https://doi.org/10.31891/2219-9365-2025-83-33
УДК 621.396

БОЙКО Юлій
Хмельницький національний університет
https://orcid.org/0000-0003-0603-7827
e-mail: boiko_julius@ukr.net
МІШАН Віктор
Хмельницький національний університет
https://orcid.org/0000-0002-2771-7285
e-mail: V_mishan@ukr.net
ЯВТУШЕНКО Дмитро
Хмельницький національний університет
e-mail: dima.chef98@gmail.com

ЛЕГКІ КРИПТОСИСТЕМИ В ТЕЛЕКОМУНІКАЦІЙНИХ СЕРЕДОВИЩАХ IOT І 5G: ВИКЛИКИ, АРХІТЕКТУРИ ТА КОМПРОМІСИ БЕЗПЕКИ

У статті проведено детальний аналіз архітектури безпеки мереж 5G з акцентом на багаторівневу модель захисту, що охоплює рівні NAS, AS і транспортної безпеки. Розглянуто основні криптографічні алгоритми (AES, ZUC, SNOW 3G), їх характеристики, сфери застосування та енергоефективність в умовах мобільного середовища. Описано ієрархію ключів, яка забезпечує надійність та локалізацію ризиків у разі компрометації. Представлено перспективи розвитку механізмів захисту з урахуванням зростаючих вимог до Інтернету речей (IoT), квантостійких технологій і віртуалізації мереж.

Ключові слова: Інтернет речей (IoT), 5G мережі, легка криптографія, симетричні шифри, протоколи безпеки, атаки.

BOIKO Juliy, MISHAN Viktor, YAVTUSHENKO Dmytro
Khmelnytskyi National University

LIGHTWEIGHT CRYPTOSYSTEMS IN IOT AND 5G TELECOMMUNICATION ENVIRONMENTS: CHALLENGES, ARCHITECTURES, AND SECURITY TRADE-OFFS

This paper provides a comprehensive analysis of the security architecture in 5G networks, focusing on a multi-layered protection framework that ensures confidentiality, integrity, and authenticity across various communication interfaces. The study examines three primary security layers—Non-Access Stratum (NAS) security, Access Stratum (AS) security, and transport security—highlighting their specific roles in safeguarding signaling, radio channels, and interactions between network components, respectively. Key cryptographic algorithms standardized in 5G, including AES, ZUC, and SNOW 3G, are analyzed in terms of their encryption and integrity verification capabilities, computational efficiency, and suitability for various deployment scenarios such as mobile broadband, IoT, and ultra-reliable low-latency communications (URLLC).

A detailed examination of the hierarchical key management system reveals the cascading generation of cryptographic keys from a root key securely stored in the user's USIM and the home network. This structure minimizes risks by isolating potential compromises within localized key subsets, thereby preserving overall system security. The paper also discusses transport-layer protocols such as IPsec, TLS, and DTLS, which protect inter-network communication channels between base stations, user plane functions, and core network elements.

Furthermore, the study addresses emerging challenges in 5G security, including the need for enhanced protection mechanisms against evolving threats, integration of quantum-resistant algorithms, and adaptation to virtualization and software-defined networking (SDN) paradigms. The findings offer valuable insights for researchers and industry practitioners aiming to optimize security solutions while maintaining performance and energy efficiency in next-generation mobile networks.

Keywords: Internet of Things (IoT), 5G networks, lightweight cryptography, symmetric ciphers, security protocols, attacks.

Стаття надійшла до редакції / Received 11.07.2025
Прийнята до друку / Accepted 14.08.2025

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

Активне впровадження технологій п'ятого покоління мобільного зв'язку (5G) [1, 2] та розгортання масового Інтернету речей (IoT) [3] створює нові виклики у сфері інформаційної безпеки [4]. У порівнянні з попередніми поколіннями, сучасні телекомунікаційні середовища характеризуються динамічними топологіями, високою щільністю вузлів, обмеженими енергетичними та обчислювальними ресурсами, а також широким спектром загроз — від пасивного перехоплення до активних атак із залученням IoT-ботнетів і каналів бокового витоку. Забезпечення конфіденційності, цілісності та автентичності даних у таких умовах вимагає переосмислення підходів до побудови криптографічних протоколів.

Класичні криптосистеми (AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), DES (Data Encryption Standard) тощо) [5, 6], хоча і залишаються основою сучасної криптографії, часто є надмірно ресурсоємними для обмежених пристроїв, що працюють у межах IoT або на периферії 5G-мереж. У зв'язку з цим особливого значення набуває розвиток легких (lightweight) криптографічних алгоритмів, таких як

PRESENT, SIMON, SPECK, ZUC, SNOW3G [7, 8], а також інноваційних авторських схем, адаптованих до специфіки телекомунікаційних протоколів.

Крім того, актуальною задачею є аналіз та оптимізація криптографічного стеку безпеки 5G, що охоплює як рівень доступу (NAS Security), так і рівень радіоінтерфейсу (AS Security), з урахуванням особливостей протоколів TLS/DTLS, IPSec, EEA3/ZUC тощо [9]. Розуміння принципів їх взаємодії та можливих вразливостей є критичним як для теоретичного моделювання, так і для практичної реалізації безпечних мобільних систем нового покоління. Таким чином, постає потреба в системному аналізі легких криптосистем із точки зору їх ефективності, стійкості до атак, сумісності з телекомунікаційними стандартами та компромісів між безпекою, швидкодією і енергоспоживанням.

Метою роботи є комплексне дослідження легких криптосистем, їх архітектурних особливостей та доцільності застосування в середовищах IoT та 5G з урахуванням обмежень ресурсів, потенційних векторів атак і вимог до реального часу. Основна увага зосереджена на аналізі та порівнянні відомих криптографічних алгоритмів (PRESENT, SIMON, SPECK, ZUC тощо) і безпекових стеків з точки зору їхньої безпеки, швидкодії та обчислювальної складності. Результати дослідження мають практичне значення для розробки захищених протоколів у бездротових сенсорних мережах, IoT-шлюзах, 5G-модемах та енергоефективних edge-пристроях, де класична криптографія є надмірною або неефективною.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Дослідження наукових публікацій [1–5], вивчення стандартів і нормативних актів [10], а також аналіз технічних звітів [11] дають змогу сформувати цілісне уявлення про специфіку побудови безпечних телекомунікаційних середовищ нового покоління, таких як Інтернет речей (IoT) і мережі 5G. Ці середовища відзначаються високою динамікою, великою кількістю пристроїв з обмеженими ресурсами, а також жорсткими вимогами до затримок і енергоспоживання — особливо у критичних сценаріях (URLLC, mMTC, eMBB)[12]. У цьому контексті постає необхідність у розробці легких криптографічних рішень [13], які здатні забезпечити надійний захист інформації без перевантаження обчислювальних або енергетичних ресурсів пристроїв. Традиційні алгоритми, такі як AES чи RSA [5], демонструють високу криптостійкість, однак виявляються занадто ресурсоємними для сенсорних вузлів, мікроконтролерів або енергонезалежних IoT-модулів. Це зумовлює зростаючу увагу до lightweight-криптографії, зокрема до сімейств PRESENT, SIMON, SPECK, ZUC, SNOW3G, а також до спеціалізованих авторських підходів.

