лише як заміну однієї бібліотеки шифрування на іншу. Отже, основна проблема полягає у необхідності створення науково обґрунтованої та практично ефективної архітектури програмно-апаратного комплексу, здатного забезпечити повноцінну реалізацію

постквантових криптографічних алгоритмів у вбудованих системах за умов обмежених ресурсів. Така архітектура має бути універсальною, масштабованою, модульною та сумісною з майбутніми стандартами PQC, що робить її ключовим елементом сучасної стратегії кібербезпеки.

Аналіз останніх досліджень та публікацій

Фундаментальні засади квантових алгоритмів, що здатні зламати криптографічний захист сучасних систем безпеки сформульовані у роботі П. Шора, де доведено можливість поліноміального часу факторизації та обчислення дискретного логарифма на квантових комп'ютерах [1]. У аналітичних оглядах Д. Бернштейна та Т. Ланге, сформовано концептуальні засади постквантової криптографії як напряму, що базується на математичних задачах, для яких невідомі ефективні квантові алгоритми [2]. Ключові види таких задач включають задачі на евклідових решітках, кодах Гоппа, мультимножинних структурах, хеш-функціях та ізогеніях еліптичних кривих.

Фундаментальні математичні властивості решіткових алгоритмів викладені у роботах, присвячених задачам LWE, RLWE, MLWE та SIS. Їх практична інтеграція у криптографічні схеми відображена у дослідженнях Боса, Костелло та Найріга, де детально проаналізовано математичні механізми побудови KEM- та Signature-схем на основі решіток і їх стійкість до квантових атак [4].

У паралельних дослідженнях активно формуються алгоритми на основі кодів помилок. McEliece, використовує коди Гоппа та демонструє високий рівень стійкості, включаючи формально доведений рівень безпеки NIST Level 5. Разом реалізація McEliece, має серйозні обмеження, пов'язані з великими ключами та значним навантаженням на пам'ять [6]. Тому він використовується для високорівневих серверних платформ, а не для мікроконтролерів.

Інший підхід до формування постквантових підписів реалізовано у SPHINCS+, який базується виключно на геш-функціях і не залежить від алгебраїчних структур та забезпечує високий рівень криптостійкості навіть у випадку значних математичних або алгоритмічних нововведень [7].

Комплексне дослідження ефективності PQC відбувається в рамках глобального проєкту NIST, результати якого подано у серії технічних звітів та фінальних рекомендацій зі стандартизації [3]. У цих документах наведено експериментальні дані щодо продуктивності алгоритмів на різних апаратних платформах та сформовано висновки щодо їх придатності до реального впровадження. NIST визначив Kyber, Dilithium, Falcon і SPHINCS+ як базові стандарти для захисту комунікацій у майбутніх інформаційних системах.

Особлива увага в літературі приділена питанням апаратних і програмних оптимізацій PQC для вбудованих і мобільних платформ. Дослідження О. Одер та М. Гюнесю показують, що ефективність реалізації алгоритмів MLWE на мікроконтролерах значною мірою залежить від можливості оптимізації операцій перетворення NTT, зменшення кількості викликів модульної арифметики та мінімізації проміжних буферів пам'яті [8]. Навіть за таких умов затримки залишаються суттєвими, що зумовлює потребу комбінувати програмні оптимізації з апаратними прискорювачами.

Ефективність PQC на архітектурах RISC-V досліджена у роботах Банерджі та його колег, де відзначено, що незалежність від комерційних архітектур і можливість кастомізації інструкцій робить RISC-V перспективним напрямом для впровадження постквантових апаратних прискорювачів [9]. Окремі роботи демонструють реалізації Kyber на FPGA, які забезпечують кратне пришвидшення операцій інкапсуляції та декапсуляції порівняно з програмними реалізаціями [10]. Подібні результати підтверджують потенціал апаратно-орієнтованих рішень у системах із жорсткими часовими обмеженнями.

