УДК 004.056.55

В. А. Лужецький, д-р техн. наук, проф.; Т. Г. Кирилащук

АНАЛІЗ АРХІТЕКТУР ТА КРИПТОГРАФІЧНИХ ПРИМІТИВІВ ЛЕГКОВАГОВИХ БЛОКОВИХ ШИФРІВ

У статті проведено системний аналіз архітектурних рішень та криптографічних примітивів, що використовуються в сучасних легковагових блокових шифрах, призначених для ресурсно-обмежених середовищ, зокрема IoT-пристроїв, RFID-систем та вбудованих мікроконтролерів з обмеженим обсягом пам'яті, енергоспоживанням і тактовою частотою. Розглянуто шифри Present, Gift, Led, Klein, Rectangle, Prince, Clefia, Camellia, а також сімейства Simon і Speck, які репрезентують різні підходи до побудови легковагових криптографічних алгоритмів – від класичних SP-мереж до модифікованих мереж Фейстеля та ARX-конструкцій. Основну увагу приділено аналізу структури раунду, механізмам забезпечення конфузії та дифузії, а також ролі базових криптографічних примітивів: 4- та 8-бітних S-блоків, лінійних перетворень дифузійного шару (pLayer, MDS-матриць), побітових перестановок, операцій додавання раундового ключа (Add Round Key) та циклічних зсувів. Детально охарактеризовано властивості S-блоків з позицій нелінійності, стійкості до диференційного та лінійного криптоаналізу, а також вплив їх розрядності на апаратну складність реалізації. Показано, що використання малорозрядних підстановок істотно зменшує площу кристалу в реалізаціях, однак потребує збільшення кількості раундів для досягнення необхідного рівня лавинного ефекту. Окремо розглянуто ARX-конструкції, що ґрунтуються на операціях додавання за модулем 2^n, циклічних зсувів та XOR. Продемонстровано їх переваги з точки зору програмної ефективності, відсутності залежності від табличних підстановок і стійкості до атак із використанням побічних каналів. Проведено порівняльний аналіз шифрів за розрядністю блоків і ключів, кількістю раундів, оцінками криптографічної стійкості у вигляді складності найкращих відомих атак порядку 2^k, а також показниками апаратної та програмної складності реалізації. Узагальнено, що спрощення раундових операцій і мінімізація логічної глибини сприяють зменшенню енергоспоживання та латентності, проте потребують ретельного балансування між компактністю та криптографічною надійністю. Зроблено висновок, що SP-мережеві легковагові шифри є перспективним напрямом для апаратно обмежених систем, тоді як Feistel- та ARX-конструкції забезпечують кращу масштабованість, гнучкість параметризації та ефективність у програмних реалізаціях на універсальних процесорних платформах.

Ключові слова: *легковагові блокові шифри, криптографічні примітиви, SP-мережа, мережа Фейстеля, ARX-конструкції, S-блоки, апаратна складність, криптографічна стійкість, IoT.*

Вступ

Стрімкий розвиток вбудованих систем, Інтернету речей (IoT), бездротових сенсорних мереж, RFID-технологій та інших ресурсно-обмежених платформ зумовив зростання вимог до забезпечення конфіденційності, цілісності та автентичності даних, що передаються та зберігаються. На відміну від класичних обчислювальних систем, такі пристрої характеризуються суттєвими обмеженнями за обсягом пам'яті, енергоспоживанням, обчислювальною потужністю та площею апаратної реалізації. У зв'язку з цим застосування традиційних криптографічних алгоритмів, зокрема стандартних блокових шифрів загального призначення, не завжди є доцільним або ефективним. Вирішенням зазначеної проблеми стало формування окремого напряму криптографії – легковагової криптографії, основною метою якої є розроблення алгоритмів із мінімальними апаратними та програмними витратами при збереженні прийнятного рівня криптографічної стійкості. Легковагові блокові шифри орієнтовані на оптимізацію таких показників, як площа кристалу, логічна глибина схем, енергоспоживання та латентність, що досягається шляхом використання спрощених криптографічних примітивів і спеціалізованих архітектурних рішень [1 – 3]. Сучасні легковагові блокові шифри будуються переважно на основі SP-мереж або модифікованих мереж Фейстеля та використовують обмежений набір базових операцій: малорозрядні S-блоки, побітові перестановки, операції додавання раундового ключа, циклічні зсуви та прості лінійні перетворення дифузії. Окремий клас алгоритмів базується на

ARX-конструкціях, у яких криптографічна стійкість досягається за рахунок поєднання операцій додавання за модулем 2^n, ротацій та побітового XOR без використання таблиць підстановок [4, 5]. Актуальність дослідження легковагових блокових шифрів полягає у необхідності вибору або проєктування криптографічних алгоритмів, що оптимально відповідають конкретним обмеженням апаратної реалізації та вимогам до безпеки. Різні алгоритми демонструють суттєві відмінності за кількістю раундів, розрядністю блоків і ключів, оцінками стійкості та апаратною складністю, що ускладнює їх безпосереднє порівняння.

Метою цієї роботи є аналіз архітектурних особливостей і криптографічних примітивів сучасних легковагових блокових шифрів, а також порівняння їхніх характеристик з точки зору апаратної складності, рівня стійкості та придатності для використання в ресурсно-обмежених середовищах [6 – 8].

Виклад основного матеріалу

Усі відомі легковагові блокові шифри можуть бути систематизовані за архітектурним принципом побудови раундових перетворень. Основу більшості сучасних алгоритмів становлять SP-мережі, у яких нелінійність реалізується за допомогою малорозрядних S-блоків, а дифузія – шляхом побітових або матричних перестановок. До цієї групи належать шифри PRESENT [9], GIFT [10], LED [11], KLEIN [12], RECTANGLE [13] та PRINCE [14], які демонструють мінімальні апаратні витрати та високу енергоефективність.

Шифр PRESENT. Архітектура шифру PRESENT ґрунтується на класичній SP-мережі, у якій кожен раунд складається з трьох послідовних перетворень: додавання раундового ключа, нелінійного шару підстановок та лінійного шару бітової перестановки. Алгоритм передбачає реалізацію 31 раунду для блоків довжиною 64 біти з можливістю використання ключів 80 і 128 бітів [1]. Структура шифру наведена на рис. 1.

