УДК 004.056.55

# ДОСЛІДЖЕННЯ МЕТОДІВ ФОРМУВАННЯ ВИПАДКОВИХ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІН СИМЕТРИЧНИХ ШИФРІВ

*О. О. КУЗНЕЦОВ, І. М. БІЛОЗЕРЦЕВ, А. І. ПУШКАРЬОВ, Ю. І. ГОРБЕНКО, В. В. ОНОПРІЄНКО*

Обгрунтовуються основні показники ефективності криптографічних булевих функцій та векторних відображень, які застосовуються у якості вузлів ускладнення симетричних криптоперетворень. Досліджуються евристичні методи формування криптографічних булевих функцій та нелінійних S-блоків симетричних шифрів, що відповідають встановленим вимогам безпеки. Обгрунтовуються перспективні напрямки подальших досліджень з метою удосконалення евристичних методів синтезу випадкових вузлів заміни.

*Ключові слова:* симетричні криптоперетворення, випадкові нелінійні вузли заміни, евристичні методи генерації, показники криптографічної стійкості.

## ВСТУП

Для забезпеченні послуг інформаційної безпеки (конфіденційності, цілісності, неспростовності тощо) зазвичай застосовують симетричні шифри [1, 2]. З погляду на забезпечувану стійкість, швидкодію та надійність симетричні криптоперетворення мають певну перевагу та зручність у практичному використанні [2].

Випадкові нелінійні вузли заміни (криптографічні булеві функції, векторні відображення або S-блоки) відіграють суттєву роль у забезпеченні безпеки симетричних перетворень. Зокрема їх криптографічні властивості безпосередньо впливають на стійкість шифрів до різних криптоаналітичних атак [3–19]. Отже питання синтезу випадкових вузлів заміни з необхідними криптографічними характеристиками є безумовно актуальним та важливим завданням [20–23].

## 1. КРИТЕРІЇ ТА ПОКАЗНИКИ ЕФЕКТИВНОСТІ НЕЛІНІЙНИХ ВУЗЛІВ УСКЛАДНЕННЯ

Розглянемо критерії та показники ефективності нелінійних вузлів замін, що безпосередньо впливають на рівень стійкості сучасних симетричних шифрів до різних криптоаналітичних атак [3–19].

У більшості відомих робіт в області аналізу і синтезу нелінійних вузлів замін сучасних симетричних шифрів використовується математичний апарат криптографічних булевих функцій [3–12]. При цьому векторні відображення (S-блоки) подаються сукупністю компонентних булевих функцій, властивості яких характеризують ефективність нелінійного вузла замін.

Як основні критерії і показники ефективності використовують [3–12]: збалансованість і нелінійність компонентних булевих функцій; кореляційний імунітет; критерій поширення; алгебраїчний степінь; значення функції автокореляції.

*Булевою функцією f* від $n$ змінних є функція, що здійснює відображення з поля $GF(2^n)$ усіх двійкових векторів $x = (x_1, \ldots, x_n)$ довжини $n$ у полі $GF(2)$.

Зазвичай булеві функції подаються в нормальній алгебраїчній формі.

Поле $GF(2^n)$ складається з $2^n$ векторів $\alpha_i$: $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,...,0,1),...,$ $\alpha_{2^n-1} = (1,...,1,1)$, $\alpha_i \in V_n$ де $V_n$ – векторний простір в $GF(2^n)$.

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

*Таблицею істинності* функції $f$ називається (0,1) -послідовність, визначена як $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$.

Послідовність функції $f$ є *збалансованою*, якщо її (0,1)-послідовність ((1, -1)-послідовність) містить однакову кількість нулів і одиниць (одиниць і мінус одиниць). Функція $f$ є збалансованою, якщо збалансована її послідовність.

Еквівалентне визначення: функція $f$ над $GF(2^n)$ є збалансованою, якщо її вихідні значення є рівноімовірними:

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

*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 $c = 0$.

*Вагою Хемінга* вектора $\alpha$, що позначається як $W(\alpha)$, є кількість одиниць у векторі (послідовності). *Відстанню Хемінга d(f, g)* між послідовностями двох функцій $f$ і $g$ називається кількість позицій, в яких відрізняються послідовності цих функцій.

*Нелінійність $N_S$* перетворення – мінімальна відстань Хемінга між вихідною послідовністю $S$ і усіма вихідними послідовностями афінних функцій над деяким полем:

$$N_s = \min\{d(S,\varphi)\},$$

де $\varphi$ – безліч афінних функцій.

*Нелінійність функції $N_f$* – мінімальна відстань Хемінга $N_f$ між функцією $f$ і усіма афінними функціями над $GF(2^n)$:

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

де φ – безліч афінних функцій.

