**УДК 004.056:519.2** **DOI:10.30837/rt.2025.2.221.03**

*А.М. ОЛЕКСІЙЧУК, д-р техн. наук, Ю.Р. КІНДРАТ*

# УДОСКОНАЛЕНИЙ АЛГОРИТМ ЛЕВІНА ДЛЯ ОБМЕЖЕНИХ ЙМОВІРНІСНИХ ПСЕВДОБУЛЕВИХ ФУНКЦІЙ

## Вступ

У статті О. Гольдрайха та Л. Левіна [1] доведено теорему, яку можна сформулювати таким чином. Нехай $h$ – функція, задана на множині $V_n$ двійкових векторів довжини $n$, $s \in V_n$ – невідомий фіксований вектор. Припустимо, що існує ймовірнісний алгоритм, який для довільного $x \in V_n$ знаходить за значеннями $x$ та $h(s)$ оцінку ($0$ або $1$) булевого скалярного добутку векторів $s$ та $x$ за $T$ операцій з імовірністю (відносно випадкового рівноймовірного вибору $x$, а також випадкових даних, що використовуються в алгоритмі) $1/2 \cdot (1+\varepsilon)$, $\varepsilon \in (0,1)$. Тоді існує ймовірнісний алгоритм, якій відновлює значення $s$ за значенням $h(s)$ з імовірністю помилки $\delta \in (0,1)$ зі складністю, що поліноміально залежить від $T$, $\varepsilon^{-1}$ та $\log \delta^{-1}$ (тут і далі $\log$ позначає логарифм за основою $2$). Для доведення теореми в [1] запропоновано поліноміальний алгоритм, який, говорячи мовою теорії кодування, здійснює списочне декодування коду Адамара – лінійного блокового коду, що складається з векторів значень усіх лінійних булевих функцій від $n$ змінних. Зазначений алгоритм, що носить сьогодні прізвища Гольдрайха та Левіна, а також однойменна теорема відіграють важливу роль у криптології, зокрема, при встановленні взаємоз'язку між важкооборотними (one-way) функціями та псевдовипадковими генераторами. Більш того, теорема Гольдрайха–Левіна суттєво використовується при побудові сучасних обґрунтовано стійких потокових шифрів [2 – 5], а відповідний алгоритм або його модифікації – для знаходження лінійних наближень булевих функцій [6 – 12].

Нагадаємо, що остання задача полягає в тому, щоб сформувати для довільної булевої функції $f$ від $n$ змінних та числа $\varepsilon \in (0,1)$ список усіх лінійних булевих функцій, які співпадають з функцією $f$ не менше ніж на $2^{n-1}(1+\varepsilon)$ двійкових наборах. Найбільш відомим алгоритмом розв'язання цієї задачі є алгоритм швидкого перетворення Адамара, який обчислює усі лінійні наближення булевої функції від $n$ змінних за $O(n2^n)$ операцій додавання та віднімання цілих чисел (див., наприклад, [13]). Зазначений алгоритм не є оптимальним за складністю, навіть у класі детермінованих алгоритмів [14].

Суттєве зменшення трудомісткості побудови лінійних наближень можливо за рахунок застосування модифікацій алгоритму Гольдрайха–Левіна [6 – 12], серед яких відзначимо вдосконалений алгоритм Левіна [7] зі складністю $\widetilde{O}(n\varepsilon^{-2}\log\delta^{-1})$ операцій над цілими числами, де $\widetilde{O}$ позначає оцінку з точністю до логарифмічних множників від $n$ та $\varepsilon^{-1}$. Зауважимо, що цей алгоритм (поряд з викладеним в [12]) є на сьогодні найшвидшим серед відомих алгоритмів побудови лінійних наближень булевих функцій.

Метою цієї статті є узагальнення вдосконаленого алгоритму Левіна на випадок обмежених ймовірнісних псевдобулевих функцій, тобто певних випадкових відображень множини $V_n$ у множину дійсних чисел. Основним результатом є теорема, яка встановлює нижню межу ймовірності потрапляння кожного шуканого наближення до випадкового списку, який формується з використанням наведеного алгоритму. (Зауважимо, що подібний результат відсутній у роботі [7], а його доведення проводиться за той самою схемою, що і у [10, п. 4.4], але більш простим способом).