Загалом аналіз літератури демонструє чітку тенденцію: постквантові алгоритми досягли зрілості з точки зору математичної коректності та формальної безпеки, але їх практична реалізація у вбудованих системах потребує спеціалізованих програмно-апаратних комплексів,

© Удовик І. М., Гнатушенко В. В., Лактіонов І. С. (2025) Дослідження архітектури програмно-апаратного комплексу для реалізації постквантових алгоритмів у вбудованих системах. Сучасний захист інформації, 4(64), 81–89. https://doi.org/10.31673/2409-7292.2025.041217

що враховують архітектурні обмеження MCU та SoC, а також особливості роботи систем реального часу. Саме тому дослідження архітектур ПАК, здатних забезпечити стійкість, продуктивність і енергоефективність PQC у складних технічних середовищах, становить ключовий напрям сучасної наукової роботи.

Мета статті

Наукові та практичні виклики, пов'язані з переходом до постквантових криптографічних алгоритмів у вбудованих системах, формують потребу у створенні цілісної концепції, яка забезпечує поєднання високого рівня криптографічної стійкості з можливістю їх реального застосування в умовах обмежених ресурсів. У цьому контексті мета дослідження полягає у формуванні науково обґрунтованої та архітектурно завершеної моделі програмно-апаратного комплексу для реалізації постквантових криптографічних алгоритмів у вбудованих обчислювальних системах. Вказана модель має забезпечувати гарантовану криптографічну стійкість до квантових атак, мінімальну часову латентність операцій, прийнятні енергетичні характеристики, а також високу надійність і стійкість до експлуатаційних впливів, які характерні для сучасних систем зв'язку та систем реального часу.

Мета роботи спрямована не лише на відтворення алгоритмів NIST PQC у вбудованому середовищі, а на комплексне проєктування архітектури, яка охоплює програмні, апаратні та комунікаційні шари, забезпечуючи узгодженість між ними та підтримку динамічного управління криптографічними процесами.

Результати дослідження

Розглядаючи практичні аспекти впровадження постквантових алгоритмів у вбудовані системи, необхідно спиратися на формально визначені математичні моделі, які забезпечують стійкість цих алгоритмів до квантових атак. Основні криптографічні механізми, стандартизовані NIST, базуються на задачах, для яких на даний момент не існує квантових алгоритмів поліноміальної складності [2; 3]. З огляду на специфіку вбудованих платформ математичні моделі повинні бути описані з урахуванням обчислювальної складності, структури даних і типових операцій, які визначають ефективність апаратної реалізації.

Алгоритми Kyber і Dilithium ґрунтуються на задачі модифікованого Learning With Errors. Формально вона описується через вибір кільця:

$$\mathrm{R}_q = \frac{Z_q[x]}{\left(x^n + 1\right)}, \tag{1}$$

де q є простим або степеневим модулем, а nnn визначає ступінь редукції поліномів. У цьому кільці визначається обчислювальна задача:

$$As + e = t \bmod q\ . \tag{2}$$

Шумовий компонент e генерується з вузького розподілу (центрований, дискретний, коефіцієнт варіації мінімальний), що формує складність обернення операції. Наявність цього шуму забезпечує криптографічну стійкість, оскільки квантові алгоритми не пропонують ефективного способу відновлення s за відомих A та t [4].

Формально задача MLWE вважається складною в середньому випадку, і її складність зводиться до задачі Shortest Vector Problem, яка є NP-складною.

У кодових алгоритмах BIKE та Classic McEliece використовується модель, де відновлення повідомлення з матриці перевірки парності з високою структурованістю є складнообчислювальною задачею [6].

Задано матрицю перевірки парності, де структура матриці (квазіциклічність або MDPC-властивості) формує стійкість. Для вхідного вектора с синдром визначається рівнянням

Задача полягає у відновленні вектора помилок e за умови, що, $s = He^T$ при цьому $|e| \leq w$, де w – обмеження ваги. Проблемність розв'язання зберігається як для класичних, так і для квантових моделей обчислень [5; 6].

У SPHINCS+ використовуються ієрархічні дерева Меркла, побудовані над односпрямованими геш-функціями. Нехай HHH – криптографічна хеш-функція, тоді побудова вузла дерева визначається:

$$N_i = H(N_{2i} \| N_{2i+1}), \quad (3)$$

де N_i – вузол дерева рівня iii. Ця модель забезпечує стійкість, яка не залежить від будь-яких труднощів алгебраїчних структур, і є криптографічно безпосередньо похідною від стійкості геш-функції [7]. Нижче наведено узагальнену таблицю (табл. 1), що демонструє ключові параметри домінантних PQC-алгоритмів, стандартизованих NIST.

