УДК 621.391:519.2

МЕТОД РОЗПІЗНАВАННЯ К-ВИМІРНОСТІ БУЛЕВИХ ФУНКЦІЙ, ЗАДАНИХ ЗА ДОПОМОГОЮ ОРАКУЛІВ

С. М. КОНЮШОК

Запропоновано ймовірнісний метод розпізнавання k-вимірности булевих функцій, заданих за допомогою оракулів, який має меншу трудомісткість та характеризується меншою ймовірністю помилки першого роду (при такій самій верхній межі ймовірності помилки другого роду) порівняно з аналогічним раніше відомим методом.

Ключові слова: перевірка властивостей булевих функцій, ймовірнісний метод, k-вимірна функція, перетворення Уолша-Адамара.

ВСТУП

Булеві функції (далі – БФ) є необхідними криптографічними примітивами [1]; що нерідко відіграють ключову роль у створенні багатьох потокових та блокових шифрів. У таких випадках, важливою складовою дослідження криптографічної стійкості шифрів є аналіз криптографічних властивостей відповідних булевих функцій [2]. Тому дослідження криптографічних властивостей БФ не тільки входить до переліку важливих інструментів криптоаналітика, але також має суттєве значення для оцінки стійкості криптографічних алгоритмів в процесі їх синтезу.

Слід зауважити, що криптографічні властивості БФ не є незалежними одна від одної, вони мають певні зв'язки та накладають деякі обмеження одна до одної, і це означає, що неможливо знайти функцію, яка дозволяє досягати найкращих значень за кожною з цих властивостей. Як наслідок, побудова булевої функції, яка забезпечує прийнятні з точки зору практичного використання криптографічні властивості, фактично полягає в досягненні певного стану умовного оптимуму шляхом компромісного зниження вимог до окремих криптографічних властивостей задля досягнення прийнятних значень іншими криптографічними властивостями даної БФ.

Пошук такої булевої функції нерідко може бути пов'язаний зі значним обсягом досліджень великої кількості функцій-претендентів на роль такого важливого елементу криптографічного алгоритму в процесі його розробки.

Таким чином, актуалною є задача зменшення трудомісткості визначення або оцінки значень показників, що характеризують криптографічні властивості булевих функцій шляхом пошуку новітніх або удосконалення наявних підходів.

Розглянемо більш детально одну з важливих криптографічних властивостей булевих функцій.

Так, один із підходів до застосування БФ у потокових шифрах – діяти як функція ускладнення. Задля високої криптографічної стійкості шифру, така функція повинна мати високу нелінійність. Однак, з іншої точки зору, нелінійна функція може допускати представлення себе як суперпозиції лінійних функцій та більш простої нелінійної функції. Формально, така властивість виглядає наступним чином.

Булеву функцію $g:\{0,1\}^n \to \{0,1\}$ називають k-вимірною [3, 4], $0 \le k \le n$, якщо існують функція $\phi:\{0,1\}^k \to \{0,1\}$ та $n \times k$-матриця A над полем з двох елементів такі, що для будь-якого $x \in \{0,1\}^n$ справедлива рівність $g(x) = \phi(xA)$. Функцію g називають алгебраїчно виродженою, якщо вона є k-вимірною для деякого $k < n$ та невиродженою – в іншому випадку [1, 5 – 7].

Перші результати про кореляційні властивості алгебраїчно вироджених булевих функцій належать до 70-х років минулого століття [5]. Дослідження кореляційних властивостей булевих функцій обумовлене задачами криптографічного аналізу та теорії кодування. Відзначимо роботи [8 – 10], де викладений ряд атак на генератори гами потокових шифрів, функції ускладнення яких є алгебраїчно виродженими або близькими до таких.

Наразі, задача побудови ефективних підходів до розпізнавання властивості k-вимірності булевих функцій, є актуальною, як для оцінки стійкості заданого шифру, так і з метою реалізації криптоаналітичної атаки на шифратор, як на "чорну скриньку" (тобто шифратор виступає в ролі оракула).