Результати статті надають змогу отримати більш ефективну редукцію (tight reduction) задач у відомих доведеннях псевдовипадковості генераторів гами за умови високої обчислю-

вальної складності декодування випадкових лінійних блокових кодів або розв'язання випадкових систем нелінійних булевих рівнянь [2 – 5].

**1. Постановка задачі**

Для будь-яких натуральних чисел $n,t$ позначимо $V_n$ множину двійкових векторів довжини $n$, $F_{t\times n}$ – множину $t\times n$-матриць над полем $F=\mathbf{GF}(2)$. Надалі позначатимемо $\alpha x=\alpha_1 x_1\oplus\cdots\oplus\alpha_n x_n$ булев скалярний добуток довільних двійкових векторів $\alpha=(\alpha_1,...,\alpha_n)$ та $x=(x_1,...,x_n)$.

*Ймовірнісна псевдобулева функція* від $n$ змінних визначається як випадкове відображення $g:V_n\to\mathbf{R}$ (де $\mathbf{R}$ – множина дійсних чисел) з такою властивістю: для будь-яких (не обов'язково різних) векторів $x_1,...,x_t\in V_n$ значення $g(x_1),...,g(x_t)$ є незалежними однаково розподіленими випадковими величинами. Типовим прикладом такої функції є відображення, яке задається за допомогою випадкового оракула – ймовірнісного алгоритму, який обчислює значення функції, використовуючи певні параметри, значення яких, у свою чергу, вибираються випадково та незалежно від аргументів функції з певної скінченної множини згідно з деяким законом розподілу ймовірностей, причому вибір цих значень відбувається кожен раз незалежно від того, як вони були обрані при попередніх зверненнях до функції (див., наприклад, [15, п. 3.2]). Іншим (тривіальним) прикладом ймовірнісної функції є довільна звичайна (не випадкова) псевдобулева функція.

Зафіксуємо *обмежену* ймовірнісну функцію $g:V_n\to\mathbf{R}$, тобто таку, що для деякого $C>0$ нерівність $|g(x)|\le C$ виконується для кожного $x\in V_n$ з імовірністю 1. Надалі, не обмежуючи загальності міркувань, вважатимемо $C=1$.

Позначимо $\bar{g}$ математично сподівання випадкової функції $g$, тобто звичайну псевдобулеву функцію, кожне значення $\bar{g}(x)$ якої отримується шляхом усереднення значень випадкової величини $g(x)$ за її розподілом ймовірностей, $x\in V_n$.

Нарешті, позначимо

$$\hat{g}(\alpha)=2^{-n}\sum_{x\in V_n}(-1)^{\alpha x}\bar{g}(x),\ \alpha\in V_n$$

перетворення Фур'є функції $\bar{g}$ та розглянемо для будь-яких $\varepsilon\in(0,1)$, $C_\varepsilon>0$ множину

$$L_{\bar{g},\varepsilon}=\{\alpha\in V_n:\ \hat{g}(\alpha)\ge C_\varepsilon\}. \tag{1}$$

Задача полягає у розробці ймовірнісного алгоритму, який формує за вхідними даними $(g,\varepsilon,C_\varepsilon,\delta)$, де $\delta\in(0,1)$, випадковий список $\Lambda_{g,\varepsilon}\subseteq V_n$ такий, що

$$\forall\alpha\in V_n:\ \alpha\in L_{\bar{g},\varepsilon}\Rightarrow\mathbf{P}\{\alpha\in\Lambda_{g,\varepsilon}\}\ge 1-\delta, \tag{2}$$

де ймовірність $\mathbf{P}$ обчислюється відносно розподілу функції $g$ та випадкових даних, які використовуються в самому алгоритмі.