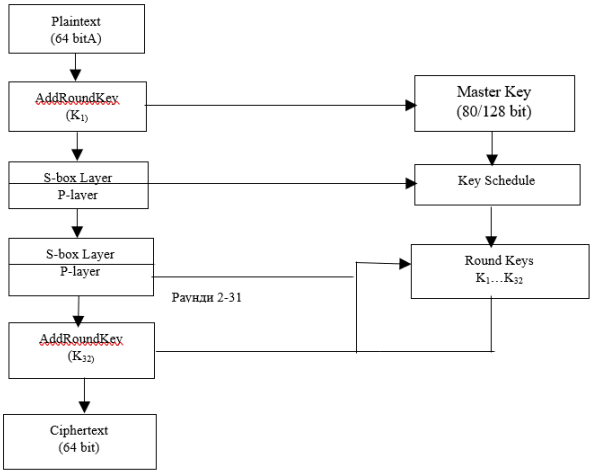

Рис 1. Структура шифру Present

Перше перетворення (Add Round Key) відповідає за введення секретної інформації у кожен раунд. На цьому етапі 64-бітний стан шифру побітово поєднується з відповідним 64-бітним раундовим ключем за допомогою операції XOR. Така операція є апаратно мінімальною за вартістю, реалізується одним логічним елементом на біт і не створює затримок, пов'язаних із складними таблицями підстановок[3]. Саме через свою простоту XOR став стандартною основою для введення ключового матеріалу в більшості легковагових шифрів [4]. У контексті PRESENT ця операція гарантує початкову залежність вихідних даних від секретного ключа й забезпечує рівномірний розподіл ключових бітів по всьому блоку.

Перетворення (S-boxLayer) є нелінійним, і забезпечує стійкість стосовно лінійних та диференціальних атак [5, 6]. У шифрі PRESENT використовується 4-бітний S-блок, який

застосовується паралельно до всіх 16 ніблів вхідного стану. Кожен з них перетворюється згідно з фіксованою таблицею підстановок, оптимізованою для реалізації у вигляді мінімальної кількості логічних функцій [7].

Перетворення (pLayer) реалізує лінійну побітову перестановку, що забезпечує дифузію [1, 8]. Кожен біт стану переноситься у нову позицію згідно з детермінованим правилом: для всіх позицій, окрім останньої, застосовується правило перестановкиi $\rightarrow$ $(16 \cdot \mathrm{i} \bmod 63)$, а біт з індексом 63 залишається на місці [1]. Така побудова спричиняє значне розсіювання впливу будь-якого бітового зміщення по всьому блоку вже після кількох раундів [6, 8]. Особливість реалізації Layer полягає в тому, що вона не вимагає виконання жодної логічної операції, а, отже, не потребує додаткових функцій і це суттєво знижує апаратні витрати на реалізацію шифру [2]. Саме ця побітова перестановка дозволяє малим S-блокам ефективно взаємодіяти між собою та забезпечує повне змішування даних у ході раундових перетворень.

Перетворення (Key Schedule) формує раундові ключі з початкового 80-бітного ключового матеріалу. При цьому використовується регістр для циклічного зсуву коду, S-блок та елементи XOR. Комбінація таких операцій створює раундові ключі, достатньо різні між собою, щоб забезпечити стійкість шифру до атак на пов'язані ключі при мінімальних апаратних ресурсах [10]. Усі ці компоненти створені таким чином, щоб забезпечити максимальну криптографічну стійкість при мінімально можливих апаратних витратах, що робить PRESENT одним із найефективніших легковагових шифрів для RFID-тегів, сенсорних мереж і мікропристроїв з надзвичайно обмеженим апаратним бюджетом [1, 11, 12]. S-блок, що використовується в цьому випадку, є S-блоком 4x4. Заміна ніблів в цьому блоці описана в таблиці 1.

Таблиця 1

Заміна ніблів

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Секретний ключ, наданий користувачем, зберігається в регістрі ключів K і представлений як $\mathrm{k}_{79}\mathrm{k}_{78} \ldots \mathrm{k}_0$. Bi-му раунді 64-бітовий раундовий ключ $\mathrm{K}_\mathrm{i} = \mathrm{k}_{63}\mathrm{k}_{62} \ldots \mathrm{k}_0$ складається з 64 лівих бітів поточного вмісту регістру K:

$$K_i = k_{63}k_{62} \ldots k_0 = k_{79}k_{78} \ldots k_{16}. \quad (1)$$

Після вилучення раундового ключа K_i, ключовий регістр $\mathrm{K}_\mathrm{i} = \mathrm{k}_{79}\mathrm{k}_{78} \ldots \mathrm{k}_0$ оновлюється таким чином [1]:

1. $[k_{79}k_{78} \ldots k_1k_0] = [k_{18}k_{17} \ldots k_{20}k_{19}]$.
2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$.
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus$ *раундовий лічильник*.

Шифр GIFT. Цей шифр було розроблено як сучасну легковагову заміну шифру PRESENT з метою збереження малої апаратної площі та водночас покращення окремих крипто статистичних властивостей, зокрема усунення виявлених слабких місць попередньої конструкції [15, 16]. Шифр реалізується у двох основних варіантах: GIFT-64, що працює з 64-бітними блоками та використовує 28 раундів шифрування, і GIFT-128, призначений для 128-бітних блоків із кількістю раундів, збільшеною до 40 [15]. В обох варіантах застосовується секретний ключ довжиною 128 біт, що забезпечує уніфікований рівень ключової безпеки незалежно від розміру блоку [15]. Архітектура шифру GIFT базується на класичній SP-мережі, в якій нелінійність реалізується за допомогою 4-бітних S-блоків, що застосовуються паралельно до всіх ніблів внутрішнього стану [15, 17]. Після шару підстановок виконується лінійне перетворення у вигляді побітової перестановки PermBits (pLayer), яка забезпечує ефективну дифузію та рівномірне поширення впливу кожного біта по всьому блоку [15]. В кожному раунді також виконується операція додавання раундового ключа (Add Round Key), що вводить ключовий матеріал у процес шифрування. Процедура

формування та оновлення ключового стану побудована таким чином, щоб забезпечити достатню різноманітність раундових ключів за мінімальних апаратних витрат [16]. Ключовий матеріал розбивається на окремі слова та регулярно модифікується шляхом застосування перестановок, використання S-блоків до визначених частин ключа та операцій XOR з раундовими константами, що підвищує стійкість шифру до атак на пов'язані ключі [18].

На етапі Add Round Key 64-бітний внутрішній стан шифру розбивається на чотири 16-бітні частини. До двох з них застосовується побітова операція XOR із відповідними бітами поточного раундового ключа, а також із шістьма бітами раундової константи [15]. Зазначене перетворення забезпечує змішування даних із ключовим матеріалом і формує початкову залежність шифртексту від секретного ключа вже на ранніх етапах раундового перетворення [19].