В [3] був запропонований ймовірнісний алгоритм розпізнавання властивостей k-вимірності. Для будь-якої функції $f:\{0,1\}^n \to \{0,1\}$, що задана за допомогою оракула, та чисел $k \in \{0,1,...,n-1\}$, $\varepsilon \in (0,1)$ цей алгоритм дозволяє перевірити гіпотезу H_0: f – k-вимірна БФ проти альтернативи H_1, яка полягає в тому, що f знаходиться на відстані (Гемінга) не меньше $2^n\varepsilon$ від множини k-вимірних функцій.

Зазначений алгоритм полягає в генерації незалежних випадкових рівноймовірних векторів $h_1, ..., h_l \in V_n$ та переверці рівностей

$$f(h_j \oplus Z_{ij}) = f(Z_{ij}),\ i \in \overline{1,m} \qquad (1)$$

для кожного $j \in \overline{1,l}$, де Z_{ij} – незалежні в сукупності випадкові рівноймовірні вектори з V_n, що не залежать від $h_1, ..., h_l$. Позначимо ν_l число значень $j \in \overline{1,l}$, для яких виконуються рівності (1). Тоді гіпотеза H_0 приймається, якщо $\nu_l \cdot l^{-1} \geq 0{,}9 \cdot 2^{-k}$ та відхиляється у протилежному випадку. В [3] пропонується вибрати $l = 2^k C$, $m = 2^k k\, \varepsilon^{-1} C'$, де $C, C' = const$, що зводить до оцінки трудомісткості алгоритму $O(2^{2k} k\, \varepsilon^{-1})$ запитів до оракула f (або $O(n 2^{2k} k\, \varepsilon^{-1})$ двійкових операцій).

Для оцінювання ймовірності помилки першого роду (тобто ймовірності того, що тест "не визнає" такою k-вимірну функцію) в [3] використовується нерівність Чернова:

$$\mathrm{P}\left(\frac{\nu_l}{l} < 0{,}9 \cdot 2^{-k} \mid H_0\right) \leq$$

$$\leq \mathrm{P}\left(\frac{\nu_l}{l} - \mathrm{E}\frac{\nu_l}{l} < -0{,}1 \cdot 2^{-k} \mid H_0\right) \leq$$

$$\leq \exp\left\{-0{,}02 \cdot \frac{C}{2^k}\right\}. \qquad (2)$$

Зауважимо, що вираз у правій частині (2) залежить від k та не прямує до нуля, якщо k є (як завгодно повільно) зростаючою функцією від n, наприклад, $k = \lceil \log n \rceil$, $n \to \infty$.

У роботі [11] запропонований більш ефективний імовірнісний тест k-вимірності, трудомісткість якого складає $O(2^k k^2\, \varepsilon^{-1})$ запитів до оракула (або $O(n\, 2^k k^2\, \varepsilon^{-1})$ двійкових операцій). При цьому верхня межа ймовірності помилки першого роду запропонованого тесту не залежить від k, а верхня межа ймовірності помилки другого роду є по суті така ж сама, що й для тесту з [3]. Показано також, що при певному природному змінюванні альтернативи H_1 можна побудувати однобічний (з нульовою ймовірністю помилки першого роду) тест k-вимірності, трудомісткість якого складає $O(n(2^k + k\varepsilon^{-2})\log(2^k + k\varepsilon^{-2}))$ двійкових операцій.

Вказаний тест покладено в основу методу розпізнавання k-вимірності булевих функцій, заданих за допомогою оракулів формальний опис якого запропоновано в даній статті.

1. НАУКОВІ ОСНОВИ МЕТОДУ, ЩО ПРОПОНУЄТЬСЯ

Основна ідея, покладена в основу методу, що пропонується, полягає в тому, щоб не вибирати вектори $h_1, ..., h_l$ наугад, а сформувати їх з використанням допоміжної процедури таким чином, щоб множина зазначених векторів з високою ймовірністю містилася у множині I_f, якщо f є k-вимірною функцією. Для цього пропонується розглянути звуження функції f на випадково вибраний підпростір векторного простору V_n. Зазначимо, що ідея застосування таких звужень під час перевірки різноманітних властивостей булевих функцій, імовірно, бере початок з роботи [12] та лежить в основі ймовірнісних алгоритмів тестування степеня поліномів від декількох змінних над полем з двох елементів [13, 14]. У даному випадку ця ідея реалізується наступним чином.

