2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.3

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПОБУДОВИ ТА ВЛАСТИВОСТЕЙ S-БЛОКІВ РЯДУ СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Леонід Скрипник, Олександр Дирда*

*Спеціальний факультет СБ України НТУУ "КПІ", *ДСТСЗІ СБ України*

Анотація: **Розглянуто методи побудови та властивості збалансованих булевих відображень (S-блоків) нелінійних вузлів ускладнення сучасних криптографічних алгоритмів. Проведено порівняльний аналіз властивостей S-блоків криптографічних алгоритмів Rijndael, Skipjack, Whirlpool, Twofish, Crypton, Snow, E2, Square, Safer+, Торнадо та інших. Наведено приклад трьох 8×8 S-блоків, в яких координатні функції мають високі показники нелінійності, задовольняють "суворому лавинному критерію" та властивості кореляційної імунності першого порядку.**

Summary: **The construction methods and properties of balanced Boolean mappings (S-boxes) to be used in cryptographic transformations of up-to-date cryptographic algorithms are considered.The comparative analysis of properties of S-boxes to be used in Rijndael, Skipjack, Whirpool, Twolish, Crypton, Snow, E2, Square, Safer+, Tornado and others cryptographic algorithms is presented. An example of 8x8 S-boxes, that have high nonlinearity and meet to strict avalanche criterion and correlation immunity of first degree is given.**

Ключові слова: **Криптографічний алгоритм, нелінійний вузол ускладнення, S-блок, координатні функції.**

Вступ

Сучасні симетричні криптографічні алгоритмі, зокрема, блокові шифри, як правило, є складовими шифрами, тобто являють собою композицію простих перетворень, кожне з яких дає свій внесок у сумарне "розсіювання" та "перемішування". Такий підхід до побудови шифрів був запропонований К. Шенноном ще у середині минулого століття [1].

Одним з простих перетворень, яке використовується під час синтезу сучасних складових шифрів і забезпечує "розсіювання" та „перемішування", є $n \times m$ S-блок, який є функцією $S: V_n \to V_m$, де $n \geq m$, а V_k – лінійний простір бітових векторів довжини k [1]. S-блок розміру $n \times m$ може бути поданий як система з m двійкових (булевих) функцій від n змінних кожна, тобто, $S = (f_1, f_2, ..., f_m)$, де $f_j : V_n \to \{0,1\}$, $j = \overline{1,m}$. Функції f_j носять назву координатних функцій.

В криптографічних алгоритмах, як правило, використовуються $n \times m$ S-блоки, які реалізують збалансовані булеві відображення, для яких $\forall\, v \in V_m \quad \left|\{u \in V_n | S(u) = v\}\right| = 2^{n-m}$. Очевидно, що всі координатні функції таких S-блоків є збалансованими (рівноймовірними) двійковими функціями, тобто, $\left\|f_j\right\| = 2^{n-1}$, $j = \overline{1,m}$. Збалансоване булеве відображення при $n = m$ реалізує бієктивну (взаємно-однозначну) функцію, отже, S-блок реалізує підстановку на множині $\{0, 1, ..., 2^n - 1\}$.

Від властивостей S-блоків суттєво залежить криптографічна стійкість складових шифрів, що диктує необхідність синтезу S-блоків, які є усталеними відносно сучасних методів криптографічного аналізу.

В сучасних криптографічних алгоритмах S-блоки, як правило, є фіксованими, тобто, не залежать від ключа. Винятком з правила є лише декілька шифрів, зокрема, ГОСТ 28147-89, RC4, Blowfish. Такий підхід дозволяє під час синтезу шифрів будувати S-блоки з певними криптографічними властивостями.

Під час побудови S-блоків для криптографічних алгоритмів, як правило, враховують наступні параметри [1, 2]:

- ✓ нелінійність координатних функцій, яка визначається як відстань до класу афінних функцій;
- ✓ нелінійність підстановки, яка визначається як відстань до класу афінних функцій для будь-якої нетривіальної лінійної комбінації координатних функцій;
- ✓ кількість одиничних циклів у цикловій структурі підстановки;
- ✓ порядок кореляційного імунітету координатних функцій;
- ✓ степінь нелінійності координатних функцій;
- ✓ кількість термів у алгебраїчній нормальній формі координатних функцій;
- ✓ максимальне значення в таблиці диференційних різниць підстановки.

Варто зауважити, що розробка вимог до S-блоків є складною математичною задачею [1]. Це пояснюється тим, що деякі параметри двійкових функцій є суперечливими, тобто, збільшення одного параметру призводить до зменшення іншого. Як приклад, при збільшенні порядку кореляційної імунності двійкової функції зменшується її степінь нелінійності. Таким чином, під час синтезу S-блоку необхідно вибрати деякий компроміс між різними параметрами.

На криптографічну стійкість шифрів впливає розмір S-блоків. У загальному випадку, чим більше параметри n та m S-блоків, тим складніше знайти статистичні відхилення, які необхідні для використання методів криптографічного аналізу [1]. "Великі" *S*-блоки є більш стійкими до методів диференційного та лінійного криптографічного аналізу, однак, потребують більше пам'яті для їх зберігання. S-блоки розміру 4 × 4 використовуються в криптоалгоритмах Lucifer, ГОСТ 28147-89, Serpent, SC2000; 5 × 5 і 6 × 6 – в SC2000; 6 × 4 – в DES; 7 × 7 і 9 × 9 – в MISTY1; 12 × 8 – в LOKI; 16 × 16 – в IDEA; 8 × 32 – в MARS, Blowfish, CAST, Khufu, Khafre, Sober-t32; 8 × 64 – в Tiger; 8 × 8 – в Skipjack, Rijndael, Snow, Square, Shark, Treyfer, Twofish, RC2, RC4, MD2, Anubis, E2, DESX, Camellia, Crypton, CS, Khazad, Q, Safer+, Whirlpool, Magenta, Hierocrypt-3, Turing, Scream, HBB, Squafer, BelT тощо.

Залежно від того, які параметри визначаються приоритетними, різняться методи побудови S-блоків.

Одним з методів синтезу S-блоків є "випадковий" вибір підстановок без перевірки будь-яких додаткових умов. S-блоки, згенеровані цим методом, не є оптимізованими відносно методів лінійного та диференційного криптографічного аналізу. Як приклад, такий метод синтезу S-блоків використовується у блоковому шифрі Khafre, при цьому використовуються таблиці випадкових чисел. У блоковому шифрі RC2 S-блок згенеровано з використанням числа $\pi = 3.14159...$

Для ряду шифрів S-блоки генеруються з використанням датчика випадкових або псевдовипадкових чисел, при цьому вибираються підстановки, що задовольняють певним умовам, які вибираються таким чином, щоб протистояти відомим методам лінійного та диференційного криптоаналізу. Прикладом підстановки, згенерованої саме цим методом, є S-блок геш-функції Whirlpool. При синтезі підстановки здійснювалась перевірка наступних умов:

– $\left|\{x \in V_8 \mid S(x) = x\}\right| = 0$, що означає відсутність в підстановці циклів одиничної довжини (нерухомих елементів);

– $\forall x \in V_8 \ \left|\{y \in V_8 \mid S(y) \oplus y = S(x) \oplus x\}\right| \le 2$.