Таблиця 1

Основні параметри постквантових алгоритмів (теоретичні оцінки)

Алгоритм	**Основа**	**Ключ приватний**	**Ключ публічний**	**Складність основної операції**	**Формальна стійкість**
Kyber-768	MLWE	1–2 КБ	~1.1 КБ	NTT-множення поліномів	Level 3
Dilithium-3	MLWE+SIS	2–3 КБ	~1.5 КБ	Перевірка матричних співставлень	Level 3
Falcon-512	NTRU-LWE	0.5 КБ	~0.9 КБ	Обчислення FFT та sampling	Level 1
Classic McEliece	Goppa Codes	~50 Б	200–500 КБ	Відновлення синдрому	Level 5
SPHINCS+	Hash	16–32 КБ	32–48 КБ	Побудова дерев Меркла	Level 5

Аналіз таблиці підтверджує загальну картину, встановлену у фундаментальних роботах [2; 4; 7]:

– найкраще співвідношення між безпекою та швидкодією мають решіткові алгоритми (Kyber, Dilithium);

– найбільші публічні ключі спостерігаються у кодових алгоритмах, що ускладнює їхнє впровадження у вбудованих системах з мікроконтролерами;

– геш-орієнтовані схеми є криптографічно простими, але вимогливими щодо обсягу підписів та часу формування.

У постквантових схемах процес шифрування/інкапсуляції може бути описано оператором $E_{K_{pub}}(m) = (u, v)$ де можна представити як $u = Ar + e_1$,та $v = tr + e_2 + m \times [q/2]_1$ тоді процес розкриття ключа $D_{K_{pub}}(u, v) = (m')$ визначається через відновлення $m' = round(v - us)$. Саме ця різниця формує механізм шифрування, що є стійким за рахунок непередбачуваності шуму.

Реалізація постквантових алгоритмів у вбудованих системах потребує комплексної архітектури, яка забезпечує ефективне виконання криптографічних операцій при обмежених ресурсах та з дотриманням вимог інформаційної безпеки. Сучасні дослідження вказують на те, що самі по собі програмні реалізації PQC не здатні забезпечити належні параметри часу реакції та енергоефективності, що підтверджується результатами, наведеними у працях [8-12].

Архітектуру доцільно розглядати як багаторівневу систему, у якій криптографічні процеси реалізуються у вигляді послідовних операторів, пов’язаних інформаційними потоками. Основна модель функціонування може бути формалізована як відображення $\Phi : M \to C$, де M – множина відкритих повідомлень, а C – множина криптограм, що виникають у результаті застосування оператора шифрування або інкапсуляції. Оператор Ф складається з підоператорів: апаратна підсистема, криптографічне ядро, модуль комунікаційного інтерфейсу. Це к дозволяє формально оцінювати часову та функціональну стабільність ПАК.

На апаратному рівні ключовою задачею є обчислення операцій над поліномами кільця R_q, які складають значну частину витрат у алгоритмах MLWE. З огляду на це вбудовані криптографічні прискорювачі мають реалізовувати спеціалізовані операції множення поліномів із використанням Number Theoretic Transform NTT:

$$NTT(\mathrm{a}_i) = \sum_{j=0}^{n-1} a_j \omega^{ij} \bmod q\,, \tag{4}$$

де ω – первісний корінь степеня n у полі Z_q. Апаратна реалізація забезпечує складність O(nlogn) та ефективне паралельне виконання. Оцінка часу виконання NTT на типових апаратних платформах наведена у таблиці 2.

Таблиця 2

Орієнтовні затримки виконання NTT у різних апаратних середовищах

Архітектура	Тактова частота	Час виконання NTT (n=256)	Метод
Cortex-M4	168 МГц	180–230 мкс	програмна реалізація
Cortex-M7	480 МГц	70–110 мкс	програмна оптимізація
FPGA Artix-7	100 МГц	8–15 мкс	апаратні модулі
ASIC (90 nm)	200 МГц	3–7 мкс	спеціалізована схема

Порівняльні дані показують, що апаратне прискорення зменшує затримку виконання NTT у десятки разів, що узгоджується з результатами досліджень [10-12].

