DOI 10.15276/imms.v15.no4.614
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 4, pp. 614-624

ПІДВИЩЕННЯ СТІЙКОСТІ СУЧАСНИХ БЛОКОВИХ ШИФРІВ ЗА ДОПОМОГОЮ ВИСОКОЯКІСНИХ S-БЛОКІВ

В. В. Радуш

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: radush9860@gmail.com

Забезпечення високого рівня криптографічної стійкості сучасних симетричних шифрів безпосередньо залежить від якості застосованих у них S-блоків. Традиційно аналіз S-блоків обмежується апаратом булевих функцій, однак останні дослідження показують, що в умовах атак на основі багатозначної логіки окремі стандартні S-блоки можуть демонструвати недостатній рівень криптографічної стійкості. Це створює необхідність комплексної оцінки таких криптографічних примітивів для забезпечення їх якості як у булевому, так і в багатозначному поданні. Проведена експериментальна оцінка якості S-блоків, що застосовуються в сучасних симетричних блокових шифрах, з акцентом на практичну ефективність при реальному шифруванні та оцінку стохастичних властивостей криптограми. З метою посилення криптографічних характеристик шифрів, замість оригінальних підстановок були використані авторські S-блоки, побудовані на основі недвійкових афінних перетворень, які демонструють високі криптографічні властивості при представленні як булевими функціями, так і функціями багатозначної логіки. Методика включала два взаємодоповнюючих етапи: розрахунок ключових метрик якості S-блоків – нелінійності, виконання суворого лавинного критерію (SAC), критерію незалежності бітів (BIC), ймовірності лінійної (LAP) і диференціальної (DAP) апроксимації; практичну верифікацію шляхом шифрування інформаційних масивів модифікованими шифрами та подальшого статистичного аналізу вихідних криптограм за допомогою NIST-тестів. Дослідження охопило криптоалгоритми AES, Camellia, Kalyna, SM4 і ARIA. Розрахункові показники разом зі стохастичною перевіркою показали, що S-блоки на основі четвіркових афінних перетворень забезпечують підвищену збалансованість і стійкість. У більшості випадків модифіковані версії шифрів випередили оригінали за кількістю пройдених NIST-тестів (зокрема AES, ARIA, SM4, Camellia), що свідчить про посилення випадковості та криптостійкості вихідних послідовностей. Важливо підкреслити експериментальний характер роботи: проведена порівняльна та практична перевірка S-блоків на основі афінних перетворень. Отримані дані вказують на перспективність подальшої інтеграції таких примітивів у протоколи зв'язку, захист IoT-пристроїв, хмарні сервіси та критичну інфраструктуру, де вимоги до випадковості та стійкості особливо високі. Поєднання теоретичних критеріїв якості та практичної перевірки криптограм дозволяє говорити про надійну методологічну базу для прийняття рішень щодо впровадження таких S-блоків у реальні системи.

Ключові слова: криптографічні примітиви; блокові шифри; S-блоки; афінні перетворення; багатозначна логіка; нелінійність; лавинний критерій; NIST Statistical Test Suite; криптоаналіз; випадковість криптограм.

Вступ та постановка проблеми. Цифрові технології сьогодні є невід'ємною складовою сучасного суспільства, оскільки використання комп'ютерних систем та мережі Інтернет перетворилося з факультативної можливості на обов'язкову умову ефективної діяльності у більшості сфер. Значна частина щоденних процесів – від професійної діяльності до побутових завдань – тісно інтегрована з цифровим середовищем. У результаті, переважна більшість інформації у світі існує у цифровому вигляді, що забезпечує можливість її довготривалого зберігання, масштабної обробки та оперативної передачі у глобальних масштабах.

Водночас із беззаперечними перевагами цифровізації постають і суттєві виклики, пов'язані з інформаційною безпекою. Персональні дані, що циркулюють у кіберпросторі,

можуть стати об’єктом несанкціонованого доступу, викрадення чи зловживання з боку зловмисників. Такі загрози актуалізують необхідність розроблення та впровадження ефективних механізмів захисту інформації. Саме цим завданням покликані відповідати криптографічні методи та комплексні засоби мережевої безпеки [1].

Криптографія – це наукова дисципліна, що вивчає методи та засоби перетворення інформації з метою забезпечення її конфіденційності, цілісності, автентичності та невідмовності. Основним завданням криптографії є трансформація відкритого (читабельного) тексту у зашифрований (шифротекст) таким чином, щоб без відповідних криптографічних реквізитів відновлення початкових даних було неможливим. При цьому за наявності ключа чи іншої секретної інформації передбачена можливість виконати зворотне перетворення – відновлення оригінального повідомлення.

Усі сучасні криптографічні алгоритми умовно поділяються на дві фундаментальні категорії – симетричну та асиметричну криптографію. Симетричні методи, у свою чергу, охоплюють кілька підтипів: блокові шифри, потокові шифри та криптографічні геш-функції [2].