Для деяких шифрів S-блоки будуються на основі *S*-блоків меншої розмірності. Прикладом є 8×8 *S*-блок шифру Crypton, який побудовано на основі двох S-блоків розміру 4×4.

Для ряду шифрів S-блоки будуються конструктивно з використанням детермінованого алгоритму. Прикладом є шифри Rijndael, Square, Shark, Camellia, Q, Торнадо. Для цих шифрів S-блок є композицією операції обчислення зворотного елемента у скінченному полі Галуа $GF(2^8)$ і аффінного перетворення. У шифрі Rijndael утворюючим поліномом поля $GF(2^8)$ є поліном $x^8 + x^4 + x^3 + x + 1$, а в афінному перетворенні $Ax \oplus b$ використовуються циркулянтна матриця A, яка визначається вектором (10001111), а також вектор $b = (11000110)$ [4]. У шифрі Hierocrypt використовується композиція бітової перестановки $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 8 & 6 & 2 & 4 & 1 \end{pmatrix}$, операції піднесення у 247 степінь у полі $GF(2^8)$, а також операції додавання з числом 7. Утворюючим поліномом поля є поліном $x^8 + x^6 + x^5 + x + 1$ [3]. Для потокового шифру Snow використовується операція $x^7 + \gamma$ у полі $GF(2^8)$, де $\gamma = x^4 + x^2 + 1$ – фіксований

поліном. Утворюючим поліномом поля є поліном $x^8 + x^5 + x^3 + x + 1$. В алгоритмі Safer+ підстановка будується на основі піднесення до степеня у мультипликативній групі $F^*_{2^8+1}$, в алгоритмі IDEA – на основі аналогічної операції у групі $F^*_{2^{16}+1}$ [6].

Залежно від вибору підхода, який застосовується під час синтезу підстановки, різняться властивості підстановок. Зокрема, підстановки, які будуються на основі детермінованого алгоритму, як правило, мають високи показники нелінійності.

Основна частина

У статті розглядаються властивості *S*-блоків криптографічних алгоритмів Rijndael, Skipjack, Whirlpool, Twofish, Crypton, Snow, E2, Square, Safer+, MD2, RC2, Camellia, Q, CS, Anubis, Hierocrypt-3, Turing, Торнадо, BelT, DESX. Для зручності подання порівняльних характеристик вибрані ті алгоритми, в яких використовуються *S*-блоки однієї розмірності, а саме, 8 × 8.

Серед зазначених алгоритмів шифри Rijndael, Twofish, Crypton, E2, Square, Safer+ розглядались у проекті створення Advanced Encryption Standard (AES), алгоритми Whirlpool, Camellia, Snow, Q, CS, Anubis, Hierocrypt-3 – у проекті New European Schemes for Signatures, Integrity, and Encryption (NESSIE). Алгоритм Skipjack розроблено Агенцією національної безпеки США, блоковий шифр "Торнадо" розроблено АТ "Інститут інформаційних технологій" (м. Харків), блоковий шифр "BelT" розроблено Національним науково-дослідним центром прикладних проблем математики і інформатики Білоруського державного університету та Державним центром безпеки інформації при Президенті Республіки Білорусь. Особливий інтерес викликають алгоритми Rijndael та Skipjack, які є діючими стандартами FIPS 197 та FIPS 185 відповідно.

Зауваження. В алгоритмах Square, Camellia, Q, Торнадо використовується декілька *S*-блоків. Для проведення досліджень вибрано один з них.

У табл. 1 наведені країни, в яких розроблялись криптоалгоритми, а також тип алгоритму.

Таблиця 1

Алгоритм	Країна	Тип алгоритму	Алгоритм	Країна	Тип алгоритму
Rijndael	*Бельгія*	Блоковий шифр	Turing	*Австралія*	Потоковий шифр
Skipjack	*США*	Блоковий шифр	RC2	*США*	Блоковий шифр
Whirlpool	*Бельгія,Бразилія*	Геш-функція	Hierocrypt-3	*Японія*	Блоковий шифр
Twofish	*США*	Блоковий шифр	Camellia	*Японія*	Блоковий шифр
Crypton	*Південна Корея*	Блоковий шифр	Q	*США*	Блоковий шифр
Snow	*Швеція*	Потоковий шифр	CS	*Франція*	Блоковий шифр
E2	*Японія*	Блоковий шифр	Anubis	*Бельгія, Бразилія*	Блоковий шифр
Square	*Бельгія*	Блоковий шифр	Торнадо	*Україна*	Блоковий шифр
Safer+	*США*	Блоковий шифр	BelT	*Білорусія*	Блоковий шифр
MD2	*США*	Геш-функція	DESX	*США*	Блоковий шифр

Не рідким є випадок, коли одні й тіж S-блоки використовуються в декількох шифрах. Наприклад, підстановка шифру Anubis використана у шифрі Khazad, підстановка шифру Square – у шифрі Shark, підстановка шифру Skipjack – у шифрі Sober-t16, підстановка шифру Rijndael – у шифрах Scream, HBB, Squafer.

Надалі розглядаються ряд параметрів координатних функцій та S-блоків.

У табл. 2 наведена порівняльна характеристика нелінійності S-блоків за параметрами:

- ✓ $n_1, n_2, ..., n_8$ – нелінійність координатних функцій (відстань до класу аффінних функцій), $n_j = N(f_j),\ j = \overline{1,8}$, де $N(f) = \min_{l \in A_n} \|f \oplus l\|$, A_n – клас афінних функцій від n змінних, $\|f\|$ – вага Хемінга функції f;
- ✓ N – нелінійність підстановки, яка визначається як мінімальна нелінійність нетривіальних лінійних комбінацій координатних функцій S-блоку, $N = N(S) = \min_{a \in V_n \setminus 0,\ b \in \{0,1\}} N(a_1 f_1 \oplus ... \oplus a_n f_n \oplus b)$ [10];
- ✓ λ – максимальна за модулем кореляція між лінійними функціями і нетривіальними лінійними

комбінаціями координатних функцій S-блоку.

Кореляція між двійковими функціями f та g визначається за формулою

$$c(f,g)=\frac{\left|\{x\in V_n \mid f(x)=g(x)\}\right|}{2^{n-1}}-1=1-\frac{\|f\oplus g\|}{2^{n-1}}.$$

Параметр λ пов'язаний з параметром N співвідношенням $\lambda=1-\frac{N}{2^{n-1}}$.

