https://doi.org/10.31891/2219-9365-2025-82-39
УДК 004.056.55

ЯРЕМА Олег
Тернопільський національний технічний університет імені Івана Пулюя
e-mail: yarema_oleg@i.ua
https://orcid.org/0009-0009-8709-7813
ЗАГОРОДНА Наталія
Тернопільський національний технічний університет імені Івана Пулюя
e-mail: zagorodna.n@gmail.com
https://orcid.org/0000-0002-1808-835X

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ВПЛИВУ ДИФЕРЕНЦІАЛЬНОЇ РІВНОМІРНОСТІ НА СТІЙКІСТЬ S-БЛОКІВ ДО РІЗНИХ ТИПІВ КРИПТОАНАЛІЗУ

У статті досліджено вплив диференціальної рівномірності на стійкість до різних видів криптоаналізу та складність генерації 4-бітних S-блоків для використання в малоресурсних пристроях. Проведено порівняльний аналіз стійкості згенерованих блоків до диференціального, лінійного криптоаналізу та зламу грубою силою на прикладі запропонованого експериментального шифру. Актуальність даної теми дослідження зумовлена швидким розповсюдженням малоресурних пристроїв, зокрема пристроїв Інтернету речей (IoT), та необхідності забезпечення їх інформаційної безпеки. Використання малих та ефективних криптографічних шифрів є критично важливим для таких пристроїв.

В рамках цього дослідження було згенеровано множину 4-бітних S-блоків з різними значеннями диференціальної рівномірності. Для оцінки криптографічної стійкості цих блоків, було розроблено спрощену схему блокового шифру на базі SPN (substitution permutation network). Проведено порівняльний аналіз стійкості згенерованих S-блоків до диференціального, лінійного криптоаналізу та зламу грубою силою шляхом застосування відповідних криптографічних методів для зламу експериментального шифру.

Проведено аналіз отриманих експериментальних даних, результати якого подано у вигляді зведених таблиць. Результати проведеного дослідження чітко демонструють залежність між значеннями дифереціальної рівномірності S-блоків та їх здатністю протистояти диференціальному криптоаналізу. В той самий час показано, що диференціальна рівномірність не впливає на метод зламу грубою силою. Порівняння результатів оцінки стійкості до диференціального та лінійного криптоаналізу наочно ілюструють важливість комплексного підходу до проектування S-блоків з врахуванням усіх криптографічних властивостей, оскільки оптимізація лише однієї криптографічної властивості не гарантує високих показників стійкості до всіх типів криптографічних атак.

Отримані експериментальні результати мають важливе практичне значення для розробки безпечних та ефективних криптографічних шифрів, що можуть бути застосовані в умовах обмежених ресурсів IoT-пристроїв, а також у системах, що передбачають динамічну генерацію легких S-блоків для підвищення криптографічної стійкості і унеможливлення проведення деяких криптографічних атак.

Ключові слова: диференціальний криптоаналіз, блокові шифри, лінійний криптоаналіз, диференціальна рівномірність, лінійність, S-блоки.

YAREMA Oleh, ZAGORODNA Nataliya
Ternopil Ivan Puluj National Technical University

EXPERIMENTAL RESEARCH OF DIFFERENTIAL UNIFORMITY INFLUENCE ON RESISTANCE OF S-BOXES TO DIFFERENT TYPES OF CRYPTANALYSIS

The impact of differential uniformity on the resistance of 4-bit S-blocks to different types of cryptanalysis and the complexity of their generation for use in low-resource devices is investigated in this paper. A comparative analysis of the resistance of the generated blocks to differential, linear cryptanalysis and brute force attack is carried out on the example of the proposed experimental cipher. The relevance of this research topic is due to the rapid spread of low-resource devices, in particular Internet of Things (IoT) devices, and the need to ensure their information security. The use of small and efficient cryptographic ciphers is critical for such devices.

As part of this study, a set of 4-bit S-blocks with different differential uniformity values was generated. To evaluate the cryptographic strength of these blocks, a simplified block cipher scheme based on SPN (substitution permutation network) was developed. A comparative analysis of the resistance of the generated S-blocks to differential, linear cryptanalysis and brute force was carried out by applying appropriate cryptographic methods to break the experimental cipher.

The analysis of the obtained experimental data is presented in the form of summary tables. The results of the study clearly demonstrate the dependence between the values of the differential uniformity of S-blocks and their ability to resist differential cryptanalysis. At the same time, it is shown that the differential uniformity does not affect the brute force cracking method. Comparison of the results of assessing the resistance to differential and linear cryptanalysis clearly illustrates the importance of an integrated approach to the design of S-blocks, taking into account all cryptographic properties, since optimizing only one cryptographic property does not guarantee high resistance to all types of cryptographic attacks.

