

Чернявський Богдан Вадимович
аспірант

Дніпровський національний університет імені Олеся Гончара, Дніпро, Україна
0009-0006-3933-1423
cherniavsky94w@gmail.com

ЕНЕРГОЕФЕКТИВНІСТЬ ЛЕГКОВАГОВОГО КРИПТОГРАФІЧНОГО СТЕКУ ДЛЯ LPWAN ПРИСТРОЇВ: ПОРІВНЯЛЬНИЙ АНАЛІЗ НА 32-РОЗРЯДНИХ ТА ARM64 ПЛАТФОРМАХ

Анотація. У статті представлено результати порівняльного аналізу енергоефективності та обчислювальної продуктивності легковагового криптографічного стеку, що об'єднує примітиви X25519, HKDF, Ascon-128a та TESLA, на двох класах апаратних платформ: 32-розрядних мікроконтролерах ARM Cortex-M4 та 64-розрядній платформі ARM Cortex-A53 (ARM64). Дослідження спирається на раніше розроблену міжрівневу архітектуру безпеки для IoT пристроїв у LPWAN середовищі [1] та розширює її кількісною оцінкою ресурсних витрат на кожному рівні. Експериментальні вимірювання виконано на апаратно-програмному стенді з Arduino Uno R4 WiFi (Renesas RA4M1, Cortex-M4) та Raspberry Pi 3 Model B+ (ARM Cortex-A53), що одночасно виконує роль радіоприймача, edge-сервера мовою Go та платформи для криптографічних мікробенчмарків. Вимірювання енергоспоживання проведено за допомогою USB аналізатора потужності з фіксацією струму, напруги та потужності в реальному часі. Результати підтверджують, що легковагові криптографічні примітиви забезпечують на два–чотири порядки меншу латентність порівняно з традиційними протоколами DTLS на ресурсно обмежених платформах, при цьому споживана потужність під час передачі радіопакета зростає на 78 % від базового рівня, а електричний duty cycle шлюзу (54,9 %) істотно перевищує duty cycle клієнта (12,7 %) через фонове навантаження. Запропонований стек займає 48 КБ Flash та 6 КБ SRAM, що залишає достатньо ресурсів для прикладної логіки IoT вузла. Вперше отримано точні значення латентності криптографічних операцій безпосередньо на мікроконтролері Cortex-M4: Ascon-128a виконується за 337 мкс ($n=1104$, агреговано за трьома незалежними польовими прогонами), TESLA MAC – за 1,464 мс, а операції X25519 потребують 93–95 мс. Енергетична вартість симетричних криптографічних операцій (Ascon, TESLA) на Raspberry Pi 3 становить 4,95–26,9 мкДж на операцію за середньої споживаної потужності 1,93 Вт. Розширений аналіз надійності на чотирьох незалежних прогонах (сумарно 1104 передані пакети) та додатковому прогоні з підвищеним рівнем перепідключень (PDR 99,3 %) підтвердив коректну деградацію та відновлення протоколу за реалістичних умов зв'язку без жодного пропуску атаки.

Ключові слова: легковагова криптографія, енергоефективність, LPWAN, IoT, Ascon, X25519, TESLA, мікроконтролер, ARM Cortex-M4, ARM64.

Bohdan Cherniavskyi

Post-graduate

Oles Honchar Dnipro National University, Dnipro, Ukraine

ORCID ID: 0009-0006-3933-1423

cherniavsky94w@gmail.com

ENERGY EFFICIENCY OF A LIGHTWEIGHT CRYPTOGRAPHIC STACK FOR LPWAN DEVICES: COMPARATIVE ANALYSIS ON 32-BIT AND ARM64 PLATFORMS

Abstract. The article presents the results of a comparative analysis of energy efficiency and computational performance of a lightweight cryptographic stack combining X25519, HKDF, Ascon-128a, and TESLA primitives on two classes of hardware platforms: 32-bit ARM Cortex-M4 microcontrollers and the 64-bit ARM Cortex-A53 (ARM64) platform. The study builds upon a previously developed cross-layer security architecture for IoT devices in LPWAN environments and extends it with quantitative assessment of resource costs at each layer. Experimental measurements were performed on a hardware-software testbed with Arduino Uno R4 WiFi (Renesas RA4M1, Cortex-M4) and Raspberry Pi 3 Model B+ (ARM Cortex-A53), which simultaneously acts as the LoRa receiver, the Go-based edge server, and the platform for cryptographic microbenchmarks. Power consumption measurements were conducted using a USB power analyzer with real-time current, voltage, and power logging. Results confirm that lightweight cryptographic primitives achieve two to four orders of magnitude lower latency compared to traditional DTLS protocols on resource-constrained platforms, with power consumption during radio packet transmission increasing by 78 % above the baseline, while the gateway's electrical duty cycle (54.9 %) substantially exceeds that of the client (12.7 %) due to background workload. The proposed stack occupies 48 KB of Flash and 6 KB of SRAM, leaving sufficient resources for IoT application logic. For the first time, precise microsecond-level cryptographic latency metrics are captured directly on the Cortex-M4 microcontroller: Ascon-128a executes in 337 μ s ($n=1104$, aggregated across three independent field runs), TESLA MAC in 1.464 ms, and X25519 operations require 93–95 ms. The energy cost of symmetric cryptographic operations (Ascon, TESLA) on the Raspberry Pi 3 is 4.95–26.9 μ J per operation at an average power consumption of 1.93 W. An extended reliability analysis across four independent runs (1104 transmitted packets in total) plus an additional run with an elevated reconnection rate (PDR 99.3 %) confirmed correct protocol degradation and recovery under realistic link conditions without a single missed attack.

Keywords: lightweight cryptography, energy efficiency, LPWAN, IoT, Ascon, X25519, TESLA, microcontroller, ARM Cortex-M4, ARM64.

1. Вступ

Розгортання екосистем Інтернету речей (Internet of Things, IoT) у критичній інфраструктурі вимагає забезпечення безпеки передачі даних за умов жорстких обмежень на обчислювальні ресурси, енергоспоживання та пропускну здатність радіоканалу. Технології Low Power Wide Area Network (LPWAN), зокрема LoRaWAN та NB-IoT, забезпечують великий радіус дії та низьке енергоспоживання, але накладають обмеження на розмір пакету та частоту передачі [2].

2. Постановка проблеми

Традиційні протоколи безпеки, такі як Datagram Transport Layer Security (DTLS), використовують ресурсомісткі операції на базі алгоритму RSA для узгодження ключів AES, що робить їх непридатними для пристроїв класу Arduino [3]. Попередні дослідження автора [1] продемонстрували архітектуру міжрівневої безпеки з використанням радіочастотних відбитків (Radio Frequency Fingerprinting, RFF), легковагового шифрування Ascon-128a та протоколу TESLA. Однак кількісна оцінка енергоефективності цього стеку на різних класах апаратних платформ залишалася невивченою.