Таблиця 2

Алгоритм	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	N	Λ
Rijndael	112	112	112	112	112	112	112	112	112	0.125
Crypton	96	96	96	96	96	104	104	96	96	0.25
E2	112	112	108	108	106	108	104	110	100	0.21875
MD2	102	106	106	102	102	100	104	104	90	0.296875
RC2	102	104	104	102	102	100	106	98	94	0.265625
Safer+	100	108	102	100	100	98	102	94	82	0.359375
Skipjack	104	104	108	108	108	104	104	106	100	0.21875
Snow	96	96	96	96	96	96	96	96	96	0.25
Square	112	112	112	112	112	112	112	112	112	0.125
Twofish	104	100	100	100	104	96	104	104	96	0.25
Whirlpool	106	102	108	102	104	100	108	102	96	0.25
Торнадо	112	112	112	112	112	112	112	112	112	0.125
Camellia	112	112	112	112	112	112	112	112	112	0.125
Q	112	112	112	112	112	112	112	112	112	0.125
CS	96	112	96	96	96	96	96	96	96	0.25
Anubis	106	106	104	104	106	108	104	96	94	0.265625
Hierocrypt-3	112	112	112	112	112	112	112	112	112	0.125
Turing	104	106	108	104	104	104	106	104	94	0.265625
BelT	108	108	106	108	104	106	106	106	102	0.203125
DESX	100	106	98	106	104	108	102	102	92	0.28125

За параметрами нелінійності N та, відповідно, λ найгірший показник має S-блок шифру Safer+.

Високі показники нелінійності мають S-блоки шифрів Rijndael, Camellia, Square, Торнадо, Camellia, Q, Hierocrypt-3. Це пояснюється тим, що такі показники мають операції x^{-1} та x^{247} у скінченному полі Галуа $GF(2^8)$ [7]. Досить високі показники нелінійності мають координатні функції і S-блок взагалі шифрів Skipjack та BelT. Алгоритм, за яким було згенеровано S-блок криптоалгоритму Skipjack, не опубліковано, однак, можливо зробити висновок, що саме показники нелінійності були обрані приорітетними параметрами під час синтезу S-блоку цього шифру. Таблиці істинності координатних функцій S-блоку шифру BelT вибирались як певні відрізки довжини 255 лінійної рекурентної послідовності (ЛРП) з примітивним мінімальним поліномом $x^8+x^6+x^5+x^2+1$ над скінченним полем Галуа $GF(2)$, при цьому у фіксовану позицію ЛРП вставлявся 0. Показники нелінійності S-блоку шифру BelT є найкращими серед „псевдовипадкових" S-блоків, при синтезі яких не використовувались операції обчислення зворотного елемента у скінченному полі Галуа $GF(2^8)$.

У табл. 3 наведена емпірічна оцінка ймовірності показника нелінійності для збалансованих двійкових функцій, а на рис. 1 – гістограма цього показника.

Таблиця 3

N(f)	***p***	***N(f)***	***p***	***N(f)***	***p***
78	2e-07	90	0.0005874	102	0.201442
80	2e-07	92	0.001924	104	0.298348
82	1.4e-06	94	0.0058106	106	0.252922
84	1.4e-05	96	0.0164342	108	0.0750068
86	4.62e-05	98	0.0429566	110	0.0032184
88	0.0001722	100	0.101113	112	2.6e-06

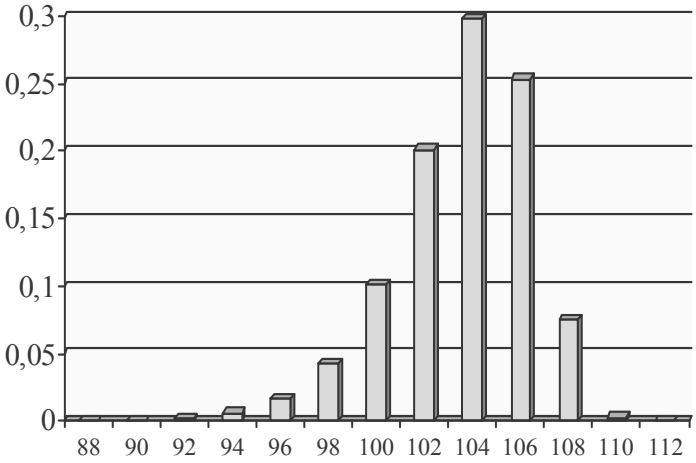

Рисунок 1 – Імовірність нелінійності для збалансованих двійкових функцій від 8 змінних.

Імовірність того, що нелінійність збалансованої двійкової функції не нижче 100, дорівнює ≈ 0.93. Імовірність того, що $n_j \geq 100$, $j = \overline{1,8}$ при "випадковій" генерації *S*-блоку дорівнює ≈ 0.56.

З використанням алгоритму послідовного спрямованого перебору координатних функцій можливо побудувати S-блок, усі координатні функції якого будуть мати високі показники нелінійності. Приклад такого S-блоку наведено нижче.

```
20 1e d0 e5 a5 19 6e bb 5e cf 1b a7 4d 11 dc 25
36 c2 d2 97 18 e6 0c 5a 85 99 df dd 32 d9 d8 06
d7 3b 76 e4 f3 1a e7 22 bf c5 8e 61 33 57 84 5d
52 58 a2 b3 45 98 bc cc 3c c7 ef cd 26 4b b2 5c
42 9a eb 67 de b4 e9 4c ee b8 e2 c0 fb 6f da 40
e1 c8 6a 09 38 02 72 bd 5f 3f 39 05 16 4f fa 8c
a8 8d fc 78 ff 73 37 92 f6 9b 1d 90 47 d6 a1 e0
d1 64 6b 7a f2 af 23 10 56 f5 4e 80 a3 b9 d5 b5
9c 87 1f 60 24 ac b6 b7 34 d4 6d 63 35 a0 86 48
ce ba 68 3d e3 ea 1c 9e 43 89 e8 96 83 74 8a 2b
69 03 44 f0 c3 93 2a b0 08 95 2c 51 0a 54 f8 0f
00 94 2e 30 21 49 41 53 7f 29 82 f9 70 75 ad 15
91 77 ca 31 a4 f1 f7 8f 17 fe c1 7b 5b 0e 79 9f
2d be 71 ab f4 c6 55 ed 3e 6c a6 65 c4 50 7c cb
a9 62 46 0b 12 c9 d3 27 ae aa 28 7e 66 14 2f 3a
7d ec 59 9d 4a 81 88 07 0d b1 fd db 13 8b 04 01
```

Для цього *S*-блоку $n_j = 112$, $j = \overline{1,8}$, $N = 98$, $\lambda = 0.234375$.