The obtained experimental results are of great practical importance for the development of secure and efficient cryptographic ciphers that can be used in conditions of limited resources of IoT devices, as well as in systems that provide for the dynamic generation of lightweight S-blocks to increase cryptographic security and prevent some cryptographic attacks.

Keywords: differential cryptanalysis, block ciphers, cryptographic strength, differential uniformity, S-boxes.

Стаття надійшла до редакції / Received 14.04.2025
Прийнята до друку / Accepted 10.05.2025

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

Криптографічні алгоритми є невід'ємною частиною сучасної інформаційної безпеки. Блокові шифри є фундаментом криптографії та використовуються в багатьох стандартних протоколах. Відкритість стандартів блокових шифрів, можливість їх використання у різних режимах, високий рівень криптостійкості робить їх надвичайно важливими для захисту даних. S-блоки є ключовим елементом всіх блокових шифрів, адже саме вони є джерелом нелінійності, необхідної для протидії різноманітним криптографічним атакам. Зі зростанням кількості малоресурсних пристроїв, таких як пристрої Інтернету речей (IoT), виникає нагальна потреба в легких та ефективних криптографічних рішеннях, де S-блоки відіграють важливу роль. Криптографічні властивості S-блоків, що вико ристовуються в міжнародних стандартах, та їх стійкість до відомих методів криптоаналізу є ґрунтовно дослідженими світовою спільнотою криптоаналітиків. В той самий час забезпечення конфіденційності та цілісності інформації в IoT-пристроях з обмеженими ресурсами вимагає використання малих S-блоків, криптостійкість та ефективність генерації яких вимагає додаткових досліджень. Таким чином, розробка малих S-блоків з високими криптографічними властивостями, що можуть бути ефективно реалізовані в умовах обмежених обчислювальних ресурсів, є актуальною науково-практичною задачею.

Крім того, для практичного застосування в динамічних криптографічних системах може знадобитися швидка перегенерація S-блоків, тому дослідження залежності між їх стійкістю до відомих видів криптоаналізу та швидкістю генерації S-блоків з необхідними криптографічними властивостями є вкрай важливим. Повинен існувати потенційний компроміс між криптографічною якістю S-блоку та часом, необхідним для його генерації, особливо для малих блоків, що використовуються в ресурсообмежених середовищах. Диференціальний криптоаналіз є одним з найбільш ефективних відомих на сьогодні методів зниження криптостійкості блокових шифрів. Диференціальна рівномірність (differential uniformity) — це важлива характеристика S-блоку, яка показує, наскільки він стійкий до диференціального криптоаналізу. Отже, систематичне дослідження взаємозв'язку між диференціальною рівномірністю малих S-блоків та складністю їхньої випадкової генерації, є актуальним науковим та практичним завданням для забезпечення безпеки інформації в екосистемі IoT та інших малоресурсних платформах.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Аналіз існуючих досліджень криптостійкості S-блоків підкреслює їхню важливість як нелінійних компонентів у блокових шифрах [1, 2]. В [3] приділяється значна увага розробці методів генерації S-блоків з бажаними криптографічними властивостями. Окремі дослідження розглядають застосування малих (або легких) S-блоків, у контексті обмежених ресурсів, характерних для IoT-пристроїв [4, 5], або пропонують конкретні приклади таких блоків з певними оптимізованими характеристиками [6, 7]. Однак, часто бракує системного аналізу криптографічних властивостей широкої множини випадково згенерованих S-блоків фіксованого невеликого розміру та їхньої стійкості до різних видів атак [8].

Хоча існують дослідження, що аналізують стійкість окремих S-блоків до диференціального криптоаналізу [9], бракує систематичного вивчення того, як саме різні рівні диференціальної рівномірності впливають на опір цілої множини малих S-блоків цьому типу атак у порівнянні зі складністю їхнього зламу методом грубої сили. Розуміння цієї залежності для великої кількості блоків, а не окремих прикладів, є важливим для оцінки їхньої практичної безпеки. Крім того, залишається малодослідженим питання про те, як різні значення диференціальної рівномірності впливають на складність та часові витрати випадкової генерації таких блоків, особливо тих, що відповідають певним криптографічним вимогам [10]. Така інформація могла б бути критично важливою для розробки блокових шифрів з динамічною генерацією S-блоків, де необхідно враховувати не лише криптографічну стійкість, але й ефективність їхнього створення в реальному часі [11]. Дослідження [12, 13] пропонують різні методи динамічної генерації S-блоків, зокрема в контексті малоресурсних пристроїв та IoT [14, 15], проте потребують подальшого вивчення їхньої ефективності та впливу на криптографічну стійкість у великих множинах випадково згенерованих блоків.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: проведення дослідження впливу диференціальної рівномірності випадково згенерованих 4-бітних S-блоків на їх стійкість до диференціального криптоаналізу та зламу грубою силою, а, також, оцінка складності їх випадкової генерації.