Наступним виконується нелінійне перетворення SubCells (S-boxLayer), яке полягає у застосуванні 4-бітної підстановки до кожного ніблу внутрішнього стану [15]. Перетворення реалізується за допомогою фіксованого 4-бітного S-блоку відповідно до таблиці 2. Використання мало розрядних S-блоків обумовлене прагненням до спрощення апаратної реалізації, зменшення логічної глибини схеми та мінімізації апаратних витрат [17].

S-блок забезпечує нелінійність шифру та підвищує його криптографічну стійкість, формуючи складні залежності між бітами в межах кожного ніблу внутрішнього стану. Останнє раундове перетворення – PermBits (pLayer) – виконує лінійну побітову перестановку, що забезпечує дифузію та сприяє рівномірному поширенню впливу кожного біта по всьому блоку даних упродовж наступних раундів [15, 20]. Кожен біт 64-бітного блоку переставляється за правилом:

$$P(i) = (16 \cdot i) mod 63, для\ i = 0..62; P(63) = 63. \quad (2)$$

Наведена побітова схема дозволяє розподіляти виходи S-блоків між різними ніблами у наступних раундах, сприяючи повному змішуванню даних після декількох ітерацій.

Таблиця 2

Нелінійне перетворення

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	A	4	C	6	F	3	9	2	D	B	7	5	0	8	E

4-бітні S-блоки дають просту нелінійність, а побітова перестановка забезпечує хорошу дифузію за мінімальної апаратної вартості, але ускладнює ефективну програмну реалізацію (через побітові операції) [15]. Простір ключа перетасовується через перестановки, S-блоки та XOR-константи [18].

Для кожного з 28 раундів визначено унікальну 6-бітну раундову константу, що використовується для перетворення Add Round Key [15]. Вона вводить додаткову незалежність між раундами та захищає від симетрій у послідовності раундових ключів [21]. Значення цих констант наведено в таблиці 3.

Таблиця 3

Набір констант

№ раунду	Константа (hex)
1	01
9	37
17	1D
25	21

Апаратна реалізація шифру GIFT повністю відповідає вимогам, що висуваються до пристроїв класу IoT, зокрема щодо обмежень на апаратну площу, енергоспоживання та логічну складність [22 – 24]. Завдяки своїм структурним особливостям і низьким апаратним

витратам алгоритм також застосовується як базовий примітив у схемах автентифікованого шифрування з асоційованими даними (AEAD), зокрема в конструкції GIFT-COFB [3], що додатково підтверджує його практичну придатність для використання в ресурсно-обмежених середовищах. У цілому GIFT вважають сучасним для легковагових застосувань, але реалізація в ПЗ потребує оптимізації [15, 26].

Шифр PRINCE. Цей шифр призначений для шифрування 64-бітних блоків даних із використанням 128-бітного секретного ключа та базується на спеціальній конструкції типу α-reflection [27, 28], яка забезпечує симетричність процесів зашифрування та розшифрування. Завдяки цій властивості операція розшифрування може бути реалізована шляхом застосування тієї самої раундової структури, що й для зашифрування, але з модифікованим ключем, що істотно спрощує апаратну реалізацію [27].

Алгоритм PRINCE побудований на основі SP-мережі та використовує 4-бітні S-блоки для реалізації нелінійного шару підстановок [27, 29]. Ключовий матеріал містить спеціальну складову α, яка дозволяє здійснювати швидке перетворення між ключами зашифрування та розшифрування без необхідності окремого ключового розкладу. Такий підхід зменшує апаратні витрати та дозволяє ефективно реалізувати обидві криптографічні операції в межах однієї схеми. PRINCE орієнтований на досягнення збалансованого компромісу між латентністю та рівнем безпеки. Завдяки лише 12 раундам шифр забезпечує низьку затримку в формуванні результату, що є критично важливим для високошвидкісних апаратних застосувань [27]. Водночас така раундова структура стала предметом ґрунтовного криптоаналізу, зокрема в контексті лінійних, диференціальних атак і атак на слабкі ключі [30, 31]. Опубліковані результати досліджень свідчать, що за умов цільових обмежень, пов'язаних із мінімізацією латентності, PRINCE є прийнятним криптографічним примітивом [30]. З огляду на зазначені властивості, шифр PRINCE рекомендують використовувати у сценаріях, де основним критерієм є мінімальна затримка обробки даних, зокрема в апаратних шлюзах реального часу та мережевих ASIC із жорсткими обмеженнями на кількість тактів обчислення [27, 32].

Шифр RECTANGLE. Шифр орієнтований на шифрування блоків даних довжиною 64 біти та підтримує використання секретних ключів довжиною 80 і 128 біт. Архітектура RECTANGLE побудована за структурою класичної SP-мережі та передбачає реалізацію 25 раундів перетворень [33]. Нелінійний шар (S-layer) реалізується за допомогою 16 незалежних 4×4 S-блоків, об'єднаних у перетворення SubColumn, а лінійний шар (P-layer) реалізований у вигляді комбінації побітових перестановок, що забезпечує ефективну дифузію та водночас є зручним для реалізації bit-slice-оптимізацій [33, 34]. Така організація дозволяє досягти балансу між апаратною ефективністю та продуктивністю програмних реалізацій. Дослідження [35] були спрямовані на аналіз стійкості стосовно диференціальних, лінійних та інтегральних атак, зокрема для меншої кількісті раундів. Результати досліджень показали, що RECTANGLE забезпечує компроміс між високою програмною ефективністю і помірною криптографічною стійкістю [35, 36]. Цей шифр рекомендують для реалізації на платформах де доступні 32-/64-бітні блоки і використовуються bit-slice техніки (мікроконтролери з можливістю SIMD-подібних операцій або оптимізовані софт-реалізації) [33, 34].

Шифр LED. Шифр побудований на основі SP-мережі, у якій нелінійний шар підстановок реалізується за допомогою 4-бітних S-блоків, а лінійні перетворення включають операції ShiftRows та MixColumnsSerial, концептуально подібні до відповідних операцій шифру AES, але адаптовані для роботи з 4-бітними елементами [37,38]. Така архітектура забезпечує достатній рівень дифузії та нелінійності за мінімальних апаратних витрат, що відповідає вимогам легковагової криптографії [37]. Особливістю шифру LED є те, що операція додавання ключа виконується не в кожному раунді, а після кожних чотирьох раундових кроків [37]. Такий підхід дозволяє суттєво спростити апаратну логіку та зменшити площу реалізації, однак водночас накладає певні особливості на криптоаналіз і вимагає уважного розгляду стійкості алгоритму в умовах скороченого введення ключового матеріал [39]. Загалом шифр LED вважається безпечним для широкого кола легковагових застосувань за умови дотримання обмежень, пов'язаних із використанням ключового розкладу, що

підтверджується результатами досліджень [39, 40]. З огляду на надзвичайно малі апаратні витрати, LED рекомендується застосовувати у пристроях, де критичним параметром є мінімізація площі кристалу апаратної реалізації, зокрема в RFID-системах та надмалих IoT-пристроях [37, 41].