У табл. 4 наведена порівняльна характеристика властивостей S-блоків за наступними параметрами:

- ✓ $d_1, d_2, ..., d_8$ – степінь нелінійності координатних функцій;
- ✓ ν – степінь нелінійності S-блоку – мінімальна степінь нелінійності функцій, які є нетривіальними

лінійними комбінаціями координатних функцій;

- ✓ $e = \left|\{x \in V_n \mid S(x) = x\}\right|$ – кількість одиничних циклів в підстановці;
- ✓ $t = \max\limits_{x \in V_n} \left|\{y \in V_n \mid S(y) \oplus y = S(x) \oplus x\}\right|$;
- ✓ $c = \left|0.5 - \max\limits_{i,j=\overline{1,n}} c_{ij}\right|$ – максимальне відхилення від 0.5 для корреляційних коефіцієнтів підстановки, де

$c_{ij} = p\left(x_i = 1 \Big/ f_j = 1\right)$ – кореляційний коефіцієнт між j -м «виходом» та i -м «входом» S -блоку.

Таблиця 4

Алгоритм	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	v	e	t	c
Rijndael	7	7	7	7	7	7	7	7	7	0	4	0.063
Crypton	5	5	5	5	5	5	5	5	5	1	6	0.125
E2	7	7	7	7	7	7	7	7	6	0	5	0.055
MD2	7	7	7	7	7	7	7	7	6	0	5	0.063
RC2	7	7	7	7	7	7	7	7	6	0	5	0.102
Safer+	6	6	7	7	7	7	7	7	6	3	4	0.094
Skipjack	7	7	7	6	7	7	7	7	6	0	5	0.063
Snow	3	3	3	3	3	3	3	3	3	3	4	0.063
Square	7	7	7	7	7	7	7	7	7	2	5	0.055
Twofish	6	6	6	6	6	6	6	6	6	1	4	0.094
Whirlpool	7	7	7	7	7	7	7	7	7	0	2	0.102
Торнадо	7	7	7	7	7	7	7	7	7	0	4	0.047
Camellia	7	7	7	7	7	7	7	7	7	0	4	0.055
Q	7	7	7	7	7	7	7	7	7	0	4	0.047
CS	5	5	3	4	5	5	5	5	3	16	16	0.125
Anubis	7	7	7	7	7	7	7	7	7	0	2	0.063
Hierocrypt-3	7	7	7	7	7	7	7	7	7	1	4	0.063
Turing	7	7	7	7	7	7	7	7	6	0	4	0.086
BelT	7	7	7	7	7	7	7	7	6	0	6	0.063
DESX	7	7	7	7	7	7	7	7	7	1	4	0.086

Як видно з табл. 4, низькі показники параметрів d та v мають шифри Crypton, Snow, CS, що є недоліком цих шифрів.

За емпіричною оцінкою для збалансованої двійкової функції від 8 змінних $d = 6$ з імовірністю $p = 0.003844$ і $d = 7$ з імовірністю $p = 0.996156$.

У табл. 5 наведена порівняльна характеристика властивостей S -блоків за параметрами, які визначають усталеність відносно диференційного методу криптографічного аналізу [9]. Диференційні характеристики підстановки розглядаються для чотирьох можливих комбінацій операцій додавання за модулем 2 ($\oplus$) та додавання за модулем 2^n (+). Відносно бінарних операцій o_1 та o_2, які задані на V_n, максимальне значення у таблиці різниць підстановки обчислюється за формулою

$$R_{o_1 o_2} = \max_{\alpha,\beta \in V_n, \alpha \neq 0} \sum_{x \in V_n} I\{S(x\, o_1\, \alpha) = S(x)\, o_2\, \beta\},$$

де $I\{\varepsilon\}$ – індикатор події ε.

Таблиця 5

Алгоритм	$R_{\oplus\oplus}$	R_{++}	$R_{\oplus+}$	$R_{+\oplus}$	Алгоритм	$R_{\oplus\oplus}$	R_{++}	$R_{\oplus+}$	$R_{+\oplus}$
Rijndael	4	7	6	7	Whirlpool	8	6	8	7
Crypton	8	8	8	8	Торнадо	4	7	6	6
E2	10	7	7	8	Camellia	4	7	6	6
MD2	10	7	7	7	Q	4	7	6	7
RC2	12	7	7	8	CS	16	12	16	16
Safer+	128	2	10	128	Anubis	8	8	8	8
Skipjack	12	7	8	7	Hierocrypt-3	4	7	7	7
Snow	6	7	9	8	Turing	12	8	7	8
Square	4	7	6	6	BelT	8	7	6	3
Twofish	10	8	10	8	DESX	10	8	8	7

Найкращі показники параметра $R_{\oplus\oplus}$ мають S-блоки алгоритмів Rijndael, Camellia, Square, Торнадо, Q, Hierocrypt-3, отже, *S*-блоки цих шифрів є оптимізованими відносно методів диференційного криптографічного аналізу.

У табл. 6 наведена емпірична оцінка параметру $R_{\oplus\oplus}$ для 8×8 S-блоків.

Таблиця 6

$R_{\oplus\oplus}$	8	10	12	14	16	18	20
p	3.75e-05	0.39579	0.53999	0.05986	0.00402	0.00029	2.5e-05

Найгірші показники параметрів $R_{\oplus\oplus}$, R_{++}, $R_{\oplus+}$, $R_{+\oplus}$ мають S-блоки алгоритмів Safer+ та CS.

Як видно з табл. 4, тільки алгоритми Whirlpool і Anubis мають $t = 2$. Цей параметр було вибрано приоритетним під час побудови S-блоків цих шифрів.

У табл. 7 наведена емпірична оцінка ймовірності значень параметра t, на рис. 2 – гістограма значень цього параметра.

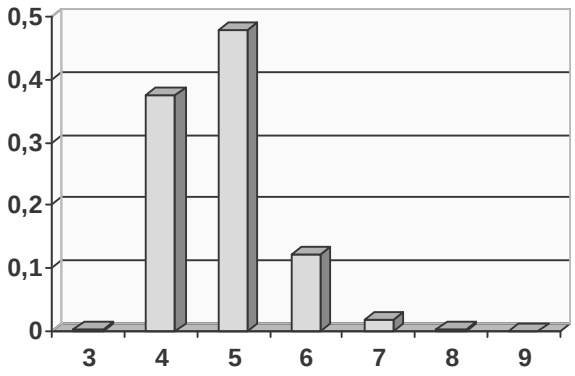

Рисунок 2 – Імовірність значення параметра t для 8×8 S-блоків.

Таблиця 7

t	p	t	p	t	p	t	p
2	1e-08	5	0.478798	8	0.00232881	11	2.21e-06
3	0.00403405	6	0.121073	9	0.00025997	12	1.6e-07
4	0.374978	7	0.0184999	10	2.634e-05	13	2e-08

Імовірність відсутності одиничних циклів в підстановці обчислюється за формулою

$$p = \sum_{k=0}^{2^n-1} \frac{(-1)^k}{k!}.$$

Для $n = 8$ ця ймовірність дорівнює 0.368.

У табл. 8 наведена емпірічна оцінка ймовірності значення параметра e для 8×8 S-блоків.