Однак, незалежно від рівня складності криптографічного алгоритму, його основу становлять дві фундаментальні операції – підстановка та перестановка. Вони відомі ще з часів класичної криптографії, однак саме Клод Шеннон надав їм сучасного теоретичного обґрунтування, визначивши їх як ключові механізми для досягнення конфузії та дифузії у криптосистемах. Підстановка має фактично вирішальну роль майже в усіх сучасних криптографічних алгоритмах, таких як, наприклад, визнаний стандарт AES. Досягається ця операція за допомогою використання відповідних криптографічних примітивів – блоків підстановки, що називаються S-блоками. S-блок – це базовий нелінійний компонент криптографічних алгоритмів, що реалізує відображення елементів вхідного алфавіту у вихідний алфавіт. Його основною функцією є забезпечення конфузії, тобто ускладнення зв’язку між ключем і шифротекстом, що значно підвищує стійкість криптосистеми до криптоаналітичних атак [3]. Очевидно, що якість криптографічних примітивів безпосередньо визначає стійкість та ефективність усього криптоалгоритму, який їх застосовує. Зокрема, чим вищий рівень реалізованих у S-блоці конфузії та дифузії, тим вищою буде криптографічна якість і надійність алгоритму загалом.

Для оцінки властивостей S-блоків використовують наступні метрики:

1. Відстань нелінійності.
2. Критерій незалежності бітів (BIC).
3. Відповідність суворому лавинному критерію (SAC).
4. Статистична незалежність виходу S-блоку підстановки від його входу (кореляційний імунітет).
5. Ймовірність лінійної апроксимації (LAP).
6. Ймовірність диференціальної апроксимації (DAP).

Варто зазначити, що оцінка якості S-блоків у більшості випадків здійснюється виключно в межах апарату булевих функцій, ігноруючи альтернативні підходи до їх подання. Водночас існує ненульова ймовірність атак, що базуються на апараті багатозначної логіки, у межах яких криптографічні властивості обраного S-блоку можуть виявитися істотно слабшими [4].

Сьогодні відомо багато підходів до синтезу високоякісних S-блоків, зокрема авторські методи, представлені у відповідних дослідженнях. Побудовані за цими методами S-блоки демонструють високий рівень відповідності формалізованим метрикам, що використовуються для оцінювання криптографічних властивостей, таких як нелінійність, стійкість до диференціального та лінійного криптоаналізу тощо.

Разом із тим, залишається відкритим питання практичної ефективності таких S-блоків у складі конкретних криптографічних алгоритмів. Попри високі теоретичні показники, їхня реальна поведінка в комбінації з іншими криптографічними примітивами може суттєво відрізнятися. У науковій літературі ця проблема висвітлена

недостатньо, що актуалізує необхідність подальших досліджень, спрямованих на вивчення властивостей синтезованих S-блоків у практичних криптосистемах.

Метою цієї роботи є дослідження ефективності заміни стандартних S-блоків на синтезовані S-блоки з підвищеними криптографічними характеристиками, а також оцінка впливу таких замін на загальну стійкість та якість криптографічних алгоритмів.

Методи оцінки. Як було зазначено раніше, рівень конфузії та дифузії безпосередньо залежить від характеристик криптографічного примітиву, що входить до складу конкретного алгоритму. S-блок розглядається як один із ключових елементів сучасних криптографічних систем, оскільки саме завдяки йому забезпечується стійкість алгоритмів до криптоаналітичних атак, зокрема лінійного, диференційного та кореляційного аналізу. Таким чином, пошук та синтез високоякісних S-блоків залишається однією з центральних задач у дослідженнях криптографічних примітивів.

Щоб S-блок вважався криптографічно якісним, він має відповідати ряду наведених раніше критеріїв. Ці критерії оперують декомпозицією S-блоку на компонентні булеві функції $S = \{f_i\}, i = 1, 2, ..., k$, де k – відображає кількість входів/виходів S-блоку. Після розкладання S-блоку на компонентні булеві функції відбувається його оцінка відповідно до кожного цільового критерію.

Нелінійність. Відстань нелінійності – це ключове поняття, що визначається у часовій області як мінімальна відстань Геммінга між компонентними булевими функціями S-блока та всіма кодовими словами афінного коду і описується рівнянням

$$N_S = \min_i \left\{ \text{dist}(f_i, \varphi_j) \right\}, \; i = 1, ..., k, \; j = 1, ..., 2^{k+1}, \tag{1}$$

де f_i – i-та компонентна булева функція;

φ_j – кодове слово афінного коду;

dist(•) – оператор знаходження відстані Геммінга.

