УДК 621.3.06

І.Д.ГОРБЕНКО, д-р. техн. наук, О.В.ПОТІЙ, канд. техн. наук, Ю.А.ІЗБЕНКО, канд. техн. наук

ДОСЛІДЖЕННЯ АНАЛІТИЧНИХ І СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ БУЛЕВИХ ФУНКЦІЙ КРИПТОАЛГОРИТМУ RIJNDAEL (FIPS 197)

Однією з найважливіших складових схем симетричних криптоперетворень (блокових і потокових шифрів, хеш-функцій) є нелінійні перетворення. Нелінійні перетворення значною мірою визначають стійкість криптоперетворень до методів криптоаналізу. Як правило, нелінійні перетворення будуються на основі використання нелінійних булевих функцій [1]. Крім того, нерідко обговорення стійкості нелінійних перетворень (блоків підстановки) здійснюється в термінах стійкості булевих функцій. У наслідок цього в останні роки методи побудови високо нелінійних булевих функцій і аналіз їхньої стійкості у теорії захисту інформації є областю широких досліджень. Відомий ряд методів побудови необхідних булевих функцій, що забезпечують побудову функцій з високими показниками стійкості [2-7]. Дані методи використовують різні підходи до побудови нелінійних функцій та різні показники стійкості. Тому важливим є дослідження властивостей нелінійних перетворень криптоалгоритму Rijndael з урахуванням відомих показників стійкості і порівняння цих перетворень з перетвореннями, що використовують на практиці в інших криптоалгоритмах з використанням булевих функцій.

Проведений аналіз свідчить, що в якості основних показників стійкості нелінійних булевих функцій можна використовувати [2-7]:

1. Збалансованість функції.
2. Нелінійність функції, N_f.
3. Кореляційний іммунітет функції, $KI(k)$.
4. Критерій розповсюдження (суворий лавинний критерій) функції, $KP(k)$.
5. Алгебраїчний степінь функції, $deg(f)$.

Додатковими показниками стійкості є [6-9]:

1. Алгебраїчний степінь кожної змінної функції, $deg(f, x_i)$.
2. Кількість термів функції, $term(f)$.
3. Кількість термів функції, що містять змінну x_i, $term_{x_i}(f)$.
4. Коефіцієнт рівномірності мінімізації кореляції, $k_{рм}$.
5. Абсолютне значення кореляції функції, C_f.
6. Кількість векторів num_1 та num_2, при яких функція не задовольняє чи задовольняє критерію розповсюдження, а також num_3 і num_4, при яких функція не задовольняє чи задовольняє кореляційному імунітету.

Основні поняття і визначення

В цьому підрозділі приводяться основні поняття та визначення, які базуються на роботах [1-3, 8] та наших дослідженнях [9].

Булевою функцією f від n змінних є функція, що здійснює відображення усіх двійкових векторів $x = (x_1, \ldots, x_n)$ довжини n з поля $GF(2^n)$ у поле $GF(2)$. Звичайно булеві функції представляються в алгебраїчній нормальній формі і розглядаються як сума добутків складових координат. Поле $GF(2^n)$ складається з 2^n векторів α_i: $\alpha_0 = (0,\ldots,0,0), \alpha_1=(0,\ldots..,0,1),\ldots, \alpha_{2^n-1} = (1,\ldots,1,1)$, $\alpha_i \in V_n$, де V_n – векторний простір над $GF(2^n)$.

Послідовністю функції f називається послідовність символів (1,-1), визначена як $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$. *Таблицею істинності функції f* називається

послідовність символів (0,1), визначена як ($f(\alpha_0), f(\alpha_1),\ f(\alpha_{2^n-1})$). Послідовність функції f є *збалансованою*, якщо послідовність її символів (0,1) (послідовність символів (1,-1)) містить однакову кількість нулів і одиниць (одиниць і мінус одиниць):

$$| \{x \mid f(x) = 0 \} | = | \{x \mid f(x) = 1 \}| = 2^{n-1}. \quad (1)$$

Функція f є збалансованою, якщо збалансована її послідовність.

Афінною функцією f називається функція виду $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, де $a_j,\ c \in GF(2)$, $j = 1, 2,..., n$. Функція f називається *лінійною*, якщо $c = 0$.