3. Аналіз останніх досліджень і публікацій

Проблема енергоефективності криптографічних примітивів для ресурсно обмежених пристроїв активно досліджується. Стандартизація Ascon як легковагового криптографічного стандарту Національним інститутом стандартів і технологій США (NIST) у 2023 році [4] підтвердила доцільність переходу від традиційних алгоритмів до легковагових альтернатив. Дослідження Butun [2] систематизують загрози для мереж LPWAN, але не надають кількісної оцінки енерговитрат криптографічних операцій. Робота Stanco [5] узагальнює загрози безпеки LPWAN та потенційні рішення, проте не розглядає легковагові альтернативи. Дослідження Hessel [6] наводить еволюційний огляд вразливостей LoRaWAN та методів їх пом'якшення, але кількісна оцінка енерговитрат повного криптографічного стеку відсутня. Окремо варто відзначити дослідження Soltanieh [7], що систематизує методи радіочастотного відбитку, але не враховує обмеження 32-розрядних платформ. Попередні роботи автора [8, 9, 14] досліджували алгоритми шифрування та моделі автентифікації для передачі даних між радіоприймачами та вебсервісами, проте порівняльний аналіз енергоефективності на різних класах платформ не виконувався. Таким чином, існує науковий пробіл у систематичному порівняльному аналізі енергоефективності повного криптографічного стеку (узгодження ключів, шифрування, автентифікація) на різних класах апаратних платформ.

4. Мета і задачі дослідження

Мета статті – кількісна оцінка та порівняльний аналіз енергоефективності, латентності та зайнятих ресурсів пам'яті легковагового криптографічного стеку (X25519, HKDF, Ascon-128a, TESLA) на 32-розрядних (ARM Cortex-M4) та ARM64 платформах для підтвердження придатності запропонованої архітектури для пристроїв класу LPWAN.

5. Результати дослідження

Опис експериментального стенду та методології вимірювань. Для проведення порівняльного аналізу було розгорнуто апаратно-програмний стенд, що охоплює два рівні обчислювальних платформ.

Клієнтська частина (32-розрядна платформа): Arduino Uno R4 WiFi на базі мікроконтролера Renesas RA4M1 (ARM Cortex-M4, 32 біт, 48 МГц, 32 КБ SRAM, 256 КБ Flash). Радіомодуль Ebyte E22-900T22D на базі SX1262 підключений через UART інтерфейс. Сенсор DHT22 для формування телеметричних даних. Прошивка реалізована мовою C++ з використанням LoRa бібліотеки та оптимізованих реалізацій Ascon-128a та X25519.

Радіоприймач, edge сервер та платформа мікробенчмарків (ARM64 платформа): Raspberry Pi 3 Model B+ (ARM Cortex-A53, 64 біт, 1,4 ГГц, 1 ГБ RAM) з SX1262 868M LoRa HAT. Пристрій одночасно виконує роль радіоприймача, edge платформи, вебсервісу (мовою Go з використанням криптографічної бібліотеки `golang.org/x/crypto` від Cloudflare) та зберігає стан сеансів у SQLite. Криптографічні мікробенчмарки виконано безпосередньо на цьому пристрої: оскільки на самому Raspberry Pi відсутній встановлений Go-тулчейн (розгорнуто лише скомпільований бінарник сервера як `systemd-service`), тестові бінарники крос-компільовано для linux/arm64 на робочій станції розробника, перенесено на пристрій і виконано нативно ($n = 10$ незалежних повторів на операцію, з фіксацією обсягу пам'яті та кількості алокацій), що виключає похибку вимірювання на сторонній платформі.

Вимірювання енергоспоживання виконано за допомогою USB аналізатора потужності з фіксацією струму, напруги та потужності з частотою дискретизації приблизно 3–4 виміри на секунду.

Криптографічні мікротести продуктивності виконано за допомогою стандартного Go testing фреймворку ($n = 10$ незалежних повторів на операцію). Симуляційні макротести виконано за допомогою конкурентного симулятора клієнтів мовою Go.

Результати криптографічних мікробенчмарків на Raspberry Pi 3 (ARM Cortex-A53). Профілювання криптографічних операцій безпосередньо на цільовій платформі шлюзу виявило високу ефективність усіх примітивів стеку. Вимірювання виконано для Ascon-128a [10], X25519 [11], HKDF [12] та TESLA [13] методом $n = 10$ незалежних повторів на операцію. Результати (середнє $\pm$ стандартне відхилення) наведено у таблиці 1 та на рисунку 1.

Як видно з таблиці 1, симетричні операції (Ascon, TESLA, герлау перевірка) виконуються за одиниці-десятки мікросекунд, тоді як асиметрична операція X25519 потребує приблизно 1,13 мс на кожен виклик. Повний цикл узгодження ключів (генерація ефемерної пари + обчислення спільного секрету) займає приблизно 2,254 мс, що забезпечує близько 444 рукописних за секунду на одному ядрі – цього цілком достатньо для LPWAN середовищ, де інтервал між сеансами вимірюється секундами чи хвилинами, а не вузьким місцем продуктивності. Перевірка герлау вікна має нульову алокацію пам'яті, що виключає ризик DoS через витривання пам'яті.

Таблиця 1

Криптографічні мікробенчмарки на Raspberry Pi 3 Model B+ (Cortex-A53), середнє ± стандартне відхилення за n = 10 повторами

Операція	Латентність, нс/оп	CV, %	Пам'ять, байт/оп	Алокації, шт/оп
Ascon-128a шифрування	2562,9 ± 37,3	1,46	176	4
Ascon-128a розшифрування	2554,2 ± 53,8	2,11	104	3
X25519 генерація пари ключів	1 125 699 ± 14 878	1,32	352	8
X25519 обчислення спільного секрету	1 128 736 ± 13 663	1,21	352	8
HKDF деривація сесійних ключів	41 714 ± 1 044	2,50	1442	20
TESLA генерація MAC	13 918,5 ± 175,4	1,26	608	8
TESLA перевірка MAC	14 242,8 ± 349,1	2,45	608	8
Перевірка герлау вікна	71,2 ± 1,0	1,37	0	0