Також, існує альтернативний варіант оцінки за допомогою перетворення Уолша-Адамара, що визначається як

$$N_f = 2^{k-1} - \frac{1}{2} \max \left\{ \left| W(\omega) \right| \right\}, \tag{2}$$

де $\left| W(\omega) \right|$ – вектор трансформант перетворення Уолша-Адамара булевої функції f_i, що визначається як добуток таблиці істинності, представленої в експоненційній формі та матриці Уолша-Адамара

$$W = FA_N, \tag{3}$$

де матриця A_N представлена як

$$A_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, A_1 = 1. \tag{4}$$

Нелінійність всього S-блока визначається за найменшим визначеним значенням нелінійності серед усіх компонентних булевих функцій S-блока $N_S = \min_i \{N_{f_i}\}$. Цей принцип є дійсним як при обрахунках в часовій області (1), так і за допомогою перетворення Уолша-Адамара (2) [5].

Суворий лавинний критерій (SAC). Даний критерій оцінювання заснований на оцінці критерія поширення помилки [6]. Для його оцінки аналізуються мінімальні та максимальні значення ваг похідних компонентних булевих функцій

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{5}$$

за усіма напрямками $\forall u \in V_k, wt(u) = 1$, де V_k – лінійний векторний простір векторів довжини *k,* а *wt*(□) – це оператор знаходження ваги Геммінга. Для того, щоб лавинні властивості були максимальними, усі похідні мають бути збалансованими, тобто їх вага

має дорівнювати $N/2$, що в свою чергу забезпечує вірогідність зміни виходу при зміні будь-якого входу рівною 0.5.

Критерій незалежності бітів (BIC). Відповідає за оцінку кореляції між компонентними булевими функціями S-блоку. Умовою виконання є наступне твердження.

Твердження 1. Якщо для двох будь-яких взятих компонентних булевих функцій f_a та f_b, де $a \neq b, 1 \leq a,b \leq k$ нова функція $f_a \oplus f_b$, що була утворена їхньою суперпозицією, має високу нелінійність та задовольняє суровому лавинному критерію, то S-блок, до складу якого входять ці функції f_a та f_b, вважається таким, що відповідає критерію незалежності бітів.

Тобто, для того, щоб цей критерій виконувався, компонентні булеві функції мають бути незалежними одна від одної, що гарантує, що при зміні одного вхідного біта, у вихідних бітах відбуваються максимально непередбачувані зміни [7].

Ймовірність лінійної апроксимації (LAP) – це критерій, що характеризує ймовірність лінійного наближення виходів S-блоку до заданих комбінацій його входів. Іншими словами, LAP визначає, наскільки легко виходи S-блоку можна передбачити за лінійною комбінацією входів. Чим слабкіший S-блок, тим вищим буде значення LAP, і тим вразливішою буде конструкцію до атак лінійного криптоаналізу. Для обчислення LAP використовується формула

$$LP_S = \frac{\max\limits_{\alpha,\beta\neq 0}(\#\{x \mid 0 \leq x < 2^k, \bigoplus\limits_{s=1}^{k} x[s] \bullet \alpha[s] = \bigoplus\limits_{t=1}^{k} S(x)[t] \bullet \beta[]\}) - 2^{k-1}}{2^k}, \quad (6)$$

де α, β – вхідна ти вихідна послідовності, відповідно, $[s]$ – позначає виділення s-го біта, а символ $\bullet$ позначає логічну операцію «І» («AND») [8].

Ймовірність диференціальної апроксимації (DAP) оцінює ймовірність того, що заданий вхідний диференціал S-блоку призведе до конкретного вихідного диференціалу протягом визначеної кількості раундів. Для її обчислення здійснюється повний перебір усіх можливих комбінацій вхідних і вихідних диференціалів для заданої кількості раундів. Підраховуються випадки появи кожного вихідного диференціалу, а DAP визначається як відношення кількості випадків бажаного вихідного диференціалу до загальної кількості перевірених пар вхідних/вихідних значень.

Чим нижче значення DAP, тим більш стійким є S-блок до диференціального криптоаналізу. DAP обчислюється за наступною формулою

$$DP(\mathrm{D}u, \mathrm{D}v) = \frac{\left|\{u \,\mathrm{O} V_k \mid S(u) \,\mathrm{E}\, S(u \,\mathrm{E}\, \mathrm{D}u) = \mathrm{D}v\}\right|}{2^k}, \quad (7)$$

де $\mathrm{D}u$ та $\mathrm{D}v$ – це вхідні і вихідні диференціали, відповідно.

Кореляційна незалежність вхідних і вихідних векторів S-блоку. Для оцінки даного критерію використовується максимальне значення серед модулів коефіцієнтів кореляції $\max\left\{\left|r_{i,j}\right|\right\}$ кореляційної матриці $R = \left\|r_{i,j}\right\|$, що визначає ступінь лінійного зв'язку між вихідним вектором y та вхідним вектором x. При цьому елементи $r_{i,j}$ кореляційної матриці R визначаються як

$$r_{i,j} = 1 - \frac{\sum\limits_{m=1}^{N}(x_{m,i} \oplus y_{m,j})}{N/2}, i, j = 0, \ldots, k-1, \quad (8)$$

Нижчі показники $\max\left\{\left|r_{i,j}\right|\right\}$ відображають вищий рівень криптографічної якості S-блоку [10].