Як приклад, розглянемо важливий окремий випадок, в якому функція $g$ визначається за формулою $g(x)=(-1)^{f_\omega(x)}$, якщо $x\in M$; $g(x)=0$, якщо $x\in V_n\setminus M$, де $f_\omega:M\to\{0,1\}$ – часткова булева функція, задана на певній множині $M\subseteq V_n$ потужності $T$, $\omega$ – випадковий елемент, розподілений на певній скінченній множині $\Omega$. В цьому випадку для будь-якого $\alpha\in V_n$ виконується рівність

$$\mathbf{P}_X\{f_\omega(X)=\alpha X\}=1/2\cdot\left(1+T^{-1}\sum_{x\in M}(-1)^{f_\omega(x)\oplus\alpha x}\right),$$

де $X$ – випадковий вектор з рівномірним розподілом на $M$. Звідси випливає, що

$$\mathbf{P}_{X,\omega}\{f_\omega(X)=\alpha X\}=1/2\cdot\left(1+T^{-1}\sum_{x\in V_n}(-1)^{\alpha x}\overline{g}(x)\right)=1/2\cdot(1+2^nT^{-1}\hat{g}(\alpha)).$$

Отже, при $C_\varepsilon=2^{-n}T\varepsilon$ множина (1) збігається з сукупністю всіх векторів $\alpha\in V_n$, які задовольняють умову $\mathbf{P}_{X,\omega}\{f_\omega(X)=\alpha X\}\geq 1/2(1+\varepsilon)$. Зокрема, якщо $|\Omega|=1$, $M=V_n$ і $C_\varepsilon=\varepsilon$, то поставлена вище задача зводиться до побудови списку "високоймовірних" лінійних наближень звичайної булевої функції $f$, тобто таких лінійних функцій $l_\alpha(x)=\alpha x$, $x\in V_n$, які збігаються з $f$ не менше ніж на $2^{n-1}(1+\varepsilon)$ вхідних наборах. Для розв'язання останньої задачі можна скористатися одним з відомих ймовірнісних алгоритмів [6 – 12].

**2. Отримані результати**

Алгоритм побудови множини $\Lambda_{g,\varepsilon}$, який викладено нижче, є узагальненою версією вдосконаленого алгоритму Левіна [7]. Він залежить від натуральних параметрів $l$, $t$ і має такий вигляд.

1. Згенерувати незалежні в сукупності випадкові вектори $X_1,...,X_t$ та $Z_{ij}$ ($i\in\overline{1,n}$, $j\in\overline{1,l}$), кожен з яких має рівномірний розподіл на множині $V_n$.

2. Сформувати таблицю розміром $2ln\times 2^t$, рядки якої занумеровані трійками $(i,\ j,\ \nu)$, де $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$, а стовпці – векторами $u\in V_t$, таку, що на перетині будь-якого рядка з номером $(i,\ j,\ \nu)$ і стовпця з номером $u$ знаходиться елемент

$$g_{i,j,\nu}(u)=\begin{cases}g(uX\oplus Z_{ij}\oplus\nu e_i),\ \text{якщо}\ u\neq 0;\\ 0,\ \text{якщо}\ u=0,\end{cases}\qquad(3)$$

де $X$ – матриця з рядками $X_1,...,X_t$, $e_i$ – двійковий вектор довжини $n$, усі координати якого, за виключенням $i$-ї, дорівнюють нулю.

3. Помножити кожен рядок зазначеної таблиці на матрицю Адамара $H_t$, використовуючи алгоритм швидкого перетворення Адамара, та отримати нову таблицю з елементами

$$h_{i,j,\nu}(a)=\sum_{u\in V_t}g_{i,j,\nu}(u)(-1)^{ua},\qquad(4)$$

де $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$, $a=(a_1,...,a_t)\in V_t$; покласти

$$s_{i,j,\nu}(a)=\begin{cases}0,\ \text{якщо}\ h_{i,j,\nu}(a)\geq 0;\\ 1,\ \text{якщо}\ h_{i,j,\nu}(a)<0\end{cases}\qquad(5)$$

для будь-яких $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$ та $a\in V_t$.