На рис. 1 представлено узагальнену концептуальну схему криптографічних вимог до середовища IoT/5G. Зліва показано архітектурні та функціональні особливості, які формують контекст криптозахисту — зокрема, обмеженість ресурсів, мобільність пристроїв, масштабність підключень та специфіка трафіку в середовищі 5G. У центрі зосереджено типові загрози: перехоплення, підміна вузлів, атаки через побічні канали. Праворуч деталізовано вимоги до криптографії — легкість реалізації, висока швидкодія, енергоефективність, стійкість до фізичних атак, а також перспективна вимога — квантова стійкість. Дана схема дозволяє узагальнити взаємозв'язки між технічними обмеженнями, загрозами та функціональними властивостями криптозасобів у телекомунікаційних середовищах.

Рис. 1. Вимоги до криптографії в контексті IoT та 5G

Подальшу деталізацію структурної організації захищеної взаємодії між IoT-пристроями і мережею 5G представлено на рис.2. Блок-схема ілюструє типову архітектуру маршрутизації даних від пристрою до хмарної платформи з проходженням через вузли edge-обробки, ядро 5G-мережі та сервіси зберігання/обробки. В кожному з етапів впроваджуються відповідні безпекові механізми: від легких симетричних шифрів на сенсорах до наскрізного шифрування в хмарі. Значна увага приділяється автентифікації, запобіганню підміні, сертифікації пристроїв, а також захисту від атак типу man-in-the-middle. Таким чином, рис. 2 демонструє повний цикл захисту в системі, де кожен рівень має власні специфічні вимоги і обмеження щодо реалізації криптографічних рішень.

Рис. 2. Блок-схема архітектури захищеної взаємодії компонентів IoT у мережі 5G

Аналіз наукової літератури [3-10] показує, що одним із основних напрямів у забезпеченні захисту є симетрична криптографія, оскільки вона забезпечує мінімальні витрати ресурсів і високу продуктивність. На рис. 3 представлено типову модель симетричної криптосистеми, де один і той самий ключ використовується для шифрування і дешифрування. Потік даних проходить через передавач, шифратор, канал, дешифратор і приймач. Пунктирною стрілкою позначено напрямок передавання ключа, який звичайно не передається основним каналом, а узгоджується заздалегідь або передається окремим способом. Ця модель ілюструє принципову перевагу симетричних шифрів у контексті IoT — простота реалізації, низькі затримки, можливість апаратного прискорення.

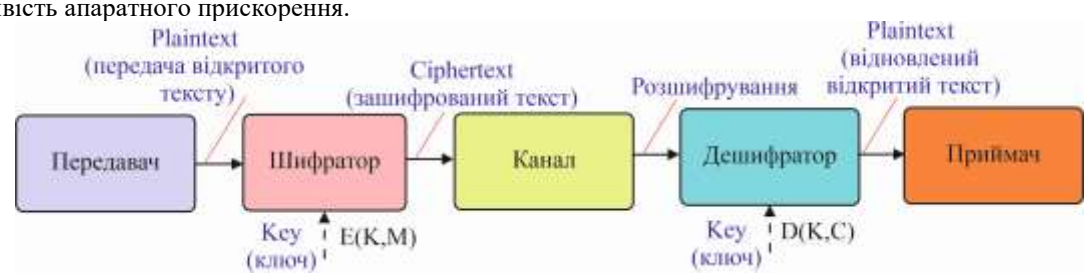

Рис. 3. Структура симетричної криптосистеми: пунктирна стрілка означає, що ключ не передається по основному каналу, а є частиною внутрішнього процесу — або попередньо переданий, або спільно узгоджений (тобто той самий або симетричний ключ застосовується для відновлення повідомлення); E(K,M) - позначення криптографічної операції шифрування (Encryption); D(K,C) - позначення криптографічної операції дешифрування (Decryption) [14]

Окрему увагу слід приділити легким блочним шифрам [14], які базуються на архітектурі Substitution-Permutation Network (SPN). На рис. 4 подано структуру одного з найвідоміших lightweight-алгоритмів — PRESENT. Шифрування в PRESENT реалізується в 31 раунд, кожен з яких складається з додавання ключа (XOR), нелінійного перетворення (*S*-Box) та перестановки (*P*-Layer). Особливістю алгоритму є компактна 4-бітна *S*-Box, яка забезпечує криптостійкість при мінімальних апаратних витратах. Завдяки своїй простій, але ефективній структурі, PRESENT став популярним у вбудованих системах, смарт-картках і сенсорах. Його архітектура забезпечує баланс між захистом та продуктивністю, що робить його особливо привабливим для використання в IoT/5G.

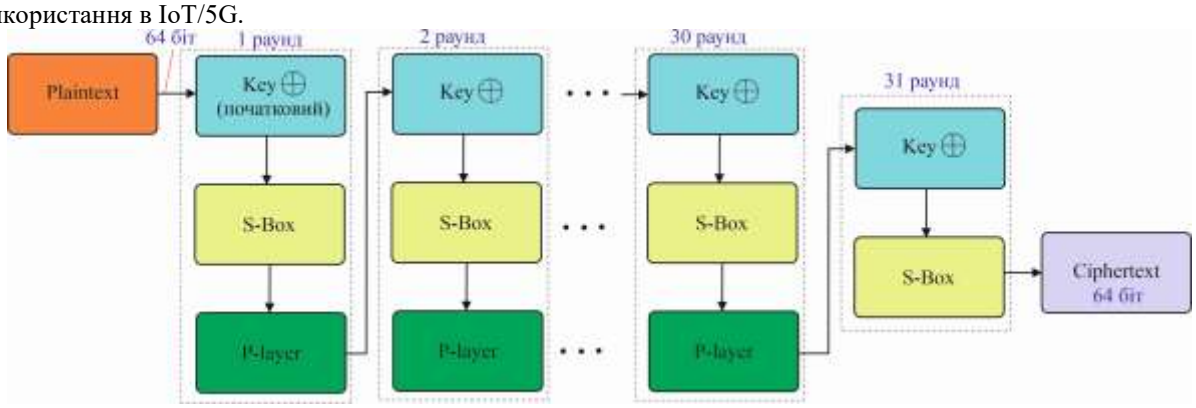

Рис. 4. Структурну схема блочного шифру типу Substitution-Permutation Network (SPN) на прикладі криптографічного алгоритму PRESENT: $\oplus$ - це операція побітового додавання за модулем 2 (XOR) між даними та раундовим ключем

Крім блочних, активно використовуються і потокові шифри — такі як Trivium, Grain, Spritz [15], які ідеально підходять для режимів реального часу. Вони ґрунтуються на генерації псевдовипадкових бітів і мають надзвичайно малу затримку. Потокові шифри також зручні для реалізації у пристроях, де важлива швидка реакція на події або передавання коротких повідомлень.

