DOI 10.15276/imms.v12.no3.219
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 219-225

МЕТОД СИНТЕЗУ ВИСОКОЯКІСНИХ S-БЛОКІВ НА ОСНОВІ ФУНКЦІЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

В.В. Радуш, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1. radiosquid@gmail.com

Криптографічний S-блок є найважливішим компонентом сучасних шифрів, від якості якого у великій мірі залежить ефективність, криптографічна захищеність та швидкодія шифрів, які на ньому засновані. На сьогоднішній день, через розвиток квантового криптоаналізу, а також появу можливих атак на криптографічні алгоритми шляхом їх опису за допомогою функцій багатозначної логіки, стає актуальним завдання розробки алгоритмів синтезу S-блоків, які були б високоякісними не тільки при їх представленні компонентними булевими функціями, але і при будь-якому іншому представленні компонентними функціями багатозначної логіки. При цьому, більша частина представлених в літературі існуючих методів синтезу S-блоків орієнтована лише на дослідження їх криптографічної якості при представленні компонентними булевими функціями. У даній роботі на основі S-блоків довжини N=16, що відповідають суворому лавинному критерію компонентних булевих та 4-функцій, представлено метод синтезу великої множини потужності J=117588 S-блоків практично цінної довжини N=256, що одночасно відповідають строгому лавинному критерію компонентних булевих функцій, строгому лавинному критерію компонентних 4-функцій, а також критерію кореляційного імунітету компонентних булевих функцій, тобто володіють ідеальними матрицями коефіцієнтів кореляції векторів виходу та входу. Висока криптографічна якість розроблених S-блоків при їх представленні компонентними булевими та 4-функціями дозволяє рекомендувати їх для практичного застосування як у задачах підвищення ефективності існуючих криптоалгоритмів, так і при розробці перспективних шифрів, тоді як потужність класу синтезованих S-блоків дозволяє застосовувати їх у якості довгострокового ключа.

Ключові слова: S-блок, критерій розповсюдження помилки, кореляційний імунітет, функція багатозначної логіки.

Введення і постановка задачі

Одним з найважливіших криптографічних примітивів, що визначає ефективність, рівень криптографічної захищеності, а також швидкодію сучасних симетричних криптоалгоритмів, є S-блок [1]. На сьогоднішній день, чимало публікацій присвячено питанням синтезу S-блоків за критеріями криптографічної якості їх компонентних булевих функцій. Однак, через появу публікацій [2], де зазначаються можливості атак проти криптографічних конструкцій із застосуванням їх опису функціями багатозначної логіки, все більш гостро стає питання про необхідність побудови криптографічних конструкцій із врахуванням їх можливого уявлення функціями багатозначної логіки. Оскільки, найуживанішою довжиною сучасних S-блоків є довжина $N = 256$, йдеться, у першу чергу, про врахування криптографічної якості компонентних булевих функцій, 4-функцій та 16-функцій. Зараз вже створено методи синтезу S-блоків, які характеризуються високою криптографічною якістю як при представленні компонентними булевими функціями, так і компонентними функціями багатозначної логіки. Зокрема, відомий метод синтезу S-блоків, що відповідають суворому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій [3]. Однак, як показують проведені дослідження,

отримані у роботі [3], результати можуть стати основою для побудови більш досконалих методів синтезу S-блоків, які одночасно відповідатимуть як суворому лавинному критерію компонентних булевих функцій та 4-функцій, так і критерію кореляційного імунітету компонентних булевих функцій, що означає ідеальність їх матриць коефіцієнтів кореляції.

Метою цієї роботи є підвищення криптографічної якості підстановлювальних конструкцій сучасних шифрів шляхом розробки методу синтезу високоякісних S-блоків на основі функцій багатозначної логіки.

Застосовувані критерії криптографічної якості

Розглянемо основні критерії криптографічної якості, у відповідності до яких виконуватиметься синтез S-блоків.

2.1. Суворий лавинний критерій

Визначення відповідності S-блока суворому лавинному критерію при його представленні булевими функціями базується на дослідженні його компонентних булевих функцій за допомогою наступних визначень.

Визначення 1 [4]. Похідною за напрямом $u \in V_k$ булевої функції f називається булева функція

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{1}$$

де V_k — лінійний векторний простір двійкових векторів довжини k, $\oplus$ — підсумовування по модулю 2.