4. Для кожного $a\in V_t$ виконати таку процедуру:

4.1. Для кожного $i\in\overline{1,n}$ обчислити

$$s_{i,1,0}(a)\oplus s_{i,1,1}(a),\ s_{i,2,0}(a)\oplus s_{i,2,1}(a),\ \ldots,\ s_{i,l,0}(a)\oplus s_{i,l,1}(a)\qquad(6)$$

та покласти $\alpha_i$ рівним елементу (0 або 1) з найбільшою частотою зустрічаємості в послідовності (6).

4.2. Додати отриманий вектор $\alpha = (\alpha_1, \ldots, \alpha_n)$ до списку $\Lambda_{g,\varepsilon}$, що формується.

Отже, в результаті виконання алгоритму буде побудовано випадковий список, який складається з $2^t$ (не обов'язково різних) двійкових векторів $\alpha$ довжини $n$.

Наступне твердження випливає безпосередньо з опису наведеного алгоритму.

**Твердження.** Для будь-якої ймовірнісної функції $g: V_n \to [-1,1]$ та довільного числа $\varepsilon \in (0,1)$ алгоритм формує список $\Lambda_{g,\varepsilon}$, використовуючи $T_g 2^{t+1} nl + O(2^t tnl)$ операцій (додавання, віднімання та порівняння з нулем дійсних чисел або двійкових векторів довжини $n$), де $T_g$ – максимальна складність обчислення одного значення функції $g$.

Доведемо теорему, яка встановлює нижню межу ймовірності події $\{\alpha \in \Lambda_{g,\varepsilon}\}$ для будь-якого $\alpha \in L^-_{g,\varepsilon}$ та надає змогу з'ясувати, яким чином слід вибирати параметри $l$ і $t$ алгоритму для заздалегідь означених $g, \varepsilon, C_\varepsilon, \delta$.

**Теорема.** Нехай $g: V_n \to [-1,1]$ – ймовірнісна функція, $\varepsilon \in (0,1)$, $\theta \in (0, 1/4)$ і $L^-_{g,\varepsilon}$ – множина вигляду (1). Позначимо $\tilde{Z}$ набір випадкових векторів $Z_{ij}$, які генеруються на першому кроці алгоритму. Тоді для будь-якого $\alpha \in L^-_{g,\varepsilon}$ виконується нерівність

$$\mathbf{P}_{g,X,\tilde{Z}}\{\alpha \in \Lambda_{g,\varepsilon}\} \geq (1 - \exp\{-8l\theta^2\})^n \left(1 - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}\right) \tag{7}$$

за умови, що кожен з двох співмножників у правій частині є додатним числом.

**Доведення.** Введемо випадкові величини

$$\xi_\alpha(X, Z) = (2^t - 1)^{-1} \sum_{u \in V_t \setminus \{0\}} (-1)^{(uX \oplus Z)\alpha} g(uX \oplus Z),\ \alpha \in V_n, \tag{8}$$

$$\eta_a(X, Z) = (2^t - 1)^{-1} \sum_{u \in V_t \setminus \{0\}} (-1)^{ua} g(uX \oplus Z),\ a \in V_t, \tag{9}$$

де $Z$ – випадковий вектор з рівномірним розподілом на множині $V_n$, який не залежить від випадкових функції $g$ та матриці $X$. Для будь-яких $x \in F_{t \times n}$ (значення випадкової матриці $X$) та $a \in V_t$ задамо ймовірнісну булеву функцію

$$f_{x,a}(z) = \begin{cases} 0, \text{ якщо } \eta_a(x,z) \geq 0; \\ 1, \text{ якщо } \eta_a(x,z) < 0,\ z \in V_n. \end{cases} \tag{10}$$

Зауважимо, що на підставі рівностей (3) – (5) для будь-яких $i \in \overline{1,n}$, $j \in \overline{1,l}$, $\nu \in \{0,1\}$, $a \in V_t$ виконуються рівності

$$h_{i,j,\nu}(a) = (2^t - 1)\eta_a(X, Z_{ij} \oplus \nu e_i),\ s_{i,j,\nu}(a) = f_{X,a}(Z_{ij} \oplus \nu e_i). \tag{11}$$

Зафіксуємо довільний вектор $\alpha \in L_{g,\varepsilon}$ та доведемо низку допоміжних тверджень.