Шифр KLEIN. Структура KLEIN ґрунтується на SP-мережі, яка схожа на архітектуру шифру AES, однак спрощена з метою зменшення апаратної складності реалізації та адаптації до умов обмежених ресурсів [42]. Алгоритм шифрування реалізується у таких варіантах KLEIN-64, KLEIN-80 та KLEIN-96, які оперують 64-бітними блоками даних і використовують секретні ключі довжиною 64, 80 та 96 біт відповідно. Залежно від довжини ключа шифр передбачає виконання 12, 16 або 20 раундів перетворень [42]. Нелінійний шар реалізується за допомогою 4-бітних S-блоків, а лінійний шар включає етап MixColumn, адаптований для роботи з малорозрядними елементами. Процедура формування раундових ключів є полегшеною та базується на застосуванні перестановок і раундових констант, що дозволяє зменшити апаратні витрати без істотного зниження криптографічної стійкості. Завдяки таким конструктивним рішенням шифр KLEIN досягає збалансованого співвідношення між рівнем безпеки та швидкодією в ресурсно-обмежених середовищах. Результати численних криптографічних досліджень [44, 45] показують, що в більшості типових сценаріїв застосування для пристроїв з обмеженими обчислювальними та апаратними можливостями KLEIN є достатньо ефективним і практичним криптографічним примітивом.

Іншу групу утворюють шифри, побудовані на мережах Фейстеля та їх узагальнених модифікаціях, зокрема CLEFIA, Camellia та SIMON [46 – 48]. Такі конструкції спрощують реалізацію зворотного перетворення та дозволяють використовувати більш складні нелінійні функції безвтрати оборотності [46, 49]. Окремо виділяються ARX-конструкції, представлені шифром SPECK, у яких криптографічна стійкість досягається за рахунок комбінації операцій додавання, циклічних зсувів і XOR, що забезпечує високу програмну ефективність [50 – 52].

Шифр CLEFIA. Шифр реалізований на основі 4-гілкової узагальненої мережі Фейстеля (GeneralizedFeistelNetwork (GFN)) [53] для 128-бітного блоку даних і підтримує ключі довжиною 128/192/256 біт та має відповідно 18/22/26 раундів [7]. Його архітектура спроєктована для збалансованої ефективності програмної та апаратної реалізації, а рівень безпеки відповідає AES-класу [53, 54]. У структурі шифру на кожному раунді використовується дві різні нелінійні функції F_0 та F_1, що підвищує криптостійкість та забезпечує кращу дифузію даних порівняно з класичною двогілковою мережею Фейстеля [53]. Раундові перетворення передбачають використання операції XOR, нелінійних функцій F_0 і F_1 та матриць дифузії M_0/M_1, що показано на рис. 2 [53].

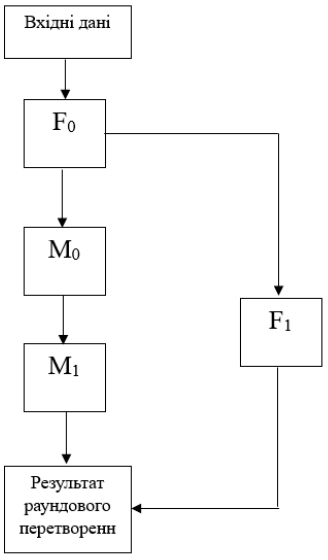

Рис. 2. Структура раундових перетворень

Кожна з функцій F_0 та F_1 працює з 32-бітним вхідним словом та 64-бітним підключем.

Функція F_0 використовує 8-бітні S-блоки S_0 та S_1, узяті з архітектури AES і реалізує такі перетворення:

$$F^0(X,K) = M^0\left(S^1\left(S^0(X \oplus K)\right)\right) \quad (3)$$

Функція F_1 має схожу структуру, але використовує S-блоки S_2 та S_3 та обчислюється за формулою:

$$F_1(X,K) = M_1(S_3(S_2(X \oplus K))) \quad (4)$$

Матриці розсіювання M_0 та M_1 здійснюють лінійне перетворення у полі GF(2^8). Метою є поширення впливу кожного біта вхідних даних на кілька позицій вихідних даних.

Шифр CLEFIA рекомендують застосовувати у довгострокових захисних системах, інфраструктурах цифрової ідентифікації, IoT-пристроях середнього класу, криптомодулях корпоративного рівня [8]**.**

Шифр Camellia. Цей шифр побудований на основі модифікованої мережі Фейстеля, яка здійснює перетворення 128-бітних блоків даних за кількість раундів, що визначається довжиною ключів(128, 192 або 256 біт). Класична двогілкова мережа Фейстеля [55] доповнена внутрішніми функціями розширеної дифузії та додатковими нелінійними перетвореннями, що підвищують рівень стійкості до сучасних аналітичних атак [56]. У кожному раунді застосовується функція F, яка працює з 64-бітною половиною блоку та виконує підстановки на 8-бітних S-блоках, запозичених з архітектури AES, а також лінійні перетворення, спрямовані на забезпечення глибокої дифузії [56]. Однією з особливостей шифру є наявність вбудованих функцій FL та FL^{-1}, що реалізуютьсяна певних етапах шифрування, залежно від довжини ключа [56]. Функція FL є нелінійним перетворенням, яке використовує поєднання операцій AND, OR, XOR та циклічних зсувів для посилення взаємозв'язку між бітами вхідних даних і ключа. Її завдання полягає у підвищенні стійкості шифру до лінійного аналізу та розширенні простору можливих внутрішніх станів, що ускладнює побудову диференціальних характеристик шифру [56, 57]. Функція FL^{-1} є оберненим варіантом FL і забезпечує збереження структури, необхідної для правильної реалізації процесу розшифрування [56]. Обидві функції розташовуються симетрично при зашифруванні та розшифруванні, що дозволяє зберегти властивість оборотності не збільшуючи кількість елементарних операцій. Camellia вважається надійним і безпечним вибором для промислових систем, де потрібна висока сумісність, довгострокова криптографічна стійкість та ефективність, а також для середовищ з обмеженими обчислювальними ресурсами [7, 56].