Досягнення поставленої мети вимагає виконання наступних завдань:

1. Згенерувати множину S-блоків для різних значень диференціальної рівномірності та зафіксувати кількість спроб, необхідних для генерації кожного блоку.

2. Розробити спрощену схему блокового шифру.

3. Експериментально оцінити стійкість згенерованих S-блоків до диференціального криптоаналізу та зламу грубою силою на основі запропоновано блокового шифру та вимірювання кількості операцій, необхідних для успішного зламу.

4. Проаналізувати отримані результати для визначення залежностей між диференціальною рівномірністю, складністю генерації та стійкістю до диференціального криптоаналізу.

5. Виконати порівняльний аналіз результатів диференціального та brute-force аналізу досліджуваних S-блоків.

6. Визначити подальші перспективні напрями дослідження на основі отриманих результатів та висновків.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Загалом, S-блок є нелінійним перетворенням, яке відображає блок вхідних бітів фіксованої довжини в блок вихідних бітів певної довжини. Його основна функція полягає у забезпеченні нелінійності в шифрі, що є критично важливим для протидії лінійному криптоаналізу та іншим статистичним атакам. Без нелінійних компонентів шифр був би лінійною функцією відкритого тексту та ключа, що робило б його вразливим до відносно простих криптографічних атак [16].

Дві фундаментальні криптографічні властивості S-блоків, що безпосередньо впливають на їхню стійкість до статистичних методів криптоаналізу, є нелінійність та диференціальна рівномірність.

Нелінійність S-блоку, що є мірою його відмінності від афінних булевих функцій, є ключовою властивістю для протидії лінійному криптоаналізу. Висока нелінійність ускладнює побудову лінійних апроксимацій, які використовуються для встановлення статистичних зв'язків між відкритим текстом, шифротекстом і ключем, що може призвести до розкриття секретної інформації. Вимірювання нелінійності S-блоку проводиться за рахунок складання таблиці лінійних апроксимацій (Linear Approximation Table, LAT), яка відображає кореляції між лінійними комбінаціями вхідних та вихідних бітів S-блоку. Значення в цій таблиці використовуються для визначення лінійної вразливості S-блоку [17].

Іншою важливою властивістю є диференціальна рівномірність, яка характеризує стійкість S-блоку до диференціального криптоаналізу. Диференціальна рівномірність вираховується за рахунок побудови таблиці диференціального розподілу (Difference Distribution Table, DDT). Ця таблиця відображає, скільки разів кожна можлива вхідна різниця призводить до кожної можливої вихідної різниці. Бажаною є низька диференціальна рівномірність, що означає рівномірний розподіл вихідних різниць для кожної ненульової вхідної різниці, оскільки вона ускладнює передбачення поширення різниць через S-блок і, відповідно, проведення успішного диференціального криптоаналізу. Висока диференціальна рівномірність може свідчити про існування вхідних різниць, які з великою ймовірністю призводять до певних вихідних різниць, що може бути використано для відновлення секретного ключа [18].

На першому етапі експерименту було випадково згенеровано множину S-блоків 4x4 біта, тобто таких, що приймають 4 біти на вхід і відображають їх в 4 біти на виході. Частіше за все такі S-блоки зображують у вигляді таблиці пошуку (lookup table) або звичайної таблиці підстановки чи словника. Вибір такого розміру блоку зумовлений його широким використанням у дослідженнях, що представляють нові S-блоки для ресурсообмежених систем [19], а також застосуванням подібного розміру в уже існуючих популярних легких шифрах, таких як PRESENT [20]. Для кожного згенерованого блоку проводилася оцінка його диференціальної рівномірності (за таблицею диференціального розподілу). До подальшого аналізу включалися лише ті блоки, які відповідали попередньо встановленим критеріям щодо цієї криптографічної властивості; інші згенеровані блоки відкидалися. Експеримент передбачав генерацію S-блоків для семи різних значень диференціальної рівномірності: 2, 4, 6, 8, 10, 12 та 14. Для кожного з цих семи значень було згенеровано по 10 унікальних S-блоків, що сформувало загальну множину з 70 S-блоків. Під час генерації кожного S-блоку з зафіксованою мірою диференціальної нерівномірності фіксувалася кількість спроб, необхідних для його генерації та обчислення його криптографічних характеристик.