**1⁰.** Справедлива нерівність

$$\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z) = \alpha Z\} \geq 1 - \frac{1}{(2^t - 1)\, C_\varepsilon^2}. \tag{12}$$

Дійсно, на підставі рівностей (8), (9)

$$\eta_{X\alpha}(X,Z)=(2^t-1)^{-1}\sum_{u\in V_t\setminus\{0\}}(-1)^{(uX)\alpha}g(uX\oplus Z)=(-1)^{\alpha Z}\xi_\alpha(X,Z).$$

Крім того, згідно з формулою (10), $\eta_{X\alpha}(X,Z)=|\eta_{X\alpha}(X,Z)|(-1)^{f_{X,X\alpha}(Z)}$. Отже, подія $\{\xi_\alpha(X,Z)>0\}$ тягне подію $\{f_{X,X\alpha}(Z)=\alpha Z\}$, звідки випливає, що

$$\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge\mathbf{P}_{g,X,Z}\{\xi_\alpha(X,Z)>0\}. \tag{13}$$

Далі, випадкові вектори $uX\oplus Z$ ($u\in V_t\setminus\{0\}$) є попарно незалежними та рівноймовірними, звідки на підставі означення ймовірнісної функції випливає, що доданки у правій частині рівності (8) є попарно незалежними та однаково розподіленими випадковими величинами. Звідси, враховуючи обмеженість функції $g$, отримаємо такі співвідношення: $\mathbf{E}\xi_\alpha(X,Z)=\hat g(\alpha)$, $\mathbf{D}\xi_\alpha(X,Z)\le(2^t-1)^{-1}(1-\hat g(\alpha)^2)\le(2^t-1)^{-1}$, де символи $\mathbf{E}$ та $\mathbf{D}$ позначають відповідно математичне сподівання та дисперсію відносно розподілу $\mathbf{P}_{g,X,Z}$. Отже, згідно з нерівністю Чебишова отримаємо, що

$$\mathbf{P}_{g,X,Z}\{|\xi_\alpha(X,Z)-\hat g(\alpha)|\ge C_\varepsilon\}\le C_\varepsilon^{-2}\mathbf{D}\xi_\alpha(X,Z)\le C_\varepsilon^{-2}(2^t-1)^{-1}. \tag{14}$$

Нарешті, оскільки $\alpha\in L_{g,\varepsilon}$, тобто $\hat g(\alpha)\ge C_\varepsilon$, то

$$\mathbf{P}_{X,Z}\{\xi_\alpha(X,Z)\le 0\}\le\mathbf{P}_{X,Z}\{|\xi_\alpha(X,Z)-\hat g(\alpha)|\ge C_\varepsilon\}. \tag{15}$$

З нерівностей (13) – (15) випливає формула (12).

**$2^0$.** Для будь-якого $\theta\in(0,1/4)$ виконується нерівність

$$\mathbf{P}_X\{\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge 3/4+\theta\}\ge 1-\frac{1}{(2^t-1)\,C_\varepsilon^2(1/4-\theta)}. \tag{16}$$

Для доведення нерівності (16) скористаємося співвідношеннями

$$\mathbf{P}\{\xi\le C\}=1-\mathbf{P}\{\xi>C\}\ge 1-C^{-1}\mathbf{E}\xi,\ C>0,$$

справедливими для будь-якої невід'ємної випадкової величини $\xi$, вважаючи

$$\xi=1-\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\},\ C=1/4-\theta.$$

В результаті отримаємо, що

$$\mathbf{P}_X\{\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge 3/4+\theta\}\ \ge\ 1\ -\ \frac{\mathbf{E}_X(1-\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\})}{1/4-\theta}\ =$$

$$=\ \frac{\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}-3/4-\theta}{1/4-\theta}.$$

Звідси на підставі формули (12) випливає нерівність (16).