Для довільної функції $f$ нелінійність $N_f$ над $GF(2^n)$ може досягати

$$N_f \le 2^{n-1} - 2^{n/2-1}.$$

Для збалансованої функції $f$ над $GF(2^n)$ ($n \ge 3$) нелінійність $N_f$ може досягати:

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

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

Функція $f$ має *кореляційний імунітет* порядку $k$, якщо вихідна послідовність функції $y \in Y$ статистично не залежить від будь-якої підмножини з $k$ вхідних координат :

$$\forall \{x_1,...,x_k\} \;\; P(y \in Y \mid \{x_1,...,x_k\} \in X) \;=\; P(y \in Y).$$

Еквівалентне визначення кореляційного імунітету в термінах перетворення Уолша: функція $f$ над полем $GF(2^n)$ має кореляційний імунітет порядку $k$, $KI(k)$, якщо її перетворення Уолша задовольняє рівності $F(\omega) = 0$ для усіх $\omega \in V_n$ такий, що $1 \le W(\omega) \le k$:

$$\forall \omega \in V_n \;\; F(\varpi) \;=\; 0 \quad KI(f) = k \;.$$

Перетворення Уолша $F(\omega)$ функції $f$ над полем $GF(2^n)$ визначається тоді, як що набуває дійних значень функція

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

де $\omega \in V_n$, $f(x)$, $\langle \omega, x \rangle \in N$ ($\langle \omega, x \rangle$ – скалярний добуток $w_1x_1 \oplus \ldots \oplus w_nx_n$.

*Кореляційно-імунна функція* $k$-го порядку – функція, що має кореляційний імунітет порядку $k$. Збалансовані кореляційно-імунні функції називаються еластичними функціями.

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

– *критерію поширення* відносно вектора $a$, КР($a$), якщо функція $f(x) \oplus f(x \oplus a)$ є збалансованою, $x \in V_n$, де $x = (x_1, x_2, \ldots, x_n)$

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

– *критерію поширення* міри $k$, КР($k$), якщо задовольняється критерій поширення відносно усіх векторів $a \in V_n$ при $1 \le W(a) \le k$:

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

– *суворому лавинному критерію* (СЛК), якщо $f$ задовольняє критерій поширення степеня 1:

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

*Алгебраїчний степінь deg(f)* є степінь найдовшого доданка функції, поданої в алгебраїчній нормальній формі.

Автокореляційна функція $\hat{r}(s)$ для $s \in 0 \ldots 2^n - 1$ визначена як

$$\hat{r}(s) = \sum_{x=0}^{2^n-1} \hat{f}(x) \hat{f}(x \oplus s).$$

Говорять, що функція $f$ задовольняє *характеристику поширення* $m$, якщо

$$(1 \le |s| \le m) \Rightarrow |\hat{r}(s)| = 0.$$

Аналогічно, автокореляція $AC(f)$ функції $f$ визначається як модуль найбільшого значення $\hat{r}(s)$. :

$$AC(f) = \max_{s \ne 0} \left| \sum_x \hat{f}(x) \hat{f}(x \oplus s) \right| = \max_{s \ne 0} |\hat{r}(s)|.$$

Автокореляція забезпечує витік інформаційного потоку з входу на вихід функції. У деяких випадках дуже сильний взаємозв'язок може бути представлений як лінійна структура (для яких справедлива рівність $f(x) \oplus f(x \oplus s) = 1$ або $f(x) \oplus f(x \oplus s) = 0$). Вони, як правило, уникаються.

Розглянуті критерії і показники ефективності S-блоків відображають здатність нелінійного вузла протистояти атакам певного типу. Нелінійність, критерій поширення і кореляційна імунність характеризують здатність протистояти кореляційним атакам, алгебраїчний ступінь і автокореляція – аналітичним атакам, збалансованість – статистичним.

Найбільшого розвитку в ході формування та аналітичного опису властивостей векторних відображень (S-блоків) набули методи булевої алгебри та, зокрема, булевих функцій [3–16]. Дійсно, оскільки булева функція $f(x)$ від $n$ змінних – це відображення

$$f(x) : GF(2)^n \to GF(2),$$

де $x = (x_1, \ldots, x_n)$, тоді векторну функцію можна подати через множину булевих функцій так:

*Векторна* $(n,m)$ *булева функція* (S-блок) – це відображення

$$F = F(x_1,...,x_n) = (f_1(x_1,...,x_n),...,f_m(x_1,...,x_n)) :$$

$$GF(2)^n \to GF(2)^m. \qquad (1)$$

Зрозуміло, що кожна компонентна функція $f_i, i = 1,...,m$ – це булева функція від $n$ змінних.