Визначення 2 [4]. Булева функція $f(x)$ задовольняє критерію розповсюдження помилки щодо вектора $u \in V_k$ — КР(u) якщо її похідна за напрямом u є збалансованою функцією, тобто

$$p\{f(x) = f(x \oplus u)\} = 0.5. \tag{2}$$

Визначення 3 [4]. Булева функція f задовольняє строгому лавинному критерію (СЛК), якщо вона задовольняє критерію розповсюдження помилки КР(u) щодо всіх векторів ваги Гемінґа 1, тобто

$$p\{f(x) = f(x \oplus u)\} = 0.5, \quad \forall u \in V_k, \quad wt(u) = 1. \tag{3}$$

При представленні S-блока компонентними функціями багатозначної логіки для дослідження його відповідності строгому лавинному критерію відбувається на основі наступних визначень.

Визначення 4 [5]. Вагою $\varpi(u)$ q-значного вектора назвемо кількість його ненульових компонентів.

Визначення 5 [5]. Похідною функції f у напрямку вектора u назвемо функцію

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \,(\mathrm{mod}\, q), \tag{4}$$

де $\underset{q}{\oplus}$ означає додавання по модулю q.

Визначення 6 [5]. Функція q-значної логіки $f(x)$ задовольняє строгому лавинному критерію, якщо її похідні за напрямами u одиничної ваги $\varpi(u) = 1$ є збалансованими функціями, тобто їх значення $0,1,...,q-1$ приймаються з рівними

ймовірностями: $p(D_u f(x) = i(\mathrm{mod}\, q)) = 1/q$ для всіх $i = 0,1,...,q-1$. Інакше висловлюючись, $K^0 = K^1 = ... = K^{q-1}$, де K^i — кількість наборів значень змінних, у яких похідна набуває значення i.

2.2. Критерій кореляційного імунітету

Визначення відповідності S-блока критерію кореляційного імунітету відбувається шляхом дослідження його компонентних булевих функцій на основі наступних визначень.

Визначення 7 [6]. Підфункцією булевої функції $f(x)$, $x \in V_k$ називається функція f', отримана підстановкою в f констант "0" або "1" замість частини змінних. Якщо підставимо в функцію f константи $\sigma_{i_1},\cdots,\sigma_{i_s}$ замість змінних $x_{i_1},\cdots,x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$. Якщо замість змінної x_i константа не підставлена, то x_i називається вільною змінною.

Визначення 8 [6]. Булева функція $f(x)$, $x \in V_k$ називається кореляційно-імунною порядку m, $1 \le m \le k$, якщо вага Геммінга буде дорівнювати $wt(f') = wt(f)/2^m$, для будь-якої її підфункції f' від $k-m$ змінних.

Визначення кореляційного імунітету тісно пов'язане з такою характеристикою S-блока, як його матриця коефіцієнтів кореляції [7] $R = \left\| \rho_{\nu,\mu} \right\|$, $\nu, \mu = 1,2,...,k$, елементи якої обчислюються відповідно до наступної формули

$$r_{\nu,\mu} = 1 - 2^{-(k-1)} \sum_{z=1}^{N} \left(x_{z,\nu} \oplus y_{z,\mu} \right) = 0, \quad \nu,\mu = \overline{1,k}, \tag{5}$$

де $\{x_i\}$ і $\{y_j\}$ — двійкові вектори входу та виходу S-блока.

Відомо, що якщо всі компонентні булеві функції S-блока є кореляційно імунними порядку $m = 1$, то такий S-блок характеризується ідеальною матрицею коефіцієнтів кореляції, тобто $\rho_{\nu,\mu} = 0$, $\nu, \mu = 1,2,...,k$.

Метод синтезу криптографічно високоякісних S-блоків

Дослідження показали, що побудова S-блоків, що характеризуються високою криптографічною якістю як компонентних булевих функцій, так і компонентних функцій багатозначної логіки, може здійснюватися у рекурентний спосіб.

В якості основи роботи представленого методу застосовується метод побудови S-блоків, що відповідають СЛК компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій, який було запропоновано у роботі [3], та який наводимо для повноти викладу матеріалу.

Метод М1

Крок 1. В якості вхідного матеріалу для даного методу буде використовуватися множина S-блоків довжини $N = 16$, що відповідають СЛК 4-функцій, які були побудовані у [5]. Дана множина має потужність $J = 245760$.

Крок 2. Задається функція F_m, яка представляє собою старшу компонентну 4-функцію в розкладанні S-блоку на 4-функції.