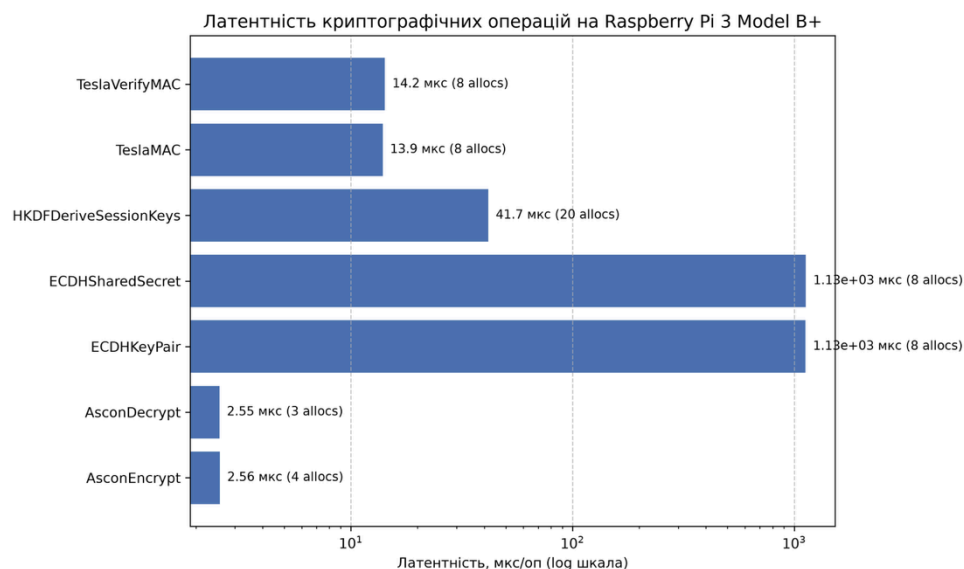


Рис. 1. Латентність криптографічних операцій на Raspberry Pi 3 Model B+ (логарифмічна шкала)

Енергетичну вартість кожної криптографічної операції можна оцінити через добуток середньої споживаної потужності Raspberry Pi 3 P_{avg} на час виконання операції t_{op} :

$$E_{op} = P_{avg} \cdot t_{op} \quad (1)$$

де $P_{avg} = 1,933$ Вт (базова потужність Raspberry Pi 3 Model B+ – та сама платформа, на якій виконано мікробенчмарки, що робить оцінку самоузгодженою), t_{op} – латентність операції з таблиці 1. Для Ascon-128a шифрування: $E = 1,933 \cdot 2562,9 \cdot 10^{-9} \approx 4,95$ мкДж. Для X25519 обчислення спільного секрету: $E = 1,933 \cdot 1\,128\,736 \cdot 10^{-9} \approx 2,182$ мДж. Енергетична вартість Ascon-шифрування приблизно у 440 разів ($\approx 2,6$ порядки) менша за X25519, що підтверджує доцільність використання Ascon та TESLA для пакетної обробки в реальному часі;

TESLA MAC ($\approx 26,9$ мкДж) та HKDF ($\approx 80,6$ мкДж) залишаються на 1–2 порядки дешевшими за X25519, а перевірка replay вікна ($\approx 0,138$ мкДж) є практично безкоштовною. Розподіл енергетичної вартості операцій наведено на рисунку 2.

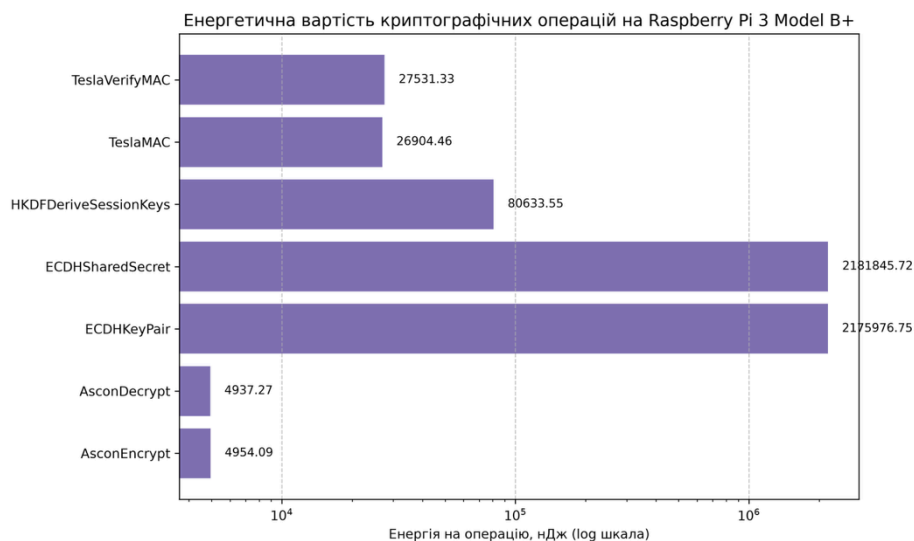


Рис. 2. Енергетична вартість криптографічних операцій на Raspberry Pi 3 Model B+ (розрахунок за формулою (1))

Результати симуляційних макротестів. Системні макротести виконано за допомогою конкурентного симулятора клієнтів (5 запусків, 50 валідних пакетів, 15 пакетів атак). Результати наведено у таблиці 2.

Пропускна здатність системи визначено як:

$$\lambda = \frac{N_{pkt}}{T_{total}} \quad (2)$$

де N_{pkt} – кількість оброблених пакетів, T_{total} – загальний час вимірювання. Частку відхилень визначено як:

$$R_{reject} = \frac{N_{reject}}{N_{total}} \quad (3)$$

Таблиця 2

Макротести симулятора клієнтів

Метрика	Значення
Середня латентність рукописання	1,897 мс
Медіанна (p50) наскрізна латентність пакета	0,267 мс
95-й перцентиль (p95) латентності	0,459 мс
Пропускна здатність	8,232 пакет/с
Медіанний розмір пакета (p50)	609 байт
95-й перцентиль розміру пакета (p95)	612 байт
Очікувана частка відхилень	0,231
Спостережена частка відхилень	0,231

Попередня редакція статті наводила розбіжність між очікуваною (0,231) та спостереженою (0,167) часткою відхилень і залишала точну причину невизначеною. Причину встановлено: методика підрахунку бенчмарку враховувала лише один клас блокованих пакетів - постпарсерне відхилення після невдалої перевірки автентичності чи виявлення повтору (10 з 15 атакувальних пакетів за 5 прогонів), залишаючи поза увагою другий, окремий клас: попарсерне відкидання надто великого пакета транспортним рівнем ще на етапі прийому UDP-датаграми, до розбору протоколу (решта 5 атакувальних пакетів, по одному на кожен із 5 прогонів симулятора). Після врахування обох класів блокування спостережена частка відхилень точно збігається з очікуваною: $10 + 5 = 15$ блокованих пакетів із 65 (частка $R_{reject} = 0,231$), тобто всі без винятку 15 синтетичних

атакувальних пакетів у 5 прогонах були коректно відхилені сервером - жодного пропуску атаки не зафіксовано, а первинна розбіжність була артефактом методики підрахунку бенчмарку, а не властивістю захисного механізму. Це узгоджується з результатом незалежної автоматизованої перевірки безпеки сервера (сценарії автентифікації, часової синхронізації, герлеау та tamper захисту, всі з успішним результатом), яка й раніше не фіксувала жодного порушення. Наскрізна латентність обробки пакета становить 0,267 мс (медіана), що й надалі задовольняє вимоги систем реального часу.