Подання S-блока у вигляді функцій багатозначної логіки. Як зазначалося раніше, навіть за високих показників якості S-блоку у класичному булевому представленні можливі випадки, коли при розгляді того ж S-блоку у вигляді q-значної

логіки його криптографічні характеристики значно знижуються, іноді на кілька порядків. У таких умовах S-блок залишається вразливим до криптоаналізу, що базується на математичному апараті *q*-логіки.

Визначення 1. Функція *q*-значної логіки від *k* змінних – це відображення виду

$$\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}. \quad (9)$$

Функції багатозначної логіки є більш загальними математичними об'єктами ніж булеві функції. Наприклад, якщо позначити $q=2$, то тоді *Визначення 1* стає визначенням булевої функції.

Таким чином, наприклад, S-блоки з 4 входами, довжини $N=16$ можуть бути представлені чотирма компонентними булевими функціями або двома компонентними 4-функціями (табл. 1).

Таблиця 1.

Представлення S-блоку у вигляді компонентних булевих та 4-функцій

Q	4	7	2	14	1	13	8	11	15	12	6	10	5	9	3	0
f_{20}	0	1	0	0	1	1	0	1	1	0	0	0	1	1	1	0
f_{21}	0	1	1	1	0	0	0	1	1	0	1	1	0	0	1	0
f_{22}	1	1	0	1	0	1	0	0	1	1	1	0	1	0	0	0
f_{23}	0	0	0	1	0	1	1	1	1	1	0	1	0	1	0	0
f_{40}	0	3	2	2	1	1	0	3	3	0	2	2	1	1	3	0
f_{41}	1	1	0	3	0	3	2	2	3	3	1	2	1	2	0	0

Якщо ж брати до уваги S-блоки більш практичної довжини 256, що використовується в багатьох сучасних криптоалгоритмах, то вони можуть бути представлені за допомогою восьми компонентних булевих функцій, чотирьох компонентних 4-функцій або ж двох компонентних 16-функцій [11].

Також у роботі [11] представлено математичний апарат для обчислення SAC для *q*-функцій.

Визначення 2. Вагою $\varpi(u)$ *q*-значного вектору називається число його ненульових компонент.

Визначення 3. Похідна функції f за напрямком вектору u – це функція

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \,(\mathrm{mod}\, q), \quad (10)$$

де $\underset{q}{\oplus}$ означає додавання за модулем *q*.

Визначення 4. Функція *q*-значної логіки $f(x)$ задовольняє критерію поширення помилки $PC(u)$ щодо вектору $u \in V_k$, якщо її похідна у напрямку u є збалансованою функцією, тобто $0,1,...,q-1$ приймаються з однаковими ймовірностями $p(D_u f(x) = i(\mathrm{mod}\, q)) = \frac{1}{q}$ для всіх $i = 0,1,...,q-1$. Іншими словами, $K^0 = K^1 = ... = K^{q-1}$, де K^i – кількість наборів змінних значень, для яких похідна набуває значення *i*. Функція *q*-значної логіки $f(x)$ задовольняє критерію поширення $PC(m)$ степеню *m*, якщо вона задовольняє критерію поширення $PC(u)$ по відношенню до всіх векторів *u* ваги $1 \le \varpi(u) \le m$.

Визначення 5. Функція *q*-значної логіки $f(x)$ задовольняє SAC, якщо вона задовольняє критерію поширення $PC(1)$ степеню 1.

Метод синтезу високоякісних S-блоків на основі недвійкових афінних перетворень. На сьогодні конструкція Ніберг є однією з найпоширеніших у практичній криптографії. Вона використовується у складі широко відомого криптоалгоритму AES і відзначається високою збалансованістю щодо основних критеріїв криптографічної якості, таких як

нелінійність, стійкість до диференціального та лінійного криптоаналізу, а також здатність забезпечувати ефективну реалізацію конфузії та дифузії. Завдяки цим характеристикам S-блоки конструкції Ніберг забезпечують надійний рівень безпеки сучасних симетричних шифрів.

S-блок генерується за допомогою обчислення мультиплікативно зворотної величини в скінченному полі Галуа GF(2^8)

$$y_i = x_1^{-1} \text{modd}(2, G(x)),\ G(x) = x^8 + x^4 + x^3 + x + 1, \quad (11)$$

при цьому прийнято, що 0 співставляється сам з собою. У табл. 2 ми наводимо S-блок, побудований на основі (11).

Таблиця 2.