Позначимо $F_{m \times n}$ множину матриць розміру $m \times n$ над полем $F = \mathrm{GF}(2)$. Для будь-якої матриці $X \in F_{t \times n}$, де $k < t < n$, позначимо $f_X(u) = f(uX)$, $u \in V_t$ звуження функції f на підпростір, що породжується рядками матриці X.

Теорема 1. Якщо $f : V_n \to \{0,1\}$ – k-вимірна функція, то функція f_X також є k-вимірною. При цьому ймовірність події, яка полягає в тому, що при випадковому рівноймовірному виборі $t \times n$-матриці X множина $\{aX : a \in I_{f_X}\}$ міститься у множині I_f, є не менше за $1 - 2^{k-t}$.

Доведення. Встановимо ряд допоміжних властивостей k-вимірних булевих функцій. Наступна лема по суті співпадає з твердженням 2 у статті [7].

Лема 1. Функція $f : V_n \to \{0,1\}$ є k-вимірною у тому і тільки тому випадку, коли існують число $l \in \overline{0,k}$, матриця $A \in F_{n \times l}$ та функція $g : V_l \to \{0,1\}$ такі, що

$$f(x) = g(xA),\ x \in V_n. \qquad (3)$$

Якщо при цьому l є найменшим числом із зазначеною властивістю, то $I_f = \{\alpha \in V_n : \alpha A = 0\}$ і $\dim I_f = n - l$.

Назвемо представлення k-вимірної функції f у вигляді (3), яке відповідає найменшому можливому значенню $l \in \overline{0,k}$, незвідним представленням цієї функції.

Наслідок 1. Представлення (3) є незвідним тоді й тільки тоді, коли $rank\, A = l$ та $I_g = \{0\}$.

Лема 2. Нехай (3) є незвідним представленням k-вимірної функції f, де $g : V_l \to \{0,1\}$, $l \in \overline{0,k}$. Тоді

для будь-якої матриці $X \in F_{t\times n}$, де $k < t < n$, функція f_X є k-вимірною. Більш того, якщо $rank\, XA = l$, то

$$\{aX : a \in I_{f_X}\} \subseteq I_f . \quad (4)$$

Доведення. З рівності (3) випливає, що $f_X(u) = f(uX) = g(u(XA))$, $u \in V_t$. Отже, на підставі леми 3.1 f_X є k-вимірною функцією.

Нехай зараз $rank\, XA = l$. Оскільки представлення (3) є незвідним, то, згідно з наслідком 3.1, $I_g = \{0\}$. Отже, $f_X(u) = g(u(XA))$, $u \in V_t$ є незвідним представленням функції f_X і на підставі леми 3.1 $I_{f_X} = \{a \in V_t : aXA = 0\}$. Таким чином, якщо $a \in I_{f_X}$, то для будь-якого $z \in V_n$.

$$f(aX \oplus z) = g(aXA \oplus zA) = g(zA) = f(z),$$

тобто $aX \in I_f$, що й треба було довести.

Лема 3. Нехай $\alpha_1,...,\alpha_l \in V_n$ – лінійно незалежні вектори і $l \le t < n$. Тоді ймовірність того, що при випадковому рівноймовірному виборі матриці $X \in F_{t\times n}$ вектори $X\alpha_1,...,X\alpha_l$ є лінійно залежними, не перевищує 2^{l-t}.

Доведення. Якщо вектори $X\alpha_1,...,X\alpha_l$ лінійно залежні, існує ненульовий вектор $\alpha = c_1\alpha_1 \oplus \cdots \oplus c_l\alpha_l$ ($c_i \in F$, $i \in \overline{1,l}$) такий, що $X\alpha = 0$. Ймовірність останньої події дорівнює 2^{-t}. Отже, ймовірність того, що вектори $X\alpha_1,...,X\alpha_l$ є лінійно залежними не перевищує $(2^l - 1)2^{-t}$.