На другому етапі дослідження кожен із 70 згенерованих S-блоків використовувався як нелінійний елемент у експериментальному блоковому шифрі, що базується на спрощеній структурі SPN (substitution-permutation network). Рисунок 1 ілюструє загальну структуру цього шифру. Як видно зі схеми, алгоритм шифру складається з п’ятьох послідовних раундів. На вхід кожного раунду R подається вихід попереднього раунду R_{i-1} (для першого раунду – відкритий текст P) та частина загального 20-бітного ключа K. 20-бітний ключ K на початку роботи алгоритму поділяється на п’ять 4-бітних підключів K1, K2, K3, K4, K5, які використовуються відповідно в першому, другому, третьому, четвертому та п’ятому раундах шифрування. На виході п’ятого раунду R5 формується зашифрований текст C розміром 4 біти.

ISSN 2219-9365

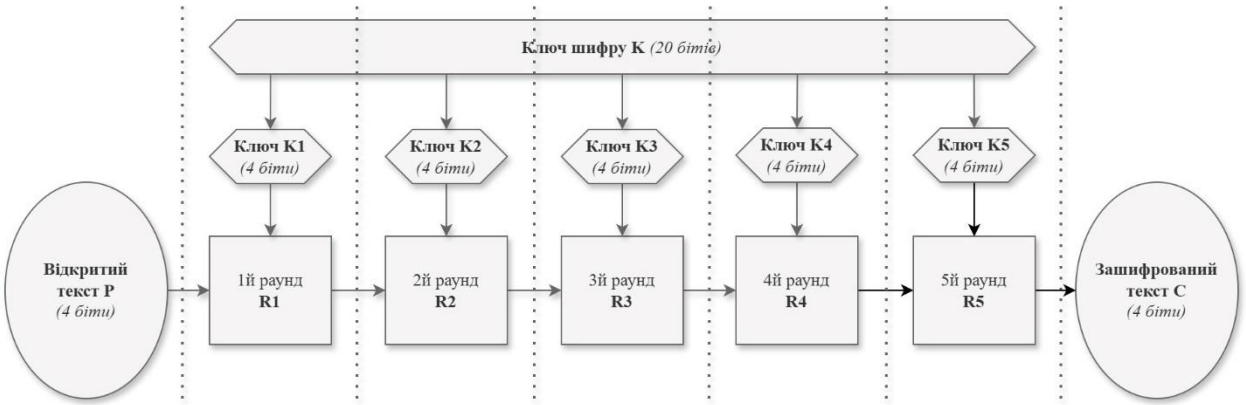

Рис. 1. Будова експериментального шифру

На рисунку 2 зображено структуру окремого раунду експериментального шифру. Кожен раунд складається з двох основних операцій:

1. Додавання за модулем два (XOR) входу раунду з 4-бітним підключем K_i. На рисунку це відображено як операція $\oplus$, тобто $XOR(R_{i-1}, K_i)$.

2. Проходження результату операції XOR через 4-бітовий S-блок, який приймає 4 біти на вхід та повертає 4 біти на вихід і в цій реалізації предсталений таблицею підстановки значень.

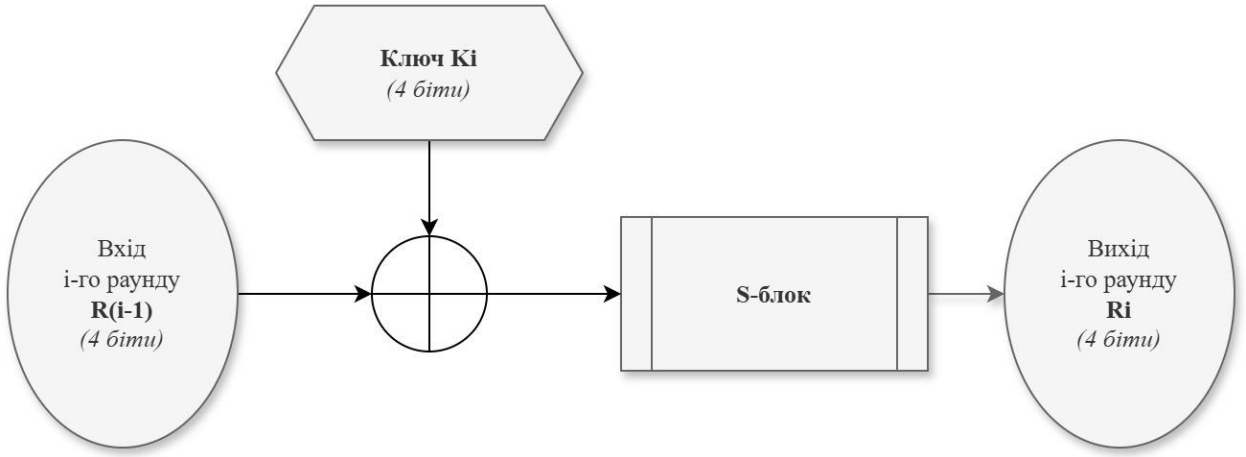

Рис. 2. Будова окремого раунду експериментального шифру

Як було зазначено раніше, загалом було згенеровано 70 4-бітних S-блоків, кожен з яких був протестований в експериментальному блоковому шифрі. Після цього для кожного зашифрованого повідомлення здійснювалася оцінка стійкості двома методами:

1. Злам методом грубої сили (brute force аналіз): Зафіксовано кількість спроб випадкового перебору 20-бітного ключа, необхідних для успішного розшифрування повідомлення.

2. Диференціальний криптоаналіз: Проводився аналіз стійкості шифру до диференціального криптоаналізу з використанням фіксованого S-блоку. Для реалізації атаки на основі відомого відкритого тексту було проведено шифрування 5 різних 4-бітних повідомлень. Вимірювалася кількість проведених циклів диференціального криптоаналізу шифру з обраним S-блоком.

На завершальному етапі експерименту всі отримані дані, включаючи значення диференціальної рівномірності, кількість спроб генерації S-блоків, а також мінімальні, максимальні та середні значення циклів, витрачених на диференціальний криптоаналіз та злам грубою силою для кожної групи S-блоків, було систематизовано та представлено у таблиці 1 для подальшого аналізу та порівняння. Ця таблиця стала основою для виявлення залежностей між досліджуваними параметрами та оцінки ефективності різних значень диференціальної рівномірності щодо стійкості та складності генерації S-блоків.

З наведених даних можна зробити кілька висновків. По-перше, генерація блоків з максимально малими значеннями диференціальної рівномірності (тобто такими, які є максимально стійкими до диференціального криптоаналізу) або з максимально високими (тобто такими, які мають мінімальну стійкість до диференціального криптоаналізу) потребує більших затрат в часі, ніж генерація блоків з відносно середніми значеннями характеристики. По-друге, можна виділити кілька групи блоків з різними значеннями

диференціальної рівномірності, які, проте, мають в середньому однакову криптостійкість. Так, для прикладу, блоки з диференціальною рівномірністю 6, 8 та 10 мають приблизно однакову криптографічну стійкість, а значить їх можна розглядати як одну загальну групу. По-третє, як і очікувалось, відсутня кореляція між диференціальною рівномірністю S-блоків та їх стійкістю до методу грубої сили.

Таблиця 1

Зведення даних по генерації та зламу S-блоків

Диференціальна рівномірність, абс-не знач-ня	Кількість спроб генерації одного S-блока			Кількість проведених циклів диференціального криптоаналізу			Кількість циклів перебору грубої сили		
	мін.	середнє	макс.	мін.	середнє	макс.	мін.	середнє	макс.
2	1188	**1550**	1941	49	**111**	282	256	**333**	383
4	2	**17**	33	18	**41**	88	242	**303**	356
6	2	**5**	7	12	**15**	25	155	**263**	396
8	2	**4**	7	9	**14**	24	173	**301**	408
10	2	**16**	58	10	**14**	19	185	**266**	354
12	19	**189**	362	6	**10**	16	215	**320**	420
14	288	**620**	925	4	**6**	8	199	**315**	380

Хоча дане дослідження зосереджувалося на впливі диференціальної рівномірності на стійкість 4-бітних S-блоків до диференціального криптоаналізу та зламу грубою силою, додатково був проведений лінійний криптоаналіз згенерованих блоків. Як ілюструє таблиця 2, що містить узагальнені дані щодо стійкості до диференціального та лінійного криптоаналізу згенерованих блоків з різними значеннями диференціальної рівномірності, зосередження уваги виключно на оптимізації однієї криптографічної властивості може призвести до незбалансованих S-блоків. Зокрема, блоки з високою стійкістю до диференціального криптоаналізу можуть демонструвати посередні значення лінійності та, як наслідок, бути вразливими до лінійного криптоаналізу. Це наочно демонструє, що для забезпечення загальної стійкості криптографічних систем необхідно враховувати весь спектр ключових характеристик S-блоків, а не лише одну з них. Отримані результати підкреслюють важливість комплексного підходу до оцінки криптографічної стійкості.