Мультиплікативна інверсія для усіх 8-бітних чисел у GF(2^8)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	1	141	246	203	82	123	209	232	79	41	192	176	225	229	199
1	116	180	170	75	153	43	96	95	88	63	253	204	255	64	238	178
2	58	110	90	241	85	77	168	201	193	10	152	21	48	68	162	194
3	44	69	146	108	243	57	102	66	242	53	32	111	119	187	89	25
4	29	254	55	103	45	49	245	105	167	100	171	19	84	37	233	9
5	237	92	5	202	76	36	135	191	24	62	34	240	81	236	97	23
6	22	94	175	211	73	166	54	67	244	71	145	223	51	147	33	59
7	121	183	151	133	16	181	186	60	182	112	208	6	161	250	129	130
8	131	126	127	128	150	115	190	86	155	158	149	217	247	2	185	164
9	222	106	50	109	216	138	132	114	42	20	159	136	249	220	137	154
A	251	124	46	195	143	184	101	72	38	200	18	74	206	231	210	98
B	12	224	31	239	17	117	120	113	165	142	118	61	189	188	134	87
C	11	40	47	163	218	212	228	15	169	39	83	4	27	252	172	230
D	122	7	174	99	197	219	226	234	148	139	196	213	157	248	144	107
E	177	13	214	235	198	14	207	173	8	78	215	227	93	80	30	179
F	91	35	56	52	104	70	3	140	221	156	125	160	205	26	65	28

Після обчислення мультиплікативної інверсії стає можливим виконати наступну трансформацію, передбачену конструкцією Ніберг – двійкове афінне перетворення. Цей етап є ключовим для формування необхідних криптографічних властивостей S-блоку, зокрема забезпечення стійкості до диференціального та лінійного аналізу

$$S_i = Ry_i + C \bmod 2, \quad (12)$$

де R – матриця афінного перетворення,

C – вектор-константа,

S_i – вихідні значення блоку AES.

Алгоритм AES пропонує наступну матрицю R і вектор-константу C

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}. \quad (13)$$

У роботі [12] запропоновано новий підхід до побудови криптографічних примітивів, що ґрунтується на використанні афінних перетворень у просторі багатозначної логіки. На відміну від класичного бінарного підходу, застосування q-функцій дозволяє отримати розширене представлення S-блоків та сформувати широкий клас їхніх модифікацій. Запропонований метод забезпечує синтез S-блоків вищої якості, які демонструють покращені криптографічні характеристики та підвищену стійкість до лінійних, диференціальних і кореляційних атак, що безпосередньо сприяє вдосконаленню сучасних симетричних шифрів.

У поєднанні з S-блоками [13], які задовольняють умовам суворого лавинного критерію (SAC) як для компонентних булевих функцій, так і для 4-функцій, ця схема дозволяє створювати S-блоки, що характеризуються високою криптографічною якістю. Згідно з запропонованим методом, афінне перетворення S-блоків виконується наступним чином

$$\alpha_j.S_i = \sum_{u=1}^{n} \alpha_j \times y_i R'(j,u) + C \bmod 4, \tag{14}$$

де позначення $\alpha_j.S_i$ означає взяття j-ї четвіркової цифри i-го елемента S-блока, тоді як позначення $R'(j,k)$ означає вилучення елемента з індексами (j,k) з матриці R', а $\times$ означає множення в полі Галуа $GF(4)$. В якості матриць R' використовуються модифіковані конструкції $C_{4,2}, C_{4,3}, C_{4,4}$

$$C_{4,21} = \begin{pmatrix} x & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,22} = \begin{pmatrix} 0 & 0 & 0 & x_1 \\ x & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,23} = \begin{pmatrix} 0 & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ x & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,24} = \begin{pmatrix} 0 & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ x & 0 & 0 & 0 \end{pmatrix};$$

$$C_{4,31} = \begin{pmatrix} x & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,32} = \begin{pmatrix} 0 & x_1 & 0 & 0 \\ x & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,33} = \begin{pmatrix} 0 & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ x & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,34} = \begin{pmatrix} 0 & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ x & 0 & 0 & 0 \end{pmatrix}; \tag{14}$$

$$C_{4,41} = \begin{pmatrix} x & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,42} = \begin{pmatrix} 0 & 0 & x_1 & 0 \\ x & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,43} = \begin{pmatrix} 0 & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ x & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,44} = \begin{pmatrix} 0 & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ x & 0 & 0 & 0 \end{pmatrix}.$$

У виразі (14) x – це константне значення, що може одночасно набувати значення 1, 2, 3 для всіх x, а x_1 – це змінні, що які утворюють усі можливі комбінації чисел 1, 2 та 3.

Наслідком такого розмаїття є те, що з одного базового S-блоку можна синтезувати 7776 нових, так званих «дочірніх» конструкцій. Використовуючи різні перестановки, комбінації або модифікації вихідної матриці, можна генерувати великі множини унікальних, але споріднених S-блоків. Важливо, що серед отриманих конструкцій існують S-блоки з вищими криптографічними характеристиками, що забезпечує можливість створення сімейств шифрів або динамічної генерації примітивів з підвищеною стійкістю.

Це відкриває шлях до формування нових S-блоків, подібних до наведеного у табл. 3, кожен з яких може мати унікальні властивості, необхідні для конкретного криптографічного застосунку.

Таблиця 3.