Лему доведено.

Виходячи з останніх двох лем, неважко переконатися в справедливості теореми 1. Дійсно, розглянемо незвідне представлення k-вимірної функції f у вигляді (3), де $g : V_l \to \{0,1\}$, $l \in \overline{0,k}$. Згідно з лемою 2, при випадковому рівноймовірному виборі матриці $X \in F_{t\times n}$ ймовірність події (4) є не менше ймовірності події $\{rank\, XA = l\}$, яка більше або дорівнює $1 - 2^{l-t} \ge 1 - 2^{k-t}$ на підставі леми 3.

Отже, теорему доведено.

2. ФОРМАЛЬНИЙ ОПИС МЕТОДУ РОЗПІЗНАВАННЯ *K*-ВИМІРНОСТІ БУЛЕВИХ ФУНКЦІЙ, ЗАДАНИХ ЗА ДОПОМОГОЮ ОРАКУЛІВ

Метод призначений для оцінки та обгрунтування стійкості блокових та потокових шифрів.

Основним показником ефективності є трудомісткість виражена в числі запитів до оракулу при заданих верхніх межах ймовірностей помилки першого та другого роду.

Додатковим показником ефективності є трудомісткість, виражена в числі двійкових операцій при заданих верхніх межах ймовірностей помилки першого та другого роду.

Сутність методу полягає в тому, щоб не вибирати вектори $h_1,...,h_l$ наугад, а сформувати їх з використанням допоміжної процедури таким чином, щоб множина зазначених векторів з високою ймовірністю містилася у множині I_f, якщо f є k-вимірною функцією. Це відрізняє запропонований метод від раніше відомого [3], який полягає в генерації незалежних випадкових рівноймовірних векторів $h_1,...,h_l \in V_n$.

Вхідними даними для застосування методу є такі параметри:

$$f : V_n \to \{0,1\};\ k \in \overline{0,n-1};\ \varepsilon \in (0,1);$$

$$t = k + c;\ m = 2^{t+4} t\, \varepsilon^{-1}\delta^{-1},$$

де $c \in \mathrm{N}$, $\delta \in (0, 1/2)$, $c, \delta = const$.

Припущення та обмеження: вважається, оракул, яким задана булева функція має нехтувано малий час оброблення запиту.

Алгоритм реалізації методу складається з двох кроків.

Крок 1. Згенерувати випадкову рівноймовірну $t \times n$-матрицю X, побудувати множину $Sp(f_X)$, за якою знайти базис $a_1,...,a_l$ векторного простору I_{f_X} (дуального до підпростору, що породжується множиною $Sp(f_X)$). Перевірити умову

$$l \ge t - k, \quad (5)$$

за виконанням якої перейти до кроку 2. У протилежному випадку – прийняти гіпотезу H_1 (f знаходиться на відстані не менше $2^n\varepsilon$ від множини k-вимірних функцій).

Крок 2. Для кожного $j \in \overline{1,l}$ покласти $h_j = a_j X$, згенерувати незалежні випадкові рівноймовірні вектори $Z_{1j},...,Z_{mj}$ та перевірити рівності (3.1). За виконанням зазначених рівностей для всіх $j \in \overline{1,l}$ прийняти гіпотезу H_0 (f – k-вимірна функція), у протилежному випадку – прийняти гіпотезу H_1.

Оцінка ефективності методу.

Теорема 3.2. Наведений алгоритм виконує $O(2^k k^2\, \varepsilon^{-1})$ запитів до оракула f та має трудомісткість $O(n\, 2^k k^2\, \varepsilon^{-1})$ двійкових операцій. При цьому ймовірність помилки першого роду (відхилити вірну гіпотезу H_0) не перевищує 2^{-c}, а ймовірність помилки другого роду (відхилити вірну гіпотезу H_1) не перевищує $\max\{5 \cdot 2^{-c-1}, \delta + \exp\{-7c2^c\}\}$.

