

Ключові слова: автентифікація, біометричні методи, Face ID, електронний підпис.

Ключевые слова: аутентификация, биометрические методы, Face ID, электронная подпись.

Keywords: authentication, biometric methods, Face ID, electronic signature.

Баландіна Наталя Миколаївна

*Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки*

ДОСЛІДЖЕННЯ НЕЛІНІЙНОСТІ S-БЛОКА НА ОСНОВІ ТЕОРІЇ ДИНАМІЧНОГО ХАОСУ ПРИ ЙОГО УЯВЛЕННІ ФУНКЦІЯМИ БАГАТОЗНАЧНОЇ ЛОГІКИ

Стійкість сучасних криптографічних алгоритмів у великій мірі залежить від криптографічних властивостей S-блоків, що застосовуються у них. Класичний підхід [1] до оцінки криптографічної якості S-блоків передбачає їх уявлення за допомогою математичного апарату булевих функцій, до яких застосовується стандартний набір критеріїв криптографічної якості: нелінійність, лавинні характеристики, кореляційні характеристики.

Однак дослідники все більш наполягають [2] на необхідності вивчення не тільки криптографічних показників компонентних булевих функцій сучасних шифрів, а також їх компонентних функцій багатозначної логіки (ФБЛ). Сьогодні існує набір критеріїв криптографічної якості ФБЛ, подібний до набору [1], створеного для булевих функцій. Відомі також публікації, присвячені дослідженню криптографічної якості відомих шифрів при їх виявленні за допомогою ФБЛ [3, 4].

Тим не менш, сучасні дослідження показують, що одними з найперспективніших методів синтезу S-блоків, є методи, засновані на теорії динамічного хаосу, яка дозволяє отримати підстановлювальні конструкції, що є

високоякісними з точки зору їх уявлення булевими функціями, тоді як їх властивості при уявленні за допомогою ФБЛ, залишаються невідомими.

Метою цієї роботи є дослідження та порівняльний аналіз нелінійних властивостей S-блока на основі теорії динамічного хаосу при його уявленні за допомогою ФБЛ.

Задля ясності подальшого викладу матеріалу коротко розглянемо сучасний підхід до вимірювання нелінійності булевих функцій та ФБЛ. Традиційним методом є оцінка відстані нелінійності булевих функцій у часовій області [5], що передбачає знаходження мінімуму серед відстаней Гемінга від досліджуваної булевої функції до кожного з кодових слів афінного коду. Іншим методом знаходження відстані нелінійності є метод, заснований на дослідженні максимального значення серед модулів коефіцієнтів перетворення Уолша-Адамара.

У [2] метод оцінки відстані нелінійності булевих функцій в області коефіцієнтів перетворення Уолша-Адамара був узагальнений на випадок ФБЛ. У цьому випадку відстань нелінійності визначається за такою основною формулою

$$N_f = \begin{cases} q^k - \max \{ |\Omega_f| \}, & q > 2; \\ 2^{k-1} - \frac{1}{2} \max \{ |W_f| \}, & q = 2, \end{cases} \quad (1)$$

де Ω_f — коефіцієнти перетворення Віленкіна-Крестенсона ФБЛ, які знаходять шляхом множення її експоненціальної таблиці істинності, представленої над алфавітом

$$z_k = e^{j \frac{2\pi}{q} k}, \quad k \in \{0, 1, \dots, q-1\}, \quad (2)$$

на матрицю Віленкіна-Крестенсона, рядки якої можна представити у вигляді

$$v_t(x) = e^{j \frac{2\pi}{q} \sum_{i=1}^k t_i x_i}, \quad (3)$$

де q — основа системи числення,

t_i — i -й елемент числа, записаного в позиційній q -ічній системі числення,

k — кількість елементів у q -ічному представленні значення N , що визначає довжину вибірки сигналу, $N = q^k$.

У випадку булевих функцій у формулі (1) замість перетворення Віленкіна-Крестенсона використовується перетворення Уолша-Адамара. Матриця перетворення Уолша-Адамара будується відповідно до такої рекурентної конструкції

$$A_{2^k} = \begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix}, \quad (4)$$

де $A_1 = 1$.