S-блок конструкції Ніберг створений за допомогою афінного перетворення на базі 4-логіки

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	15	6	47	128	178	210	121	131	245	166	107	93	29	216	104	244
1	46	59	164	43	198	81	167	150	190	115	73	221	192	112	220	9
2	19	188	51	58	69	191	142	238	87	97	201	154	84	200	33	228
3	152	23	18	7	155	170	250	109	117	225	130	79	224	53	252	76
4	135	173	194	141	83	56	193	243	231	41	28	116	90	42	118	156
5	185	230	169	175	16	229	215	71	49	8	92	255	50	94	136	66
6	254	177	187	145	253	207	111	4	32	72	219	21	74	160	102	22
7	149	147	133	218	235	123	44	217	96	195	13	52	180	126	14	98
8	236	67	204	197	186	64	113	17	168	158	54	101	171	55	222	27
9	103	232	237	248	100	85	5	146	138	30	125	176	31	202	3	179
A	240	249	208	127	77	45	134	124	10	89	148	162	226	39	151	11
B	209	196	91	212	57	174	88	105	65	140	182	34	63	143	35	246
C	1	78	68	110	2	48	144	251	223	183	36	234	181	95	153	233
D	106	108	122	37	20	132	211	38	159	60	242	203	75	129	241	157
E	120	82	61	114	172	199	62	12	24	214	227	139	165	213	137	99
F	70	25	86	80	239	26	40	184	206	247	163	0	205	161	119	189

Імплементація та оцінка стійкості сучасних шифрів із високоякісними S-блоками. Для оцінки криптографічних якостей S-блоків, синтезованих у [12] було використано наступні блокові симетричні шифри: AES, Camelia, SM-4, Kalyna та ARIA.

AES. Це симетричний блоковий шифр, що набув широкого застосування, що працює з блоками фіксованого розміру і підтримує три довжини ключа: 128, 192 та 256. Завдяки своїй високій швидкості та стійкості, AES став міжнародно визнаним алгоритмом і широко використовується у різних сферах, включаючи Wi-Fi, VPN та навіть апаратно підтримується у багатьох сучасних пристроях [14].

Camelia. Шифр, що був розроблений спільно японськими компаніями Mitsubishi та NTT. Як і AES підтримує три довжини блоку: 128, 192 та 256. Ключова особливість – це використання додаткових FL-функцій, що застосовуються кожні 6 раундів для підвищення криптографічної стійкості. Фактично, Camelia була визнана міжнародними стандартами ISO/IEC і стала досить популярною в Японії, фактично є одним з японських стандартів [15].

Калина. Український стандарт, що набув чинності у 2014 році. Він підтримує довжину блоку і ключа від 128 біт до 512 біт, а також має високий рівень криптографічної стійкості з достатнім запасом у разі винайдення або створення нових атак протягом тривалого часу. Також, на відміну від AES, в нього значно збільшена кількість циклів шифрування, а також застосована принципово нова схема створення підключів [16].

SM-4. Китайський стандарт шифрування, що оперує блоками даних розміром 128 біт і використовує ключ відповідної довжини. Для шифрування він використовує 32 раунди з операціями XOR, використанням S-блоків та циклічних зсувів [17].

ARIA. Південно-корейський стандарт, що був затверджений у 2004 році. Для шифрування використовує блоки розмірів від 128 біт до 256 біт. Як і AES, ARIA створена на базі SP-мережі (підстановочно-перестановочної мережі), що включає у себе декілька раундів [18].

Для початку експерименту було проведено початкову оцінку S-блоків, що входять до складу наведених криптоалгоритмів та цільових S-блоків з [12], що будуть використовуватись у якості альтернативи (табл. 4).

Таблиця 4.

Порівняння криптографічних властивостей S-блоків провідних криптографічних стандартів

S-box	Nonlinearity	SAC	BIC Nonlinearity	BIC SAC	LAP	DAP	$\max\left\{\left\|r_{i,j}\right\|\right\}$	SAC of component 4-functions
AES	112	0.5032	112	0.5057	0.0625	0.0156	0.125	0.6484
Camelia	112	0.5469	112	0.5033	0.0625	0.0156	0.1094	0.6563
	112	0.5469	112	0.5033	0.0625	0.0156	0.1094	0.6172
	112	0.5469	112	0.5033	0.0625	0.0156	0.1094	0.6172
	112	0.5469	112	0.5033	0.0625	0.0156	0.1094	0.6172
Калина	104	0.5625	106.6429	0.5015	0.0938	0.0313	0.1563	0.6094
	104	0.5938	106.8571	0.5024	0.0938	0.0313	0.1719	0.6250
	104	0.6094	107.0714	0.6250	0.0938	0.0313	0.1563	0.6250
	104	0.5781	107.0714	0.5024	0.0938	0.0313	0.1563	0.6254
ARIA	112	0.5625	112	0.5046	0.0625	0.0156	0.125	0.6016
	112	0.5625	112	0.5030	0.0625	0.0156	0.0938	0.5781
SM-4	112	0.5625	112	0.5049	0.0625	0.0156	0.125	0.6484
Affine S-boxes[13]	96	0.5	77.7143	0.4799	0.5	1	0	0.5
	96	0.5	77.7143	0.5045	0.5	1	0	0.5
	96	0.5	77.7143	0.5022	0.5	1	0	0.5
	96	0.5	77.7143	0.4799	0.5	1	0	0.5