Доведення. Почнемо з формулювань трьох допоміжних тверджень. Перше з них доведено в [15] та використовується в [3] як "факт 9". Друге твердження являє собою "факт 11" з [3], а третє – варіант нерівності Чебишова (див. твердження 4 в [3]).

Нагадаємо, що для функції $f:V_n\to\{0,1\}$ множина $Sp(f)$ визначається як сукупність усіх векторів $\alpha\in V_n$ таких, що $\hat f(\alpha)\neq 0$.

Лема 4. Для будь-якої функції $f:V_n\to\{0,1\}$ виконується рівність $I_f=Sp(f)^\perp$; іншими словами, простір I_f складається з векторів $y\in V_n$, що задовольняють умову: $y\alpha=0$ для будь-якого $\alpha\in Sp(f)$.

Лема 5. Нехай Z – випадковий рівноймовірний вектор на множині V_n. Тоді для будь-яких $f:V_n\to\{0,1\}$, $y\in V_n$ виконується рівність

$$\mathrm{P}_Z\{f(y\oplus Z)\neq f(Z)\}=\sum_{\substack{\alpha\in V_n:\\ y\alpha=1}}|\hat f(\alpha)|^2.$$

Лема 6. Нехай $\xi=\sum_{i=1}^N\xi_i$, де $\xi_1,\dots,\xi_N$ – попарно незалежні випадкові величини такі, що $0\le\xi_i\le\tau$, $i\in\overline{1,N}$. Тоді, якщо $\mathrm{E}\xi>0$, то для будь-якого $\delta>0$ справедлива нерівність $\mathrm{P}\{\xi\le(1-\delta)\mathrm{E}\xi\}\le\dfrac{\tau}{\delta^2\mathrm{E}\xi}$.

Лема 7. Алгоритм реалізації методу характеризується ймовірністю помилки першого роду не більше за 2^{-c}, виконує $O(2^k k^2\,\varepsilon^{-1})$ запитів до оракула f та має трудомісткість $O(n\,2^k k^2\,\varepsilon^{-1})$ двійкових операцій.

Доведення. Перше твердження леми випливає з теореми 1 та леми 4. Дійсно, якщо f є k-вимірною функцією, то такою ж є функція f_X. Отже, рівність (5) напевно виконується, і тест може здійснити помилку тільки в тому випадку, коли на кроці 2 порушується хоча б одна з рівностей (1). Проте на підставі теореми 1 ймовірність останньої події є не більше за $2^{k-t}=2^{-c}$, що й треба було довести.

Оцінимо трудомісткість алгоритму. На кроці 1 для обчислення значень функції f_X потрібно здійснити 2^t запитів до оракула f, кожен з яких вимагає порядка nt двійкових операцій. Далі, для знаходження коефіцієнтів Уолша-Адамара функції f_X треба виконати $O(2^t t)$ додавань або віднимань не більш ніж t-розрядних цілих чисел, що складає $O(2^t t^2)$ двійкових операцій. Такий саме час знадобиться для побудови базису векторного простору I_{f_X} за допомогою методу Гауса. На кроці 2 перевірка рівностей (1) для кожного з отриманих $l\le t$ базисних векторів вимагатиме не більше за $2mt$ запитів до оракула f, що складає $O(nmt)$ двійкових операцій.

Таким чином, з урахуванням значень параметрів m і t, загальне число запитів до оракула дорівнює $O(2^t+mt)=O(2^k k^2\,\varepsilon^{-1})$, а підсумкова трудомісткість алгоритму – $O(n2^t t+2^t t^2+nmt)=O(n2^k k^2\,\varepsilon^{-1})$ двійкових операцій.

Лему доведено.