Сімейство шифрів SIMON і SPECK. До складу цього сімейства входять алгоритми шифрування із розміром блоку від 32 до 128 бітів та довжиною секретного ключа від 64 до 256 бітів. Залежно від обраної комбінації параметрів блоку й ключа шифри реалізують від 32 до 72 раундів перетворень [9]. Така параметрична гнучкість дозволяє адаптувати SIMON до різних вимог щодо рівня безпеки та апаратних обмежень, що робить це сімейство придатним для широкого спектра ресурсно-обмежених пристроїв [9, 58].

У шифрі SIMON раундова структура відповідає класичній мережі Фейстеля з двома гілками. Вхідний блок даних довжиною 64 або 128 бітів розділяється на дві рівні частини, при цьому в кожному раунді нове значення правої частина обчислюється як побітова операція XOR між лівою частиною та результатом нелінійної функції, застосованої до правої частини з додаванням відповідного раундового ключа [9]. Нелінійність у SIMON досягається шляхом поєднання трьох циклічних зсувів на різні кількості бітів та операції побітового AND, що забезпечує необхідну диференціальну стійкість алгоритму [60]. На відміну від класичних SP-мереж, у яких нелінійність реалізується за допомогою S-блоків із таблицями підстановок, у шифрі SIMON відсутні табличні операцій і використовуються виключно прості логічні операції [9]. Такий підхід дозволяє досягти надзвичайно малої апаратної складності [58, 59]. Гнучка підтримка різних розмірів блоків і ключів дає змогу застосовувати SIMON як у надмалих мікроконтролерах, так і в пристроях середнього класу, де основними вимогами є компактність та енергоефективність.

На відміну від SIMON, шифр SPECK орієнтований передусім на досягнення високої програмної ефективності [9]. Його раундова структура не використовує мережу Фейстеля у класичному розумінні, хоча формально може бути представлена у двогілковому вигляді. Кожен раунд SPECK складається з двох основних операцій: одну половину блоку циклічно зсувають вправо та додають до іншої половини за модулем 2^n, після чого отриманий результат поєднується з раундовим ключем за допомогою операції XOR (табл. 4). Друга половина блоку, у свою чергу, циклічно зсувається вліво тапоєднується операцією XOR з оновленим значенням першої половини [9]. Мінімалістична конструкція SPECK, заснована виключно на ARX-операціях (Addition-Rotation-XOR), забезпечує високу швидкодію на 8-, 16-, 32- та 64-бітних мікроконтролерах, де операції додавання та циклічних зсувів виконуються значно ефективніше, ніж табличні підстановки або складні нелінійні перетворення [1, 10]. Це робить SPECK доцільним вибором для програмних реалізацій у ресурсно-обмежених обчислювальних середовищах [1].

Таблиця 4

Раундові ключі шифру SIMON

M	k_{i+m}
2	$k_1 \oplus k_{i+1} >>> 3 \oplus k_{i+1} >>> 4 \oplus c \oplus z_j[i]$
3	$k_1 \oplus k_{i+2} >>> 3 \oplus k_{i+2} >>> 4 \oplus c \oplus z_j[i]$
4	$k_i \oplus k_{i+1} \oplus k_{i+1} >>> 1 \oplus k_{i+3} >>> 3 \oplus k_{i+3} >>> 4 \oplus c \oplus z_j[i]$

ARX (Add-Rotate-XOR) – це клас криптографічних конструкцій, у яких криптографічна стійкість досягається шляхом поєднання трьох базових операцій: додавання за модулем 2^n, циклічних зсувів та побітової операції XOR [61]. Кожна з цих операцій має арифметичну або логічну природу, а їх узгоджене використання дозволяє сформувати достатній рівень нелінійності та дифузії без залучення S-блоків або складних перемішувальних шарів. Додавання за модулем 2^nвносить нелінійність у бітовий простір за рахунок перенесень (carry), які поширюються між розрядами та створюють складні міжбітові залежності. Циклічні зсуви забезпечують перерозподіл бітів у межах слова, формуючи залежності між їх позиціями та сприяючи швидкому розсіюванню впливу окремих бітів на значну частину внутрішнього стану. Побітова операція XOR, у свою чергу, реалізує лінійне змішування проміжних значень і ключового матеріалу, є апаратно та програмно простою, а також не потребує використання додаткової пам'яті. Комбінація зазначених операцій у кожному раунді створює криптографічну складність, яка істотно ускладнює застосування лінійного та диференціального криптоаналізу, зберігаючи водночас високу обчислювальну ефективність. Відсутність таблиць підстановок робить ARX-конструкції незалежними від доступу до пам'яті, що є особливо важливим для процесорів із малими кешами та обмеженою кількістю регістрів. Крім того, оскільки всі ARX-операції ефективно підтримуються сучасними процесорними архітектурами, шифри цього класу демонструють високу продуктивність на 32- та 64-бітних платформах [61, 62]. Саме з цих причин шифр SPECK, як типовий представник ARX-підходу, добре масштабується під різні розрядності обчислювальних систем і вважається одним із найшвидших легковагових алгоритмів у програмній реалізації [10].

Аналіз та узагальнення результатів порівняльного дослідження

Наведений аналіз блокових шифрів, побудованих на основі SP-мереж, показує, що з метою мінімізації логічної глибини схем апаратної реалізації, площі кристалу та енергоспоживання використовуються лише 4-бітні S-блоки, тоді як в більшості сучасних блокових шифрів використовують 8-бітні S-блоки. Спрощення нелінійних і лінійних перетворень зумовлює зменшення дифузії в межах одного раунду, тому для забезпечення потрібного рівня дифузії збільшують кількість раундів — зазвичай це від 25 до 40 раундів. У результаті досягається рівень стійкості порядку $2^{60} - 2^{70}$, достатній для застосування в IoT- та RFID-системах. Важливу роль у забезпеченні дифузії в легковагових SP-мережах відіграють

побітові перестановки (pLayer, PermBits), які виконують функцію лінійного шару без використання складних матричних операцій. Такі перестановки забезпечують перерозподіл виходів S-блоків між різними ніблами внутрішнього стану в наступних раундах, що сприяє поступовому поширенню впливу кожного біта по всьому блоку даних. Хоча побітові перестановки не збільшують нелінійність окремого раунду, їх систематичне застосування у поєднанні з S-блоками дозволяє досягти повного лавинного ефекту після декількох раундів. Перевагою такого підходу є надзвичайно мала апаратна складність реалізації, оскільки перестановки не потребують логічних елементів і реалізуються лише за рахунок з'єднань. Саме поєднання малорозрядних S-блоків і простих побітових перестановок визначає архітектурну ефективність більшості легковагових SP-шифрів.