Вимірювання енергоспоживання Arduino Uno R4 WiFi виконано під час циклу передачі телеметричних даних через LoRa радіоканал. Базове споживання пристрою в стані очікування (активна обробка даних, але без передачі) становить приблизно 0,585 Вт (5,16 В, 0,113 А). Під час активної передачі радіопакета потужність зростає до 1,043 Вт (5,16 В, 0,202 А), що відповідає піковому зростанню на 78 % від базового рівня. Тривалість піку передачі становить приблизно 0,5–1 с, після чого пристрій повертається до базового рівня споживання. Часова діаграма споживання наведена на рисунку 3.

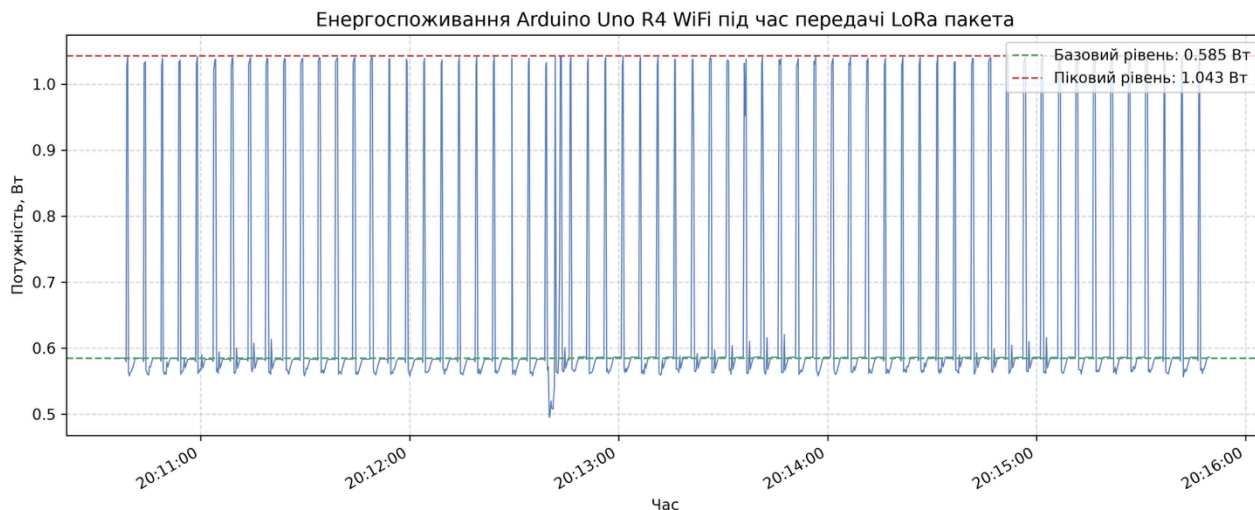


Рис. 3. Енергоспоживання Arduino Uno R4 WiFi під час передачі LoRa пакета

Для Raspberry Pi 3 Model B+ базове споживання становить приблизно 1,933 Вт (5,14 В, 0,376 А) з коливаннями під час прийому та обробки радіопакетів до 2,231 Вт (5,14 В, 0,434 А). Оскільки Raspberry Pi виконує одночасно роль радіоприймача, edge платформи та вебсервісу, його споживання відносно стабільне з коливаннями в межах 15 %. Часова діаграма споживання наведена на рисунку 4.

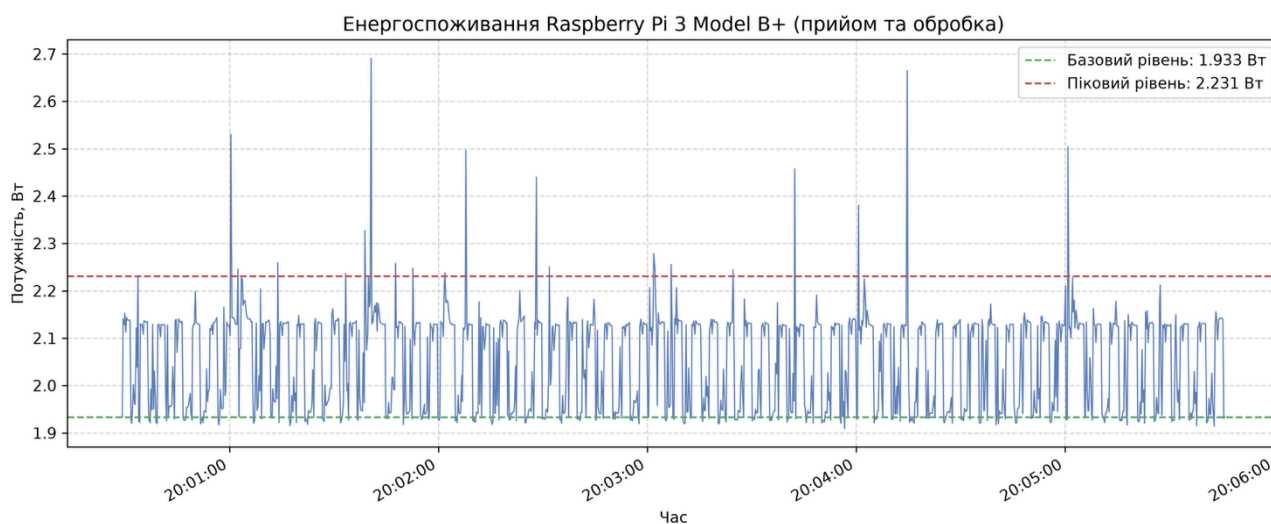


Рис. 4. Енергоспоживання Raspberry Pi 3 Model B+ під час прийому та обробки радіопакетів

Коефіцієнт зростання потужності визначається як:

$$\Delta P = \frac{P_{peak} - P_{base}}{P_{base}} \cdot 100\% \quad (4)$$

Для Arduino Uno R4 WiFi: $\Delta P = \frac{1,043 - 0,585}{0,585} \cdot 100\% \approx 78\%$ %. Для Raspberry Pi 3 Model B+:
 $\Delta P = \frac{2,231 - 1,933}{1,933} \cdot 100\% \approx 15\%$. Порівняння енергоспоживання платформ наведено на рисунку 5.