Для оцінки ймовірності помилки другого роду скористаємося методом, що запропоновано в [3]. Зафіксуємо число $\theta\in(0,1)$ та розглянемо множини

$$B(\theta)=\{\alpha\in V_n\setminus\{0\}:|\hat f(\alpha)|\ge\theta\},$$

$$S(\theta)=\{\alpha\in V_n\setminus\{0\}:|\hat f(\alpha)|<\theta\}.$$

Покажемо спочатку, що якщо множина $B(\theta)$ породжує простір вимірності більше за k (і, отже, f напевно не є k-вимірною функцією), то Алгоритм реалізації методу здійснить помилку з нехтовно малою ймовірністю.

Лема 8. Нехай функція f є такою, що множина $B(\theta)$ містить щонайменше $k+1$ лінійно незалежних векторів $\alpha_1,\dots,\alpha_{k+1}$. Тоді ймовірність того, що Алгоритм реалізації методу здійснить помилку (тобто прийме f за k-вимірну функцію), не перевищує

$$p_1=2^{1-c}+(k+1)(1-\theta^2)^m 2^{k+c-1}. \qquad (6)$$

Доведення. Нехай алгоритм здійснює помилку. Тоді або вектори $X\alpha_1,\dots,X\alpha_{k+1}$ лінійно залежні (згідно з лемою 3, ймовірність цієї події становить не більше за $2^{k+1-t}=2^{1-c}$), або вони є лінійно незалежними, і тоді щонайменше один з них, скажимо, α_i, $i\in\overline{1,k+1}$, не належить множині $Sp(f_X)$. Оскільки на підставі леми 4 $I_{f_X}=Sp(f_X)^\perp$, то щонайменше один з базисних векторів $a_1,\dots,a_l$ простору I_{f_X} не є ортогональним вектору α_i. Отже, існує ненульовий вектор $a\in V_t$ такий, що $aX\alpha_i=1$ і для вектора $h_j=aX$ виконуються рівності (1). Таким чином, ймовірність помилки алгоритму не перевищує

$$2^{1-c}+\mathrm{P}_{X,Z_1,\dots,Z_m}\left(\bigcup_{i=1}^{k+1}\bigcup_{a\in V_t\setminus\{0\}}M_{i,a}\right)\le$$

$$\le 2^{1-c}+(k+1)2^t\max_{\substack{i\in\overline{1,k+1},\\ a\in V_t\setminus\{0\}}}\mathrm{P}_{X,Z_1,\dots,Z_m}\left(M_{i,a}\right),$$

де $M_{i,a}=\left\{aX\alpha_i=1, f(aX\oplus Z_s)=f(Z_s), s\in\overline{1,m}\right\}$.

Далі, на підставі незалежності та рівноймовірності випадкової матриці X та векторів $Z_1, \dots, Z_m$ для будь-яких $i \in \overline{1,k+1}$, $a \in V_t \setminus \{0\}$ виконується рівність

$$\mathrm{P}_{X,Z_1,\dots,Z_m}\left\{aX\alpha_i = 1, f(aX \oplus Z_s) = f(Z_s), s \in \overline{1,m}\right\} =$$

$$= \sum_{\substack{y \in V_n: \\ y\alpha_i = 1}} 2^{-nt} \sum_{\substack{X \in F_{t\times n}: \\ aX = y}} \left(\mathrm{P}_Z\{f(y \oplus Z) = f(Z)\}\right)^m .$$

При цьому, якщо $y\alpha_i = 1$, то на підставі леми 5 та умови $\alpha_i \in B(\theta)$ справедливі такі співвідношення:

$$\mathrm{P}_Z\{f(y \oplus Z) \neq f(Z)\} = \sum_{\substack{\alpha \in V_n: \\ y\alpha = 1}} |\hat{f}(\alpha)|^2 \geq |\hat{f}(\alpha_i)| \geq \theta^2 .$$

Отже,

$$\mathrm{P}_{X,Z_1,\dots,Z_m}\left\{aX\alpha_i = 1, f(aX \oplus Z_s) = f(Z_s), s \in \overline{1,m}\right\} \leq$$

$$\leq \sum_{\substack{y \in V_n: \\ y\alpha_i = 1}} 2^{-nt} \sum_{\substack{X \in F_{t\times n}: \\ aX = y}} (1-\theta^2)^m = \frac{1}{2}(1-\theta^2)^m .$$

З отриманих нерівностей випливає, що ймовірність помилки алгоритму не перевищує значення (6). Лему доведено.