**$3^0$.** Нехай значення $x$ випадкової матриці $X$ є таким, що $\mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z)=\alpha Z\}\ge 3/4+\theta$, де $\theta\in(0,1/4)$. Тоді ймовірність $\pi_{n,l}(\theta)$ події, яка полягає в тому, що для кожного $i\in\overline{1,n}$ елемент $\hat\alpha_i$ з найбільшою частотою зустрічаємості у випадковій послідовності

$$\xi_j^{(i)}=f_{x,x\alpha}(Z_{ij}\oplus e_i)\oplus f_{x,x\alpha}(Z_{ij}),\ j\in\overline{1,l}, \tag{17}$$

дорівнює $\alpha_i$, є не менше ніж $(1-\exp\{-8l\theta^2\})^n$.

Для доведення помітимо, що на підставі означення ймовірнісної функції випадкові величини $\xi_j^{(i)}$ ($i \in \overline{1,n}$, $j \in \overline{1,l}$) є незалежними в сукупності. Отже,

$$\pi_{n,l}(\theta) = \prod_{i=1}^{n} \mathbf{P}\{\hat{\alpha}_i = \alpha_i\}. \tag{18}$$

Далі, для будь-якого $i \in \overline{1,n}$

$$\xi_j^{(i)} \oplus \alpha_i = (f_{x,x\alpha}(Z_{ij} \oplus e_i) \oplus \alpha(Z_{ij} \oplus e_i)) \oplus (f_{x,x\alpha}(Z_{ij}) \oplus \alpha(Z_{ij})),\ j \in \overline{1,l}, \tag{19}$$

звідки випливає, що

$$\mathbf{P}_{g,\tilde{Z}}\{\xi_j^{(i)} \neq \alpha_i\} \le \mathbf{P}_{g,\tilde{Z}}(\{f_{x,x\alpha}(Z_{ij} \oplus e_i) \oplus \alpha(Z_{ij} \oplus e_i) = 1\} \cup \{f_{x,x\alpha}(Z_{ij}) \oplus \alpha(Z_{ij}) = 1\}) \le$$
$$\le 2\mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z) \neq \alpha Z)\} \le 2(1/4 - \theta) = 1/2 - 2\theta,\ j \in \overline{1,l}. \tag{20}$$

Крім того, елемент з найбільшою частотою зустрічаємості в послідовності (17) не збігається з $\alpha_i$ тоді й тільки тоді, коли число одиниць в послідовності (19) є більше за число нулів, тобто виконується умова $\sum_{j=1}^{l}(\xi_j^{(i)} \oplus \alpha_i) > l/2$. При цьому послідовність (19) є схемою Бернуллі з параметрами $(l, p_i)$, де за формулою (20) $p_i = \mathbf{P}_{g,\tilde{Z}}\{\xi_j^{(i)} \neq \alpha_i\} \le 1/2 - 2\theta$, $i \in \overline{1,n}$. Звідси на підставі відомої оцінки Чернова випливає, що

$$\mathbf{P}_{g,\tilde{Z}}\{\hat{\alpha}_i = \alpha_i\} = \mathbf{P}_{g,\tilde{Z}}\left\{\sum_{j=1}^{l}(\xi_j^{(i)} \oplus \alpha_i) - lp_i > l(1/2 - p_i)\right\} \le$$
$$\le \exp\{-2l(1/2 - p_i)^2\} \le \exp\{-8l\theta^2\},\ i \in \overline{1,n}. \tag{21}$$

Таким чином, внаслідок формул (18) та (21) виконується нерівність $\pi_{n,l}(\theta) \ge (1 - \exp\{-8l\theta^2\})^n$, що й треба було довести.