Таблиця 8

e	0	1	2	3	4	5
p	0.36782	0.367868	0.184009	0.0612748	0.0153547	0.0030791
e	6	7	8	9	10	
p	0.0005061	7.48e-05	1.22e-05	1e-06	1e-07	

Додатковими характеристиками, які розглядаються для координатних функцій підстановки, є кількість термів (одночленів) у поліномі Жегалкина двійкової функції, а також кількість термів, які містять змінну x_i, де $i = \overline{1,8}$. У табл. 9 наведена кількість термів для координатних функцій, яка позначена $\mu_1, \mu_2, ..., \mu_8$ відповідно.

Таблиця 9

Алгоритм	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
Rijndael	132	133	145	136	131	114	112	110
Торнадо	117	131	133	130	116	130	123	136
Whirlpool	142	131	128	134	128	130	130	125
Square	128	123	122	134	132	127	131	125
Snow	48	48	45	38	38	41	41	52
Skipjack	130	127	127	122	128	140	137	124
Crypton	51	66	63	74	105	91	87	81
E2	128	121	130	131	124	119	128	124
MD2	136	130	123	126	123	144	116	122
RC2	123	126	137	133	116	127	136	119
Safer+	56	46	108	119	130	121	138	160
Twofish	116	120	126	122	112	123	127	111
Camellia	126	129	133	129	135	126	132	127
Q	132	133	145	136	131	114	112	118
CS	47	46	17	20	81	74	59	48
Anubis	127	135	139	132	139	121	134	134
Hierocrypt-3	132	128	116	121	119	128	119	124
Turing	121	119	137	138	131	130	122	137
BelT	125	130	137	133	137	132	122	122
DESX	133	135	118	127	126	125	122	133

Низькі показники цього параметра мають координатні функції S-блоків шифрів Crypton, Snow та CS.

Далі розглянемо S-блок як вузол накладення гами, тобто, $S(x) = (x_1 \oplus g_1, ..., x_n \oplus g_n)$, g_j – двійкова функція від n змінних. Позначимо $\gamma_j = \|g_j\|$.

У табл. 10 надані значення параметра γ_j для координатних функцій підстановки.

Таблиця 10

Алгоритм	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
Rijndael	116	120	122	128	136	128	140	132
Торнадо	126	124	136	134	134	118	140	132
Whirlpool	130	130	126	138	128	132	142	120
Square	122	114	138	126	140	120	136	122
Snow	136	120	128	120	128	128	120	120
Skipjack	136	122	130	124	130	116	138	140
Crypton	128	128	128	128	128	128	128	128
E2	118	136	122	128	132	132	126	126
MD2	136	124	126	126	122	136	136	136
RC2	130	124	124	130	128	126	134	128

Алгоритм	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
Safer+	128	120	124	126	128	126	130	152
Twofish	140	124	120	132	128	128	120	144
Camellia	126	122	120	132	138	136	134	114
Q	116	120	122	128	136	128	140	132
CS	128	128	128	128	96	96	96	96
Anubis	136	128	124	128	128	116	124	112
Hierocrypt-3	122	126	136	118	128	128	120	134
Turing	128	124	118	138	126	130	124	130
BelT	136	134	136	122	124	122	120	136
DESX	116	120	136	136	128	140	136	140

Як видно з табл. 10, тільки шифр Crypton реалізує вузол накладення рівноймовіної гами. Нижче наведена матриця кореляційних коефіцієнтів для S-блоку шифру Crypton.

$$\begin{pmatrix} 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.375 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.5 & 0.5625 & 0.5 & 0.375 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.375 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.4375 & 0.4375 & 0.5 & 0.5 & 0.46875 & 0.46875 & 0.5 \\ 0.5 & 0.5 & 0.4375 & 0.5 & 0.5625 & 0.5 & 0.46875 & 0.53125 \\ 0.5 & 0.5 & 0.5 & 0.5 & 0.40625 & 0.46875 & 0.5 & 0.53125 \\ 0.5625 & 0.5 & 0.5 & 0.4375 & 0.5 & 0.5625 & 0.53125 & 0.5 \end{pmatrix}$$

Кореляційні коефіцієнти на головній діагоналі матриці дорівнюють 0.5, тобто, i-ий вихід статистично не залежить від i-го входу, що забезпечує рівноймовірність гами.

Можливо побудувати S-блоку, усі кореляційні коефіцієнти якого будуть дорівнювати 0.5. Для такого S-блоку всі коррдинатні функції повинні бути кореляційно-імунними функціями першого порядку [5]. Такі функції є 1-рівноймовірними, тобто, рівноймовірними є усі підфункції, які утворюються в результаті підстановки 0 та 1 замість i-ої змінної.

Нижче наведено приклад такого *S*-блоку.

```
71 59 44 4c b7 bd 09 77 28 7b 62 34 80 b3 e5 9d
38 91 0d a7 18 d7 c3 5e 3b fd 20 f6 96 dd f0 06
26 6b 1c 75 41 81 40 be 51 9b 30 5c fc cf 52 ea
cb a9 97 ab 90 7a 48 e1 03 0c 66 ec 58 ae 2d 0a
36 ba e7 ce 8e 25 f8 74 47 0f 4d d6 e9 54 87 d3
ef e4 92 a4 1e 5a 79 7e 84 73 23 0b 99 c2 94 b9
8f 95 39 ac 3f 9a 31 13 a5 fb 4f df 0e f2 32 4a
b8 60 50 35 c9 c5 e8 2a 02 46 85 f1 c6 22 ed ff
eb c0 9f 00 65 64 aa 43 78 88 db 4b b5 24 cc 8b
de 07 bc bb e6 01 bf d9 fa a1 d5 a6 6e 10 2f 8d
f5 16 d1 d2 67 4e b2 b4 7d 27 98 2b 1f c7 93 ee
56 63 cd 3e 76 68 86 d0 da 9e 61 a2 33 5d 2c 11
ca 8a 49 a8 e0 12 ad 1b 3a 72 83 7c 3c c4 1a 70
57 dc 42 82 6a 7f 04 21 f4 29 53 15 6f b1 5b 6d
3d 05 b6 f7 89 c1 fe 2e a0 8c e2 08 b0 55 45 f9
1d d8 5f 6c e3 a3 17 19 9c 69 f3 d4 af 14 c8 37
```

Для цього S-блоку $n_1 = n_2 = n_8 = 108$, $n_3 = n_4 = n_5 = n_6 = n_7 = 112$, $N = 96$, $\lambda = 0.25$, $\nu = 6$, $d_j = 6$, $\gamma_j = 128$, $j = \overline{1,8}$, $R_{\oplus\oplus} = 12$, $e = 0$, $t = 3$, $c = 0$. Значення параметрів d_j, $j = \overline{1,8}$ є максимально можливим для кореляційно-імунних функції [5]. Усі кореляційні коєфіцієнти c_{ij}, $i = \overline{1,8}$, $j = \overline{1,8}$ дорівнюють 0.5.