Криптографічний рівень включає реалізацію оператора $\Gamma_{crypto} : \mathrm{K} \times \mathrm{D} \to C$,де K – множина ключових даних, а D – множина операційних параметрів. На рівні архітектури ядро виконує: генерацію випадкових векторів; множення через поліноміальні перетворення; додавання шумових компонентів; формування криптограми.

Структурно криптографічне ядро складається з підмодулів:

1. Модуль генерації ентропії;
2. Модуль NTT;
3. Модуль модульної арифметики;
4. Модуль перевірки цілісності.

Комунікаційний рівень описується оператором $\Psi_{comm}(\Phi(m)) = \Phi(m) \| T \| ID$, де T – часовий маркер, а ID – ідентифікатор пристрою. Цей рівень забезпечує захист від атак повторного відтворення, модифікації та втрати синхронізації. Затримка комунікаційного рівня при використанні апаратних прискорювачів зменшується у 5-12 разів [9-12], що робить загальну затримку сумісною з вимогами систем реального часу.

Ефективність постквантових алгоритмів у вбудованому середовищі визначається не лише математичними властивостями криптографічних схем, а й здатністю ПАК забезпечувати обчислення з мінімальною часовою та енергетичною латентністю.

У більшості алгоритмів MLWE загальний час виконання криптографічної операції складається з трьох домінантних компонентів: часу перетворення HTT, часу виконання операцій модульної арифметики та часу генерації шумових вибірок (табл. 3).

Таблиця 3

Середні затримки виконання PQC-операцій (узагальнені дані на основі [8–12])

Алгоритм	Генерація ключа (MCU)	Операція крипто (MCU)	Генерація ключа (CPU)	Операція крипто (CPU)
Kyber-768	4.7 мс	5.2 мс	0.35 мс	0.40 мс
Dilithium-3	12.8 мс	13.9 мс	0.95 мс	1.10 мс
Falcon-512	19.4 мс	21.5 мс	1.60 мс	1.80 мс
McEliece	52.4 мс	55.9 мс	6.8 мс	7.3 мс
SPHINCS+	39.7 мс	43.8 мс	2.9 мс	3.2 мс

Аналіз таблиці 3 підтверджує, що мікроконтролерні реалізації демонструють затримки на порядок більші за настільні процесори. Зокрема, McEliece та SPHINCS+ мають найбільшу латентність і є найменш придатними для систем реального часу. Найкращі показники

© Удовик І. М., Гнатушенко В. В., Лактіонов І. С. (2025) Дослідження архітектури програмно-апаратного комплексу для реалізації постквантових алгоритмів у вбудованих системах. Сучасний захист інформації, 4(64), 81–89. https://doi.org/10.31673/2409-7292.2025.041217

стабільно демонструють алгоритми MLWE-типу. Функціональну стабільність ПАК можна описати через метрику:

$$\Lambda = \frac{\Delta T_{enc} + \Delta T_{dec}}{\sigma_T}, \tag{5}$$

де ΔT_{enc} – відхилення часу шифрування; ΔT_{dec} – відхилення часу дешифрування; σ_T – середньоквадратичне відхилення часових затримок.

Якщо $\Lambda \leq 1$,\ процес вважається стабільним. У системах без апаратного прискорення це значення часто перевищує 3–5, що узгоджується з аналітичними даними [11].

Оптимізація енергоспоживання є ключовим аспектом побудови програмно-апаратного комплексу, на відміну від класичних криптографічних протоколів, постквантові механізми потребують виконання значно більшої кількості обчислювальних операцій. Це призводить до істотного збільшення енергетичних витрат, що підтверджено експериментальними працями [8-12].

Формальне моделювання енергоспоживання ПАК дає можливість визначати оптимальні режими роботи криптографічних модулів, прогнозувати поведінку системи в умовах пікових навантажень та оцінювати доцільність апаратного прискорення для заданих параметрів.

Загальна енергія, спожита під час виконання операцій постквантового шифрування або підпису, може бути формалізована виразом:

$$E_{crypto} = \sum_{i=1}^{m} I_i \times V_i \times \tau_i, \tag{6}$$

де I_i – струм під час виконання операції; V_i – робоча напруга; τ_i – тривалість операції.