Алгебраїчною нормальною формою функції називається її подання у вигляді

$$f(x_1,...,x_n) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \le i < j \le 1} a_{ij} x_i x_j \oplus ... \oplus a_{12...n} x_1 x_2 \cdots x_n \ .$$

Вагою Хеммінга вектора α (послідовності символів (0,1)), що позначається як $W(\alpha)$, є кількість одиниць у даному векторі (послідовності). *Відстанню Хеммінга* $d(f,g)$ між послідовностями двох функцій f і g є кількість позицій, у яких послідовності цих функцій відрізняються.

Нелінійність функції N_f - мінімальна відстань Хеммінга N_f між функцією f і множиною афінних функцій над $GF(2^n)$:

$$N_f = min\ \{d(f,\varphi)\}, \quad (2)$$

де φ - множина афінних функцій. Для збалансованої функції f над $GF(2^n)$ ($n \ge 3$) нелінійність N_f може досягати:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2\ , n = 2k, \\ \left\lfloor\!\left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor\!\right\rfloor, n = 2k+1, \end{cases}$$

де $\lfloor\!\lfloor x \rfloor\!\rfloor$ - максимальне парне ціле, менше або рівне x.

Функція f має *кореляційний імунітет* порядку k, $KI(k)$, якщо її перетворення Уолша задовільняє умові $F(\omega) = 0$ для усіх $\omega \in V_n$ таких, що $1 \le W(\omega) \le k$:

$$\forall \omega \in V_n \qquad F(\omega) = 0, \quad (3)$$

де перетворення Уолша $F(\omega)$ функції f над полем $GF(2^n)$ визначається у вигляді дійсних значенньь функції

$$F(\omega) = 2^{-n} \sum\nolimits_x (-1)^{f(x) \oplus \langle \omega, x \rangle}\ ,$$

$\langle \omega,x \rangle \in N$ ($\langle \omega,x \rangle$ - скалярний добуток $w_1x_1 \oplus \ldots \oplus w_nx_n$). Функція, що має кореляційний імунітет порядку k, називається кореляційно-імунною функцією *k-го* порядку.

Функція f над полем $GF(2^n)$ задовольняє:

- критерію розповсюдження щодо вектора α, $KP(\alpha)$, якщо функція $f(\mathrm{x}) \oplus f(\mathrm{x} \oplus \alpha)$ є збалансованою, $x \in V_n$, де $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2}; \quad (4)$$

- критерію розповсюдження степеня k, $KP(k)$, якщо задовольняється критерій розповсюдження щодо усіх векторів $\alpha \in V_n$ при $1 \le W(\alpha) \le k$:

$$P(f(\mathrm{x}) = f(x \oplus \alpha)) = \frac{1}{2} \qquad \forall \alpha : 1 \le W(\alpha) \le k; \quad (5)$$

- суворому лавинному критерію, *СЛК*, якщо f задовольняє критерію розповсюдження степеня 1:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2} \qquad \forall \alpha : W(\alpha) = 1. \quad (6)$$

Алгебраїчний степінь $deg(f)$ функції визначається степенем самого довгого доданку функції $term_j$, представленої в алгебраїчній нормальній формі:

$$deg\ (f) = \max_{0 \le j \le 2^n} \deg(term_j)\ . \tag{7}$$

Для збалансованих булевих функцій справедливий вираз:

$$k + deg(f) \le n - 1. \tag{8}$$

Алгебраїчний степінь кожної змінної x_i, $deg(f, x_i)$, визначається степенем самого довгого доданка функції, що містить x_i:

$$deg\ (f, x_i) = \max_{0 \le i < n} \deg(term_{x_i})\ . \tag{9}$$

Кількість термів функції, $term(f)$, визначається кількістю термів, з яких складається функція, представлена в алгебраїчній нормальній формі:

$$\text{term}(f) = \min_{0 \le j < 2^n} term_j\ . \tag{10}$$

Кількість термів функції, що містять змінну x_i, $term_{x_i}(f)$, визначається кількістю термів функції, що містять перемінну x_i:

$$term_{x_i}\ (f) = \min_j term_j(x_i) \tag{11}$$

Коефіцієнт рівномірності мінімізації кореляції

$$k_{рм} = \frac{k_{гр}}{r\ \cdot c_{ср}}, \tag{12}$$

де $k_{гр}$ - граничний коефіцієнт кореляції, r – вага ненульових значень коефіцієнтів кореляції, $c_{ср}$ – середнє значення коефіцієнта кореляції, і

$$r = \left| \frac{B}{2^n} - 2^{n-1} \right|, \qquad c_{ср} = \frac{\sum_{i=1}^{2^n} c_i}{2^n},$$

$$k_{гр} = \frac{\left|1 - 2^n\right| \cdot (c_n + c_{n+2})}{2},\ \text{для } V_{n+1} \quad \text{і} \qquad k_{гр} = \left|1 - 2^n\right| \cdot c_n,\ \text{для } V_n,$$

$$c_i(f, L_w) = 2^{-n} \sum_x (-1)^{f(x)} (-1)^{wx} = 2^{-n}\ \hat{F}(w), \tag{13}$$

де B – загальна кількість ненульових значень коефіцієнтів кореляції, c_i – значення коефіцієнта кореляції функції з множиною всіх афінних функцій L_w, c_n - коефіцієнт кореляції бент-функції з множиною всіх афінних функцій L_w над V_n, c_{n+2} – коефіцієнт кореляції бент-функции з множиною всіх афінних функцій L_w над V_{n+2}, визначає степінь рівномірності мінімізації функції кореляції.

Абсолютне значення функції кореляції

$$C_f = max\ |\ c(f, \ell_i)|, \tag{14}$$

визначає максимальне значення коефіцієнта кореляції функції f над V_n , $\ell_i \in L$, де ℓ_i, L – лінійна функція і множина усіх лінійних функцій відповідно.

Кількість векторів num_1 і num_2, при яких функція не задовільняє чи задівольняє критерію розповсюдження, визначається як

$$num_1\ = nPC(k), \tag{15}$$

$$num_2\ = PC(k), \tag{16}$$

де $nPC(k)$, $PC(k)$ – вектори, що не задовольняють чи задовольняють критерію розповсюдження.

Кількість векторів num_3 і num_4, при яких функція не задовільняє чи задовільняє кореляційному іммунітету, визначається як

$$num_3\ = nKI(k), \tag{17}$$

$$num_4 = KI(k), \quad (18)$$

де $nKI(k)$, $KI(k)$ - вектори, при яких функція не задовольняє чи задовольняє кореляційному імунітету.

Дослідження аналітичних властивостей нелінійних булевих функцій алгоритму Rijndael

Дослідження аналітичних властивостей виконувалось згідно показників, наведених у попередньому розділі.

З метою проведення дослідження аналітичних властивостей нелінійного перетворення по наявним послідовностям функцій (блоку підстановки) були відновлені поліноміальні форми нелінійних функцій FIPS 197, що складають блок підстановки, у відповідності з процедурою, наведеною у [3]. Процедура відновлення поліноміальної форми нелінійних функцій по послідовності ξ функції дозволяє по відомій послідовності $\xi = \varepsilon_0 \varepsilon_1 \ldots \varepsilon_{2^n-1}$ відновити вихідну форму булевих функцій.

Наявність поліноміальних форм булевих функцій, що використовуються, дозволяє досліджувати їх аналітичні властивості.

Основні показники стійкості.

Згідно виразу (1) функції Rijndael були перевірені на збалансованість. Всі функції є збалансованими, тобто кількість нулів n_0 в вихідній послідовності функції дорівнює кількості одиниць n_1: $n_0 = n_1 = 2^{8-1} = 128$.

Нелінійність функцій оцінювалась згідно виразу (2) як відстань Хемінга між послідовністю (таблицею істиності) функції та множиною послідовностей (таблиць істиності) афінних функцій (табл.1).

Степінь кореляційного іммунітету, $KI(k)$ визначався згідно виразу (3). Встановлено, що використовуємі функції не є кореляційно імунними (табл.1).

Степінь критерію розповсюдження, $KP(k)$, визначався згідно виразу (5). Встановлено, що використовуємі функції не задовольняють критерію розповсюдження (табл.1).

Алгебраїчний степінь $deg(f)$ визначався згідно виразу (7). Встановлено, що алгебраїчний степінь всіх функцій дорівнює $deg(f_1) = \ldots = deg(f_8) = 7$ (табл.1). Це максимально досяжний степінь для збалансованих функцій (8).