Оптимізація окремих криптографічних показників однієї із компонентних функцій $f_i, i = 1,...,m$ із (1) може призвести до суттєвого погіршення показників інших функцій і навпаки. Отже необхідно розробити математичний апарат та відповідне програмне забезпечення, які при прийнятній обчислювальній складності забезпечать комплексне підвищення основних криптографічних показників усіх компонентних булевих функцій $f_i, i = 1,...,m$ із виразу (1) та всіх їхніх лінійних комбінацій.

Очевидно, що перевірка усіх можливих критеріїв значно зменшить швидкодію алгоритму генерації, тому до переліку критеріїв слід включати лише найбільш критичні, з точки зору стійкості до основних видів криптоаналітичних атак. Сукупність усіх можливих критеріїв оцінки розділятимемо на *безумовні* та *умовні* [2].

До безумовних критеріїв належать ті критерії, виконання яких є обов'язковим, тобто безумовним, для забезпечення генерованою підстановкою криптографічної стійкості від основних видів крипто-аналітичних атак [2]. У свою чергу до умовних критеріїв належать додаткові критерії ефективності, які можна застосувати для порівняння між собою нелінійних вузлів, що відповідають безумовним критеріям [2].

Далі розглянемо перелік обраних безумовних критеріїв, яким має відповідати байтова бієктивна підстановка, тобто при $n = m = 8$.

1. *Нелінійність.* Даний критерій забезпечує стійкість до лінійного криптоаналізу [3–19]. Дійсно, для S-блоку S розмірністю $n \times m$ співвідношення між його нелінійністю $N_F$ і максимумом таблиці лінійних апроксимацій $LAT_{\max}$ записується в такий спосіб:

$$N_F = 2^{n-1} - LAT_{\max}.$$

Позначимо цей критерій $W_{\delta 1}$.

2. *Алгебраїчний степінь.* Максимальне значення алгебраїчного степеня забезпечує стійкість до статистичних атак [3–19]. Позначимо цей критерій $W_{\delta 2}$.

3. *Максимум таблиці диференційних різниць (або δ - рівномірність).* Мінімізація значення нетривіального максимуму таблиці різниць забезпечує високий рівень стійкості до диференційного критоаналізу [3–19]. Для S-блоку S розмірністю $n \times m$ співвідношення між його автокореляцією $AC$ і максимумом *таблиці диференційних різниць* $DDT_{\max}$ має вигляд [8]:

$$DDT_{\max} \geq 2^{n-m} + 2^{-m} AC.$$

Позначимо цей критерій $W_{\delta 3}$.

4. *Алгебраїчний імунітет.* Значення алгебраїчного імунітету $AI = 3$ значно підвищує її стійкість до алгебраїчних атак [11, 12]. Позначимо цей критерій як $W_{\delta 4}$.

5. *Відсутність фіксованих точок та циклів менше за 4.* Даний критерій S-блоків застосовується у більшості шифрів для захисту від статистичних атак [3–19]. Відповідно, позначимо цей критерій $W_{\delta 5}$.

Докладне визначення та порядок розрахунку окремих криптографічних показників наведено, наприклад, у [3–8].

З урахуванням наведених вище безумовних критеріїв $W_{\delta 1} - W_{\delta 5}$ відповідно до [2], можна сформувати *функцію відповідності* підстановки:

$$f_{фв}(\ ) = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5}.$$

Функція відповідності становить безумовний інтегральний критерій, за допомогою якого можна оцінити якість згенерованого S-блоку та прийняти рішення про його відповідність вимогам криптографічної стійкості.

До умовних належать ті критерії, виконання яких є бажаним, але не обов'язковим результатом [2]. Наприклад, складність або час генерації підстановки бажано зменшити, бо це прискорить досягнення мети – формування S-блоку із необхідними (безумовними) показниками стійкості.

Отже, мету та завдання розробки методів генерації нелінійних вузлів заміни можна формально подати у вигляді безумовного інтегрального критерію при мінімізації складності (часу):

$$S \to \min \left| \left\{ f_{фв}(\ ) = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5} \right\}.$$

Вирішення зазначеного завдання полягає у пошуку сукупності певних перетворень (комплементацій) над компонентними булевими функціями $f_i, i = 1,...,m$ із (1), які за кінцеве число кроків дозволять досягти встановлених (бажаних) значень криптографічних показників.

Проведемо аналіз та порівняльні дослідження різних методів генерації нелінійних вузлів ускладнення.

## 2. МЕТОДИ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ВУЗЛІВ УСКЛАДНЕННЯ

Методи генерації криптографічних булевих функцій можна умовно розділити на три типи: методи випадкової генерації, алгебраїчні методи та евристичні методи [12, 20, 22, 23].