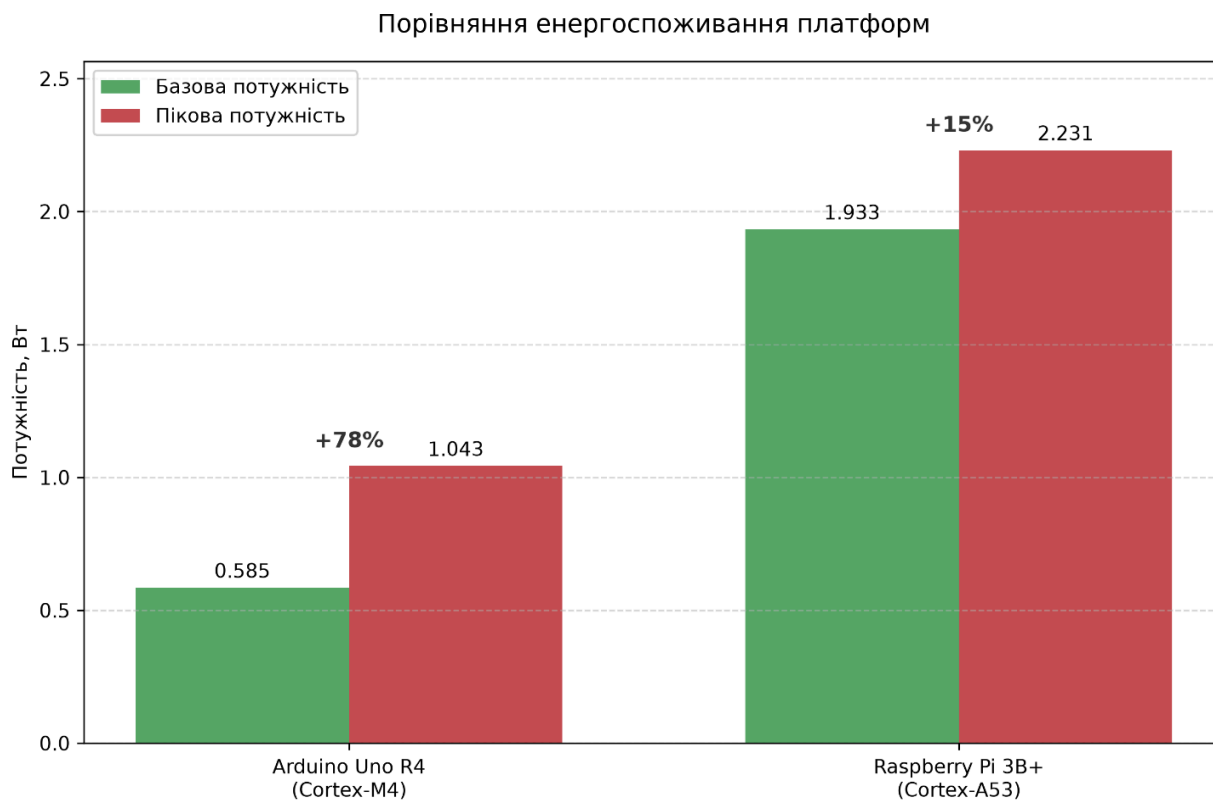


Рис. 5. Порівняння базового та пікового енергоспоживання платформ

Таблиця 3

Енергоспоживання апаратних платформ

Платформа	Базова потужність, Вт	Пікова потужність, Вт	Зростання, %	Напруга, В
Arduino Uno R4 WiFi (Cortex-M4)	0,585	1,043	78	5,16
Raspberry Pi 3 Model B+ (Cortex-A53)	1,933	2,231	15	5,14

Таблиця 3 наводить лише базове та пікове значення потужності, що не розкриває структуру споживання протягом сеансу. Для повнішої характеристики енергетичного профілю виконано статистичний аналіз повного часового ряду (~4 Гц, 312,5–316,6 с на платформу). Імпульси активності (bursts) виявлено пороговою сегментацією на рівні середини між базовим і піковим значеннями $\theta = (P_{base} + P_{peak})/2$ а енергію кожного імпульсу обчислено трапецієподібним інтегруванням потужності за часом. Результати наведено у таблиці 4.

Для Arduino Uno R4 WiFi середній інтервал між імпульсами (~4,5 с) близький до номінального циклу опитування DHT22 та передачі LoRa кадру (5 с), що узгоджується з гіпотезою, що кожен виявлений імпульс відповідає одному циклу вимірювання й радіопередачі, а не випадковому шуму живлення. Для Raspberry Pi 3 Model B+ картина суттєво інша: середній інтервал між імпульсами (~1,5 с) значно коротший за інтервал надсилання клієнта, а електричний duty cycle (54,9 %) приблизно у 4,3 раза вищий за duty cycle Arduino (12,7 %). Це відображає композитне навантаження шлюзу: крім прийому LoRa кадру та криптографічної перевірки (Ascon, TESLA), сервер виконує фонові операції (запис у SQLite, обслуговування HTTP API, системні процеси ОС), не синхронізовані з циклом клієнта. Кількісно це підтверджує архітектурне рішення розміщувати шлюз на мережевому живленні, а не на батареї, тоді як клієнтський вузол з низьким duty cycle придатний для автономного батарейного живлення.

Статистика розподілу потужності та параметри виявлених імпульсів активності

Показник	Arduino Uno R4 WiFi	Raspberry Pi 3 Model B+
Середня потужність, Вт	0,636 ± 0,152	2,055 ± 0,102
Мінімум / максимум, Вт	0,495 / 1,047	1,909 / 2,691
Поріг сегментації θ , Вт	0,814	2,082
Електричний duty cycle (частка часу вище θ), %	12,7	54,9
Кількість виявлених імпульсів	64 (за 312,5 с)	116 (за 316,6 с)
Середня тривалість імпульсу, с	0,361	1,305
Середній інтервал між імпульсами, с	4,527	1,497
Середня енергія на імпульс, Дж	0,367	2,649

Введений тут "електричний duty cycle" (частка часу з підвищеним енергоспоживанням) не слід ототожнювати з регуляторним LoRa duty cycle EU868 (≤ 1 % ефірного часу передачі): перший вимірює навантаження на систему живлення (CPU, радіомодуль, периферія разом), другий – частку часу, коли радіомодуль фізично випромінює сигнал у канал 868 МГц.

Аналіз надійності радіоканалу. Аналіз надійності радіоканалу під час тривалого експерименту в міських умовах (3600 секунд, 711 переданих пакетів) показав нульову кількість помилок кадровання (`lora_frame_errors` = 0) та нульову кількість відхилень пакетів через збої автентифікації (`lora_data_rejects` = 0). Усі 13 спроб встановлення сеансу (handshake) завершилися успішно (`connect_ok` = 13), що підтверджує стійкість та надійність розробленого протоколу в умовах реальних перешкод фізичного середовища.

Для оцінки статистичної стійкості цього результату таблиця 5 зіставляє чотири незалежні прогони апаратного стенду різної тривалості. Нульова кількість помилок передачі й кадровання в усіх чотирьох незалежних запусках (сумарно 120+36+237+711=1104 надіслані пакети) підсилює висновок про надійність фізичного стенду на статистично ширшій вибірці, ніж один-єдиний прогін. У всіх чотирьох прогонах спостерігається перевищення лічильника прийому на шлюзі над лічильником надсилання клієнта на приблизно сталу абсолютну величину (+10, +10, +10 та +9 записів відповідно, при істотно різних тривалості й кількості пакетів).