Важливим викликом у проєктуванні легких криптосистем є досягнення необхідного рівня криптостійкості при обмежених обчислювальних ресурсах. На рис. 5 представлено трикутник компромісів у легкій криптографії (lightweight cryptography trade-off triangle), що дозволяє порівняти кілька алгоритмів шифрування в трикомпонентному просторі за критеріями Security (Безпека) — стійкість алгоритму до відомих

атак; Performance (Продуктивність) — швидкодія реалізації, затримки обробки; Area (Площа) — апаратна складність (кількість логічних елементів, пам'яті тощо). На візуалізації чітко видно компроміси, коли AES має найвищу криптостійкість, але низьку продуктивність та апаратну ефективність, PRESENT навпаки демонструє максимальну ефективність за апаратними параметрами, але нижчу безпеку, а SIMON вирізняється збалансованим профілем.

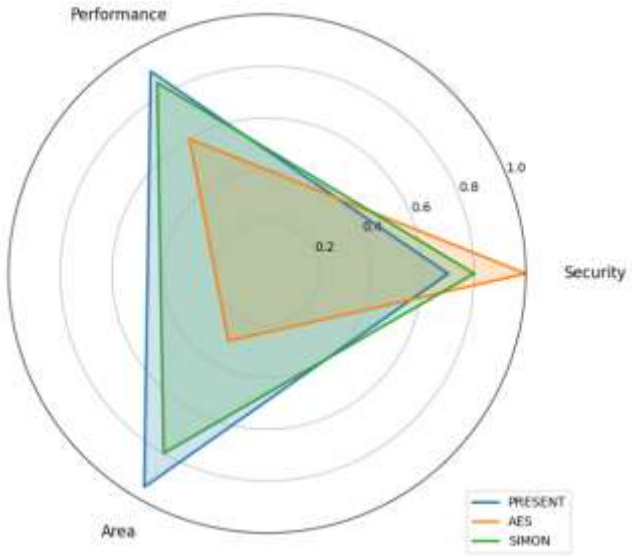

Рис. 5. Трикутник компромісів у легкій криптографії

Стрімкий розвиток технологій IoT та 5G розширює цифрову поверхню атак. Обмеження пристроїв, відсутність оновлень, низький рівень автентифікації роблять такі системи привабливими для зловмисників. Стосовно вразливостей IoT, однією з ключових проблем є обмежені ресурси пристроїв, що не дозволяють використовувати складні криптографічні алгоритми без суттєвих оптимізацій. Через це зростає ризик використання спрощених або застарілих методів захисту. Ще одним критичним аспектом є відсутність механізмів оновлення прошивки. Багато пристроїв IoT не мають підтримки автоматичних оновлень, що сприяє збереженню відомих вразливостей протягом усього терміну експлуатації. Проблему також становить використання заводських паролів або повна відсутність автентифікації. Це відкриває можливості для несанкціонованого доступу до пристроїв з мінімальними зусиллями з боку зловмисника. Особливості атак у 5G пов'язана з тим, що значно розширюється площа атаки через використання віртуалізації мережевих функцій (NFV) і програмно-керованих мереж (SDN). Це створює нові точки входу та вразливості на рівні інфраструктури. Атаки на радіоінтерфейс також залишаються актуальними. До них належать перехоплення переданих даних, їх глушіння, підміна (spoofing) або спотворення сигналу. Такі загрози ускладнюють гарантування цілісності та достовірності інформації. Загрози для MEC (Multi-access Edge Computing — технології обчислення на краю мережі з багатьма точками доступу) пов'язані з тим, що обробка даних здійснюється ближче до користувача — на краю мережі. Атаки на ці вузли можуть призвести до компрометації локальної інфраструктури, витоку даних або зниження доступності сервісів. Окрему категорію становлять DoS- та DDoS-атаки, які є особливо небезпечними для сервісів, що працюють у реальному часі. Такі атаки можуть повністю паралізувати обслуговування критичних застосувань, зокрема в охороні здоров'я, транспорті чи промисловості.

На схемі моделі загроз у середовищі IoT/5G, рис. 6, показано взаємодію пристрою з векторами атак, що оточують його ззовні. В центрі знаходиться IoT-пристрій (наприклад, смарт-сенсор), який взаємодіє з мережею, хмарними обчисленнями та інфраструктурою передачі даних.

Рис. 6. Модель загроз у середовищі IoT та 5G

В таблиці 1 систематизовано типові атаки для IoT і 5G.
На рис. 6 представлено класифікацію атак на IoT/5G системи.

Таблиця 1

Типові атаки для IoT і 5G

Тип атаки	Ціль атаки	Потенційний вплив
Підміна вузлів (spoofing)	Ідентифікація, автентифікація	Незаконний доступ, перехоплення даних
Атака "людина посередині" (MitM- Man-in-the-Middle)	Канал зв'язку між вузлами	Модифікація або викрадення даних
Витік побічних каналів	Апаратна реалізація	Отримання криптографічних ключів
Brute-force та криптоаналіз	Шифрування даних	Декодування секретної інформації
DoS/DDoS-атаки	Інфраструктура зв'язку	Порушення роботи сервісів, недоступність