Асимптотична оцінка ймовірності побудови кореляційно-імунної функції першого порядку від n змінних при "випадковій" генерації двійкової функції обчислюється за формулою

$$p_{\hat{e}.i.}(n) \sim 0.5 \exp\left(n \left(\ln \sqrt{\frac{\pi}{2}} + \left(\frac{n}{2} - 1 \right) \ln 2 \right) \right)^{-1}$$

Зокрема, $p_{к.і.}(8) \approx 10^{-6}$.

Емпірична оцінка ймовірності побудови збалансованої кореляційно-імунної функції від n змінних при "випадковій" генерації збалансованої двійкової функції наведена в таблиці 11.

Таблиця 11

n	4	5	6	7	8
$p_{к.і.}(n)$	0.0174029	0.00134697	5.57267e-05	1.10605e-06	4.20106e-08

У випадку, коли підстановка використовується у шифрі колонної заміни, розглядається ще один параметр – порядок підстановки.

Порядком підстановки g називається найменше число e, таке, що $g^e = 1$. Порядок підстановки позначається $ord(g)$. Він дорівнює найменшому спільному кратному довжин циклів підстановки.

У табл. 12 наведена порівняльна характеристика властивостей *S*-блоків за параметром *ord*.

Таблиця 12

Алгоритм	*ord*	Алгоритм	*ord*
Rijndael	277182	Safer+	6888
Торнадо	1141140	Twofish	15534090
Whirlpool	20640	Camellia	2490
Square	543720	Q	277182
Snow	75582	CS	2
Skipjack	400860	Anubis	2
Crypton	19163760	Hierocrypt-3	15340536
E2	17472	Turing	42570
MD2	1182384	BelT	185640
RC2	41678	DESX	278760

Як видно з табл. 12, підстановки шифрів CS, Anubis є інволюціями, тобто їх циклова структура містить цикли довжини 1 та 2. Це означає, що для цих шифрів оберненою підстановкою є сама підстановка.

Ще одним параметром двійкових функцій є коефіцієнт розповсюдження помилки (КРП). КРП функції f за змінною x_j називається величина $k_j^f = \frac{1}{2^n} \sum_x (f(x) \oplus f(x^j))$, де вектори $x, x^j \in V_n$ відрізняються тільки j-ою координатою. КРП функції f називається величина $K_f = \sum_{j=1}^{n} k_j^f$.

У табл. 13 наведена порівняльна характеристика властивостей *S*-блоків за параметром K_f. КРП для координатної функції f_j позначено через K_j, $j = \overline{1,8}$.

Таблиця 13

Алгоритм	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
Rijndael	3	4	3	4	3	4	4	4
Торнадо	3	4	4	4	4	4	3	4
Whirlpool	4	4	3	3	4	4	4	4
Square	3	3	4	3	4	4	3	4
Snow	4	4	4	3	4	3	4	4
Skipjack	4	4	3	4	4	4	3	3
Crypton	3	3	4	3	3	4	4	3
E2	3	3	4	4	4	4	3	4
MD2	4	3	4	4	4	3	4	3
RC2	4	3	4	4	3	4	3	4

Алгоритм	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
Safer+	4	3	4	4	4	4	4	4
Twofish	3	3	3	3	4	3	4	4
Camellia	3	3	4	3	4	4	4	3
Q	3	4	3	4	3	4	4	4
CS	3	3	3	3	3	3	3	3
Anubis	4	4	4	4	4	4	3	3
Hierocrypt-3	4	3	3	4	4	3	3	4
Turing	4	4	4	3	4	4	4	3
BelT	4	3	3	4	4	4	4	4
DESX	3	3	4	3	3	3	4	3

За емпіричною оцінкою для збалансованої двійкової функції від 8 змінних $K_f = 3$ з імовірністю $p = 0.423388$ і $K_f = 4$ з імовірністю $p = 0.576612$.

Параметр КРП тісно пов'язаний з "суворим лавинним критерієм (СЛК)" (англ. – Strict Avalanche Criterion (SAC)) [12].

Двійкова функція f задовольняє СЛК, якщо при заміні одного довільного біта на доповнення функція змінюється з імовірністю 0.5, тобто

$$p(f(x) = f(x \oplus a)) = \frac{1}{2} \quad \forall a \in V_n : \|a\| = 1 .$$

Якщо двійкова функція f задовольняє СЛК, то КРП функції f за будь-якою змінною дорівнює $\frac{1}{2}$, а КРП функції приймає максимальне значення $n/2$.

Основною вимогою до статистичних властивостей криптографічного алгоритму є „статистична безпека" [3]. Рівень статистичної безпеки, що забезпечується криптоалгоритмом, може бути визначений з використанням одного з відомих пакетів статистичного тестування. Одним із статистичних тестів для блокових шифрів, який було використано при проведенні конкурсу NESSIE, був кореляційний тест [3]. Для цього тесту обчислюються матриця „залежностей" та матриця „відстаней" [15]. Стосовно $n \times n$ S-блоку матриця „залежностей" – це матриця A розміру $n \times n$, елемент a_{ij} якої дорівнює кількості вхідних векторів $x \in V_n$, для яких зміна i-го біта призводить до зміни j-го біта у векторі $y = S(x)$, а матриця „відстаней" – це матриця B розміру $n \times (n+1)$, елемент b_{ij} якої дорівнює кількості вхідних векторів $x \in V_n$, для яких зміна i-го біта призводить до зміни j бітів у векторі $y = S(x)$.

Ступінь „повноти" d_c обчислюється за формулою $d_c = 1 - \left|\{a_{ij} \middle| a_{ij} = 0\}\right| \cdot n^{-2}$, ступінь „суворого лавинного критерію" d_{sa} – за формулою $d_{sa} = 1 - n^{-2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left| \frac{2a_{ij}}{2^n} - 1 \right|$, ступінь „лавинного ефекту" d_a – за формулою $d_a = 1 - n^{-2} \sum_{i=1}^{n} \left| \frac{1}{2^n} \sum_{j=1}^{m} 2jb_{ij} - n \right|$.

У табл. 14 наведена порівняльна характеристика властивостей S-блоків за параметрами d_c, d_{sa} і d_a.

Таблиця 14

Алгоритм	d_c	d_{sa}	d_a	Алгоритм	d_c	d_{sa}	d_a
Rijndael	1	0.947	0.985	Safer+	0.984	0.863	0.919
Торнадо	1	0.945	0.983	Twofish	1	0.922	0.964
Whirlpool	1	0.929	0.982	Camellia	1	0.962	0.990

Алгоритм	d_c	d_{sa}	d_a	Алгоритм	d_c	d_{sa}	d_a
Rijndael	1	0.947	0.985	Safer+	0.984	0.863	0.919
Square	1	0.955	0.989	Q	1	0.947	0.985
Snow	1	0.945	0.984	CS	0.969	0.751	0.870
Skipjack	1	0.917	0.977	Anubis	1	0.924	0.981
Crypton	1	0.922	0.957	Hierocrypt-3	1	0.943	0.980
E2	1	0.937	0.976	Turing	1	0.931	0.986
MD2	1	0.947	0.978	BelT	1	0.941	0.981
RC2	1	0.929	0.986	DESX	1	0.928	0.984

Як видно з табл. 14, найгірші показники за параметрами d_c, d_{sa} і d_a мають S-блоки шифрів Safer+ та CS.