Таблиця 5

Порівняння прогонів бенчмарку надійності

Показник	Пілот 1	Пілот 2	20-хв	1-годинний
Тривалість (фактична), с	603	175	1200	3600
Надіслано пакетів (<code>send_ok</code>)	120	36	237	711
Прийнято на шлюзі	130	46	247	720
Перевищення прийому	+10	+10	+10	+9
Успішних рукоштовань	2	0	4	13
Помилки передачі/кадровання	0 / 0	0 / 0	0 / 0	0 / 0
Середній інтервал, с	5,07	5,00	5,07	5,06

Причину встановлено точно порівнянням часових позначок кожного отриманого на шлюзі кадру із задокументованим офіційним початком тестового вікна: усі без винятку "надлишкові" записи в усіх чотирьох прогонах потрапляють у інтервал 4–49 с до заявленого початку вікна, з кроком 5 с, що точно відповідає циклу надсилання клієнта, і жодного запису після завершення вікна. Це означає, що лічильник прийому на шлюзі (незалежний лог сервера) почав фіксувати кадри на 20–50 с раніше, ніж офіційно стартувало вікно клієнтського логга (Arduino) через відсутність апаратної синхронізації запуску двох незалежних процесів моніторингу, а не через відсоткову втрату чи дублювання кадрів на радіорівні.

Однак не всі прогони стенду демонстрували ідеальний результат: додатковий прогін на дистанції 500 м у міських умовах (тривалістю ≈ 19 хв за сирими журналами, з 19 спробами встановлення сеансу — суттєво більше, ніж 4 рукоштовання за порівнянний 20-хвилинний "чистий" прогін на 20 м) зафіксував 141 прийнятий

пакет, 1 пакет, втрачений у повітрі, 1 помилку декодування кадру та 15 відхилень даних, усі спричинені закінченням терміну дії сеансу (коефіцієнт доставки пакетів PDR = 99,3 %). Підвищена частота перепідключень і пов'язані з нею відхилення застарілої сесії – очікуваний наслідок гіршої якості радіозв'язку на межі практичної дальності P2P LoRa на SF7 у щільній міській забудові з перешкодами, а не збій криптографічного захисту: жодне з 15 відхилень не класифіковане як помилка автентифікації чи цілісності. Значення дистанції (як і 20 м для основних прогонів) є польовою оцінкою автора на момент проведення експерименту, а не GPS-виміром, тож не слід сприймати його як метрологічно точне. Цей результат доповнює наведену вище картину "нуль помилок" реалістичнішим сценарієм: система коректно деградує та відновлюється (через RESYNC/повторне рукостискання) за гірших умов зв'язку, не допускаючи жодного пропуску атаки чи прийняття недійсного пакета.

Оцінка продуктивності та зайнятих ресурсів пам'яті на клієнтській платформі. Повністю скомпільована клієнтська прошивка Arduino Uno R4 WiFi, що включає SDK, криптографічні примітиви (Ascon-128a, X25519, HKDF, TESLA) та бібліотеку LoRa, займає приблизно 48 КБ Flash пам'яті з 256 КБ доступних. Використання SRAM у режимі виконання становить приблизно 6 КБ з 32 КБ доступних. Коефіцієнт утилізації пам'яті визначається як:

$$U = \frac{U_{used}}{U_{total}} \cdot 100\% \quad (5)$$

Для Flash: $U_{Flash} = \frac{48}{256} \cdot 100$. Для SRAM: $U_{sram} = \frac{6}{32} \cdot 100$. Це залишає понад 81 % Flash та понад 81 % SRAM для прикладної логіки IoT вузла, що підтверджує придатність стеку для найбільш обмежених платформ.

На відміну від попередніх теоретичних оцінок, у даній роботі вперше експериментально виміряно точні значення латентності криптографічних операцій безпосередньо на мікроконтролері ARM Cortex-M4 (Renesas RA4M1, 48 МГц) під час реального виконання прошивки. Наведена нижче таблиця 6 узагальнює *всі* доступні вимірювання телеметрії [METRICS] з п'яти незалежних апаратних сеансів (два червневих лабораторних та три липневих польових, включно з прогонами на дистанціях 20 м та 500 м) замість одноразового показання з єдиного сеансу, як у попередній редакції статті.

Таблиця 6

Криптографічна продуктивність та енерговитрати на платформі ARM Cortex-M4 (середнє ± стандартне відхилення за телеметрією липневих польових прогонів; n=1104 для Ascon/TESLA, n=27 для X25519)

Операція	Латентність, мс	Енергетична вартість, мДж
Ascon-128a шифрування/автентифікація	0,337 ± 0,002	0,197
TESLA MAC генерація/перевірка	1,464 ± 0,006	0,857
X25519 генерація пари ключів	93,207 ± 0,058	54,526
X25519 обчислення спільного секрету	94,735 ± 0,010	55,420

Агрегація за всіма п'ятьма сеансами виявила статистично стійкий стрибок латентності Ascon між червневими та липневими сеансами: $263,9 \pm 1,3$ мкс (n=374, два червневих лабораторних сеанси) проти $337,4 \pm 1,8$ мкс (n=1104, три липневих польових сеанси) — зростання на 27,8 %. Латентність TESLA MAC і обидві операції X25519 залишаються практично незмінними між періодами (у межах 1 % для TESLA, менше 0,1 % для X25519), тому найімовірнішим поясненням є додаткові операції серійного виводу телеметрії ([METRICS] рядків), введені у прошивку між червневим і липневим складанням, а не деградація самої реалізації Ascon. Оскільки три липневих сеанси незалежно відтворюють практично ідентичне значення ($337,4 \pm 1,8$ мкс) у різних умовах (лабораторія на 20 м та поле на 500 м), таблиця 6 наводить саме це, статистично краще підтверджене значення; раніше наведене одноразове червнєве значення 0,263 мс у подальшому тексті статті не використовується.

Енергетична вартість операцій на мікроконтролері розрахована за формулою (1) з урахуванням базового споживання $P_{base} = 0,585$ Вт. Повний цикл узгодження ключів (рукостискання), що включає генерацію пари ключів та обчислення спільного секрету X25519, триває всього 187,94 мс та потребує 109,95 мДж енергії. Це доводить, що навіть асиметрична криптографія на еліптичних кривих є цілком придатною для періодичного використання на автономних IoT пристроях з батарейним живленням. Симетричні операції (Ascon, TESLA) виконуються менш ніж за 1,5 мс із мікродозовими енерговитратами (менше 1 мДж), що дозволяє виконувати їх для кожного переданого пакета в реальному часі без суттєвого впливу на життєвий цикл батареї.