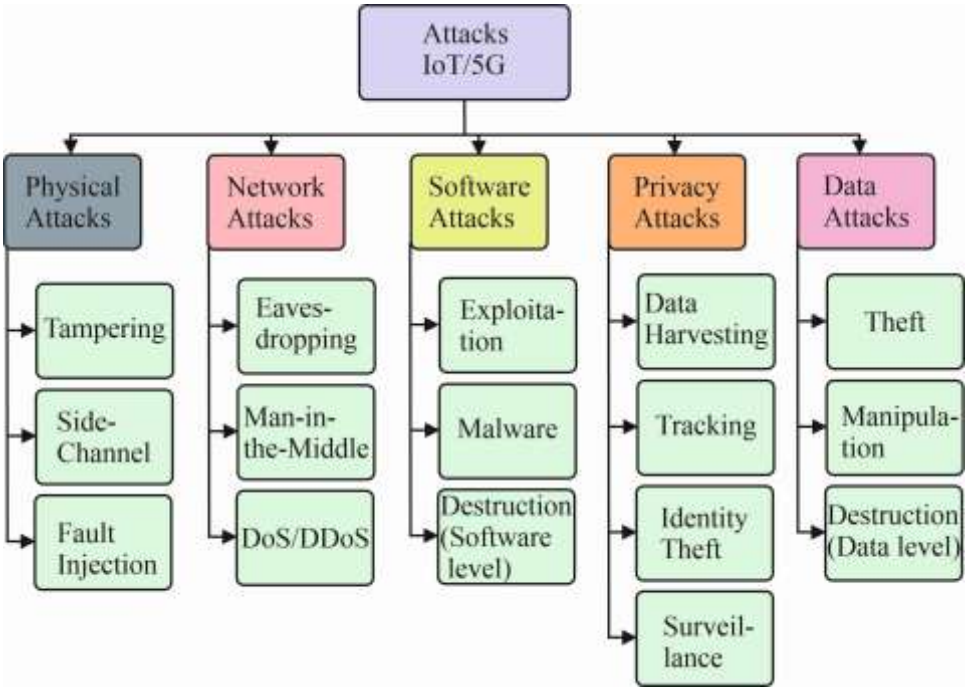

Рис. 7. Класифікація атак на IoT/5G системи

На рис. 7 представлено класифікацію атак на системи IoT та 5G у вигляді дерева категорій. Ця класифікація охоплює п'ять основних напрямів: фізичні, мережеві, програмні атаки, атаки на конфіденційність та атаки на дані. До фізичних атак належать tampering — безпосереднє фізичне втручання в обладнання з метою зміни його функціонування або отримання доступу до критичних компонентів, side-channel атаки — отримання конфіденційної інформації за допомогою аналізу електромагнітного випромінювання, часу обробки або споживання енергії, а також fault injection — цілеспрямоване створення збоїв (наприклад, зміна напруги або вплив лазера) для обходу захисних механізмів. Мережеві атаки включають eavesdropping — несанкціоноване прослуховування мережевого трафіку, що дозволяє зловмиснику отримувати приватні дані; атаки типу MitM (Man-in-the-Middle), під час яких перехоплюються або змінюються дані, що передаються між сторонами; а також DoS/DDoS — атаки на відмову в обслуговуванні, спрямовані на перевантаження інфраструктури та порушення доступності сервісів. Програмні атаки охоплюють exploitation — використання вразливостей програмного забезпечення для несанкціонованого доступу; впровадження шкідливого ПЗ (malware), яке може порушувати роботу пристрою, викрадати дані або забезпечувати прихований контроль; destruction на рівні програмного забезпечення — повне виведення системи з ладу шляхом навмисної модифікації або видалення критичних компонентів. Атаки на конфіденційність включають data harvesting — масовий збір персональних або службових даних без дозволу користувача, tracking — відстеження місцезнаходження та поведінки пристроїв або користувачів, identity theft — крадіжку особистих даних для видавання себе за іншу особу, а також surveillance — безперервний контроль за діями користувачів з метою шпигування або маніпуляції. Нарешті, атаки на дані включають theft — викрадення інформації, що може бути використане зловмисниками для шантажу або фінансової вигоди; manipulation — навмисне спотворення даних для впливу на прийняття рішень або

порушення функціонування системи; destruction на рівні даних — повне знищення або пошкодження інформації, що нерідко має незворотні наслідки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

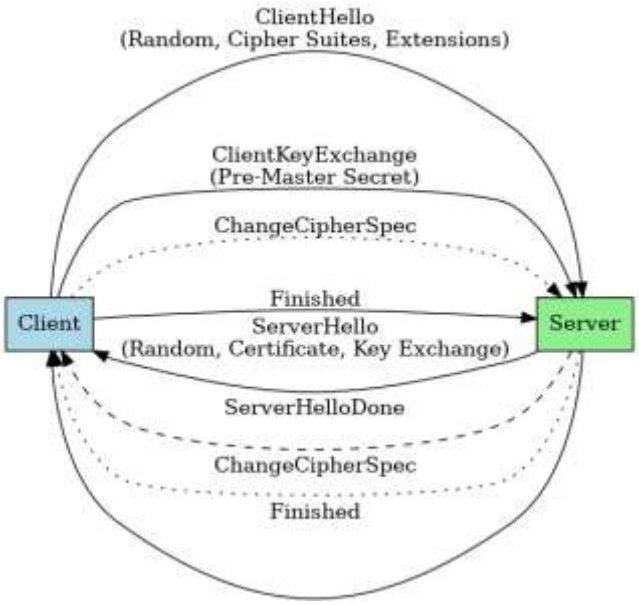

Рис. 8. Блок-схема TLS/DTLS-з'єднання, яка демонструє процес рукостискання між клієнтом (Client) і сервером (Server): прямі стрілки — повідомлення від клієнта до сервера; зворотні стрілки — відповідь сервера клієнту; пунктирна стрілка — повідомлення ServerHelloDone; точкова стрілка — повідомлення ChangeCipherSpec

В сучасних телекомунікаційних системах, особливо в контексті IoT та 5G, криптографія є невід'ємною складовою безпекових протоколів. Вона забезпечує конфіденційність, цілісність та автентифікацію даних, реалізуючись через протоколи TLS, DTLS, IPSec, а також спеціалізовані алгоритми, зокрема ZUC та 128-EEA3/128-EIA3. Протокол TLS (Transport Layer Security) є основним стандартом для захисту трафіку в інтернеті, підтримуючи як симетричне (AES, ChaCha20), так і асиметричне шифрування (RSA, ECDSA). Одним з ключових механізмів TLS є HMAC — алгоритм автентифікації повідомлень, що базується на хеш-функціях, наприклад, SHA-256 (1). Він передбачає подвійне хешування з використанням внутрішнього (ipad) та зовнішнього (opad) заповнення, що дозволяє досягти високого рівня криптографічної надійності. Для систем із обмеженими ресурсами, таких як IoT, застосовується оптимізована версія — TLS-PSK (pre-shared key), яка усуває потребу у витратному обміні відкритими ключами.

$$\mathrm{HMAC}(K, m) = H((K' \oplus \mathrm{opad}) \,\mathrm{P}\, H((K' \oplus \mathrm{ipad}) \,\mathrm{P}\, m)) \tag{1}$$

де H - хеш-функія (SHA-256 - Secure Hash Algorithm, з довжиною вихідного хешу — 256 біт (32 байти)); K - ключ; m - повідомлення; $\oplus$ — побітове XOR, ‖ — конкатенація (додавання зліва направо), ipad — внутрішній пад (0x36 повторення до довжини блоку, тобто послідовність байтів коли байт 0x36 (шістнадцяткове представлення байта) повторюється стільки разів, скільки потрібно, щоб отримати повний блок хеш-функції); opad — зовнішній пад (0x5c повторення до довжини блоку).

На рис. 8 подано узагальнену блок-схему TLS/DTLS-з'єднання, яка ілюструє фазу рукостискання (handshake) між клієнтом і сервером, включаючи обмін повідомленнями, узгодження параметрів шифрування, передачу pre-master secret і перехід до зашифрованої комунікації. Протокол DTLS є адаптацією TLS для ненадійних середовищ передачі, зокрема UDP, що характерно для IoT-мереж. Він передбачає захист від втрат і повторів пакетів, а також зберігає криптографічні властивості TLS. Широко використовується, зокрема, в CoAP — легковаговому протоколі для обміну даними між пристроями з обмеженими можливостями.