Нижче наведено приклад *S*-блоку, усі координатні функції якого задовольняють СЛК.

```
e6 a9 29 84 26 c0 93 06 88 f9 97 76 b6 d2 fc c2
e4 1f cd 6b c3 04 87 0a 11 a8 a5 3a 8a 05 d5 82
14 3f 4d 2c a3 73 58 f3 23 d3 3c 2f f8 ea 19 60
c9 f5 ad 59 de eb 72 80 63 ba bb 50 a6 48 9b b5
52 36 5e 7f ca 46 f2 6c 7e e3 aa b3 f4 f6 64 c8
55 f7 02 43 5b 0f 24 db e0 2a 56 c4 1b 42 9e e8
9d a0 7b 89 fb 35 1c 18 22 10 da 45 fe 0d d9 00
5c 34 ff 8c 03 95 25 08 94 bf c7 53 96 be 5a 90
cc 09 15 4b 3d 13 6e 68 b1 fd 4a 4c 91 0e a4 e7
44 47 a7 16 9a b4 99 b2 62 8e 7d 6f 8f dc ee 17
b8 54 ce c5 38 9c d6 d4 27 e2 74 0b 1a 07 92 cf
bd 8b 83 e1 49 2d ef 9f 3b e9 ed 61 4f af bc 0c
b0 70 7a 67 98 65 cb f0 ec e5 57 a1 fa 21 20 75
1e 7c 40 8d 37 2e 81 01 3e 32 33 51 5d 85 79 78
d8 6d ab 69 12 a2 2b 30 f1 d7 5f ae d0 dd 41 d1
b7 1d c1 4e 71 28 77 b9 c6 39 66 31 6a 86 ac df
```

Для цього S-блоку $n_j = 110$, $N = 96$, $\lambda = 0.25$, $\nu = 7$, $d_j = 7$, $j = \overline{1,8}$, $R_{\oplus\oplus} = 12$, $e = 0$, $t = 3$. Матриця „залежностей" для цього S-блоку є рівномірною зі значенням 128, а параметри d_c, d_{sa} і d_a дорівнюють 1.

Одним із варіантів реалізації булевих відображень є матрична реалізація, яка використовується при синтезі булевих відображень у логічних схемах з можливістю програмування [13]. Розглянемо булеве відображення $S = (f_1, f_2, ..., f_m)$, де $f_j : V_n \to \{0,1\}$, $j = \overline{1,m}$. Множину змінних координатних функцій позначимо через $X = \{x_0, x_1, ..., x_{n-1}\}$. Для кожної координатної функції f_j, $j = \overline{1,m}$ побудуємо мінімальну диз'юнктивну нормальну форму (МДНФ). Через $\Phi = \{\varphi_1, ..., \varphi_p\}$ позначимо множину елементарних кон'юнкцій, кожна з яких входить до МДНФ, принаймні, однієї з координатних функцій. Позначимо $\widetilde{X} = \{x_0, \overline{x_0}, x_1, \overline{x_1}, ..., x_{n-1}, \overline{x_{n-1}}\}$.

Через $X(\varphi_i)$ будемо позначати підмножину змінних з множини $\widetilde{X}$, які входять до кон'юнкції φ_i.

Булеве відображення може бути подано як $S = \overline{\overline{\left(M_1 \overline{x}\right)^T} M_2}$, де $M_1 = \left(m_{ij}^{(1)}\right)_{p \times 2n}$, $m_{ij}^{(1)}$ дорівнює 1 якщо $x_j \in X(\varphi_i)$ або $\overline{x_j} \in X(\varphi_i)$, і 0 у іншому випадку, $M_2 = \left(m_{ij}^{(2)}\right)_{p \times m}$, $m_{ij}^{(2)}$ дорівнює 1 якщо $\varphi_i \in$ МДНФ(f_j), і 0 у іншому випадку.

Таке подання булевого відображення використовують у випадку, коли табличний спосіб задання відображення є неможливим, зокрема, при великій кількості змінних.

У табл. 15 наведена порівняльна характеристика властивостей *S*-блоків за параметром кількості елементарних кон'юнкцій у множині Φ, яка визначає кількість рядків матриць M_1 та M_2. Цей параметр

відображає „складність” *S*-блоку з точки зору запису у МДНФ.

Таблиця 15

Алгоритм	***p***	Алгоритм	***p***	Алгоритм	***p***
Rijndael	416	E2	412	CS	299
Торнадо	411	MD2	436	Anubis	419
Whirlpool	423	RC2	419	Hierocrypt-3	419
Square	427	Safer+	433	Turing	420
Snow	422	Twofish	406	BelT	429
Skipjack	405	Camellia	424	DESX	420
Crypton	395	Q	416		

Ще одним методом генерації S-блоку є використання операції піднесення в степінь примітивного елемента у мультипликативній групі скінченного поля Галуа $GF(2^n)$. Такі *S*-блоки носять назву експоненційних (англ. – exponential) [14].

У роботі [14] доведено, що для параметра нелінійності таких *S*-блоків виконується нерівність $N \geq 2^{n-1} - 1 - 2^{\frac{n}{2}-1} \max\limits_{b \in V_n \setminus 0} \prod(b)$, де $\prod(b) = \dfrac{1}{2^n - 1} \sum\limits_{h=1}^{2^n-1} \prod\limits_{k \in K(b)} \left| \tan\left(\dfrac{\pi 2^k h}{2^n - 1} \right) \right|$, $K(b)$ – множина індексів ненульових бітів вектора b.

Для $n = 8$ нелінійність експоненційних *S*-блоків лежить у діапазоні $[96, 102]$.