Допоміжні показники стійкості.

Алгебраїчний степінь кожної змінної, $deg(f, x_i)$, визначався згідно виразу (9).

Кількість термів функції, $term(f)$, визначалась згідно виразу (10).

Кількість термів функції, $term_{x_i}(f)$, що має змінну x_i, визначалась згідно виразу (11).

Коефіцієнт рівномірності мінімізації кореляції функції, $k_{рм}$, визначався згідно виразу (12).

Абсолютне значення кореляції функції, C_f, визначалось згідно виразу (14).

Кількість векторів num_1 та num_2, при яких функція не задовольняє та задовольняє критерію розповсюдження, визначалась згідно виразів (15) і (16) відповідно.

Кількість векторів num_3 та num_4, при яких функція не задовольняє та задовольняє кореляційному іммунітету, визначалась згідно виразів (17) і (18) відповідно.

В табл.1 наведені основні показники стійкості нелінійних функцій.

Таблиця 1

	Збалансованість	Нелінійність,N_f	Степінь кореляційного іммунітету, $KI(k)$	Степінь критерію розповсюдження, $KP(k)$	Алгебраїчний степінь функції, $deg(f)$
f_1	Так	114	0	0	7
f_2	Так	114	0	0	7
f_3	Так	112	0	0	7
f_4	Так	112	0	0	7
f_5	Так	112	0	0	7
f_6	Так	114	0	0	7
f_7	Так	114	0	0	7
f_8	Так	112	0	0	7

Аналіз табл.1 свідчить, що використовуємі функції є збалансованими, високо нелінійними та мають високий алгебраїчний степінь. Збалансованість функцій свідчить про стійкість до статистичних атак. Висока нелінійність функцій (112, 114) свідчить про високу стійкість функцій до кореляційних атак (максимально досяжна нелінійність для збалансованих функцій від восьми змінних дорівнює 118). Алгебраїчний степінь дорівнює 7 і є максимально досяжним для збалансованих функцій; високий степінь свідчить про стійкість до інтерполяційних і алгебраїчних атак.

Досліджувані функції не задовольняють критерію розповсюдження та не є кореляційно-іммунними функціями. Ефект розповсюдження забезпечується за рахунок застосування циклової функції. Відсутність кореляційного іммунітету можна пояснити тим, що, згідно (8), збільшення степеня кореляційного іммунітету обумовлює пониження алгебраїчного степеня. Тому розробники надали перевагу не кореляційному іммунітету, а високому алгебраїчному степеню. Більш детальний аналіз даних показників наведено в табл.4-7. В табл.2, 3 наведено допоміжні показники стійкості нелінійних функцій.

Таблиця 2

	Алгебраїчний степінь кожної перемінної, $deg(f, x_i)$	Кількість термів функції, $term(f_i)$	Коефіцієнт рівномірності мінімізації кореляції функції, $k_{рм}$	Абсолютне значення кореляції функції, C_f
f_1	7	131	1.175947	0,125
f_2	7	132	1.175947	0,125
f_3	7	145	1.175947	0,125
f_4	7	136	1.175947	0,125
f_5	7	131	1.175947	0,125
f_6	7	113	1.175947	0,125
f_7	7	111	1.175947	0,125
f_8	7	110	1.175947	0,125

Аналіз табл.2 свідчить, що функції мають високі допоміжні показники стійкості. Алгебраїчний степінь кожної змінної $deg(f, x_i)$, як і алгебраїчний степінь функції $deg(f)$, є максимальним і гарантує стійкість до атаки диференціалів вищих порядків. Кількість термів функції, $term(f_i)$, є високою (110-145) та забезпечує стійкість до інтерполяційних атак. Кількість термів функцій лежить у межах $term(f)/2 \pm 18$, де $term(f) = 2^n$ – загальна кількість всіх можливих мономів над простором V_n. Коефіцієнт рівномірності мінімізації кореляції функції, $k_{рм}$, та абсолютне значення кореляції функції C_f, мають низькі значення та забезпечують стійкість до кореляційних атак. За останніми двома показниками дані функції наближаються до бент-функцій (1 і 0,0625 відповідно), які, як відомо, мають мінімальну кореляцію з множиною всіх афінних функцій.