Таблиця 2

Результати багатокритеріального ранжування S-блоків від найкращого до найгіршого

Диференціальна рівномірність, абсолютне значення	**Кількість проведених циклів диференціального криптоаналізу**			**Кількість проведених циклів лінійного криптоаналізу**		
	мін.	**середнє**	**макс.**	**мін.**	**середнє**	**макс.**
2	49	**111**	282	6	**9**	14
4	18	**41**	88	7	**9**	14
6	12	**15**	25	7	**9**	11
8	9	**14**	24	7	**8**	9
10	10	**14**	19	7	**9**	13
12	6	**10**	16	7	**9**	11
14	4	**6**	8	8	**10**	15

Отримані в ході експерименту дані чітко вказують на перспективність подальших досліджень. Зокрема, в майбутньому можна провести порівняльний аналіз взаємозв'язку між диференціальною рівномірністю та лінійністю для ширшої множини 4-бітних S-блоків, а також комплексне вивчення їхньої стійкості до лінійного та диференціального криптоаналізу. Крім того, криптографічну стійкість шифрів, що використовують такі S-блоки, можна підвищити за рахунок горизонтального масштабування, яке передбачає збільшення розміру оброблюваних повідомлень і ключів та, відповідно, збільшення кількості S-блоків в одному раунді, а також за рахунок вертикального масштабування, що полягає у збільшенні кількості раундів у шифрі. У зв'язку з цим, доцільним є розгляд впливу цих методів масштабування, а також інших криптографічних властивостей для всебічної оцінки стійкості малих S-блоків, що є важливим для їхнього застосування в ресурсообмежених середовищах.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ У ДАНОМУ НАПРЯМІ

Було проведено експериментальні дослідження 4-бітних S-блоків для встановлення зв’язку між їх диференціальною рівномірністю, стійкістю до диференціального криптоаналізу та зламу грубою силою, а також складністю їх випадкової генерації. Аналіз множини згенерованих S-блоків підтвердив, що нижчі значення диференціальної рівномірності, як правило, корелюють з вищою стійкістю до диференціального аналізу, проте вимагають більших обчислювальних ресурсів для їх генерації. Додатково, отримані S-блоки були досліджені на стійкість до лінійного криптоаналізу. Порівняльний аналіз стійкості до диференціального

та лінійного криптоаналізу підкреслив важливість комплексного підходу до оцінки криптографічної міцності S-блоків, оскільки висока стійкість до одного типу атаки не гарантує загальної безпеки.

Перспективи подальших досліджень у цьому напрямі включають розширення експериментальної бази для глибшого вивчення взаємозв'язку між різними криптографічними характеристиками малих S-блоків та їхньою стійкістю до ширшого спектру криптографічних атак. Особливу увагу слід приділити розробці ефективних методів генерації S-блоків з оптимальним балансом між криптографічною стійкістю та вартістю їхнього створення для застосування в малоресурсних пристроях та динамічних криптосистемах. Також важливим є проведення детального аналізу впливу різних значень диференціальної рівномірності на складність генерації S-блоків з урахуванням інших критеріїв.

Література

1. Systematic literature review: trend analysis on the design of lightweight block cipher / A. A. Zakaria та ін. *Journal of king saud university - computer and information sciences*. 2023. URL: https://doi.org/10.1016/j.jksuci.2023.04.003 (дата звернення: 13.05.2025).

2. Azam N. A., Hayat U., Ayub M. A substitution box generator, its analysis, and applications in image encryption. *Signal processing*. 2021. Т. 187. С. 108144. URL: https://doi.org/10.1016/j.sigpro.2021.108144 (дата звернення: 13.05.2025).

3. Xu Y., Wang Q. Searching for balanced s-boxes with high nonlinearity, low differential uniformity, and improved dpa-resistance. *Lecture notes in computer science*. Cham, 2020. С. 95–106. URL: https://doi.org/10.1007/978-3-030-62974-8_6 (дата звернення: 07.05.2025).

4. Sevin A., Mohammed A. A. O. A survey on software implementation of lightweight block ciphers for IoT devices. *Journal of ambient intelligence and humanized computing*. 2021. URL: https://doi.org/10.1007/s12652-021-03395-3 (дата звернення: 13.05.2025).

5. Zhong Y., Gu J. Lightweight block ciphers for resource-constrained environments: a comprehensive survey. *Future generation computer systems*. 2024. URL: https://doi.org/10.1016/j.future.2024.03.054 (дата звернення: 13.05.2025).

6. Panchami V., Mathews M. M. A substitution box for lightweight ciphers to secure internet of things. *Journal of king saud university - computer and information sciences*. 2023. URL: https://doi.org/10.1016/j.jksuci.2023.03.004 (дата звернення: 13.05.2025).

7. Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box / B. M. Alshammari та ін. *Symmetry*. 2021. Т. 13, № 1. С. 129. URL: https://doi.org/10.3390/sym13010129 (дата звернення: 13.05.2025).