Перейдемо до доведення співвідношення (7). Для будь-якого $\alpha \in L_{g,\varepsilon}^{-}$ розглянемо такі події:

$$A_\alpha = \{x \in F_{t\times n} :\ \mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z) = \alpha Z\} \ge 3/4 + \theta\},$$
$$B_\alpha(x) = \{(g, \tilde{z} = (z_{ij} \in V_n : i \in \overline{1,n}, j \in \overline{1,l})) :\ \forall\, i \in \overline{1,n}\ \textit{елемент}$$
$$\textit{з найбільшою частотою зустрічаємості в послідовності}$$
$$f_{x,x\alpha}(z_{ij} \oplus e_i) \oplus f_{x,x\alpha}(z_{ij}),\ j \in \overline{1,l},\ \textit{дорівнює}\ \alpha_i\},\ x \in F_{t\times n}.$$

З наведеного опису алгоритму та рівностей (11) випливає, що подія $\{\alpha \in \Lambda_{g,\varepsilon}\}$ настає у випадку, коли відбувається подія $\{X \in A_\alpha, (g, \tilde{Z}) \in B_\alpha(X)\}$. Отже,

$$\mathbf{P}_{g,X,\tilde{Z}}\{\alpha \in \Lambda_{g,\varepsilon}\} \ge \mathbf{P}_{g,X,\tilde{Z}}\{X \in A_\alpha, (g, \tilde{Z}) \in B_\alpha(X)\} = \sum_{x \in A_\alpha} \mathbf{P}_{g,X,\tilde{Z}}\{X = x, (g, \tilde{Z}) \in B_\alpha(x)\} =$$
$$= \sum_{x \in A_\alpha} \mathbf{P}_X\{X = x\} \mathbf{P}_{g,\tilde{Z}}\{(g, \tilde{Z}) \in B_\alpha(x)\}.$$

Далі, згідно з твердженням $3^0$, для будь-якого $x \in A_\alpha$ справедлива нерівність

$$\mathbf{P}_{g,\tilde{Z}}\{(g, \tilde{Z}) \in B_\alpha(x)\} \ge (1 - \exp\{-8l\theta^2\})^n. \tag{22}$$

При цьому на підставі твердження $2^0$

$$\mathbf{P}_X\{X \in A_\alpha\} \geq 1 - \frac{1}{(2^t - 1)\, C_\varepsilon^2 (1/4 - \theta)}. \tag{23}$$

Отже, за умови додатності виразів у правих частинах нерівностей (22), (23) справедлива нерівність (7). Таким чином, теорему повністю доведено.

Безпосередньо з теореми та твердження перед нею випливає такий результат.

**Наслідок.** Нехай $g(x) = (-1)^{f(x)}$, $x \in V_n$, де $f$ – ймовірнісна булева функція від $n$ змінних, $l = \left\lceil 8\ln(2n\delta^{-1}) \right\rceil$, $t = \left\lceil \ln(16\varepsilon^{-2}\delta^{-1} + 1) \right\rceil$, $\varepsilon, \delta \in (0,1)$. Тоді наведений алгоритм будує випадковий список $\Lambda_{g,\varepsilon}$ розміру $2^t$, який задовольняє умову (2), використовуючи $T_f 2^{t+1} nl + O(2^t tnl)$ операцій (додавання, віднімання та порівняння з нулем цілих чисел або двійкових векторів довжини $n$), де $T_f$ – максимальна складність обчислення одного значення функції $f$.

Для доведення достатньо покласти у формулі (7) $\theta = 1/8$, $C_\varepsilon = \varepsilon$ та скористатися оцінкою

$$(1 - \exp\{-8l\theta^2\})^n \left(1 - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}\right) \geq 1 - n\exp\{-8l\theta^2\} - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}.$$

**Висновки**

У статті представлено узагальнення вдосконаленого алгоритму Левіна [7] на випадок обмежених ймовірнісних псевдобулевих функцій. Основним результатом є теорема, яка встановлює нижню межу ймовірності потрапляння кожного шуканого наближення до випадкового списку, що формується з використанням наведеного алгоритму. Розгляд таких функцій є необхідним для розповсюдження можливості застосування вдосконаленого алгоритму Левіна (замість оригінального алгоритму Гольдрайха–Левіна [1]) у відомій схемі доведення стійкості потокових шифрів [2 – 5]. Зокрема, результати статті надають можливість отримати більш ефективну редукцію задач у доведеннях псевдовипадковості деяких відомих генераторів гами за умови високої обчислювальної складності декодування випадкових лінійних блокових кодів або розв'язання випадкових систем нелінійних булевих рівнянь. Отримані результати також можуть бути використані для знаходження лінійних апроксимацій шифрувальних перетворень блокових шифрів, що є важливим при побудові лінійних атак на них.