Теорія динамічного хаосу є альтернативним рішенням для синтезу сучасних S-блоків. В даний час є багато публікацій, присвячених синтезу S-блоків на основі хаотичних відображень. Ми представляємо дослідження одного з якісних S-блоків на основі хаотичних відображень, який був запропонований в [5]

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

Результати дослідження нелінійності S-блока (5), при його уявленні за допомогою компонентних булевих функцій, а також компонентних ФБЛ, наведені в табл. 1.

Таблиця 1 — Значення нелінійності компонентних функцій S-блока,
синтезованого на основі теорії динамічного хаосу

Булеві функції							
f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}	f_{26}	f_{27}
112	112	112	112	112	112	112	112
4-функції				16-функції			
f_{40}	f_{41}	f_{42}	f_{43}	f_{161}	f_{162}		
219.1218	216.6046	219.9445	217.5292	219.3823	216.5184		

Аналіз даних табл. 1 показує, що нелінійність компонентних функцій S-блока (5) на основі хаотичного відображення є стабільною в булевому випадку і нестійкою у випадку представлення компонентними 4-функціями і 16-функціями. У випадку компонентних булевих функцій нелінійність S-блока дорівнює $N_{s,2}=112$, що становить 93.3% від максимального значення. При представленні S-блока за допомогою компонентних 4-функцій нелінійність дорівнює $N_{s,4}=216.6046$, що становить 90.25% від максимального значення. При представленні компонентними 16-функціями нелінійність дорівнює $N_{s,16}=216.5184$, що становить 90.22% від максимального значення.

Задля порівняння властивостей S-блока (5) з існуючими аналогами скористаємося даними дослідження [6], та побудуємо відповідну порівняльну табл. 2.

Таблиця 2 — Порівняння нелінійних властивостей S-блока (5),
побудованого на основі теорії динамічного хаосу та відомих аналогів

S-блок	AES (без афінного перетворення)	Калина	BelT	Кузнєчїк	Хаотичне відображення (5)
--------	---------------------------------------	--------	------	----------	---------------------------------

$N_{f_{2i}}$, мінімальне значення	112	104	104	102	112
$N_{f_{4i}}$, мінімальне значення	216.5538	211.7281	215.5031	213.9524	216.6046
$N_{f_{16i}}$, мінімальне значення	212.4385	201.1621	223.4209	208.5308	216.5184

Аналіз даних табл. 2 приводить до висновку, що S-блок (5), побудований на основі теорії динамічного хаосу перевищує за показниками нелінійності S-блоки відомих криптоалгоритмів: AES (США), Калина (Україна), BelT (Білорусь), Кузнечік (Росія).

Відзначимо основні результати проведених досліджень:

1. Проведено дослідження та порівняльний аналіз нелінійних властивостей S-блока, побудованого на основі теорії динамічного хаосу при його уявленні за допомогою булевих функцій та ФБЛ з відомими аналогами.

2. Встановлено, що S-блок на основі хаотичних відображень показує результати, які перевищують результати S-блоків відомих криптоалгоритмів. Причому, найбільша перевага відзначається при представленні S-блоків за допомогою 16-функцій.

3. Таким чином, S-блоки на основі теорії динамічного хаосу є перспективними криптографічними конструкціями, які мають суттєві значення показників криптографічної якості не тільки при їх виявленні за допомогою булевих функцій, але і при уявленні за допомогою ФБЛ.

Список використаної літератури:

1. Жданов О.Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М.: ИНФРА-М, 2013. 90 с.
2. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики. Монография. М: Научная мысль, 2020. 192 с.
3. Sokolov A. V. Djiofack Temgoua Vanissa Noel. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019. P. 96—106.
4. Sokolov A. V., Radush V. V. Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. Informatics & Mathematical Methods in Simulation, 2019. No. 9 (3). P. 111-119.
5. Hussain I., Anees A., Al-Maadeed T. A. et al., Construction of S-Box Based on Chaotic Map and Algebraic Structures. Symmetry. 11. 351. 2019.
6. Kazakova N. F., Karpinski M., Sokolov A. V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. Procedia Computer Science. Vol. 192. P. 2731-2741.

Ключові слова: криптографія, S-блок, нелінійність, булева функція, функція багатозначної логіки.

Ключевые слова: криптография, S-блок, нелинейность, булева функция, функция многозначной логики.

Keywords: cryptography, S-box, nonlinearity, Boolean function, many-valued logic function.