У таблиці 5 наведено узагальнені характеристики легковагових шифрів, побудованих на основі SP-мереж. Аналіз таблиці показує, що шифри PRESENT, GIFT та LED мають найменші значення апаратної складності (у GE), що робить їх найбільш придатними для реалізації в умовах жорстких ресурсних обмежень. Шифр PRINCE вирізняється мінімальною латентністю завдяки зменшеній кількості раундів, однак потребує більшої площі апаратної реалізації. Алгоритми RECTANGLE та KLEIN демонструють компроміс між апаратною та програмною реалізацією, зокрема завдяки підтримці bit-slice-оптимізацій.

Таблиця 5

Узагальнені характеристики легковагових шифрів на основі SP-мережі

Шифр	Розрядність блоку	Розрядність ключа	Кількість раундів	Апаратна складність (GE)	Особливості
PRESENT	64	80/128	31	~1570	RFID-оптимізований
GIFT	64/128	128	28/40	~1250/1500	Покращена дифузія
PRINCE	64	128	12	2000–2500	Мінімальна затримка (латентність)
RECTANGLE	64	80/128	25	~2200–2400	Bit-slice оптимізація
LED	64	64/128	32	~1200–1300	AES-подібний та компактний
KLEINE	64	80/96	12–20	~1840	Збалансований, AES-легкий

Порівняльні характеристики шифрів, побудованих на основі мереж Фейстеля, їх узагальнених модифікацій та ARX-конструкцій, наведено у таблиці 6. Як видно з результатів, шифри CLEFIA та Camellia забезпечують високий рівень криптографічної стійкості до2^{128}, але характеризуються значно більшою апаратною складністю. Натомість SIMON орієнтований на апаратну ефективність завдяки використанню простих логічних операцій, тоді як SPECK демонструє високу продуктивність у програмних реалізаціях за рахунок ARX-підходу.

Таблиця 6

Узагальнені характеристики легковагових шифрів на основі Feistel / ARX

Шифр	Структура і операції	Розрядність блоку	Розрядність ключа	Кількість раундів	Апаратна складність (GE)	Особливості
CLEFIA	GFN-Feistel (S-box + M0/M1)	128	128/192/256	18/22/26	~5000	Висока стійкість
Camellia	Feistel (S-box + FL)	128	128/192/256	18–32	~6000	ISO стандарт
SIMON	Feistel (AND,XOR,ROT)			32–72	~1200-1800	Апаратний
SPECK	ARX (ADD, ROT, XOR)			22–34	~900-1200	Швидкий у ПЗ

Висновки

Проведений аналіз легковагових блокових шифрів свідчить, що домінуючим напрямом їх розвитку є зменшення апаратної складності за умови збереження прийнятного рівня криптографічної стійкості. У роботі проведено порівняльний аналіз сучасних легковагових блокових шифрів, що застосовуються в ресурсно-обмежених обчислювальних середовищах. Показано, що архітектурна концепція таких алгоритмів ґрунтується на модульному поєднанні простих криптографічних примітивів, що дозволяє мінімізувати апаратні витрати без критичного зниження рівня безпеки.

Результати аналізу свідчать, що найбільш перспективними для надобмежених апаратних платформ є шифри сімейств GIFT, LED та PRESENT, які забезпечують оптимальний баланс між апаратною складністю та криптографічною стійкістю. Шифри CLEFIA та Camellia доцільно використовувати у системах, де пріоритетом є довгострокова безпека та відповідність стандартам, навіть за умови збільшених апаратних витрат. Алгоритми SIMON і SPECK забезпечують гнучкий вибір між апаратною та програмною ефективністю залежно від специфіки цільової платформи.

Таким чином, подальший розвиток легковагової криптографії пов'язаний з удосконаленням SP- та ARX-архітектур, оптимізацією раундових перетворень і адаптацією алгоритмів до конкретних обмежень апаратних реалізацій, що дозволяє зберігати збалансоване співвідношення між стійкістю, швидкодією та площею реалізації.

СПИСОК ЛІТЕРАТУРИ

1. PRESENT: An Ultra-Lightweight Block Cipher / Bogdanov A. et al. Cryptographic Hardwareand Embedded Systems – CHES 2007. *Lecture Notesin Computer Science*. 2007. Vol. 4727. Berlin ; Heidelberg : Springer, 2007. P. 450–466. DOI: https://doi.org/10.1007/978-3-540-74735-2_31.

2. Poschmann A. Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. *IEEE Security & Privacy*. 2009. Vol. 7, №2. P. 44–51. DOI: https://doi.org/10.1109/MSP.2009.37.

3. Katagi M., Moriai S. A Survey of Lightweight Cryptography Implementations. *IEICE Trans. Fundamentals*. 2008. Vol. E91-A, №1. P. 1–9. DOI: https://doi.org/10.1093/ietfec/e91-a.1.1.

4. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*. 1991. Vol. 4, №1. P. 3–72. DOI: https://doi.org/10.1007/BF00630563.

5. Matsui M. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology – EUROCRYPT'93. LNCS*. 1994. Vol. 765. Berlin ; Heidelberg : Springer, 1994. P. 386–397. DOI: https://doi.org/10.1007/3-540-48285-7_33.

6. Differential Attacks on Light weight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited / C. Tezcan et al. *Lightweight Cryptography for Security and Privacy – Light Sec 2016*. LNCS. 2017. Vol. 10098. Cham : Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-68116-9_4.

7. The 128-Bit Block Cipher CLEFIA (Extended Abstract) / T. Shirai et al. *Fast Software Encryption – FSE 2007*. LNCS. 2007. Vol. 4593. Berlin ; Heidelberg : Springer, 2007. P. 181–195. DOI: https://doi.org/10.1007/978-3-540-74619-5_12.

8. Heys H. M. A Tutorial on Linear and Differential Cryptanalysis. *Cryptologia*. 2002. Vol. 26, №3. P. 189–221. DOI: https://doi.org/10.1080/01611194.2002.9964366.

9. The SIMON and SPECK Families of Lightweight Block Ciphers / R. Beaulieu et al. *IACR Cryptologye Print Archive*. 2013. Report 2013/404. URL: https://eprint.iacr.org/2013/404 (дата звернення: 01.03.2026).