Методи випадкової генерації, попри свою простоту, не можуть бути використані для ефективної генерації булевих функцій з високими показниками криптографічної стійкості при $n \geq 8$. Алгебраїчні методи, зі свого боку, є високоефективними та не вимагають потужних обчислювальних ресурсів, але булеві функції, сформовані із застосуванням цих методів, мають низьку алгебраїчну складність і є потенційно вразливими до деяких сучасних криптоаналітичних атак. Еврис-

тичні методи [3 – 14], серед усіх вищезгаданих, є найсучаснішими та дозволяють генерувати булеві функції з криптографічними характеристиками, що наближені до максимально можливих.

Таким чином серед різних методів генерації нелінійних вузлів заміни [14] найбільш перспективними вважаються евристичні методи [12, 13, 20–23]. Порівняно із методами випадкової генерації вони значно простіше в реалізації, а порівняно із алгебраїчними дозволяють оптимізувати різні криптографічні показники та позбутися детермінованих, тобто, заздалегідь прогнозованих конструкцій [22, 23].

В основі більшості евристичних методів лежать ітеративні процедури підвищення певних показників криптографічної стійкості нелінійного вузла заміни. Наприклад, у відомому методі градієнтного підйому [15] шляхом комплементації деякої позиції в таблиці істинності початкової функції підвищується нелінійність. Критерієм градієнтного пошуку є максимізація відстані за Хемінгом між формованою послідовністю і послідовностями лінійних функцій.

### 2.1. Метод градієнтного підйому

Суть методу полягає в підвищенні нелінійності випадкової булевої функції шляхом комплементації деякої позиції в таблиці істинності початкової функції. Кожна позиція таблиці істинності відповідає унікальним вхідним даним. Метод дозволяє створити повний список/перелік таких вхідних даних функції, що комплементація будь-якої відповідної даному входу вихідної позиції в таблиці істинності збільшуватиме нелінійність даної функції. Список/перелік таких позицій в таблиці істинності позначається як 1 - *Improvement Set* функції $f(x)$, або $1-IS_f$ [42].

*Визначення 1.* [15]. Нехай $g(x)=f(x)\oplus 1$ для $x=x_a$ та $g(x)=f(x)$ для всіх інших $x$. Якщо $N_g > N_f$, то $x_a \in 1-IS_f$.

В [15] подано швидкий систематичний метод визначення множини $1-IS_f$ заданої булевої функції шляхом використання її таблиці істинності і перетворень Уолша-Адамара. Для знаходження множини $1-IS_f$ заданої булевої функції необхідно спочатку визначити значення коефіцієнтів перетворення Уолша-Адамара, які відповідали б величинам, близьким до абсолютного значення максимального коефіцієнта, $WHT_{\max}$.

*Визначення 2.* Нехай $f(x)$, є булевою функцією з перетворенням Уолша-Адамара $F(w)$, де $WHT_{\max}$ позначає максимальне абсолютне значення $F(w)$. Тоді існуватиме одна або більше лінійних функцій $L_w(x)$, що мають мінімальну відстань до функції $f(x)$, і для даних $w$ буде справедлива рівність $|F(w)|=WHT_{\max}$.

Визначається так:

$$W_1^+ = \{w : F(w) = WHT_{\max}\} \text{ та}$$

$$W_1^- = \{w : F(w) = -WHT_{\max}\}.$$

Також визначаються множини $w$, для яких значення $WHT$ наближені до максимуму:

$$W_2^+ = \{w : F(w) = WHT_{\max} - 2\},$$

$$W_2^- = \{w : F(w) = -(WHT_{\max} - 2)\}$$

$$W_3^+ = \{w : F(w) = WHT_{\max} - 4\} \text{ та}$$

$$W_3^- = \{w : F(w) = -(WHT_{\max} - 4)\}.$$

Коли таблиця істинності змінюється рівно в одній позиції, всі значення $WHT$ змінюються на +2 або -2. З цього випливає, що для збільшення нелінійності всі значення $WHT$ у множині $W_1^+$ мають бути змінені на -2, всі значення $WHT$ у множині $W_1^-$ мають бути змінені на 2, а також всі значення $WHT$ у множині $W_2^+$ мають бути змінені на -2, всі значення $WHT$ у множині $W_2^-$ мають бути змінені на 2. Якщо перші дві умови є очевидними, то наступні дві умови потрібні для того, щоб всі інші значення $|F(w)|$ залишалися меншими, ніж $WHT_{\max}$. Дані умови можуть бути подані у вигляді простих тестів.

*Теорема 1* [15]. Нехай дана деяка булева функція $f(x)$ з $WHT\ F(w)$, і визначені множини $W^+ = W_1^+ \cap W_2^+$ та $W^- = W_1^- \cap W_2^-$. Тоді для деякого входу $x$ існує елемент з *Improvement Set* і виконуються такі дві умови:

$$f(x) = L_w(x) \text{ та для усіх } w \in W^+, \text{ та}$$

$$f(x) \neq L_w(x) \text{ та для усіх } w \in W^-.$$

Якщо функція $f(x)$ не збалансована, зниження незбалансованості може бути досягнуто використанням додаткового обмеження:

якщо $F(0) > 0$, $f(x) = 0$, інакше $f(x) = 0$.