Крок 3. Формується множина з 4-х перестановок у відповідності з наступним правилом

$$p_j = x \underset{4}{\oplus} (j \circ d), \quad x = 0,1,...,N-1, \quad j = 0,1,2,3, \tag{5}$$

де d — один з векторів довжини $k = \log_4 N$ з 1 на одній зі своїх позицій, вектор x пробігає четвіркові представлення чисел від 0 до $N-1$, $\underset{4}{\oplus}$ – додавання по модулю 4, $\circ$ — символ поелементного множення четвіркового представлення числа d на значення j.

Крок 5. Збільшуємо довжину S-блоку до значення $4N$ використовуючи наступну конструкцію

$$G_0 = \{S \mid S(p_1) \mid S(p_2) \mid S(p_3)\}. \quad (6)$$

Крок 6. Будуємо новий бієктивний S-блок довжини $4N$, що відповідає суровому лавинному критерію компонентних 4-функцій за наступним правилом

$$S_1 = \{G_1 \cdot 4^k + G_0\}, k = \log_4 N. \quad (7)$$

Проведені експерименти показують, що на основі множини S-блоків довжини $N = 16$, які були отримані в [5], шляхом використання розробленого методу можуть бути отримані S-блоки практично цінної довжини $N = 256$, що відповідають одночасно СЛК компонентних 4-функций та критерію максимального лавинного ефекту булевих функцій.

Варто зазначити, що кількість S-блоків сильно залежить від значення обраних параметрів c_1, c_2, c_3, c_4, а також від обраного вектору напрямку d. Наприклад, нехай задані наступні параметри: довжина S-блоку $N = 256$, параметри $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$ на першій та другій ітерації використання методу, а також значення $d = [0\ 1]$ на першій ітерації використання методу і $d = [0\ 0\ 1]$ на другій ітерації використання методу.

Тоді отримуємо, що з множини $J = 245760$ S-блоків довжини $N = 256$, отриманих на основі множини S-блоків довжини $N = 16$ [5], $J_1 = 3968$ S-блоків одночасно відповідають СЛК компонентних 4-функцій і критерію максимального лавинного ефекту компонентних булевих функцій.

Означена множина S-блоків є основою для побудови високоякісних S-блоків на основі запропонованого у даній роботі Методу М2, який представимо у вигляді конкретних кроків.

Метод М2

Крок 1. Застосовуючи Метод М1 виконати синтез множини з $J_1 = 3968$ високоякісних S-блоків довжини $N = 256$, що відповідають строгому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій.

Крок 2. Пробігаючи усю множину S-блоків, отриману на *Кроці 1*, виконати їх декомпозицію на компонентні 4-функції. Розкладаючи отримані 4-функції на 2 компонентні булеві функції, виділити з них такі, у яких обидві компонентні булеві функції відповідають умовам СЛК.

Після виконання *Кроку 2* ми отримуємо множину 4-функцій, потужність якої складає 14336 функцій. Одна з таких функцій має наступний вигляд

$$F_{41} = [0, 1, 3, 3, 2, 2, 2, 1, 2, 0, 3, 0, 1, 0, 3, 1, 1, 3, 3, 0, 2, 2, 1, 2, 0, 3, 0, 2, 0, 3, 1, 1, 3, 3, 0, 1, 2, 1, 2, 2, 3, 0, 2, 0, 3, 1, 1, 0, 3, 0, 1, 3, 1, 2, 2, 2, 0, 2, 0, 3, 1, 1, 0, 3, 2, 0, 0, 1, 3, 3, 2, 3, 1, 0, 1, 3, 1, 0, 2, 2, 0, 0, 1, 2, 3, 2, 3, 3, 0, 1, 3, 1, 0, 2, 2, 1, 0, 1, 2, 0, 2, 3, 3, 3, 1, 3, 1, 0, 2, 2, 1, 0, 1, 2, 0, 0, 3, 3, 3, 2, 3, 1, 0, 1, 2, 1, 0, 2, 1, 1, 2, 3, 0, 3, 0, 0, 1, 2, 0, 2, 1, 3, 3, 2, 1, 2, 3, 1, 3, 0, 0, 0, 2, 0, 2, 1, 3, 3, 2, 1, 2, 3, 1, 1, 0, 0, 0, 3, 0, 2, 1, 2, 3, 2, 1, 3, 3, 1, 1, 2, 0, 0, 3, 0, 2, 1, 2, 0, 2, 1, 3, 3, 2, 3, 0, 2, 0, 1, 1, 1, 3, 1, 3, 2, 0, 0, 3, 2, 3, 0, 2, 2, 1, 1, 1, 0, 1, 3, 2, 3, 0, 3, 2, 0, 0, 2, 2, 3, 1, 1, 0, 1, 3, 2, 3, 1, 3, 2, 0, 0, 2, 2, 3, 0, 1, 0, 1, 1, 2, 3, 1, 3, 2, 0, 0, 3]. \quad (8)$$