Протокол IPSec, у свою чергу, функціонує на мережевому рівні, забезпечуючи захист IP-пакетів. Його компоненти AH (Authentication Header) та ESP (Encapsulating Security Payload), зображені на рис. 9, відповідають за автентифікацію, контроль цілісності та шифрування даних. AH гарантує цілісність усього пакета, але не забезпечує конфіденційності, тоді як ESP додає шифрування до переданих даних, захищаючи корисне навантаження. У залежності від режиму (транспортного або тунельного), ці механізми можуть використовуватись окремо або в поєднанні. Шифрування реалізується з використанням алгоритмів AES, 3DES (потрійний DES [6]), а також хеш-функцій в наступному формалізованому вигляді:

$$\mathrm{ESP}(P) = \mathrm{Enc}(K, P) \,\mathrm{P}\, \mathrm{MAC}(K, \mathrm{Enc}(K, P)) \tag{2}$$

де P - корисне навантаження (початкове повідомлення, або пакет даних); K - ключ шифрування; $\mathrm{Enc}(K, P)$ - позначення процедури шифрування повідомлення P за допомогою ключа K; $\mathrm{MAC}(K, \mathrm{Enc}(K, P))$ - код автентичності повідомлення (Message Authentication Code), який обчислюється від зашифрованого повідомлення і теж із ключем K; ‖ — операція конкатенації (об'єднання) двох послідовностей.

Для мобільних мереж 3GPP та систем 5G розроблено спеціалізовані криптоалгоритми, серед яких ключову роль відіграє потоковий шифр ZUC. Його архітектура включає лінійні та нелінійні компоненти — зокрема, LFSR (Linear Feedback Shift Register), блок переструктурування бітів (Bit Reorganization) і нелінійну функцію *F* із *S*-box перетворенням.

Рис. 9. Структурна схема IPSec-заголовків: AH (Authentication Header) і ESP (Encapsulating Security Payload)

На рис. 10 зображено блок-схему ZUC, що демонструє всі етапи — від ініціалізації ключа й вектора до генерації криптостійкого потоку бітів. У процесі шифрування отриманий потік XOR-ується з відкритим текстом, а під час дешифрування — з шифротекстом. Основою ZUC є нелінійна структура з використанням 16-розрядних регістрів наступної конфігурації:

$$\mathbf{KS}_i = \mathrm{ZUC}(K, IV, i) \tag{3}$$

де K - ключ; IV - ініціалізаційний вектор (що забезпечує унікальність потоку для кожного сеансу або повідомлення шляхом внесення рандомізації тобто різноманіття в процес генерації потоку); i - номер такту (індекс (номер) блока ключової послідовності, який генерується); $\mathbf{KS}_i$ - це *i*-та частина (або *i*-й блок) ключової послідовності (Key Stream), яку використовують у потоковому шифруванні; ZUC - це назва потокового шифру (stream cipher), затвердженого в стандартах 3GPP (для мобільних мереж LTE і 5G), який генерує псевдовипадкову послідовність (ПВП) на основі ключа і ініціалізаційного вектора.

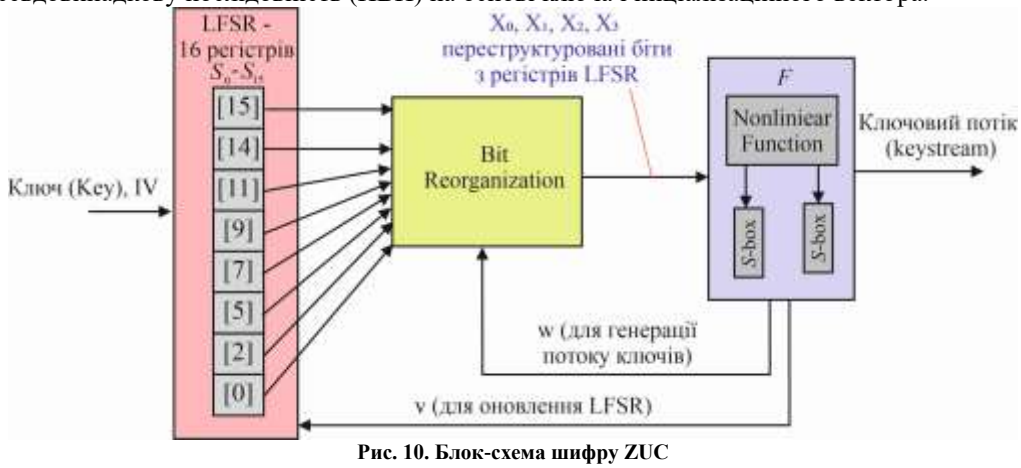

Рис. 10. Блок-схема шифру ZUC

ZUC є базовим компонентом для реалізації алгоритмів 128-EEA3 (шифрування) та 128-EIA3 (аутентифікація), що стандартизовані для LTE та 5G. У контексті EEA3, як показано у формулі (4), відбувається побітове змішування відкритого тексту з псевдовипадковим ключовим потоком. Це дозволяє досягати високої швидкодії, низького енергоспоживання та прийнятного рівня безпеки при обмежених обчислювальних можливостях пристроїв.

$$C_i = P_i \oplus \mathrm{KS}_i \tag{4}$$

де P_i - бітове повідомлення (*i*-й блок (або *i*-та частина)) відкритого тексту (Plaintext) — тобто початкових даних, які потрібно зашифрувати); C_i - зашифрований біт (*i*-й блок зашифрованого тексту (Ciphertext)); KS_i - біт ключового потоку (*i*-й блок ключової послідовності (Key Stream), псевдовипадковий

набір бітів, згенерований шифром (зокрема, ZUC)); ⊕ — операція XOR (виключне АБО) між двома бінарними послідовностями.

На рис. 11 представлено порівняльну діаграму енергоспоживання різних криптографічних протоколів при обробці 1 КБ даних. Найменше енергоспоживання демонструє ZUC, що робить його надзвичайно ефективним для енергообмежених середовищ, таких як IoT. TLS і DTLS мають вищі енергетичні витрати, але забезпечують гнучкість і підтримку широкого спектра пристроїв. IPSec, хоча й пропонує максимальний рівень безпеки, виявляється занадто ресурсоємним для пристроїв з обмеженим живленням. Підсумкові характеристики криптографічних алгоритмів систематизовано в табл. 2. Згідно з нею, ZUC вирізняється найвищою швидкодією та енергоефективністю, що підтверджує його доцільність для мобільних і вбудованих систем. TLS/DTLS залишаються стандартом для захисту інтернет-з'єднань, тоді як IPSec краще підходить для застосувань із високими вимогами до безпеки, але не підходить для обмежених пристроїв.

Поява 5G призвела до суттєвого ускладнення мережевої архітектури, яка включає розподілену мережу доступу (RAN), хмарне ядро (5GC), а також широке коло пристроїв користувачів (UE). У цьому контексті захист інформації став фундаментальним елементом функціонування інфраструктури, оскільки будь-який компонент мережі може виступати потенційним вектором атаки [14].