Критерієм градієнтного пошуку є максимізація відстані за Хемінгом між формованою послідовністю і послідовностями лінійних функцій. Після поновлення алгебраїчної форми булевої функції виробляються аналогічні операції: виконується перетворення Уолша-Адамара $WHT$ і знаходяться максимальні значення коефіцієнтів перетворення; формується множина *Improvement Set*; знаходяться елементи послідовності функції, що збігаються з елементами послідовності найближчої лінійної форми; інвертування елементів,

що збіглися, і підвищення нелінійності функції, за допомогою «віддалення» від найближчої лінійної функції. Далі виконуються чергові ітерації, аналогічні розглянутим вище.

Проведені у [16, 17, 22] дослідження показали, що метод градієнтного підйому з [15] обчислювально витратний і, з великою кількістю аргументів булевої функції, вимагає виконання значного числа повторюваних ітерацій. Для зниження обчислювальної складності в [16, 17, 22] запропоновано метод градієнтного спуску з бент-послідовностями як вхідні дані. За своєю сутністю цей метод наслідує окремі перетворення методу градієнтного підйому з [15], але, як показано у [16, 17, 22], вимагає значно менших обчислювальних витрат.

### 2.2. Метод градієнтного спуску

Даний метод заснований на комплементації позицій бент-послідовностей для градієнтного пошуку збалансованих булевих функцій за критерієм максимізації відстані Хеммінга між сформованими послідовностями і послідовностями всіх лінійних функцій. Це дозволяє знизити обчислювальні витрати на пошук булевих функцій з необхідними криптографічними властивостями [16, 17, 22].

Основною ідеєю методу градієнтного спуску є ефективне зниження нелінійності заданих бент-послідовностей при кожній з $2^{n/2-1}$ обов'язкових комплементацій. Для досягнення заданої верхньої межі нелінійності необхідно із загального числа позицій $x$ таблиці істинності, що підлягають комплементації, визначити те число позицій $y$, зміна яких має наслідком зміну $WHT$ на +2, і те число позицій $z$, зміна яких має наслідком зміну $WHT$ на -2, $x = y + z$.

Після розрахунку необхідного числа комплементацій бент-послідовності на першому кроці евристичного пошуку виконується перетворення Уолша-Адамара $WHT$ і визначається максимальна відстань за Хеммінгом до однієї або декількох послідовностей лінійних функцій $L_i(x)$. Ця операція відповідає вибору нульового значення коефіцієнтів перетворення Уолша-Адамара $WHT$, після чого формується безліч лінійних функцій, що становлять *Improvement Set*. Далі проводиться інвертування елементів послідовності бент-функції, які збігаються з елементами послідовностей лінійних функцій з безлічі *Improvement Set*. У результаті незбалансованість функції знижується, але знижується так само і нелінійність, тобто послідовність функції не є вже максимально віддаленою від послідовностей лінійних функцій $L_i(x)$. На наступній ітерації всі операції повторюються. Таким чином, як критерій градієнтного пошуку криптографічних функцій, пропонованим методом є максимізація мінімальної відстані за Хеммінгом формованої послідовності і послідовностей лінійних функцій [22].

### 2.3. Переставний метод пошуку випадкових S-блоків

У дисертації [12] та статтях [18, 19] набули подальшого розвитку евристичні методи. Зокрема, методи градієнтного пошуку булевих функцій було розширено та застосовано для генерації векторних відображень (S-блоків) з необхідними властивостями.

У розробленому в [12, 18, 19] методі пропонується використовувати той самий підхід, як і у розглянутому вище методі градієнтного спуску, однак з двома істотними відмінностями [12]:

– замість булевих функцій використовувати векторні булеві функції;

– замість бент-функцій (послідовностей) використовувати векторні булеві функції (підстановки) з максимальними показниками δ -рівномірності або з максимальним значенням нелінійності.

Зміна необхідної кількості біт у бент-послідовності не гарантує досягнення нелінійності, близької до максимальної. Для векторного випадку в [21] було доведено твердження, що при обміні місцями двох значень в деякій перестановці значення, нелінійності і δ-рівномірність відрізнятимуться на невелике значення (± 2 та ± 4, відповідно). Ґрунтуючись на цьому і було розроблено більшість відомих евристичних методів пошуку нелінійних вузлів ускладнення.

Метод, що запропоновано в [12] та досліджено в [18, 19], приймає на вхід перестановки векторну функцію $F$ з мінімальним показником δ-рівномірності і кількість значень (*NP*), які необхідно поміняти місцями для досягнення оптимальних криптографічних показників.