Таблиця 3

	Кількість термів функції, $term_{x_i}(f)$, що має змінну x_i							
	$term_{x_1}$	$term_{x_2}$	$term_{x_3}$	$term_{x_4}$	$term_{x_5}$	$term_{x_6}$	$term_{x_7}$	$term_{x_8}$
f_1	69	64	73	58	63	60	66	66
f_2	70	67	62	73	70	60	65	66
f_3	79	74	72	77	74	68	69	75
f_4	71	68	71	71	65	71	71	70
f_5	62	58	57	73	66	70	63	62
f_6	55	64	56	53	60	58	50	54
f_7	56	57	50	57	57	54	52	53
f_8	61	50	52	54	55	51	56	55

Аналіз табл.3 свідчить, що кількість термів функції, які мають змінну x_i, є фактично рівномірно розподіленим. Так, ця кількість термів функцій лежить у межах $term(f_i)/2 \pm 8$. Таким чином, даний показник, що забезпечує стійкість до інтерполяційних атак, можна вважати високим.

Як свідчать дані, наведені в таблиці 1, функції, що досліджуються, не задовольняють критерію розповсюдження (мають степінь 0) та не є кореляційно імунними, хоча дані показники в ряді робіт вважаються основними показниками стійкості. Тому доцільним є більш детальне дослідження даних показників.

Вважається, що критерій розповсюдження забезпечує динамічні властивості нелінійного перетворення: якщо заміна одного чи декількох біт на вході перетворення призводить з ймовірністю 0.5 до зміни вихідного стану, то така функція має гарні динамічні властивості, та навпаки. Тому, мабуть, більш доцільним є не досягнення будь-якого ступеню критерію розповсюдження, а досягнення того, щоб як можна більше векторів задовольняло критерію розповсюдження. В табл.4 на основі застосування (4) наведені динамічні властивості функцій.

Вважається, що кореляційний іммунітет відбиває стійкість до кореляційних атак: для протистояння атакам даного класу вихідне значення нелінійного перетворення не повинно залежати від вхідного значення. В табл. 4 на основі застосування (3) наведені кореляційні властивості функцій.

Крім того, в табл.4 наведена ймовірність найкращої лінійної апроксимації *Ap*, яка також може використовуватися при аналізі кореляційних властивостей функцій та визначається згідно виразу

$$Ap = 1 - \frac{N_f}{2^n},$$

де n – розмір векторного простору.

Таблиця 4

	Ймовірність найкращої лінійної апроксимації, *Ap*	# векторів num_2, задов. *KP*	# векторів num_1, не задов. *KP*	# векторів num_4, задов. *KI*	# векторів num_3, не задов. *KI*
f_1	$p = 0.5546875$	32(12,3%)	223(87,7%)	16(6,3%)	239(93,7%)
f_2	$p = 0.5546875$	32	223	16	239
f_3	$p = 0.5625$	32	223	16	239
f_4	$p = 0.5625$	32	223	16	239
f_5	$p = 0.5625$	32	223	16	239
f_6	$p = 0.5546875$	32	223	16	239
f_7	$p = 0.5546875$	32	223	16	239
f_8	$p = 0.5625$	32	223	16	239

Аналіз табл. 4 свідчить, що динамічні властивості функцій та їх кореляційні властивості в термінах перетворення Уолша не є задовільними. Тільки 12% всіх можливих векторів задовольняють критерію розповсюдження та тільки для 6% всіх можливих векторів вихідні значення статистично не залежать від них. Слід зазначити, що зазвичай критерій кореляційного іммунітету для блочних нелінійних перетворень не розглядається.

В табл.5 наведені динамічні властивості функцій в залежності від ваги Хемінга вхідного вектору, в табл.6 наведені узагальнені дані векторів, які задовольняють чи не задовольняють критерію розповсюдження, в процентному співвідношенні ("+" – вектор задовольняє критерію розповсюдження, "-" - вектор не задовольняє критерію розповсюдження). В табл.7 наведені кореляційні властивості функцій в залежності від ваги Хемінга вхідного вектору.