8. An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges / A. Waheed та ін. *Multimedia tools and applications*. 2023. URL: https://doi.org/10.1007/s11042-023-14910-3 (дата звернення: 13.05.2025).

9. Security evaluation of lightweight block ciphers against mixture differential cryptanalysis / J. Geng та ін. *IEEE internet of things journal*. 2024. С. 1. URL: https://doi.org/10.1109/jiot.2024.3380254 (дата звернення: 07.05.2025).

10. Study of S-box properties in block cipher / K. Mohamed та ін. *2014 international conference on computer, communications, and control technology (I4CT)*, м. Langkawi, Malaysia, 2–4 верес. 2014 р. 2014. URL: https://doi.org/10.1109/i4ct.2014.6914206 (дата звернення: 13.05.2025).

11. A survey of hardware-based AES sboxes: area, performance, and security / P. S. Curlin та ін. *ACM computing surveys*. 2025. URL: https://doi.org/10.1145/3724114 (дата звернення: 13.05.2025).

12. A novel construction of dynamic s-box with high nonlinearity using heuristic evolution / A. H. Zahid та ін. *IEEE access*. 2021. Т. 9. С. 67797–67812. URL: https://doi.org/10.1109/access.2021.3077194 (дата звернення: 07.05.2025).

13. Efficient dynamic s-box generation using linear trigonometric transformation for security applications / A. H. Zahid та ін. *IEEE access*. 2021. Т. 9. С. 98460–98475. URL: https://doi.org/10.1109/access.2021.3095618 (дата звернення: 13.05.2025).

14. James D., Priya T. L. An innovative approach for dynamic key dependent S-Box to enhance security of IoT systems. *Measurement: sensors*. 2023. С. 100923. URL: https://doi.org/10.1016/j.measen.2023.100923 (дата звернення: 13.05.2025).

15. Khudhair A. T., Maolood A. T., Gbashi E. K. A novel approach to generate dynamic s-box for lightweight cryptography based on the 3D hindmarsh rose model. *Journal of soft computing and computer applications*. 2024. Т. 1, № 1. URL: https://doi.org/10.70403/3008-1084.1003 (дата звернення: 13.05.2025).

16. Mishra G., Krishna Murthy S. V. S. S. N. V. G., Pal S. K. Dependency of lightweight block ciphers over S-boxes: a deep learning based analysis. *Journal of discrete mathematical sciences and cryptography*. 2021. С. 1–21. URL: https://doi.org/10.1080/09720529.2021.1932889 (дата звернення: 13.05.2025).

17. Kim G., Jeon Y., Kim J. Speeding up LAT: generating a linear approximation table using a bitsliced implementation. *IEEE access*. 2022. Т. 10. С. 4919–4923. URL: https://doi.org/10.1109/access.2022.3140242 (дата звернення: 13.05.2025).

18. Dunkelman O., Huang S. Reconstructing an s-box from its difference distribution table. *IACR transactions on symmetric cryptology*. 2019. С. 193–217. URL: https://doi.org/10.46586/tosc.v2019.i2.193-217 (дата звернення: 13.05.2025).

19. Resource-Efficient 4×4 s-boxes using chaotic map / P.-P. Duong та ін. *2024 1st international conference on cryptography and information security (VCRIS)*, м. Hanoi, Vietnam, 3–4 груд. 2024 р. 2024. С. 1–6. URL: https://doi.org/10.1109/vcris63677.2024.10813445 (дата звернення: 13.05.2025).

20. Aldabbagh S. S. M., Al Shaikhli I. F. T. Security of present s-box. *2012 international conference on advanced computer science applications and technologies (ACSAT)*, м. Kuala Lumpur, Malaysia, 26–28 листоп. 2012 р. 2012. URL: https://doi.org/10.1109/acsat.2012.23 (дата звернення: 13.05.2025).

References

1. Systematic literature review: trend analysis on the design of lightweight block cipher / A. A. Zakaria ta in. Journal of king saud university - computer and information sciences. 2023. URL: https://doi.org/10.1016/j.jksuci.2023.04.003 (data zvernennia: 13.05.2025).

2. Azam N. A., Hayat U., Ayub M. A substitution box generator, its analysis, and applications in image encryption. Signal processing. 2021. T. 187. S. 108144. URL: https://doi.org/10.1016/j.sigpro.2021.108144 (data zvernennia: 13.05.2025).

3. Xu Y., Wang Q. Searching for balanced s-boxes with high nonlinearity, low differential uniformity, and improved dpa-resistance. Lecture notes in computer science. Cham, 2020. S. 95–106. URL: https://doi.org/10.1007/978-3-030-62974-8_6 (data zvernennia: 07.05.2025).