Основні кроки методу наведено нижче [12].

а) Генерація підстановки $S$ на основі обраної переставної векторної булевої функції $F$.

б) Випадковий обмін місцями *NP* значень підстановки $S$ і формування підстановки $S_t$.

в) Послідовне обчислення показників залежно від їх обчислювальної складності. Якщо підстановка $S_t$ задовольняє всі критерії, крім циклових, тоді застосовується лінійно-еквівалентне перетворення для досягнення критерію відсутності фіксованих точок. За невідповідності хоча б одного з критеріїв перехід в п. б).

У результаті сформована підстановка зберігатиметься в $S_t$.

Подальші дослідження показали, що практична реалізація методу з [12] вимагає значних обчислювальних витрат – один байтовий S-блок формується в середньому за 3.5 години на однопроцесорному персональному комп'ютері (ПК) [12, 18, 19].

### 2.4. Переставний метод пошуку S-блоків із фіксованою кількістю замін

Інший метод, запропонований у [18] та розвинений у [19], що є модифікацією попередньо методу з [12], дозволяє формувати підстановки за значно мен-

ший час, або з більш високими криптографічними показниками. Сутність методу полягає в одноразовому застосуванні фіксованої кількості перестановок $NP = 22$. Тобто на кроці в) попереднього методу (див. п. 3.3) немає повернення на крок в).

В ході застосування як вхідні дані підстановки $S$ з високою нелінійністю (наприклад, $S$-блока з алгебраїчної конструкцією $F(x) = x^{254}$) вдається зберегти високі криптографічні показники та, за рахунок обміну місцями $NP$ значень підстановки, надати векторному відображенню псевдовипадкового вигляду. Обране значення $NP = 22$ дозволяє з високою ймовірністю отримати максимально можливе значення алгебраїчного імунітету (для байтового відображення дорівнює 3) та високих значень інших криптографічних показників.

Дійсно, як показано у [19] запропонований метод дозволяє значно скоротити час генерації і, наприклад, на однопроцесорному ПК за 10 хвилин сформувати збалансовану (бієктивну) байтову підстановку з такими характеристиками:

- нелінійність $N_F = 104$;
- алгебраїчний степінь $AD = 7$;
- алгебраїчний імунітет $AI = 3$;
- максимум таблиці диференціалів $DDT_{\max} = 8$;
- відсутність фіксованих точок та циклів довжиною $l \le 3$.

Проте у процесі генерації цей метод передбачає застосування фіксованої кількості перестановок елементів початкової алгебраїчної підстановки [18, 19]. Тобто нелінійні вузли, сформовані у такий спосіб, у своїй суті є детермінованими (за винятком незначної кількості пар елементів). Отже, такий метод не реалізує повною мірою випадкову генерацію, його практичне застосування є обмеженим.

## ВИСНОВКИ ТА ОБГОВОРЕННЯ

Аналізуючи розглянуті методи формування нелінійних вузлів заміни слід, перш за все, відмітити значний прогрес в їхньому вдосконаленні протягом останніх 10–15 років.

Розроблений понад 20 років тому метод градієнтного підйому [15] декілька разів вдосконалювався та відтворювався із іншими процедурами та новими ідеями евристичного пошуку. Зокрема, ідея застосування як вхідні дані високонелінійних послідовностей та бент-функцій була запропонована спершу в роботі [16], продовжена у [20] та в дисертації [22]. Замість пошуку шляхів підвищення нелінійності випадкової послідовності в методі градієнтного підйому значно швидше можна знайти збалансовану криптографічну функцію шляхом градієнтного спуску, як це показано, наприклад, у [17]. Тобто цей крок у розвитку евристичних методів синтезу криптографічних булевих функцій був надзвичайно вдалим та ефективним. На жаль, як було показано в дисертації [23], застосувати цей підхід до побудови векторних відображень (S-блоків) шляхом, наприклад, ітеративного формування компонентних функцій $f_i, i = 1,...,m$ з (1) практично неможливо. Дійсно, результати розрахунків з [23] та з інших пошукових робіт свідчать, що побудова байтових (і більшого розміру) векторних відображень через підбір компонентних функцій $f_i, i = 1,...,m$ є обчислювально недосяжною задачею.