Таблиця 5

	Кількість векторів, що задовольняють *КР*							
	w(α)=1	w(α)=2	w(α)=3	w(α)=4	w(α)=5	w(α)=6	w(α)=7	w(α)=8
f_1	0	2	6	13	6	4	0	1
f_2	1	4	9	9	7	1	1	0
f_3	1	2	8	10	6	2	3	0
f_4	1	2	10	12	3	4	0	0
f_5	2	3	3	11	9	2	2	0
f_6	2	2	4	5	15	2	1	0
f_7	2	3	3	8	10	5	1	0
f_8	2	3	4	8	11	3	1	0
	Кількість векторів, що не задовольняють *КР*							
	w(α)=1	w(α)=2	w(α)=3	w(α)=4	w(α)=5	w(α)=6	w(α)=7	w(α)=8
f_1	8	26	50	57	50	24	8	0
f_2	7	24	47	61	49	27	7	1
f_3	7	26	48	60	50	26	5	1
f_4	7	26	46	58	53	24	8	1
f_5	6	25	53	59	47	26	6	1
f_6	6	26	52	65	41	26	7	1
f_7	6	25	53	62	46	21	7	1
f_8	6	25	52	62	45	23	7	1

Таблиця 6

	Кількість векторів, що задовольняють чи не задовольняють *КР,* у процентному співвідношенні, %															
	w(α)=1		w(α)=2		w(α)=3		w(α)=4		w(α)=5		w(α)=6		w(α)=7		w(α)=8	
	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-
f_1	0	100	7,1	92,9	10,7	89,3	18,6	81,4	10,7	89,3	14,3	85,7	0	100	100	0
f_2	12,5	87,5	14,3	85,7	16,1	83,9	12,9	87,1	12,5	87,5	3,6	96,4	12,5	87,5	0	100
f_3	12,5	87,5	7,1	92,9	14,3	85,7	14,3	85,7	10,7	89,3	7,1	92,9	37,5	62,5	0	100
f_4	12,5	87,5	7,1	92,9	17,9	82,1	17,2	82,8	5,4	94,6	14,3	85,7	0	100	0	100
f_5	25	75	10,7	89,3	5,4	94,6	15,7	84,3	16,1	83,9	7,1	92,9	25	75	0	100
f_6	25	75	7,1	92,9	7,5	92,5	7,2	92,8	26,8	73,2	7,1	92,9	12,5	87,5	0	100
f_7	25	75	10,7	89,3	5,4	94,6	11,4	88,6	17,9	82,1	25	75	12,5	87,5	0	100
f_8	25	75	10,7	89,3	7,5	92,5	11,4	88,6	19,7	80,3	17,9	82,1	12,5	87,5	0	100

Аналіз таблиць 5, 6 свідчить, що динамічні властивості функцій не є задовільними: так, для векторів з w(α)=2...7 критерію розповсюдження задовольняють в найкращому випадку 37% векторів (w(α)=7, f_3), для більшості функцій дане значення не перевищує 20%.

Таблиця 7

	Кількість векторів, що задовольняє *KI*							
	w(α)=1	w(α)=2	w(α)=3	w(α)=4	w(α)=5	w(α)=6	w(α)=7	w(α)=8
f_1	0	1	3	6	5	1	0	0
f_2	1	2	5	1	5	1	1	0
f_3	0	3	1	6	5	1	0	0
f_4	1	2	2	6	5	0	0	0
f_5	0	2	4	6	3	0	1	0
f_6	1	2	2	6	3	2	0	0
f_7	1	3	1	6	2	1	2	0
f_8	0	2	3	6	2	2	1	0
	Кількість векторів, що не задовольняє *KI*							
	w(α)=1	w(α)=2	w(α)=3	w(α)=4	w(α)=5	w(α)=6	w(α)=7	w(α)=8
f_1	8	27	53	64	51	27	8	1
f_2	7	26	51	59	51	27	7	1
f_3	8	25	55	64	51	27	8	1
f_4	7	26	54	64	51	28	8	1
f_5	8	26	52	64	53	28	7	1
f_6	7	26	54	64	53	26	8	1
f_7	7	25	55	64	54	27	6	1
f_8	8	26	53	64	54	26	7	1

Аналіз табл.7 свідчить, що всі функції мають незадовільні характеристики в термінах перетворення Уолша, тобто для більшості вхідних значень функцій буде існувати статистична залежність з вихідними векторами.