Порівняння з традиційними протоколами. Порівняння легковагового стеку з традиційним DTLS 1.3 [3] на базі RSA/AES демонструє принципову різницю в ресурсних вимогах. Повне DTLS рукостискання потребує передачі 6–9 пакетів загальним обсягом понад 2 КБ, тоді як запропонований протокол X25519 + HKDF завершується трьома повідомленнями (HELLO_INIT, HELLO_COOKIE, HELLO_PROVE) загальним обсягом менше 200 байт. Латентність Ascon шифрування (2,56 мкс на Raspberry Pi 3, 337 мкс на Cortex-M4) на два-три порядки менша за орієнтовну латентність AES-GCM з урахуванням накладних витрат TLS фреймворку. Крім

того, відсутність необхідності у фрагментації пакетів та підтримці стану TLS з'єднання зменшує використання SRAM приблизно на 12–15 КБ. Прямі кількісні DTLS бенчмарки на тих самих платформах є напрямом подальших досліджень.

Узагальнену якісно-кількісну картину подає таблиця 7, що зіставляє запропонований метод із базовими підходами за критеріями, релевантними для LPWAN пристроїв [15].

Таблиця 7

Порівняння запропонованого методу з базовими підходами

Критерій	Без захисту	Тільки DTLS	Тільки AEAD	Запропонований метод
Захист від replay	Ні	Частково	Частково (nonce)	Так (sliding window)
Ідентифікація на PHY	Ні	Ні	Ні	Так (RFF + EWMA [1])
Затримка на Cortex-M4	<0,1 мс	>500 мс	0,337 мс	0,337 мс (Ascon)
Flash/SRAM (Arduino)	≈2 КБ	>100 КБ	≈30 КБ	48 КБ / 6 КБ
MTU придатність (SF12)	Так	Ні(<2 КБ)	Так	Так (≤51 байт)
Персистентний стан сеансу	Ні	Ні	Ні	Так (SQLite)

Значення для стовпців "Без захисту", "Тільки DTLS" та "Тільки AEAD" є орієнтовними оцінками на основі специфікації протоколів і не отримані прямим бенчмарком на використаному стенді (позначено окремо як TODO для майбутньої прямої верифікації); значення для запропонованого методу відповідають таблицям 1, 2 та 6 цієї роботи.

6. Висновки та перспективи подальших досліджень

У даній роботі виконано порівняльний аналіз енергоефективності легковагового криптографічного стеку (X25519, HKDF, Ascon-128a, TESLA) на двох класах апаратних платформ: 32-розрядній ARM Cortex-M4 та ARM64.

1. Криптографічні мікробенчмарки безпосередньо на Raspberry Pi 3 (ARM Cortex-A53) підтвердили мікросекундну латентність симетричних операцій (Ascon: 2,55–2,56 мкс, TESLA: 13,9–14,2 мкс, replay перевірка: 71,2 нс) та мілісекундну латентність асиметричної операції X25519 (≈1,13 мс на виклик), що забезпечує обробку близько 444 рукописних за секунду на одному ядрі. Енергетична вартість Ascon-шифрування становить ≈4,95 мДж і є приблизно у 440 разів (~2,6 порядки) меншою за X25519 (≈2,18 мДж) за формулою (1).

2. Вперше отримано точні експериментальні значення продуктивності безпосередньо на мікроконтролері ARM Cortex-M4 (48 МГц), агреговані за п'ятьма незалежними апаратними сеансами: Ascon-128a шифрування виконується за $0,337 \pm 0,002$ мс (енерговитрати 0,197 мДж), TESLA MAC — за $1,464 \pm 0,006$ мс (0,857 мДж), а повний цикл рукописання X25519 триває 187,94 мс (109,95 мДж). Це доводить практичну можливість використання сучасних асиметричних та симетричних легковагових криптографічних примітивів на ресурсно обмежених пристроях.

3. Макротести симулятора клієнтів підтвердили медіанну наскрізну латентність 0,267 мс та пропускну здатність 8,232 пакет/с; спостережена частка відхилень (0,231) точно відповідає очікуваній 0,231 після виправлення методики підрахунку бенчмарку (врахування попарсерного відкидання надто великих пакетів поряд із постпарсерним відхиленням) — усі 15 синтетичних атакуючих пакетів коректно заблоковано, що узгоджується з успішним результатом незалежної автоматизованої перевірки безпеки сервера (сценарії P0–P2).

4. Вимірювання енергоспоживання на Arduino Uno R4 WiFi показали, що пікове споживання під час передачі радіопакета зростає на 78 % від базового рівня (з 0,585 Вт до 1,043 Вт), що є прийнятним для автономних LPWAN вузлів з живленням від батарей. Для Raspberry Pi 3 Model B+ зростання становить лише 15 %, що забезпечує стабільну роботу edge сервера. Статистичний аналіз повного часового ряду показав, що електричний duty cycle Raspberry Pi (54,9 %) приблизно у 4,3 раза вищий за duty cycle Arduino (12,7 %) через фонове навантаження шлюзу (SQLite, HTTP API, OC).

5. Тривале тестування в міських умовах (3600 секунд, 711 переданих пакетів, 13 рукописних) та три додаткові незалежні прогони (сумарно 1104 передані пакети) не зафіксували жодної помилки кадрів чи передачі. Додатковий прогін на дистанції 500 м у міських умовах з підвищеною частотою перепідключень зафіксував PDR 99,3 % (141 з 142 очікуваних пакетів, 1 помилка декодування кадру, 15 відхилень через застарілу сесію) — реалістичніший сценарій деградації та коректного відновлення зв'язку, який не супроводжувався жодним пропуском атаки.

6. Зайняті ресурси пам'яті клієнтської прошивки (48 КБ Flash, 6 КБ SRAM) залишають понад 81 % ресурсів Arduino Uno R4 WiFi для прикладної логіки, що підтверджує придатність стеку для найбільш обмежених платформ.

Практичне значення роботи полягає у наданні кількісних доказів того, що легковагові криптографічні примітиви забезпечують рівень безпеки, порівнянний з традиційними протоколами, при на два–чотири порядки меншій латентності залежно від платформи та операції та в рази менших вимогах до пам'яті та енергоспоживання. Подальші дослідження будуть спрямовані на прямі порівняльні DTLS бенчмарки для кількісного зіставлення (включно зі стовпцями таблиці 7, наразі отриманими оціночно), уточнення методики симулятора макротестів та інтеграцію TinyML моделей для адаптивного профілювання радіочастотних відбитків.