4. Sevin A., Mohammed A. A. O. A survey on software implementation of lightweight block ciphers for IoT devices. Journal of ambient intelligence and humanized computing. 2021. URL: https://doi.org/10.1007/s12652-021-03395-3 (data zvernennia: 13.05.2025).

5. Zhong Y., Gu J. Lightweight block ciphers for resource-constrained environments: a comprehensive survey. Future generation computer systems. 2024. URL: https://doi.org/10.1016/j.future.2024.03.054 (data zvernennia: 13.05.2025).

6. Panchami V., Mathews M. M. A substitution box for lightweight ciphers to secure internet of things. Journal of king saud university - computer and information sciences. 2023. URL: https://doi.org/10.1016/j.jksuci.2023.03.004 (data zvernennia: 13.05.2025).

7. Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box / B. M. Alshammari ta in. Symmetry. 2021. T. 13, № 1. S. 129. URL: https://doi.org/10.3390/sym13010129 (data zvernennia: 13.05.2025).

8. An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges / A. Waheed ta in. Multimedia tools and applications. 2023. URL: https://doi.org/10.1007/s11042-023-14910-3 (data zvernennia: 13.05.2025).

9. Security evaluation of lightweight block ciphers against mixture differential cryptanalysis / J. Geng ta in. IEEE internet of things journal. 2024. S. 1. URL: https://doi.org/10.1109/jiot.2024.3380254 (data zvernennia: 07.05.2025).

10. Study of S-box properties in block cipher / K. Mohamed ta in. 2014 international conference on computer, communications, and control technology (I4CT), m. Langkawi, Malaysia, 2–4 veres. 2014 r. 2014. URL: https://doi.org/10.1109/i4ct.2014.6914206 (data zvernennia: 13.05.2025).

11. A survey of hardware-based AES sboxes: area, performance, and security / P. S. Curlin ta in. ACM computing surveys. 2025. URL: https://doi.org/10.1145/3724114 (data zvernennia: 13.05.2025).

12. A novel construction of dynamic s-box with high nonlinearity using heuristic evolution / A. H. Zahid ta in. IEEE access. 2021. T. 9. S. 67797–67812. URL: https://doi.org/10.1109/access.2021.3077194 (data zvernennia: 07.05.2025).

13. Efficient dynamic s-box generation using linear trigonometric transformation for security applications / A. H. Zahid ta in. IEEE access. 2021. T. 9. S. 98460–98475. URL: https://doi.org/10.1109/access.2021.3095618 (data zvernennia: 13.05.2025).

14. James D., Priya T. L. An innovative approach for dynamic key dependent S-Box to enhance security of IoT systems. Measurement: sensors. 2023. S. 100923. URL: https://doi.org/10.1016/j.measen.2023.100923 (data zvernennia: 13.05.2025).

15. Khudhair A. T., Maolood A. T., Gbashi E. K. A novel approach to generate dynamic s-box for lightweight cryptography based on the 3D hindmarsh rose model. Journal of soft computing and computer applications. 2024. T. 1, № 1. URL: https://doi.org/10.70403/3008-1084.1003 (data zvernennia: 13.05.2025).

16. Mishra G., Krishna Murthy S. V. S. S. N. V. G., Pal S. K. Dependency of lightweight block ciphers over S-boxes: a deep learning based analysis. Journal of discrete mathematical sciences and cryptography. 2021. S. 1–21. URL: https://doi.org/10.1080/09720529.2021.1932889 (data zvernennia: 13.05.2025).

17. Kim G., Jeon Y., Kim J. Speeding up LAT: generating a linear approximation table using a bitsliced implementation. IEEE access. 2022. T. 10. S. 4919–4923. URL: https://doi.org/10.1109/access.2022.3140242 (data zvernennia: 13.05.2025).

18. Dunkelman O., Huang S. Reconstructing an s-box from its difference distribution table. IACR transactions on symmetric cryptology. 2019. S. 193–217. URL: https://doi.org/10.46586/tosc.v2019.i2.193-217 (data zvernennia: 13.05.2025).

19. Resource-Efficient 4×4 s-boxes using chaotic map / P.-P. Duong ta in. 2024 1st international conference on cryptography and information security (VCRIS), m. Hanoi, Vietnam, 3–4 hrud. 2024 r. 2024. S. 1–6. URL: https://doi.org/10.1109/vcris63677.2024.10813445 (data zvernennia: 13.05.2025).

20. Aldabbagh S. S. M., Al Shaikhli I. F. T. Security of present s-box. 2012 international conference on advanced computer science applications and technologies (ACSAT), m. Kuala Lumpur, Malaysia, 26–28 lystop. 2012 r. 2012. URL: https://doi.org/10.1109/acsat.2012.23 (data zvernennia: 13.05.2025).