Відомо [2], що при розробці нелінійних функцій розробники намагаються рівномірно мінімізувати кореляцію нелінійних функцій з множиною всіх афінних функцій, оскільки сума всіх коефіцієнтів кореляції $c_i(f, L_w)$, (13), завжди буде дорівнювати 1:

$$\sum_i c_i\ (f, L_w) = 1. \qquad (23)$$

Аналіз виразу (23) дозволяє зробити наступні висновки:

- Сумарна кореляція не залежить від вибору функції *f*.
- Оскільки величина $\sum_i c_i$ є константою, при виборі нелінійної функції доцільно рівномірно мінімізувати кореляцію.
- Нульова кореляція з деякими лінійними функціями (фазами) визначає більш високу кореляцію з іншими лінійними функціями (фазами).

Підсумовуючи, можна зробити головний висновок: при розгляді показників стійкості нелінійних функцій необхідним є розгляд їх спектральних властивостей як властивостей, що відбивають степінь рівномірності мінімізації кореляції.

Аналіз проведених досліджень свідчить, що спектральні властивості функцій криптоалгоритму Rijndael (AES) є ідентичними та фактично мають рівномірно мінімізовані коефіцієнти кореляції. Це доводить, що вони мають високу стійкість до кореляційних атак.

Порівнянння блоків підстановок відомих симетричних криптоалгоритмів

Для адекватної оцінки результатів дослідження властивостей функцій криптоалгоритму Rijndael доцільним є розгляд властивостей функцій, що використовуються в інших криптоалгоритмах: блокових та симетричних шифрах, хеш-функціях. В якості прототипів розглядаються блоки підстановки блокового шифру *Camellia*, поточного шифру *Sober t-32* та

хеш-функції *Whirlpool* [10]. В табл.8 наведені порівняльні характеристики показників стійкості функцій, що розглядаються; всі розрахунки виконувалися за допомогою виразів (1 – 22).

Таблиця 8

	БШ Rijndael	БШ Camellia	ПШ Sober t-32	ХФ Whirlpool
	Нелінійність			
f_1	114	112	112	110
f_2	114	112	112	104
f_3	112	112	112	108
f_4	112	112	112	102
f_5	112	112	112	106
f_6	114	112	112	102
f_7	114	112	112	108
f_8	112	112	112	106
	Степінь критерію розповсюдження, $KP(k)$			
$f_1 - f_8$	0	0	0	0
	Степінь кореляційного іммунітету, $KI(k)$			
$f_1 - f_8$	0	0	0	0
	Алгебраїчний степінь функції, $deg(f)$			
$f_1 - f_8$	7	7	6	7
	Алгебраїчний степінь кожної перемінної, $deg(f, x_i)$			
$f_1 - f_8$	7	7	6	7
	Кількість термів функції, $term(f_i)$			
f_1	131	126	127	142
f_2	132	129	133	131
f_3	145	133	125	128
f_4	136	129	130	133
f_5	131	134	120	128
f_6	113	125	122	129
f_7	111	131	123	129
f_8	110	127	125	125
	Коефіцієнт рівномірності мінімізації кореляції функції, $k_{рм}$			
f_1	1.175947	1,175947	1,227053	1,212432
f_2	1,175947	1,175947	1,209524	1,251256
f_3	1,175947	1,175947	1,209524	1,233034
f_4	1,175947	1,175947	1,189715	1,248179
f_5	1,175947	1,175947	1,221154	1,248183
f_6	1,175947	1,175947	1,251232	1,302597
f_7	1,175947	1,175947	1,195313	1,233032
f_8	1,175947	1,175947	1,233010	1,254330
	Абсолютне значення кореляції функції, C_f			
f_1	0,125	0,125	0,125	0,171875
f_2	0,125	0,125	0,125	0,203125
f_3	0,125	0,125	0,125	0,140625
f_4	0,125	0,125	0,125	0,203125
f_5	0,125	0,125	0,125	0,1875
f_6	0,125	0,125	0,125	0,21875
f_7	0,125	0,125	0,125	0,15625
f_8	0,125	0,125	0,125	0,203125

Аналіз табл.8 свідчить, що нелінійні функції, які використовуються у криптоалгоритмі Rijndael, не поступаються за своїми показниками стійкості іншим існуючим нелінійним перетворенням, а за такими показниками, як нелінійність, степінь рівномірності мінімізації кореляції – і переважають. Аналіз спектральних характеристик свідчить, що за даними показниками нелінійні перетворення криптоалгоритму Rijndael не поступаються всім іншим:

ці показники аналогічні показникам криптоалгоритму Camellia та є вищими за показники криптоалгоритмів Sober t-32, Whirlpool.