Декларація про штучний інтелект. Під час підготовки цієї статті інструменти штучного інтелекту не використовувалися для генерації наукових результатів. Великі мовні моделі використовувалися виключно для перевірки орфографії, стилістичного редагування тексту та структурування статті згідно з вимогами журналу.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Чернявський, Б. В. (2026). Міжрівнева безпека IoT з використанням радіочастотних відбитків та легковагової криптографії. *Технічна інженерія*, 1(97), 324–331. [https://doi.org/10.26642/ten-2026-1\(97\)-324-331](https://doi.org/10.26642/ten-2026-1(97)-324-331)
2. Butun, I., Pereira, N., & Gidlund, M. (2020). A survey on the security of low power wide area networks: Threats, challenges, and potential solutions. *Sensors*, 20(20), 5800. <https://doi.org/10.3390/s20205800>
3. Rescorla, E., Tschofenig, H., & Modadugu, N. (2022). The Datagram Transport Layer Security (DTLS) protocol version 1.3 (RFC 9147). Internet Engineering Task Force. <https://doi.org/10.17487/RFC9147>
4. Turan, M. S., McKay, K., Chang, D., Bassham, L., Kang, J., Waller, N., Kelsey, J., & Hong, D. (2023). Status report on the final round of the NIST lightweight cryptography standardization process (NIST IR 8454). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8454>
5. Stanco, G., Navarro, A., Frattini, F., Ventre, G., & Botta, A. (2024). A comprehensive survey on the security of low power wide area networks for the Internet of Things. *ICT Express*, 10(3), 519–552. <https://doi.org/10.1016/j.icte.2024.03.003>
6. Hessel, F., Almon, L., & Hollick, M. (2023). LoRaWAN security: An evolvable survey on vulnerabilities, attacks and their systematic mitigation. *ACM Transactions on Sensor Networks*, 18(4), 1–55. <https://doi.org/10.1145/3561973>
7. Soltanieh, N., Norouzi, Y., Yang, Y., & Karmakar, N. C. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification*, 4(3), 222–233. <https://doi.org/10.1109/JRFID.2020.2968369>
8. Cherniavskyi, B. V. (2025). Cryptographic algorithms for IoT and full-size processors. *Advanced Top Technology*, 8. <https://doi.org/10.61718/att8.01>
9. Cherniavskyi, B. V., & Chernetchenko, D. V. (2025). Encryption and authentication models for data transmission between radio receivers and web services. In *Proceedings of the 3rd International Scientific and Practical Conference "Modern Science, Economy and Digital Innovation"* (pp. 145–148). International Scientific Unity. <https://doi.org/10.70286/ISU-07.05.2025>
10. Dobraunig, C., Eichlseder, M., Mendel, F., & Schl  ffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34(3), Article 33. <https://doi.org/10.1007/s00145-021-09398-9>
11. Langley, A., Hamburg, M., & Turner, S. (2016). Elliptic curves for security (RFC 7748). Internet Engineering Task Force. <https://doi.org/10.17487/RFC7748>
12. Krawczyk, H., & Eronen, P. (2010). HMAC-based extract-and-expand key derivation function (HKDF) (RFC 5869). Internet Engineering Task Force. <https://doi.org/10.17487/RFC5869>
13. Perrig, A., Song, D., Canetti, R., Tygar, J. D., & Briscoe, B. (2005). Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction (RFC 4082). Internet Engineering Task Force. <https://doi.org/10.17487/RFC4082>
14. Чернявський, Б. В., & Чернеченко, Д. В. (2025). Алгоритми шифрування: всебічне дослідження. *Наука і техніка сьогодні*, 4(45), 1642–1648. [https://doi.org/10.52058/2786-6025-2025-4\(45\)-1642-1648](https://doi.org/10.52058/2786-6025-2025-4(45)-1642-1648)
15. Xu, L., & Wang, H. (2024). A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. *Sensors*, 24(22), 7209. <https://doi.org/10.3390/s24227209>

References

1. Cherniavskyi, B. V. (2026). Cross-layer IoT security using radio frequency fingerprinting and lightweight cryptography [In Ukrainian]. *Technical Engineering*, 1(97), 324–331. [https://doi.org/10.26642/ten-2026-1\(97\)-324-331](https://doi.org/10.26642/ten-2026-1(97)-324-331)
2. Butun, I., Pereira, N., & Gidlund, M. (2020). A survey on the security of low power wide area networks: Threats, challenges, and potential solutions. *Sensors*, 20(20), 5800. <https://doi.org/10.3390/s20205800>
3. Rescorla, E., Tschofenig, H., & Modadugu, N. (2022). The Datagram Transport Layer Security (DTLS) protocol version 1.3 (RFC 9147). Internet Engineering Task Force. <https://doi.org/10.17487/RFC9147>
4. Turan, M. S., McKay, K., Chang, D., Bassham, L., Kang, J., Waller, N., Kelsey, J., & Hong, D. (2023). Status report on the final round of the NIST lightweight cryptography standardization process (NIST IR 8454). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8454>
5. Stanco, G., Navarro, A., Frattini, F., Ventre, G., & Botta, A. (2024). A comprehensive survey on the security of low power wide area networks for the Internet of Things. *ICT Express*, 10(3), 519–552. <https://doi.org/10.1016/j.icte.2024.03.003>

6. Hessel, F., Almon, L., & Hollick, M. (2023). LoRaWAN security: An evolvable survey on vulnerabilities, attacks and their systematic mitigation. *ACM Transactions on Sensor Networks*, 18(4), 1–55. <https://doi.org/10.1145/3561973>
7. Soltanieh, N., Norouzi, Y., Yang, Y., & Karmakar, N. C. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification*, 4(3), 222–233. <https://doi.org/10.1109/JRFID.2020.2968369>
8. Cherniavskyi, B. V. (2025). Cryptographic algorithms for IoT and full-size processors. *Advanced Top Technology*, 8. <https://doi.org/10.61718/att8.01>
9. Cherniavskyi, B. V., & Chernetchenko, D. V. (2025). Encryption and authentication models for data transmission between radio receivers and web services. In *Proceedings of the 3rd International Scientific and Practical Conference "Modern Science, Economy and Digital Innovation"* (pp. 145–148). International Scientific Unity. <https://doi.org/10.70286/ISU-07.05.2025>
10. Dobraunig, C., Eichlseder, M., Mendel, F., & Schl  ffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34(3), Article 33. <https://doi.org/10.1007/s00145-021-09398-9>
11. Langley, A., Hamburg, M., & Turner, S. (2016). Elliptic curves for security (RFC 7748). Internet Engineering Task Force. <https://doi.org/10.17487/RFC7748>
12. Krawczyk, H., & Eronen, P. (2010). HMAC-based extract-and-expand key derivation function (HKDF) (RFC 5869). Internet Engineering Task Force. <https://doi.org/10.17487/RFC5869>
13. Perrig, A., Song, D., Canetti, R., Tygar, J. D., & Briscoe, B. (2005). Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction (RFC 4082). Internet Engineering Task Force. <https://doi.org/10.17487/RFC4082>
14. Cherniavskyi, B. V., & Chernetchenko, D. V. (2025). Encryption algorithms: A comprehensive study [In Ukrainian]. *Science and Technology Today*, 4(45), 1642–1648. [https://doi.org/10.52058/2786-6025-2025-4\(45\)-1642-1648](https://doi.org/10.52058/2786-6025-2025-4(45)-1642-1648)
15. Xu, L., & Wang, H. (2024). A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. *Sensors*, 24(22), 7209. <https://doi.org/10.3390/s24227209>

Надійшла до редакції: 30.06.2026

Прийнята до друку: 15.09.2026

Опубліковано: 30.09.2026