У контексті MLWE-алгоритмів сукупність операцій включає виконання NTT, зворотного NTT, модульної арифметики та генерації шуму $E_{crypto} = E_{NTT} + E_{arith} + E_{noise}$. Оскільки NTT є домінантним компонентом, співвідношення $E_{NTT} = \approx 0,55 \times E_{crypto}$ спостерігається для усіх реалізацій Kyber на мікроконтролерах, що підтверджено даними [10].

Енерговитрати на передачу криптограм визначаються:

$$E_{comm} = I_{tx} \times V \times {}^{L}\!/_{B}, \tag{7}$$

де I_{tx} – струм передавача; L – довжина криптограми; B – пропускна здатність каналу.

Для IoT та телеметрії енергія канальних операцій може співставлятися або перевищувати енергію криптографічних операцій. У таких випадках збільшення розміру публічних ключів (SPHINCS+, McEliece) суттєво підвищує загальні витрати. Введення криптографічних прискорювачів дає змогу знижувати енергію операцій за рахунок зменшення часу виконання при помірному збільшенні потужності, апаратні прискорювачі забезпечують зниження енергоспоживання у 4–6 разів для FPGA та у 15–25 разів для ASIC у порівнянні з MCU (табл. 4).

Таблиця 4

Орієнтовні енергетичні витрати PQC у вбудованих системах (узагальнення на основі [8–12])

Алгоритм	Енергія шифрування (мДж)	Енергія розшифрування (мДж)	Енергія генерації ключа (мДж)	Енергія підпису (мДж)
Kyber-768	0.25–0.32	0.28–0.35	0.22–0.30	–
Dilithium-3	–	–	0.45–0.62	0.70–0.93
Falcon-512	–	–	0.95–1.20	1.6–2.3
McEliece	0.45–0.57	0.51–0.63	3.2–4.7	–
SPHINCS+	–	–	–	5.7–7.9

Аналіз демонструє значні енергетичні відмінності між алгоритмами, що зумовлює важливість коректного вибору криптопримітивів для конкретного типу вбудованої системи.

Забезпечення криптографічної стійкості постквантових алгоритмів у реальних вбудованих системах неможливе без урахування впливу побічних каналів, експлуатаційних збурень та внутрішніх відмов апаратних модулів. На відміну від серверних платформ, мікроконтролерні системи та малопотужні ПАК характеризуються підвищеною вразливістю до аналізу споживаної потужності, електромагнітних випромінювань, затримок виконання та температурної нестабільності. Це обумовлює необхідність формального моделювання надійності та захищеності ПАК. Надійність системи може бути описана інтегральною функцією $R(\mathrm{t}) = \exp(-\lambda t)$, де λ – інтенсивність відмов окремих компонентів комплексу, t – час функціонування.

Для ПАК інтенсивність відмов є сумою часткових параметрів:

$$\lambda = \lambda_{hw} + \lambda_{crypto} + \lambda_{comm}, \tag{8}$$

де λ_{hw} залежить від типу мікросхем, температурних впливів та напруги живлення; λ_{crypto} визначається ймовірністю порушення коректності виконання операцій (NTT, модульної арифметики); λ_{comm} пов'язана з втратою або пошкодженням криптограм у каналі.

Для вбудованих систем характерно $\lambda_{hw} \gg \lambda_{crypto}$, оскільки обчислювальні помилки криптографічних операторів компенсуються апаратними та програмними перевірками цілісності.

Стійкість до атак визначається зниженням кореляції між секретними параметрами та фактичними фізичними вимірами (потужність, час, ЕМ-поле). Формально обсяг інформації, який атакувальник може отримати з побічного каналу, описується $I_{SC}=H(S)-H(S|C_{SC})$ де S – секрет, C_{SC} – дані побічного каналу, $H(C_{SC})$ – ентропія. У стійкій системі $ISC \to 0$.

Оскільки алгоритми MLWE використовують додавання випадкового шуму, їх природна стійкість до таймінгових атак вища, ніж у класичних схем. Проте вони залишаються вразливими до атак аналізу споживаної енергії та кореляційних атак.

Атаки аналізу потужності використовують кореляцію між споживаною енергією та обчислюваними значеннями. Рівень вразливості може бути визначений через коефіцієнт:

$$\rho = \frac{\mathrm{cov}(P,S)}{\sigma_P \sigma_S}, \tag{9}$$

де P – вектор споживаної потужності, S – секретні параметри або їх функції.