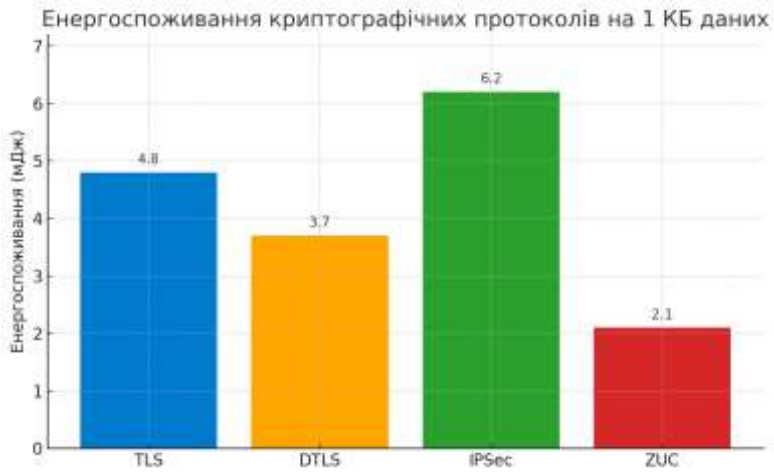

Рис. 11. Графік порівняння енергоспоживання для різних криптографічних протоколів — TLS, DTLS, IPSec, ZUC

Таблиця 2

Систематизовані показники порівняння криптографічних алгоритмів

Алгоритм	Швидкодія (Мбіт/с)	Енергоспоживання (мДж/КБ)	Рівень безпеки	Підтримка в IoT
ZUC	100–150	2.1	Високий (128 біт)	✓ (3GPP, 5G, IoT)
TLS	20–50	~4.8	Високий (до 256 біт)	✓ (Wi-Fi, HTTPS)
DTLS	10–40	~3.7	Високий (до 256 біт)	✓ (UDP IoT мережі)
IPSec	5–15	~6.2	Дуже високий (до 256 біт)	✕ (занадто ресурсоємний)

У 5G системі безпека реалізується як багаторівнева архітектура, в якій захист забезпечується на різних рівнях взаємодії. В межах стеку реалізовано три основні рівні захисту (рис. 12), що утворюють багаторівневу систему безпеки. Рівень NAS (Non-Access Stratum) відповідає за шифрування та забезпечення цілісності сигналізаційного обміну між користувацьким обладнанням (UE) та ядром мережі (функції AMF/SMF). На цьому рівні застосовуються криптоалгоритми серії NEA та NIA, які забезпечують конфіденційність службових повідомлень і захищають ідентифікатори користувача від розкриття. Рівень AS (Access Stratum) забезпечує захист радіоканалу між UE та базовою станцією (gNB), включаючи шифрування даних користувача, перевірку цілісності сигналів керування (RRC Signaling) та безпеку передачі на рівні користувацької площини (User Plane). Вищим рівнем є транспортна безпека (Transport Security), яка охоплює захист міжмережевих інтерфейсів між елементами інфраструктури, такими як gNB, UPF та компоненти ядра, через стандартизовані протоколи IPSec, TLS або DTLS (інтерфейси N2, N3, N6, N9). Такий розподіл забезпечує наскрізну криптографічну безпеку як на рівні доступу, так і всередині самої мережі.

У стандарті 5G, визначеному 3GPP [1], застосовуються три основні криптографічні алгоритми, які використовуються як для шифрування (NEA), так і для забезпечення цілісності даних (NIA). AES (NEA2/NIA2) є блочним шифром з довжиною блоку 128 біт, який забезпечує високий рівень криптостійкості та має широке апаратне прискорення. Водночас, його підвищене енергоспоживання обмежує ефективність у

мобільних та енергообмежених пристроях, зокрема в IoT. ZUC (NEA3/NIA3) — потоковий шифр, спеціально оптимізований для мобільних систем — забезпечує високу продуктивність при мінімальному споживанні енергії, що робить його особливо ефективним у сценаріях із обмеженими обчислювальними ресурсами, таких як massive MTC або URLLC. SNOW 3G (NEA1/NIA1), як спадкоємець криптографії поколінь 3G/4G, зберігає свою актуальність у системах зі зворотною сумісністю. Його швидкодія нижча, ніж у ZUC, а енергоспоживання помірне, що робить його прийнятним, але менш оптимальним для новітніх 5G-архітектур.

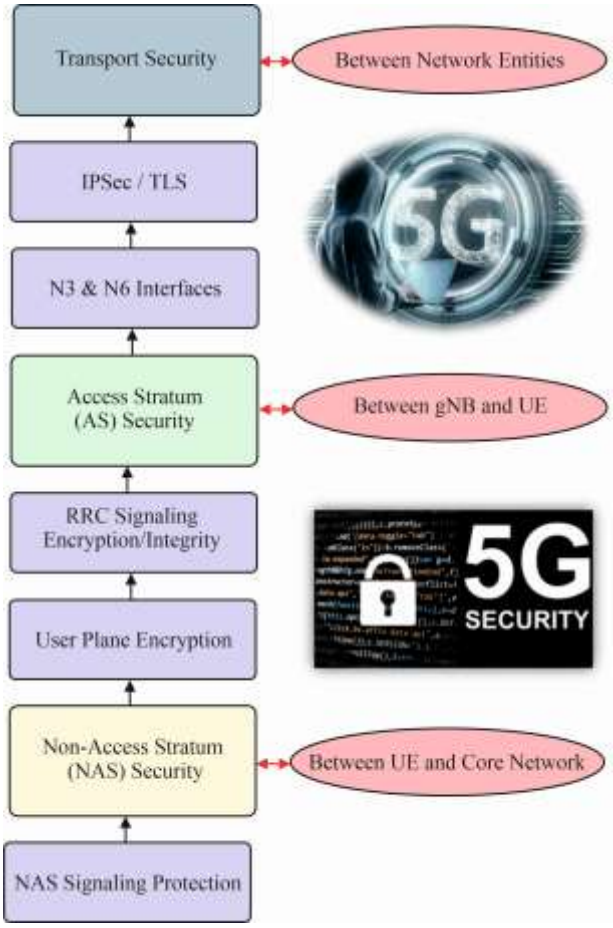

Рис. 12. Стек безпеки 5G — концептуальна схема з поділом на NAS /AS/Transport security

Порівняльна оцінка (рис. 13) свідчить, що саме ZUC демонструє найкращий баланс між пропускною здатністю та енерговитратами, особливо у пристроях з обмеженими апаратними можливостями.

Архітектура стеку безпеки в 5G побудована за принципом багаторівневої моделі, що включає три логічні рівні захисту, як показано на рис. 12. NAS Security відповідає за захист логіки керування між користувацьким обладнанням (UE) та ядром мережі, забезпечуючи конфіденційність і цілісність сигналізаційного обміну. AS Security реалізує захист фізичного радіоканалу між UE та базовою станцією (gNB), охоплюючи шифрування користувацьких даних і перевірку цілісності сигналів керування. Transport Security, у свою чергу, відповідає за безпечну взаємодію між компонентами самої мережі (інтерфейси типу N2, N3, N6), використовуючи протоколи IPSec, TLS або DTLS. Усі ці рівні активуються послідовно, формуючи наскрізну криптографічну систему захисту, яка гарантує конфіденційність, цілісність і автентичність даних від кінцевого пристрою до хмарного ядра 5G-мережі.