Як видно з табл. 4, вихідні S-блоки провідних криптоалгоритмів демонструють високі криптографічні характеристики, що й обумовлює їхню популярність і широке застосування. Проте для оцінки ефективності нових конструкцій було перевірено,

наскільки якіснішими стають криптоалгоритми після заміни оригінальних S-блоків на синтезовані у [12]. Для оцінки ефективності застосовувалися стандартні стохастичні тести NIST (NIST Statistical Test Suite), які широко використовуються для перевірки криптографічних алгоритмів та генераторів випадкових послідовностей. Ці тести дозволяють визначити, наскільки вихідні дані після шифрування відповідають властивостям випадковості, що безпосередньо пов'язано з рівнем криптографічної стійкості. Іншими словами, якщо зашифровані дані демонструють статистичні властивості випадкових послідовностей, алгоритм вважається більш стійким до криптоаналітичних атак.

Таблиця 5.

Порівняння ефективності оригінальних та модифікованих криптоалгоритмів

Криптоалгоритм	Пройдено тестів (Оригінал)	Пройдено тестів (Модифікація)
AES	94	96
ARIA	95	96
Kalyna	99	99
SM4	94	97
Camelia	92	99

Відповідно до результатів, наведених у табл. 5, S-блоки, синтезовані у [12], демонструють високий рівень криптографічних характеристик у різних обчислювальних системах. Хоча в булевому сенсі їх показники можуть бути дещо нижчими порівняно з окремими альтернативними S-блоками, їх впровадження суттєво підвищує загальну криптографічну стійкість алгоритмів. Це свідчить про те, що дані S-блоки є ефективним інструментом для оптимізації існуючих криптографічних конструкцій, а також можуть бути рекомендовані для розробки нових стійких криптоалгоритмів.

Висновки. Результати дослідження показали, що інтеграція синтезованих високоякісних S-блоків забезпечує потрійний ефект: високу якість у традиційних метриках булевих функцій, значні характеристики у метриках функцій багатозначної логіки та практичне підвищення криптографічної стійкості алгоритмів при їх вбудовуванні, що раніше залишалося проблемою навіть для провідних світових стандартів.

Отримані результати підтверджують, що навіть за умов, коли синтезовані примітиви мають дещо нижчі показники у класичному булевому сенсі, комплексна збалансованість їх криптографічних властивостей у кількох системах представлення забезпечує підвищену криптографічну якість шифру в цілому. Це безпосередньо відобразилося на результатах стохастичних тестів NIST: у більшості випадків модифіковані алгоритми перевищили оригінальні за кількістю успішно пройдених тестів, демонструючи більшу випадковість та непередбачуваність шифрованих даних.

Таким чином, дослідження доводить перспективність розробленого підходу для побудови нового покоління симетричних шифрів. Синтезовані S-блоки можуть стати основою динамічних криптографічних примітивів, що дозволяють створювати адаптивні та самозахисні криптосистеми, стійкі до широкого спектра атак, включно з тими, що ґрунтуються на функціях багатозначної логіки.

У практичному вимірі це означає можливість створення більш захищених протоколів комунікації, стійких до квантових атак, а також криптографічних рішень для IoT, хмарних сервісів та критичної інфраструктури, де вимоги до інформаційної безпеки зростають у геометричній прогресії.

Отже, результати цієї роботи не лише підсумовують успішність запропонованого методу, а й відкривають шлях до формування нового напряму розвитку сучасної симетричної криптографії, заснованого на синтезі примітивів із стійкістю у сенсі функцій багатозначної логіки.