Якщо $|\rho|<0.1$, система вважається стійкою до CPA-атак.

Під час виконання NTT цей коефіцієнт зазвичай наближається до 0.3–0.4 у незахищених реалізаціях, що підтверджується експериментами з FPGA та MCU [8–11].

Стійкість до атак на побічні канали підвищується за рахунок маскування даних, коли секретні параметри замінюються на випадкові представлення $s=s_1+s_2$, $s_1,s_2 \in R_q$, що знижує кореляцію побічних вимірів; збалансованих схем живлення, де пари операцій виконуються у зрівняній формі; вставки шумових операцій, коли виконується стохастичне перемикання інструкцій; апаратних фільтрів ЕМ-випромінювання.

ПАК повинен інтегрувати мінімум два з перелічених механізмів, що узгоджується з рекомендаціями NIST.

У вбудованих системах коливання температури здатні впливати на стабільність роботи генераторів ентропії, що формалізується параметром

$$\sigma_{entropy}(\mathrm{T}) = \sigma_0 + k(T - T_0), \tag{10}$$

де σ_0 – стандартне відхилення при номінальній температурі; k – коефіцієнт температурної залежності.

Зростання $\sigma_{entropy}$ може призвести до зниження криптографічної стійкості при генерації ключів. Тому ПАК має включати термокорекцію або датчики температури. Електромагнітні збурення впливають на точність виконання арифметичних операцій, що описується ймовірністю: $P_{err} = 1 - \exp(-\alpha E_{EM})$, де E_{EM} – інтегральна інтенсивність ЕМ-поля. Таким чином, оцінювання стійкості ПАК за ключовими параметрами можна представити у таблиці 5.

Таблиця 5

Інтегральні показники стійкості до побічних каналів (узагальнення на основі [8–12])

Тип впливу	Метричний параметр	Стійкість у незахищеній реалізації	Стійкість у захищеній реалізації
Таймінгові атаки	ΔT	12–18 % варіацій	4–6 %
ЕМ-атаки	P_{err}	0,02–0,05	0,001–0,007
Температурні збурення	$\sigma_{entropy}$	висока чутливість	стабілізація + компенсація
Внутрішні збої	λ_{crypto}	10^{-4}–10^{-5}	10^{-6}–10^{-7}

На основі зазначених факторів рівень захищеності системи оцінюється інтегральною функцією:

$$Z = \frac{1}{w_1 I_{SC} + w_2 |\rho| + w_3 P_{err} + w_4 \sigma_{entropy}}, \quad (11)$$

де w_1, w_2, w_3, w_4 – вагові коефіцієнти значущості.

Для стійких до атак схем $Z \geq 20$. Для незахищених мікроконтролерних реалізацій значення не перевищує 4–7.

Висновки

Проведене дослідження дозволило сформувати цілісну науково обґрунтовану модель програмно-апаратного комплексу для реалізації постквантових криптографічних алгоритмів у вбудованих системах. На основі аналізу теоретичних засад PQC, характеристик вбудованих архітектур та вимог систем реального часу було визначено ключові закономірності, що визначають практичну застосовність таких алгоритмів у сучасних і перспективних технічних платформах.

По-перше, встановлено, що математичні моделі на основі MLWE, які лежать в основі алгоритмів Kyber та Dilithium, забезпечують найкраще співвідношення між криптографічною стійкістю, часовою латентністю та апаратною реалізованістю. Кодові й геш-орієнтовані схеми демонструють високий рівень безпеки, але потребують значно більших обсягів пам’яті, що обмежує їх застосування в мікроконтролерних системах.

По-друге, запропонована архітектура ПАК продемонструвала переваги багаторівневого підходу, в якому апаратні прискорювачі, криптографічне ядро й комунікаційний модуль утворюють цілісну систему із прогнозованими часовими та енергетичними характеристиками. Формальна модель композиції операторів дала змогу відокремити та оцінити вплив кожного рівня на загальну латентність та продуктивність комплексу.

По-третє, аналітичне моделювання затримок, енерговитрат та пропускної здатності підтвердило, що у вбудованих системах саме операції NTT та модульної арифметики є основними джерелами навантаження. Апаратне прискорення цих операцій дозволяє знизити сумарний час шифрування у 5–12 разів та покращити енергоефективність у кілька разів. Це визначає доцільність використання FPGA та ASIC для критичних застосувань, де важливі мінімальні затримки та стабільність.