Інший вдалий крок було зроблено в дисертації [12] та наукових статтях [18, 19]. Ідею градієнтного спуску було поширено на векторні відображення не через компонентні функції $f_i, i = 1,...,m$ з (1), а шляхом застосування ітеративних процедур пошуку до вхідного високонелінійного $S$-блоку. Наприклад, застосувавши алгебраїчну конструкцію $F(x) = x^{254}$ можна сформувати бієктивне векторне відображення із нелінійністю $N_F = 112$, алгебраїчним степенем $AD = 7$, алгебраїчним імунітетом $AI = 2$ та максимумом таблиці диференціалів $DDT_{\max} = 4$. Далі, поступово змінюючи перестановкою окремі позиції таблиці замін, можна досягти значення $AI = 3$ без суттєвого погіршення інших показників, наприклад, нелінійності та δ-рівномірності. Генерація $S$-блоків у такий спосіб вимагає значного часу, але вона доступна навіть із використанням однопроцесорного ПК (потребує декілька годин на генерацію однієї байтової підстановки). Звісно, час формування буде значно меншим за випадкову генерацію [23].

Подальший розвиток методів генерації було отримано в роботах [18, 19]. Шляхом одноразового застосування фіксованої кількості перестановок $NP = 22$ вдається досить швидко (за декілька хвилин) сформувати байтовий нелінійний вузол із заданими криптографічними властивостями (навість із $N_F = 104$). Однак випадкова заміна місцями лише 22 позицій у таблиці підстановок робить цей метод обмеженим для практичного використання. Фактично, із 256 позицій в таблиці підстановок лише 44 можуть бути замінені місцями, тобто у

$$\frac{256-44}{256}\cdot 100\% \approx 83\%$$

сформовані вузли формуватимуть таке саме значення на виході, як і векторне відображення, яке використовувалося як початкове (стартове) для алгоритму генерації. Відповідно, всі формовані таким чином відображення будуть на 83% подібні вихідному і задавати не випадкову підстановку.

Як підсумок, слід зазначити, що завдання генерації випадкових підстановок із необхідними криптографічними властивостями в повному обсязі не вирішено. Отримано лише часткові, обмежені для широкого застосування результати. Метою подальших досліджень в цій галузі є розробка методів та обчислювальних алгоритмів формування випадкових нелінійних вузлів замін з необхідними (близькими до верхніх теоретичних

меж) криптографічними характеристиками. Тобто з одного боку ставиться завдання зі зниження обчислювальної складності формування S-блоку, з іншого – необхідно забезпечити виконання заданих високих показників стійкості (збалансованості, нелінійності, автокореляції, алгебраїчної імунності, циклової структури та ін.).

**Література**


[1] *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.

[2] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: монографія.– Харків: Видавництво «Форт», 2012. – 870 с.

[3] *Bart Preneel.* Analysis and Design of Cryptographic Hash Functions. [Електронний ресурс] – Режим доступа: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

[4] *Carlet C.* Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Електронний ресурс] – Режим доступа: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf

[5] *Carlet C.* Vectorial Boolean functions for Cryptography // Cambridge Univ. Press, Cambridge. – 95 p. [Електронний ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf

[6] *Clark J.A., Jacob J.L., Stepney S.* The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – p.219–231.

[7] *Zhuo Zepeng, Zhang Weiguo.* On correlation properties of Boolean functions // Chinese Journal of Electronics. Jan, Vol.20, 2011, №1, 143–146 pp.

[8] *X.-M. Zhang, Y. Zheng, and H. Imai.* Relating Differential Distribution Tables to Other Properties of Substitution Boxes. Des. Codes Cryptography, 19(1), pp. 45-63, 2000.

[9] *Ann Braeken.* Cryptographic Properties of Boolean Functions and S-Boxes. PhD thesis, Katholieke Universiteit Leuven (KUL), 2006, 221 p.

[10] *Fuller J.E.* Analysis of Affine Equivalent Boolean Functions for Cryptography: PhD Thesis / J.E. Fuller // Queensland University of Technology, 2003. – 187 p.

[11] *Andrey Pyshkin.* Algebraic Cryptanalysis of Block Ciphers Using Grobner Bases. Dissertation zur Erlangung des Grades Doktor rerum naturalium. Technischen Universit¨at Darmstadt. – Darmstadt, 2008, 118 p.

[12] *Казимиров А. В.* Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов : диссертация на соискание учёной степени кандидата технических наук : 05.13.21 – системы защиты информации – Харьков, 2013. – 190 с.

[13] *Burnett L.* Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography: PhD Thesis / L. Burnett. – Queensland University of Technology, 2005. – 204 p.

[14] *C. Easttom,* "A generalized methodology for designing nonlinear elements in symmetric cryptographic primitives," *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2018, pp. 444-449.

[15] *W. Millan, A. Clark, E. Dawson,* "Smart Hill Climbing Finds Better Boolean Functions", Proceedings of the Workshop on Selected Areas on Cryptography SAC 97, Springer-Verlag, pp. 50-63, 1997.

[16] *Y. Izbenko, V. Kovtun and A. Kuznetsov,* "The Design of Boolean Functions by Modified Hill Climbing Method," 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, 2009, pp. 356361.