Ключовим елементом криптографічного захисту в архітектурі 5G є ієрархічна модель управління ключами, яка представлена на рис. 14. У центрі цієї моделі знаходиться кореневий ключ K, що зберігається у SIM-карті користувача (USIM) та в домашній мережі оператора. Цей ключ є джерелом усіх інших ключів і ніколи не передається мережею, що забезпечує високий рівень безпеки.

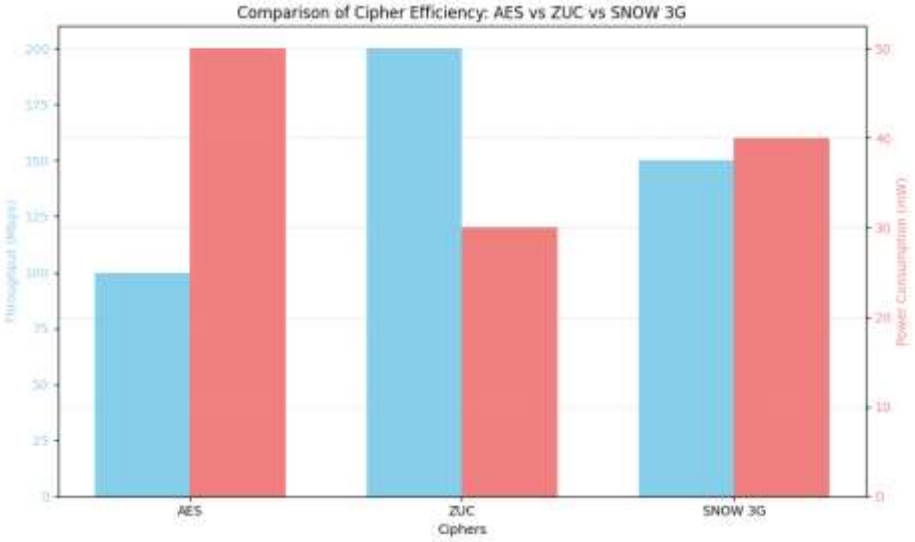

Рис. 13. Стовпчикова діаграма для порівняльної візуалізації ефективності шифрів AES, ZUC та SNOW 3G у вигляді графіка за двома параметрами: Throughput (Mbps) та Power Consumption (mW)

В процесі автентифікації з ключа K генеруються два базові ключі: CK (Cipher Key) — для шифрування даних, і IK (Integrity Key) — для перевірки їхньої цілісності. Далі з них формується ключ K_AMF, який використовується для доступу до функцій управління мобільністю та служить основою для створення ключів K_NASenc і K_NASint, що забезпечують захист сигналізації на рівні NAS. Крім того, з K_AMF генерується K_gNB — ключ для базової станції, з якого далі утворюються K_RRCenc і K_RRCint (для захисту керуючих сигналів) та K_UPenc (для шифрування користувацького трафіку на рівні User Plane). Така каскадна структура дозволяє ізолювати ризики і у випадку компрометації одного з ключів (наприклад, K_UPenc) інші залишаються захищеними, включно з кореневим значенням.

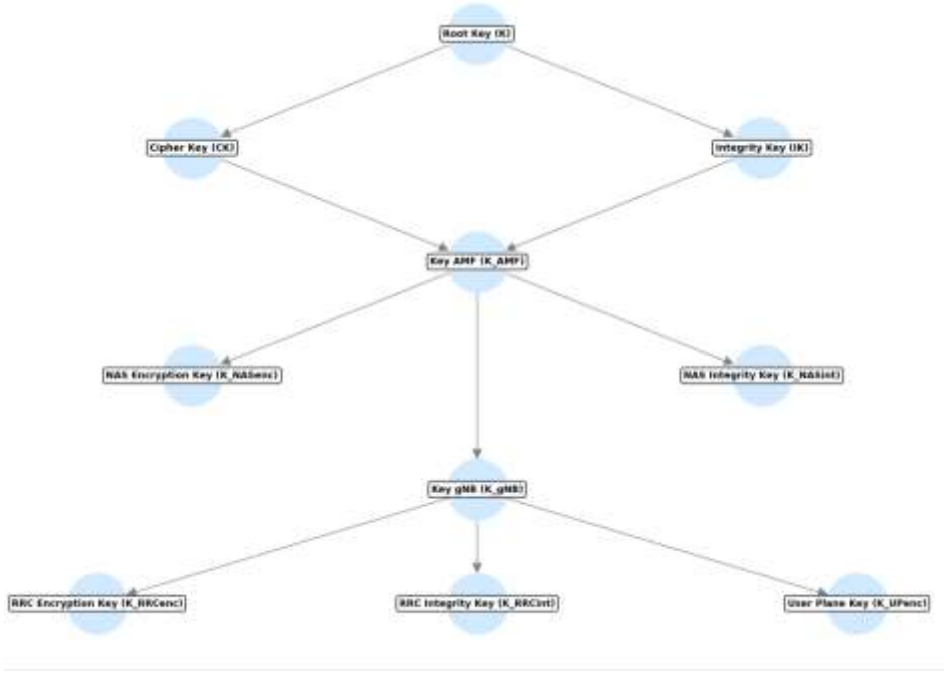

Рис. 14. Граф який відображає ієрархію ключів безпеки в 5G

Ієрархічна модель ключів (рис. 14) у 5G не лише підвищує стійкість до атак, а й дозволяє гнучко адаптувати рівень захисту до конкретного середовища використання — від інтенсивних eMBB-сценаріїв до критично важливих URLLC або масштабованих IoT-мереж. Крім того, розділення ключів за функціональними рівнями дозволяє застосовувати політики безпеки з різною тривалістю життя ключів, швидкістю ротації або реакцією на потенційні інциденти. Важливо й те, що реалізація механізмів локального оновлення ключів у gNB дає змогу не порушувати сесії користувача в разі перевиклику ключів, що особливо критично для підтримки безперервного з'єднання. Така глибока структуризація забезпечує не лише високий рівень криптозахисту, а й підвищує загальну надійність і керованість безпеки в складній архітектурі 5G-мереж [16].

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

В результаті проведеного аналізу було з'ясовано, що архітектура безпеки 5G-мереж має чітко структуровану, багаторівневу побудову, що охоплює логіку керування (NAS), радіодоступ (AS) та транспортну інфраструктуру (Transport Security). Кожен рівень підтримується окремими криптографічними механізмами та ключами, організованими в ієрархічну систему, яка мінімізує ризики компрометації. Порівняльна оцінка криптоалгоритмів (AES, ZUC, SNOW 3G) дозволила визначити їх оптимальні сфери застосування з урахуванням продуктивності та енергоефективності.