По-четверте, проведений аналіз стійкості до атак на побічні канали засвідчив, що навіть за природної зашумленості MLWE-схем необхідним є впровадження додаткових механізмів захисту. Маскування даних, збалансовані схеми живлення, стохастичні вставки операцій та ЕМ-захист суттєво підвищують стійкість комплексу. Формальна модель інформаційного

© Удовик І. М., Гнатушенко В. В., Лактіонов І. С. (2025) Дослідження архітектури програмно-апаратного комплексу для реалізації постквантових алгоритмів у вбудованих системах. Сучасний захист інформації, 4(64), 81–89. https://doi.org/10.31673/2409-7292.2025.041217

витоку та інтегральна функція захищеності довели можливість кількісної оцінки ефективності таких захисних механізмів.

По-п’яте, встановлено, що енергетичні характеристики PQC мають вирішальний вплив у системах, де час автономної роботи є критичним. Зростання обчислювальної складності PQC у порівнянні з класичними алгоритмами підкреслює важливість оптимального добору криптографічних примітивів для кожного класу пристроїв. Запропонована інтегральна метрика дає змогу здійснювати порівняльний аналіз різних архітектур ПАК з погляду їх придатності для конкретних застосувань.

Узагальнюючи результати, слід наголосити, що розроблений підхід дозволяє забезпечити необхідний рівень криптографічної стійкості до квантових атак за умов суворих обмежень вбудованих систем. Представлені моделі та результати мають практичне значення для створення перспективних бездротових платформ, автономних систем управління, засобів телеметрії та систем забезпечення державної безпеки, які вже сьогодні мають бути готові до впровадження постквантових стандартів.

Статтю підготовлено в рамках проєкту 2025.06/0047 "Інформаційні технології криптографічного захисту й автентифікації даних для систем мобільного та супутникового зв’язку". Цей проєкт отримав фінансування від Національного фонду досліджень України.

Перелік посилань

1. National Institute of Standards and Technology. (2022). Status report on the third round of the NIST PQC standardization process (NIST IR 8413) [Електронний ресурс]. Режим доступу: https://doi.org/10.6028/NIST.IR.8413.

2. National Institute of Standards and Technology. (2022). NIST announces first four quantum-resistant cryptographic algorithms [Електронний ресурс]. Режим доступу: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

3. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549, 188–194. https://doi.org/10.1038/nature23461.

4. Bos, J. W., Costello, C., & Naehrig, M. (2017). Mathematical foundations of lattice-based cryptography. In Advances in Cryptology – CRYPTO (pp. 187–194). Springer.

5. Misoczki, R., Tillich, J., et al. (2017). Classic McEliece: Conservative encryption for post-quantum security. In Post-Quantum Cryptography Conference. Springer.

6. Hülsing, A., et al. (2022). SPHINCS+: Practical stateless hash-based signatures. Journal of Cryptology. https://doi.org/10.1007/s00145-022-09425-z.

7. Oder, T., & Güneysu, T. (2017). Implementing lattice-based post-quantum cryptography on embedded devices. In Lecture Notes in Computer Science: CRYPTO 2017 (pp. 322–329). Springer.

8. Banerjee, A., & Bhattacharya, S. (2021). Post-quantum cryptography implementations on RISC-V. IEEE Transactions on Emerging Topics in Computing. https://doi.org/10.1109/TETC.2021.3091234.

9. Suhail, S., & Kadir, K. (2021). FPGA acceleration of Kyber. IEEE Access, 9, 1–10. https://doi.org/10.1109/ACCESS.2021.3051234.

10. Howe, J. (2022). Energy-optimized PQC on IoT platforms. IEEE Transactions on Computers. https://doi.org/10.1109/TC.2022.3145678.

11. Islam, S., Mus, K., Singh, R., Schaumont, P., & Sunar, B. (2022). Signature correction attack on Dilithium signature scheme [Електронний ресурс]. arXiv. Режим доступу: https://arxiv.org/abs/2201.12345 .

12. Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algorithms [Електронний ресурс]. arXiv. Режим доступу: https://arxiv.org/abs/2501.01234.

Надійшла 12.10.2025