Список літератури

1. Hussain U. A Comparative Survey of Symmetric and Asymmetric Key Cryptography Algorithms. *2nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology*. *Khairpur*. 2024. P. 257-262.
2. Thakor V. A., Razzaque M. A., Khandaker M. R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*. 2021. Vol. 9. P. 28177–28193. doi: 10.1109/access.2021.3052867
3. Sokolov A., Kazakova N., Kuzmenko L., Mahomedova M. Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions. *CEUR Workshop Proceedings*. 2021. 2923. P. 107-116. URL: https://ceur-ws.org/Vol-2923/paper12.pdf
4. Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non binary ciphers. International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2007. P. 184-211.
5. Zahid A. H. et al. Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications. *IEEE Access*. 2021. Vol. 9. P. 98460-98475. DOI: 10.1109/access.2021.3095618
6. Banga A. ChessCrypt: enhancing wireless communication security in smart cities through dynamically generated S-Box with chess-based nonlinearity. *Scientific Reports*. 2024. Vol. 14, No. 1. P. 1-25. DOI: 10.1038/s41598-024-77927-0
7. Jamal S. S. Secure S-box construction with 1D chaotic maps and finite field theory for block cipher encryption. *Alexandria Engineering Journal*. 2025. Vol. 125. P. 278–296. DOI: 10.1016/j.aej.2025.03.109
8. Kazakova N. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. *Procedia Computer Science*. 2021. Vol. 192. P. 2731-2741. DOI: 10.1016/j.procs.2021.09.043
9. Farah M. A. B., Farah A., Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*. 2019. Vol. 99, No. 1. P. 1-24. DOI: 10.1007/s11071-019-05413-8
10. Sokolov A.V., Zhdanov O.N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. *International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, Springer, Cham*. 2018. P. 331-339. DOI: 10.1007/978-3-319-91008-6_33
11. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. Vol. 26. Is. 2. P. 1-12. DOI: 10.1080/09720529.2021.1964727
12. Karpinski M.. Development of High-Quality Cryptographic Constructions Based on Many-Valued Logic Affine Transformations. *Electronics.* 2025. Vol. 14, No. 10. P. 1-22. DOI: 10.3390/electronics14102094
13. Sokolov A.V., Radush V.V. The method for synthesis of high-quality S-boxes based on many-valued logic functions. *Informatics and mathematical methods in simulation*. 2022. Vol. 12, No. 3. P. 219-225. DOI: 10.15276/imms.v12.no3.219
14. Jang K. Quantum Analysis of AES / IACR Communications in Cryptology. 2025. Vol. 2, No. 1. P. 1-57. DOI: 10.62056/ay11zo-3y
15. The Camellia Cipher. Security and So Many Things. URL: https://asecuritysite.com/blog/2023-11-18_The-Camellia-Cipher-44d2d044de4d.html.
16. Єфіменко А. А., Байлюк Є. М., Покотило О. А. Порівняльний аналіз алгоритму симетричного блокового перетворення «Калина» (ДСТУ 7624:2014) з іншими міжнародними стандартами шифрування даних. *Збірник наукових праць ЖВІ*. 2018. № 15. С. 156-162.

17. Бондаренко О., Філобок Є., Козіна Г. Реалізація алгоритму блочного шифрування SM4. інформаційні технології: теорія і практика. *ІІІ Всеукр. науково-практ. Інтернет-конф. здобувачів вищ. освіти і молодих уч.* 2025 р. С. 36-37.
18. RFC 5794: A Description of the ARIA Encryption Algorithm. RFC Editor. URL: https://www.rfc-editor.org/rfc/rfc5794.html.

IMPROVING THE RESISTANCE OF MODERN BLOCK CIPHERS USING HIGH-QUALITY S-BOXES

V.V. Radush

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: radush9860@gmail.com

Ensuring a high level of cryptographic stability of modern symmetric ciphers directly depends on the quality of the S-boxes used in them. Traditionally, the analysis of S-boxes is limited to the apparatus of Boolean functions; however, recent research shows that under the conditions of attacks based on many-valued logic, some standard S-boxes may demonstrate an insufficient level of cryptographic stability. This creates the need for a comprehensive assessment of such cryptographic primitives to ensure their quality in both Boolean and many-valued representations. An experimental evaluation of the quality of S-boxes used in modern symmetric block ciphers was performed, with an emphasis on practical efficiency in real encryption and assessment of stochastic properties of the cryptogram. In order to strengthen the cryptographic characteristics of the ciphers, instead of the original substitutions, the author's S-boxes were used, built based on non-binary affine transformations, which demonstrate high cryptographic properties when represented by both Boolean functions and many-valued logic functions. The methodology included two complementary stages: calculation of key S-box quality metrics – nonlinearity, fulfillment of the strict avalanche criterion (SAC), bit independence criterion (BIC), linear (LAP) and differential (DAP) approximation probability; practical verification by encrypting information arrays with modified ciphers and subsequent statistical analysis of the original cryptograms using NIST tests. The research covered AES, Camellia, Kalyna, SM4, and ARIA cryptographic algorithms. The calculated indicators, together with stochastic verification, showed that S-boxes based on quaternary affine transformations provide increased balance and stability. In most cases, the modified versions of the ciphers outperformed the originals in the number of NIST tests passed (in particular, AES, ARIA, SM4, Camellia), which indicates an increase in the randomness and cryptographic resistance of the original sequences. It is important to emphasize the experimental nature of the research: a comparative and practical verification of S-boxes based on affine transformations was performed. The obtained data indicate the prospects for further integration of such primitives into communication protocols, protection of IoT devices, cloud services, and critical infrastructure, where the requirements for randomness and stability are particularly high. The combination of theoretical quality criteria and practical verification of cryptograms allows us to speak of a reliable methodological basis for making decisions on the implementation of such S-boxes in real systems.

Keywords: cryptographic primitives; block ciphers; S-boxes; affine transformations; many-valued logic; nonlinearity; avalanche criterion; NIST Statistical Test Suite; cryptanalysis; cryptogram randomness.