У майбутніх дослідженнях доцільно зосередитися на адаптації моделей шифрування до умов масового IoT, дослідженні квантостійких алгоритмів у контексті 5G/6G, а також на розробці механізмів динамічного управління ключами у віртуалізованих та розподілених мережах.

Література

1. Ghosh, A., Maeder, A., Baker, M., & Chandramouli, D. (2019). 5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15. *IEEE Access, 7*, 127639-127651.

2. Pyatin, I., Boiko, J., Eromenko, O., & Parkhomey, I. (2023). Implementation and analysis of 5G network identification operations at low signal-to-noise ratio. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 21*(3), 496-505.

3. Supriya, K.S. & Lovesum S. P., J. (2024). Review on lightweight cryptography techniques and

steganography techniques for IoT environment. *International Journal of System Assurance Engineering and Management*, *15*, 4210–4228.

4. Buriachok, V.L., Duravkin, Ie.V., Lukova-Chuyko, N.V. & Skladanniy, P.M. (2019). Methods of information protection in telecommunication systems. – Kiev :KUBG, 2019, 74 c.

5. Paar, C., Pelzl, J. & Güneysu, T. (2024). The Advanced Encryption Standard (AES). Understanding Cryptography. - Springer, Berlin, Heidelberg, 2024, pp 111–146.

6. Rouvroy G. et. al. (2003). Efficient uses of FPGAs for implementations of DES and its experimental linear cryptanalysis. *IEEE Transactions on Computers*, *52*(4), 473-482.

7. Zhang, J., et.al. (2023). A Differential Fault Attack on Security Vehicle System Applied SIMON Block Cipher. *IEEE Transactions on Intelligent Transportation Systems*, *24*(11), 12900-12911.

8. Muthalagu, R. & Jain, S. (2016). Modifying LFSR of ZUC to Reduce Time for Key-Stream Generation. *Journal of Cyber Security and Mobility*, *5*(4), 257-268.

9. Heinrich, C. (2025). Transport Layer Security (TLS). Encyclopedia of Cryptography, Security and Privacy. - Springer, Cham.- 2025. – pp. 2645–2646.

10. ДСТУ ISO/IEC 29192-1:2016 - Інформаційні технології. Методи захисту. Легковагова криптографія. Частина 1. Загальні положення ; чинний від 27.12.2016, наказ № 451. – Київ : ДП «УкрНДНЦ», 2016.

11. IEEE P2413/D0.4.6. IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT). -2019. pp.1-265.

12. Yue, C., Shirvanimoghaddam, M., Vucetic, B. & Li, Y. (2023). Channel Coding and Decoding Schemes for URLLC. Ultra-Reliable and Low-Latency Communications (URLLC) Theory and Practice: Advances in 5G and Beyond. - Wiley, 2023, 119-168.

13. Pandey, S. & Bhushan, B. (2024). Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks, *Wireless Networks*, *30*, 2987–3026.

14. Бурячок, В. Л., Толюпа, С.В., Семко, В.В., Бурячок, Л.В., Складний, П.М., Лукова-Чуйко, Н.В. (2016). Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – Київ : ДУТ - КНУ, 2016, 178 с.

15. Bauer, F.L.(2025). Cryptanalysis. Encyclopedia of Cryptography, Security and Privacy. – Springer, Cham, 2025, pp. 468–471.

16. Семенко, А. І., Бойко, Ю. М., Шпур, О. М., Стрелковська, І. В., Корчинський, В. В., & Яровий, Р. О. (2024). Сучасні технології інфокомунікаційних та комп'ютерних мереж. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024. - 557 с. ISBN 978-617-853-009-9.

References

1. Ghosh A., Maeder A., Baker, M., & Chandramouli, D. (2019). 5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15. *IEEE Access*, *7*, 127639-127651.

2. Pyatin, I., Boiko, J., Eromenko, O., & Parkhomey, I. (2023). Implementation and analysis of 5G network identification operations at low signal-to-noise ratio. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *21*(3), 496-505.

3. Supriya, K.S. & Lovesum S. P., J. (2024). Review on lightweight cryptography techniques and steganography techniques for IoT environment. *International Journal of System Assurance Engineering and Management*, *15*, 4210–4228.

4. Buriachok, V.L., Duravkin, Ie.V., Lukova-Chuyko, N.V. & Skladanniy, P.M. (2019). Methods of information protection in telecommunication systems. – Kiev :KUBG, 2019, 74 c.

5. Paar, C., Pelzl, J. & Güneysu, T. (2024). The Advanced Encryption Standard (AES). Understanding Cryptography. - Springer, Berlin, Heidelberg, 2024, pp 111–146.

6. Rouvroy G. et. al. (2003). Efficient uses of FPGAs for implementations of DES and its experimental linear cryptanalysis. *IEEE Transactions on Computers*, *52*(4), 473-482.

7. Zhang, J., et.al. (2023). A Differential Fault Attack on Security Vehicle System Applied SIMON Block Cipher. *IEEE Transactions on Intelligent Transportation Systems*, *24*(11), 12900-12911.

8. Muthalagu, R. & Jain, S. (2016). Modifying LFSR of ZUC to Reduce Time for Key-Stream Generation. *Journal of Cyber Security and Mobility*, *5*(4), 257-268.

9. Heinrich, C. (2025). Transport Layer Security (TLS). Encyclopedia of Cryptography, Security and Privacy. - Springer, Cham.- 2025. – pp. 2645–2646.

10. DSTU ISO/IEC 29192-1:2016 - Informatsiini tekhnolohii. Metody zakhystu. Lehkovahova kryptohrafiia. Chastyna 1. Zahalni polozhennia ; chynnyi vid 27.12.2016, nakaz № 451. – Kyiv : DP «UkrNDNTs», 2016.

11. IEEE P2413/D0.4.6. IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT). -2019. pp.1-265.

12. Yue, C., Shirvanimoghaddam, M., Vucetic, B. & Li, Y. (2023). Channel Coding and Decoding Schemes for URLLC. Ultra-Reliable and Low-Latency Communications (URLLC) Theory and Practice: Advances in 5G and Beyond. - Wiley, 2023, 119-168.

13. Pandey, S. & Bhushan, B. (2024). Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks, *Wireless Networks*, *30*, 2987–3026.

14. Buriachok, V. L., Toliupa, S.V., Semko, V.V., Buriachok, L.V., Skladnyi, P.M., Lukova-Chuiko, N.V. (2016). Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby. – Kyiv : DUT - KNU, 2016, 178 s.

15. Bauer, F.L.(2025). Cryptanalysis. Encyclopedia of Cryptography, Security and Privacy. – Springer, Cham, 2025, pp. 468–471.

16. Semenko, A. I., Boiko, J. M., Shpur, O. M., Strelkovska, I. V., Korchynskyi, V. V., & Yarovyi, R. O. (2024). Suchasni tekhnolohii infokomunikatsiinykh ta kompiuternykh merezh. - Kyiv: European University, FO-P Biletskyi R.H., 2024. - 557 s. ISBN 978-617-853-009-9.