Тому на основі аналізу криптографічних властивостей відомих криптоалгоритмів та криптоалгоритму Rijndael можна зробити висновки, що нілінійні перетворення криптоалгоритму Rijndael мають високі показники стійкості та не поступаються за ними відомим нелінійним перетворенням.

Висновки.

1. Нелінійні функції, що використовуються в блоці підстановки БШ Rijndael, мають привабливі основні і допоміжні показники стійкості: функції є збалансованими, високо нелінійними та з високим алгебраїчним ступенем як самої функції, так і кожної перемінної, і т.і.
2. Нелінійні функції, що використовуються в блоці підстановки БШ Rijndael, мають високу стійкість до статистичних атак: їх послідовності збалансовані.
3. Нелінійні функції, що використовуються в блоці підстановки БШ Rijndael, мають високу стійкість до кореляційних атак: вони мають високу нелінійність та низькі значення коефіцієнтів рівномірної мінімізації кореляції та абсолютного значення кореляції функції.
4. Нелінійні функції, що використовуються в блоці підстановки БШ Rijndael, мають високу стійкість до інтерполяційних та алгебраїчних атак, атак криптоаналізу методом диференціалів вищих порядків: алгебраїчний степінь функції, кожної перемінної та кількість термів, що мають змінну x_i, є високими.
5. Широко використовувані при побудові нелінійних функцій критерії розповсюдження і кореляційного іммунітету на практиці не використовуються. Так, функції блоку підстановки БШ Rijndael, блоків підстановки ПШ Sober t-32 та БШ Camellia не задовольняють критеріям розповсюдження та кореляційного іммунітету.
6. Замість досягнення будь-якого ступеню критерію розповсюдження або кореляційного іммунітету розробники намагаються серед основних показників стійкості максимізувати нелінійність функції та її алгебраїчний степінь.
7. Для протистояння кореляційним атакам розробники разом з максимізацією нелінійності намагаються рівномірно мінімізувати кореляцію використовуваних функцій з множиною криптографічно слабких функцій.

Список літератури: 1.*B.Schneier*. Applied Cryptography. 2nd edition, John Wiley & Sons, New York,1996. 2.*W.Maier, O.Staffelbach*. Nonlinearity criteria for cryptographic functions // In Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562,1990. 3.*J. Seberry, X.-M. Zhang and Y.Zheng*. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // In Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995. 4.*P.Camion, C.Carlet, P.Charpin, N.Sendrier*. On Correlation-immune functions // In Advances in Cryptology – Crypto'91, vol.576, Lecture Notes in Computer Science, Springer-Verlag. - P.87-100. 5.*X.-M. Zhang and Y.Zheng*. Cryptographically resilient functions // IEEE Transactions on Information Theory, September 1997, pp.457- 478. 6.*Y.Tarannikov*. New constructions of resilient Boolean functions with maximal nonlinearity. – Moscow State University. – 2000. – http://www.mech.math.msu.ru. 7.*B.Preneel, R. Govaerts, and J. Vandewalle*. Boolean functions satisfying higher order propagation criteria // In Lecture Notes in Computer Science 547; Advances in Cryplology: Proc. Eurocrypt'91, 1991, pp. 141-152. Berlin: Springer-Verlag. 8. *С.А.Головашич*. Метод построения управляемых S-блоков с предельными показателями нелинейности. // Радиотехника. Всеукраинский межведомственный научно-технический сборник. - 1999. - № 110. - С. 84 - 90. 9.*Потий А.В, Избенко Ю.А*. Обоснование выбора метода построения криптографически стойких булевых функций // Радиотехника. Всеукраинский межведомственный научно-технический сборник. - 2002. - № 126. - С. 132 - 138. 10. NESSIE Call for Cryptographic Primitives, Version 2.2, 8th March 2000: http://cryptonessie.org.