Нижче наведено приклад експоненційного 8×8 *S*-блоку.

```
00 95 df fa 7d ab c0 60 30 18 0c 06 03 94 4a 25
87 d6 6b a0 50 28 14 0a 05 97 de 6f a2 51 bd cb
f0 78 3c 1e 0f 92 49 b1 cd f3 ec 76 3b 88 44 22
11 9d db f8 7c 3e 1f 9a 4d b3 cc 66 33 8c 46 23
84 42 21 85 d7 fe 7f aa 55 bf ca 65 a7 c6 63 a4
52 29 81 d5 ff ea 75 af c2 61 a5 c7 f6 7b a8 54
2a 15 9f da 6d a3 c4 62 31 8d d3 fc 7e 3f 8a 45
b7 ce 67 a6 53 bc 5e 2f 82 41 b5 cf f2 79 a9 c1
f5 ef e2 71 ad c3 f4 7a 3d 8b d0 68 34 1a 0d 93
dc 6e 37 8e 47 b6 5b b8 5c 2e 17 9e 4f b2 59 b9
c9 f1 ed e3 e4 72 39 89 d1 fd eb e0 70 38 1c 0e
07 96 4b b0 58 2c 16 0b 90 48 24 12 09 91 dd fb
e8 74 3a 1d 9b d8 6c 36 1b 98 4c 26 13 9c 4e 27
86 43 b4 5a 2d 83 d4 6a 35 8f d2 69 a1 c5 f7 ee
77 ae 57 be 5f ba 5d bb c8 64 32 19 99 d9 f9 e9
e1 e5 e7 e6 73 ac 56 2b 80 40 20 10 08 04 02 01
```

Для його синтезу використано утворюючий поліном $x^8 + x^5 + x^3 + x + 1$ поля $GF(2^8)$, та примітивний елемент $x^7 + x^4 + x^2 + 1$. Для цього *S*-блоку $n_1 = 102$, $n_2 = n_8 = 106$, $n_3 = n_4 = n_5 = n_6 = 108$, $n_7 = 104$, $N = 100$, $\lambda = 0.21875$, $d_j = 7$, $j = \overline{1,8}$, $\nu = 7$, $R_{\oplus\oplus} = 10$, $e = 1$, $t = 5$. Цей *S*-блок має досить високі показники нелінійності.

Експоненційні *S*-блоки доцільно використовувати у випадках, коли табличний запис підстановки є неможливим, зокрема, при великих значеннях параметра n.

Як вже вказувалось, при побудові S-блоків ряду шифрів, зокрема, блокового шифру Rijndael було використано мультиплікативне звертання елемента в полі $GF(2^8)$. Ця конструкція гарантує одержання найменших максимальних значень у таблиці розподілу різниць і лінійних апроксимацій, забезпечуючи найкращі властивості для захисту від диференційного і лінійного криптографічного аналізу.

У роботі показано, що всі 8 координатних функцій S-блоку шифру Rijndael знаходяться в одному класі щодо деякого афінного перетворення. Іншими словами, для данного шифру існують залежності між координатними функціями виду $f_j(x) = f_i(Dx) \oplus a$, де D – матриця розміру 8×8, $a \in \{0, 1\}$. Нижче, як приклад, наведено взаємозв’язок другої і третьої координатних функцій S-блоку шифру Rijndael з

першою координатною функцією.

$$f_2(x) = f_1(D_{12}x)\,,\ f_3(x) = f_1(D_{13}x) \oplus 1,$$

де $D_{12} = \begin{pmatrix} 1&0&1&1&0&0&1&0 \\ 0&1&0&1&0&1&1&0 \\ 0&0&0&1&0&0&1&0 \\ 1&0&0&1&1&0&0&0 \\ 0&1&0&1&1&1&0&0 \\ 1&0&0&0&1&1&1&0 \\ 1&1&0&1&0&0&0&0 \\ 1&0&0&0&1&1&0&1 \end{pmatrix}$, $D_{13} = \begin{pmatrix} 1&1&1&1&0&1&1&0 \\ 0&1&1&0&0&1&0&0 \\ 0&0&0&1&0&0&0&0 \\ 1&0&1&1&0&0&1&1 \\ 1&1&0&1&0&0&0&0 \\ 0&0&0&1&0&0&1&0 \\ 1&1&1&0&1&1&1&0 \\ 0&1&1&0&0&0&1&0 \end{pmatrix}$

Така сама властивість притаманна *S*-блокам шифрів Camellia, Square, Snow, Q, Hierocrypt-3, Торнадо.

Варто зауважити, що своєчасно не опубліковано будь-яких результатів, в яких ця особливість використовувалась для зменшення криптографічної стійкості зазначених шифрів.

Типовим випадком під час синтезу криптографічних алгоритмів є використання декількох S-блоків для утворення *S*-блоку більшої розмірності, як правило, 32×32. Це пов'язано з тим, що більшість шифрів орієнтовані на програмну реалізацію для 32-розрядних процесорів, а таблична реалізація 32×32 S-блоку практично неможлива. Прикладом є блоковий шифр ГОСТ 28147-89, в якому перетворення $K : V_{32} \to V_{32}$ реалізується з восьми 4×4 S-блоків та циклічного зсуву 32-бітового вектора на 11 розрядів. Іншим прикладом є алгоритм Snow, в якому використовуються чотири ідентичні 8×8 *S*-блоку та фіксована підстановка на множині потужності 32.

Висновок

У результаті аналізу властивостей *S*-блоків 20 криптографічних алгоритмів можна зробити висновок, що за більшістю параметрів переважають *S*-блоки алгоритмів Rijndael, Square, Camellia, Q, Hierocrypt-3, Торнадо, отже, найпривабливішою на теперішній час конструкцією побудови *S*-блоків є конструкція на основі мультиплікативного звертання елемента в скінченному полі Галуа $GF(2^8)$.

Література ***1*** *К. Шеннон. Работы по теории информации и кибернетике. – М.: Издательство иностранной литературы, 1963.* ***2****. Schneier B. Applied cryptography. Second edition. Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc. 1996.* ***3*** *NESSIE security report, New European Schemes for Signatures, Integrity and Encryption, 2002, NES/DOC/ENS/WP5/D20/1, ttp://www.cryptonessie.org.* ***4****. FIPS PUB 197, Advanced Encryption Standard (AES), Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), 2001, http://csrc.nist.gov/publications/.* ***5.*** *Siegenthaler T. Correlation immunity of non-linear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, v. 30, p. 776 - 780, 1984.* ***6****. Menezes A., Oorshot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.* ***7.*** *K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55 - 64.* ***8.*** *J. Fuller, W. Millan. On linear redundancy in S-boxes. In Proceedings of FSE'03. LNCS, Springer-Verlag, 2003.* ***9****. E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, New York, 1993.* ***10****. M. Matsui. Linear Cryptanalysis Method for the DES Cipher. Lecture Notes in Computer Science, Advances in Cryptology, in proceedings of Eurocrypt '93, 1993.* ***11****. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций, Дискретная математика, т. 3., вып. 2, 1991.* ***12.*** *Webster A. F., Tavers S. E. On the design of S-boxes, Advances in Cryptology, – Proc. Crypto'85, Springer-Verlag, 1986, pp. 523 - 534.* ***13****. Ачасова С. М. Алгоритмы синтеза автоматов на программируемых матрицах. – М.: Радио и связь, 1987.* ***14****. Agievich S., Afonenko A. Exponential S-boxes. National Research Center for Applied Problems of Mathematics and Informatics, Belarusian State University, http://eprint.iacr.org/2004/024.* ***15****. Serf P. The degrees of completeness of avalanche effect and of strict avalanche criterion for MARS, RC6, Rijndael, Serpent and Twofish with reduct number of rounds. Siemens AG, ZT IK 3, April 3, 2000.*