[17] *Kuznetsov, I. Moskovchenko, I. Bilozertsev, S. Kavun, T. Kuznetsova.* Heuristic Methods for the Design of Cryptographic Boolean Functions. In.: ISCI'2018: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2018, pp. 45–74.

[18] *O. Kazymyrov, V. Kazymyrova, R. Oliynykov.* A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent. [Електронний ресурс] – Режим доступа: https://eprint.iacr.org/2013/578.pdf

[19] *M. Rodinko and R. Oliynykov.* Optimization of High Nonlinearity S-boxes Generation Method. Tatra Mountains Mathematical Publications, September 2017, 70 (1): pp. 93–105.

[20] *Кузнецов А. А.* Метод построения криптографически стойких булевых функций на основе градиентного спуска / А. А. Кузнецов, Ю. А. Избенко, И. Московченко // Зб. наук. пр. Харк. ун-ту Повітр. Сил. – Х.: ХУПС, 2007. – С. 63–66.

[21] *Yu Y.* Constructing Differentially 4 Uniform Permutations from Known Ones / Yuyin Yu, Mingsheng Wang, Yongqiang Li // Chinese Journal of Electronics. – 2013. – Vol. 22, № 3. – P. 495–499.

[22] Математичні моделі та обчислювальні методи імовірнісного формування нелінійних вузлів замін симетричних криптографічних засобів захисту інформації [Текст] : автореф. дис... канд. техн. наук : 01.05.02 / Московченко Ілларіон Валерійович ; Харківський національний ун-т ім. В.Н.Каразіна. – Х., 2009. – 20 с.

[23] Обчислювальні методи синтезу нелінійних вузлів замін для підвищення ефективності симетричних криптоперетворень : автореф. дис ... канд. техн. наук: 05.13.21 / Сергій Олександрович Ісаєв. – Харків, 2013. – 22 с.


Надійшла до редколегії 25.12.2018

**Кузнєцов Олександр Олександрович**, доктор технічних наук, професор, заступник головного конструктора ПАТ «ІІТ», професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, алгебраїчна теорія кодів, обробка, передача та захист інформації.

**Білозерцев Іван Микитович**, науковий співробітник ПАТ «ІІТ», здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – криптографія, блокові симетричні шифри.

**Пушкарьов Андрій Іванович**, директор департаменту захисту інформації Адміністрації державної служби спеціального зв'язку та захисту інформації України. Галузь наукових інтересів – теорія захисту інформації, інформаційна та кібербезпека держави.

**Горбенко Юрій Іванович**, кандидат технічних наук, виконавчий директор ПАТ «ІІТ», старший науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, інфраструктура відкритих ключів.

**Онопрієнко Віктор Васильович**, кандидат технічних наук, доцент, генеральний директор ПАТ «Інститут інформаційних технологій». Галузь наукових інтересів – криптографія і автентифікація, інфраструктура відкритих ключів, теорія захисту інформації, інформаційна та кібербезпека держави.

УДК 004.056.55

Кузнецов А.А. **Исследование методов формирования случайных нелинейных узлов замен симметричных шифров** / А.А. Кузнецов, И.М. Белозерцев, А.И. Пушкарев, Ю.И. Горбенко, В.В. Ониприенко // Прикладная радиоэлектроника: науч. – техн. журнал. – 2018. – Том 17, №. 3, 4. – С. 88–95.

Обосновываются основные показатели эффективности криптографических булевых функций и векторных отображений, которые применяются в качестве узлов усложнения симметричных криптопреобразований. Исследуются эвристические методы формирования криптографических булевых функций и нелинейных S-блоков симметричных шифров, соответствующих установленным требованиям безопасности. Обосновываются перспективные направления дальнейших исследований с целью усовершенствования эвристических методов синтеза случайных узлов замены.

*Ключевые слова*: симметричные криптопреобразования, случайные нелинейные узлы замены, эвристические методы генерации, показатели криптографической стойкости.

Библиогр.: 23 наим.

UDC 004.056.55

Kuznetsov A. **Investigation of methods for forming random nonlinear nodes of replacing symmetric ciphe** / A. Kuznetsov, I.M. Belozertsev, A.I. Pushkarev, Yu. Gorbenko, V.Onopryenko // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 88–95.

The main indicators of the effectiveness of cryptographic Boolean functions and vector mappings, used as nodes of the complexity of symmetric crypto-transformations, are substantiated. Heuristic methods for the formation of cryptographical Boolean functions and nonlinear S-blocks of symmetric ciphers that meet the established security requirements are investigated. Prospects for further research with the aim of improving heuristic methods for the synthesis of random replacement nodes are substantiated.

*Keywords*: symmetric cryptotransformations, random nonlinear replacement nodes, heuristic methods of generation, indicators of cryptographic robustness.

Ref.: 23 items.