10. Rashidi B. High-through put andflexible ASIC implementations of SIMON and SPECK light weight blockciphers. Int. J. Circuit Theory and Applications. 2019. Vol. 47. DOI: https://doi.org/10.1002/cta.2640.

11. The SIMON and SPECK Lightweight Block Ciphers / R. Beaulieu et al. *Proc. 52nd ACM/EDAC/IEEE Design Automation Conf. (DAC)*. 2015. DOI: https://doi.org/10.1145/2744769.2747946.

12. PRESENT Revisited: Improved Linear Cryptanalysis of PRESENT / S. Banik et al. *IACR Cryptologye Print Archive*. 2012. Report 2012/064. URL: https://eprint.iacr.org/2012/064 (дата звернення: 01.03.2026).

13. PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications / A. Bogdanov et al. *Advances in Cryptology – ASIACRYPT 2012. LNCS*. 2012. Vol. 7658. Berlin ; Heidelberg : Springer, 2012. DOI: https://doi.org/10.1007/978-3-642-34961-4_31.

14. RECTANGLE: A Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms / W. Zhang et al. *Sci. China Inf. Sci*. 2015. DOI: https://doi.org/10.1007/s11432-015-5459-9.

15. TWINE: A Lightweight Block Cipher for Multiple Platforms / T. Suzaki et al. *Selected Areas in Cryptography – SAC 2012. LNCS*. 2013. Vol. 7707. Berlin ; Heidelberg : Springer, 2013. DOI: https://doi.org/10.1007/978-3-642-35999-6_22.

16. LED: A Lightweight Block Cipher / J. Guo et al. *Cryptographic Hardware and Embedded Systems – CHES 2011*. LNCS. 2011. Vol. 6917. Berlin ; Heidelberg : Springer, 2011. DOI: https://doi.org/10.1007/978-3-642-23951-9_18.

17. Lightweight Cryptography for Wire less Sensor Networks / G. Bansod et al. *Int. J. Computer Applications*. 2010.

DOI: https://doi.org/10.5120/1542-2073.

18. Lightweight Cryptography Standardization Process / National Institute of Standards and Technology. URL: https://csrc.nist.gov/projects/lightweight-cryptography (дата звернення: 01.03.2026).

19. FELICS – Fair Evaluation of Lightweight Cryptographic Systems / D. Dinu et al. *IACR Cryptologye Print Archive.* 2015. Report 2015/315. URL: https://eprint.iacr.org/2015/315 (дата звернення: 01.03.2026).

20. Biryukov A., Perrin L. State of the Art in Lightweight Symmetric Cryptography. *IACR Cryptologye Print Archive*. 2017. Report 2017/511. URL: https://eprint.iacr.org/2017/511 (дата звернення: 01.03.2026).

21. Plaintext Recovery Attacks Against SSH / M. R. Albrecht et al. *IEEE Symposium on Security and Privacy*. 2009. DOI: https://doi.org/10.1109/SP.2009.7.

22. Biryukov A., Velichkov V. Automatic Search for Differential Trails in ARX Ciphers. Topics in Cryptology – CT-RSA 2014. LNCS. 2014. Vol. 8366. Cham : Springer, 2014. DOI: https://doi.org/10.1007/978-3-319-04852-8_12.

23. Daemen J., Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard. Berlin ; Heidelberg : Springer, 2002. DOI: https://doi.org/10.1007/978-3-662-04722-4.

24. Knudsen L. R. Truncated and Higher Order Differentials. *Fast Software Encryption – FSE 1994. LNCS*. 1995. Vol. 1008. Berlin ; Heidelberg : Springer, 1995. DOI: https://doi.org/10.1007/3-540-60590-8_8.

25. Luby M., Rackoff C. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Computing*. 1988. Vol. 17, №2. P. 373–386. DOI: https://doi.org/10.1137/0217017.

26. Shannon C. E. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949. Vol. 28. P. 656–715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

27. Nyberg K. Differentially Uniform Mappings for Cryptography. *Advancesin Cryptology – EUROCRYPT'93. LNCS*. 1994. Vol. 765. Berlin ; Heidelberg : Springer, 1994. DOI: https://doi.org/10.1007/3-540-48285-7_6.

28. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge : Cambridge Univ. Press, 2010. DOI: https://doi.org/10.1017/CBO9780511780448.007.

29. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. NewYork : Springer, 1993. DOI: https://doi.org/10.1007/978-1-4613-9321-0.

30. Matsui M. The First Experimental Cryptanalysis of the Data Encryption Standard. Advancesin Cryptology – CRYPTO'94. LNCS. Berlin ; Heidelberg : Springer, 1994. Vol. 839. DOI: https://doi.org/10.1007/3-540-48658-5_9.

31. Biryukov A., Shamir A. Structural Cryptanalysis of SASAS. Advancesin Cryptology – EUROCRYPT 2001. LNCS. 2001. Vol. 2045. P. 394–405. DOI: https://doi.org/10.1007/3-540-44987-6_21.

32. Courtois N., Pieprzyk J. Cryptanalysis of Block Ciphers with Over defined Systems of Equations. Advancesin Cryptology – ASIACRYPT 2002. LNCS. 2002. Vol. 2501. P. 267–287. DOI: https://doi.org/10.1007/3-540-36178-2_16.

33. Integral Cryptanalysis of Block Ciphers / A. Bogdanov et al. *IACR Cryptologye Print Archive*. 2011. Report 2011/344. URL: https://eprint.iacr.org/2011/344 (дата звернення: 01.03.2026).

34. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Indianapolis : Wiley, 2010. DOI: https://doi.org/10.1002/9780470941961.

35. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin ; Heidelberg : Springer, 2010. DOI: https://doi.org/10.1007/978-3-642-04101-3.

36. Daemen J., Rijmen V. The Wide Trail Design Strategy. IACR Cryptologye Print Archive. 2002. Report 2002/001. URL: https://eprint.iacr.org/2002/001 (дата звернення: 01.03.2026).

37. Biryukov A., Khovratovich D. Related-Key Cryptanalysis of the Full AES-192 and AES-256. *Advances in Cryptology – ASIACRYPT 2009. LNCS*. 2009. Vol. 5912. P. 1–18. DOI: https://doi.org/10.1007/978-3-642-10366-6_1.

38. Dinur I., Dunkelman O., Shamir A. Improved Attacks on Full GOST. *Fast Software Encryption – FSE 2012. LNCS*. 2012. Vol. 7549. P. 9–28. DOI: https://doi.org/10.1007/978-3-642-34047-4_1.