Крок 3. З отриманої множини 4-функцій, необхідно виділити такі, що є унікальними.

Після проведення даної процедури видалення дублікатів з даної множини отримуємо в решті всього 769 підходящих функцій.

Крок 4. Виконуючи композицію отриманих 4-функцій між собою відповідно до теореми [8], генеруємо множину S-блоків, відбираючи ті, що є бієктивними.

Після виконання *Кроку 4* отримуємо множину, потужність якої складає $J = 117588$ унікальних S-блоків.

В якості прикладу у табл. 1 наведемо один з таких S-блоків.

Таблиця 1

Приклад високоякісного S-блоку, що відповідає СЛК булевих та 4-функцій

S	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**A**	**B**	**C**	**D**	**E**	**F**
00	05	00	0A	7A	5B	A1	C2	65	BF	67	DB	F4	1C	91	EE	BC
01	14	1E	4E	19	B5	D6	79	6F	7B	EF	C8	83	A5	F2	80	20
02	22	52	2D	28	EA	4D	73	89	F3	DC	97	4F	C6	94	34	B9
03	66	31	3C	36	51	47	9D	FE	E0	AB	53	C7	A8	08	8D	DA
04	41	4B	BB	46	E2	03	A6	98	A4	18	35	FC	D2	2F	FD	5D
05	5F	8F	5A	55	17	BA	AC	F6	2C	09	C0	B8	33	C1	61	E6
06	93	6E	69	63	8E	B0	CA	2B	1D	D4	8C	30	D5	75	FA	07
07	72	7D	77	A7	84	DE	3F	92	E8	90	04	21	49	CE	1B	E9
08	88	F8	87	82	40	E7	D9	23	59	76	3D	E5	6C	3E	9E	13
09	CC	9B	96	9C	FB	ED	37	54	4A	01	F9	6D	02	A2	27	70
A	AF	AA	A0	D0	F1	0B	68	CF	15	CD	71	5E	B6	3B	44	16
B	BE	B4	E4	B3	1F	7C	D3	C5	D1	45	62	29	0F	58	2A	8A
C	39	C4	C3	C9	24	1A	60	81	B7	7E	26	9A	7F	DF	50	AD
D	D8	D7	DD	0D	2E	74	95	38	42	3A	AE	8B	E3	64	B1	43
E	EB	E1	11	EC	48	A9	0C	32	0E	B2	9F	56	78	85	57	F7
F	F5	25	F0	FF	BD	10	06	5C	86	A3	6A	12	99	6B	CB	4C

У табл. 2 наведемо значення ваги Гемінґа похідних компонентних булевих функцій S-блока (табл. 1) для всіх векторів u_j одиничної ваги.

Таблиця 2

Відповідність вимогам СЛК компонентних булевих функцій синтезованого високоякісного S-блоку

u_j	$wt(D_{f_1})$	$wt(D_{f_2})$	$wt(D_{f_3})$	$wt(D_{f_4})$	$wt(D_{f_5})$	$wt(D_{f_6})$	$wt(D_{f_7})$	$wt(D_{f_8})$
00000001	128	128	128	128	128	128	128	128
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	128	128	128	128	128	128	128
00100000	128	128	128	128	128	128	128	128
01000000	128	128	128	128	128	128	128	128
10000000	128	128	128	128	128	128	128	128

Дослідження результатів, представлених у табл. 2 підтверджує відповідність S-блоку, представленого у табл. 1 умовам СЛК компонентних булевих функцій. У табл. 3 представлено значення кількостей K^0, K^1, K^2, K^3 елементів 0, 1, 2, 3 у похідних компонентних 4-функціях S-блока (табл. 1) для всіх векторів u_j одиничної ваги $\varpi(u_j) = 1$.