**Список літератури:**


1. Goldreich O., Levin L.A. A hard core predicate for all one-way functions // Proc. 21st ACM Symposium on Theory of Computing. 1989. P. 25–32.
2. Fischer J.-B., Stern J. An efficient pseudo-random generator provably as secure as syndrome decoding // EUROCRYPT'96: Proc. 15th International Conference on Theory and Application of Cryptographic Techniques. Springer, 1996. P. 245–255.
3. Gaborit Ph., Laudaroux C., Sendrier N. SYND: a very fast code-based cipher stream with a security reduction // IEEE International Symposium on Information Theory (ISIT'07). Nice, France, July 2007. P. 186–190.
4. Meziani M., Hoffmann G., Cayrel P.-L. Improving the performance of the SYND stream cipher // Progress in Cryptology – AFRICACRYPT 2012. Berlin : Springer, 2012. P. 99–116.
5. Berbain C., Gilbert H., Patarin J. QUAD: A multivariate stream cipher with provable security // Journal of Symbolic Computation. 2009. Vol. 44, № 12. P. 1703–1723.
6. Levin L.A. Randomness and non-determinism // Journal of Symbolic Logic. 1993. Vol. 58, № 3. P. 1102–1103.
7. Bshouty N., Jackson J., Tamon C. More efficient PAC-learning of DNF with membership queries under the uniform distribution // Proc. 12th Annual Conference on Computational Learning Theory. 1999. P. 286–295.
8. Goldreich O., Rubinfeld R., Sudan M. Learning polynomials with queries: the highly noisy case // SIAM Journal on Discrete Mathematics. 2000. Vol. 13, № 4. P. 535–570.

9. Kabatiansky G., Tavernier C. List decoding of Reed-Muller codes // Proc. 9th International Workshop on Algebraic and Combinatorial Coding Theory. 2008. P. 230–235.
10. Trevisan L. Some applications of coding theory in computational complexity : препринт № cs/0409044v1 / Luca Trevisan. Cornell University, 2004. 17 с. (arXiv:cs/0409044v1).
11. Fourquet R., Loidreau P., Tavernier C. Finding good linear approximations of block ciphers and its application to cryptanalysis of reduced round DES // Proc. WCC 2009. P. 501–515.
12. Abdouli A. S., Dumer I., Kabatiansky G., Tavernier C. The Goldreich-Levin algorithm with reduced complexity // Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012). Pomorie, Bulgaria, June 15–21, 2012. P. 7–14.
13. Олексійчук А. М., Курінний О. В. Методи криптоаналізу потокових шифрів : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 172 с.
14. Dumer I.I., Kabatiansky G.A., Tavernier C. List decoding of binary first-order Reed-Muller codes // Problems of Information Transmission. 2007. Vol. 43, № 3. P. 225–232.
15. Kopparty S., Saraf S. Local list decoding and testing of random linear codes from high-error // SIAM Journal on Computing. 2013. Vol. 42, № 3. P. 1302–1326.

*Надійшла до редколегії 11.03.2025*

*Відомості про авторів:*
**Олексійчук Антон Миколайович –** доктор технічних наук, професор, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", професор спеціальної кафедри № 1; Україна; e-mail: alex-dtn@ukr.net; ORCID: https://orcid.org/0000-0003-4385-4631
**Кіндрат Юлія Русланівна –** здобувачка вищої освіти ступеня магістра, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Україна; e-mail: kindrat0407@gmail.com