39. Boura C., Canteaut A. On the Influence of the Algebraic Degreeof S-boxes on the Algebraic Degree of Block Ciphers. *IACR Cryptologye Print Archive*. 2010. Report 2010/646. URL: https://eprint.iacr.org/2010/646 (дата звернення: 01.03.2026).

40. The SIMON and SPECK Lightweight Block Ciphers / R. Beaulieu et al. *Proc. 52nd ACM/EDAC/IEEE Design Automation Conf. (DAC).* 2015. DOI: https://doi.org/10.1145/2744769.2747946.

41. Report on Lightweight Cryptography. National Institute of Standards and Technology. Gaithersburg : NIST, 2017. URL: https://csrc.nist.gov/publications (дата звернення: 01.03.2026).

42. Triathlon of Lightweight Block Ciphers / D. Dinu et al. *IACR Cryptologye Print Archive*. 2015. Report 2015/209. URL: https://eprint.iacr.org/2015/209 (дата звернення: 01.03.2026).

43. GIFT: A Small Present / S. Banik et al. *Cryptographic Hardware and Embedded Systems – CHES 2017. LNCS*. 2017. Vol. 10529. Cham : Springer, 2017. P. 321–345. DOI: https://doi.org/10.1007/978-3-319-66787-4_19.

44. The LED Block Cipher / J. Guo et al. *IACR Cryptologye Print Archive*. 2011. Report 2011/449. URL: https://eprint.iacr.org/2011/449 (дата звернення: 01.03.2026).

45. Biryukov A., Perrin L., Udovenko A. Reconstruction and Cryptanalysis of Streebog. *Advancesin Cryptology – CRYPTO 2016. LNCS*. 2016. Vol. 9815. Berlin ; Heidelberg : Springer, 2016. P. 3–32. DOI: https://doi.org/10.1007/978-3-662-53018-4_2.

46. Bogdanov A., Rijmen V. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography. 2014. Vol. 70, №3. P. 369–383. DOI: https://doi.org/10.1007/s10623-013-9797-5.

47. Khovratovich D., Nikolić I. Rotational Cryptanalysis of ARX. *Fast Software Encryption – FSE 2010. LNCS.*

Berlin ; Heidelberg : Springer, 2010. Vol. 6147. P. 333–346. DOI: https://doi.org/10.1007/978-3-642-13858-3_20.

48. Automatic Search for Related-Key Differential Characteristics in ARX Ciphers / A. Biryukov et al. *IACR Cryptologye Print Archive.* 2011. Report 2011/644. URL: https://eprint.iacr.org/2011/644 (дата звернення: 01.03.2026).

49. Cryptanalysis of Reduced-Round PRESENT / L. Zhang et al. IACR *Cryptologye Print Archive*. 2009. Report 2009/004. URL: https://eprint.iacr.org/2009/004 (дата звернення: 01.03.2026).

50. Security Evaluation of TWINE / T. Suzaki et al. *IACR Cryptologye Print Archive*. 2012. Report 2012/422. URL: https://eprint.iacr.org/2012/422 (дата звернення: 01.03.2026).

51. The SKINNY Family of BlockCiphers / C. Beierle et al. *Advancesin Cryptology – CRYPTO 2016. LNCS*. Berlin ; Heidelberg : Springer, 2016. Vol. 9814. P. 3–33. DOI: https://doi.org/10.1007/978-3-662-53018-4_9.

52. Midori: A Block Cipher for Low Energy / S. Banik et al. *Advancesin Cryptology – ASIACRYPT 2015. LNCS*. Berlin ; Heidelberg : Springer, 2015. Vol. 9453. P. 411–436. DOI: https://doi.org/10.1007/978-3-662-48800-3_13.

53. Daemen J., Rijmen V. AES Proposal: Rijndael. 1999. URL: https://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf (дата звернення: 01.03.2026).

54. FIPS 197: Advanced Encryption Standard (AES) / National Institute of Standards and Technology. Gaithersburg: NIST, 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (дата звернення: 01.03.2026).

55. PRIDE: A Block Cipher for Low-Latency Applications / E. Andreeva et al. *IACR Cryptologye Print Archive*. 2014. Report 2014/516. URL: https://eprint.iacr.org/2014/516 (дата звернення: 01.03.2026).

56. PRINT cipher: A Block Cipher for IC-Printing / L. R. Knudsen et al. *Cryptographic Hardware and Embedded Systems – CHES 2010. LNCS*. Berlin ; Heidelberg : Springer, 2010. Vol. 6225. P. 16–32. DOI: https://doi.org/10.1007/978-3-642-15031-9_2.

57. Compact Implementation and Performance Evaluation of Block Ciphersin Constrained Devices / T. Eisenbarth et al. *IACR Cryptologye Print Archive*. 2007. Report 2007/221. URL: https://eprint.iacr.org/2007/221 (дата звернення: 01.03.2026).

58. Cryptanalysis of Lightweight Block Ciphers: A Survey / J.-P. Aumasson et al. *IACR Cryptologye Print Archive*. 2013. Report 2013/315. URL: https://eprint.iacr.org/2013/315 (дата звернення: 01.03.2026).

59. Lightweight Cryptography Workshop 2015 / National Institute of Standards and Technology. Gaithersburg : NIST, 2015. URL: https://csrc.nist.gov/events/lightweight-cryptography-workshop-2015 (дата звернення: 01.03.2026).

60. SIMON and SPECK Implementation Guide / R. Beaulieu et al. National Security Agency, 2013. URL: https://nsacyber.github.io/simon-speck/ (дата звернення: 01.03.2026).

61. Triathlon of Lightweight Block Ciphers for the Internet of Things / D. Dinu et al. *IACR Cryptologye Print Archive*. 2015. Report 2015/209. URL: https://eprint.iacr.org/2015/209 (дата звернення: 01.03.2026).

62. Lightweight Cryptography Finalists Announcement / National Institute of Standards and Technology. 2023. URL: https://csrc.nist.gov/projects/lightweight-cryptography/finalists (дата звернення: 01.03.2026).

Стаття надійшла до редакції 27.01.2026.
Стаття пройшла рецензування 04.03.2026.
Стаття опублікована 31.03.2026.

Лужецький Володимир Андрійович – д-р техн. наук, професор, професор кафедри захисту інформації, ORCID: 0009-0003-2218-1527, e-mail: lva.kzi2002@gmail.com.

Кирилащук Тетяна Геннадіївна – аспірант кафедри захисту інформації, ORCID: 0009-0008-4238-3560, e-mail: kgt0998@gmail.com.
Вінницький національний технічний університет.