Таблиця 3

Відповідність вимогам СЛК компонентних 4-функцій синтезованого високоякісного S-блоку

u_j	$f_{41}: K^0 / K^1 / K^2 / K$	$f_{42}: K^0 / K^1 / K^2 / K$	$f_{43}: K^0 / K^1 / K^2 / K$	$f_{44}: K^0 / K^1 / K^2 / K$
0001	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64
0002	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64
…	…	…	…	…
3333	64/64/64/64	64/64/64/64	64/64/64/64	64/64/64/64

Побудована множина високоякісних S-блоків, зокрема, S-блок, наведений у табл. 1 характеризується також ідеальною матрицею коефіцієнтів кореляції, тобто відповідністю компонентних булевих функцій критерію кореляційного імунітету порядку $m = 1$. Наприклад, матриця коефіцієнтів кореляції S-блоку (табл. 1) має наступний вигляд

$$R = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}. \qquad (9)$$

Висновки

Відзначимо основні результати проведених досліджень:

1. Запропоновано метод синтезу великої множини з $J = 117588$ криптографічно високоякісних S-блоків довжини $N = 256$, що відповідають суворому лавинному критерію компонентних булевих функцій, суворому лавинному критерію компонентних 4-функцій, а також критерію кореляційного імунітету компонентних булевих функцій, тобто володіють ідеальними матрицями коефіцієнтів кореляції.

2. Актуальна довжина S-блоків $N = 256$, їх відповідність критеріям криптографічної якості як у сенсі представлення булевими функціями, так і у сенсі представлення функціями багатозначної логіки дозволяють рекомендувати їх до практичного застосування як для покращення роботи існуючих шифрів, так і для побудови нових перспективних криптоалгоритмів. При цьому велика потужність множини побудованих S-блоків дозволяє застосовувати їх у якості довгострокового ключа.

Список літератури

1. Соколов А.В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany 2015. 100 p.
2. 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.
3. 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. P. 1-12. URL: https://doi.org/10.1080/09720529.2021.1964727
4. Forrié R. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. *Conference on the Theory and Application of Cryptograph*y. Springer, New York, NY, 1988. P. 450-468.
5. Sokolov A.V., Zhdanov O.N. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength. *Siberian Journal of Science and Technology*, 2019. Vol. 20, No. 2. P.183-190.
6. Camion P. On correlation-immune function. *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 1991. P. 86-100.
7. Mazurkov M. I. Synthesis method of optimal substitution constructions based on the criterion of zero correlation between the output and input data vectors. *Radioelectronics and Communications Systems*. 2012. Vol. 55. No. 12. P. 533-543.
8. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. *Proc. of Asiacrypt'91*. Springer Verlag, 1991. P. 59-72.

THE METHOD FOR SYNTHESIS OF HIGH-QUALITY S-BOXES BASED ON MANY-VALUED LOGIC FUNCTIONS

V.V. Radush, A.V. Sokolov

National Odesa Polytechnic University
Ukraine, Odesa, 65044, Shevchenko Ave., 1. radiosquid@gmail.com

The cryptographic S-box is the crucial component of modern ciphers which determines their efficiency, cryptographic security, and performance. Today, the development of quantum cryptanalysis, as well as the appearance of possible attacks on cryptographic algorithms by describing them using many-valued logic functions made urgent the task of developing algorithms for the synthesis of S-boxes, which would be characterized by high quality not only when represented by component Boolean functions, but also with any other representation by component functions of many-valued logic. At the same time, most of the existing methods of synthesis of S-boxes presented in the literature are focused only on the research of their cryptographic quality when represented by component Boolean functions. In this paper, on the basis of S-boxes of length N=16, which corresponds to the strict avalanche criterion of component Boolean and 4-functions, we propose a method for synthesis of a set of high cardinality equal to J=117588 of S-boxes of practically valuable length N=256, which simultaneously corresponds the strict avalanche criterion of component Boolean functions, the strict avalanche criterion of component 4-functions, as well as the criterion of correlation immunity of component Boolean functions, i.e., they have ideal matrices of correlation coefficients between output and input vectors. The high cryptographic quality of the developed S-boxes when they are represented by component Boolean and 4-functions makes it possible to recommend them for practical use both in the tasks of increasing the effectiveness of existing cryptographic algorithms and in the development of promising ciphers, while the cardinality of the class of synthesized S-boxes allows them to be used as a long-term key.

Keywords: S-box, error propagation criterion, correlation immunity, many-valued logic function.