Зауважимо, що у наведеному доведенні не використовується припущення про те, що функція f знаходиться на відстані не менше за $2^n\varepsilon$ від множини k-вимірних функцій. Залишається розглянути другий випадок, коли множина $B(\theta)$ породжує простір вимірності не більше за k. Міркування у цьому випадку значною мірою близькі до таких, що проводяться в [3]. Зокрема, наступна лема по суті співпадає з лемою 8 в [3].

Лема 9. Нехай функція f знаходиться на відстані не менше за $2^n\varepsilon$ від множини k-вимірних функцій n змінних, а множина $B(\theta)$ породжує підпростір вимірності не більше за k. Тоді

$$\sum_{\alpha \in S(\theta)} |\hat{f}(\alpha)|^2 \geq \varepsilon . \qquad (7)$$

Отже, для завершення доведення залишається оцінити ймовірність помилки алгоритму в припущенні справедливості нерівності (7).

Лема 10. Нехай виконується нерівність (7). Тоді ймовірність того, що Алгоритм реалізації методу здійснить помилку (тобто прийме f за k-вимірну функцію), не перевищує

$$p_2 = 2^{k+c}(8\varepsilon^{-1}\theta^2 + (1-\varepsilon/4)^m) . \qquad (8)$$

Доведення. Якщо алгоритм здійснює помилку, то існує, принаймні, один вектор $a \in V_t \setminus \{0\}$, для якого випадковий вектор $h_j = aX$ задовольняє рівності (1). Оскільки цей вектор має рівномірний розподіл на множині V_n, то ймовірність помилки алгоритму не перевищує

$$2^t \mathrm{P}_{Y,Z_1,\dots,Z_m}\left\{f(Y \oplus Z_s) = f(Z_s), s \in \overline{1,m}\right\}, \quad (9)$$

де $Y, Z_1, \dots, Z_m$ – незалежні в сукупності випадкові рівноймовірні вектори на V_n.

Для знаходження оцінки параметра (9) скористаємося міркуваннями, аналогічними таким, що використовуються у доведенні леми 7 в [3]. Розглянемо випадкову величину

$$\xi(Y) = \sum_{\alpha \in S(\theta)} |f(\alpha)|^2 I_\alpha(Y) ,$$

де $I_\alpha(Y)$ – індикатор події $Y\alpha = 1$, $\alpha \in S(\theta)$. Оскільки за означенням вектори $\alpha \in S(\theta)$ є ненульовими, то в силу нерівності (7)

$$\mathrm{E}\xi(Y) = \frac{1}{2} \sum_{\alpha \in S(\theta)} |f(\alpha)|^2 \geq \frac{\varepsilon}{2} . \qquad (10)$$

Крім того, випадкові величини $I_\alpha(Y)$, $\alpha \in S(\theta)$, є попарно незалежними. Отже, на підставі леми 6, означення множини $S(\theta)$ та нерівності (10)

$$\mathrm{P}_Y\left\{\xi(Y) \leq \frac{1}{2}\mathrm{E}\xi(Y)\right\} \leq \frac{\max\limits_{\alpha \in S(\theta)} |\hat{f}(\alpha)|}{1/4 \cdot \mathrm{E}\xi(Y)} \leq 8\theta^2\varepsilon^{-1} .$$

Помітимо зараз, що

$$\mathrm{P}_{Y,Z_1,\dots,Z_m}\left\{f(Y \oplus Z_s) = f(Z_s), s \in \overline{1,m}\right\} \leq$$

$$\leq \mathrm{P}_Y\left\{\xi(Y) \leq \frac{1}{2}\mathrm{E}\xi(Y)\right\} + \mathrm{P}_{Y,Z_1,\dots,Z_m}(M_Y) \leq$$

$$\leq 8\theta^2\varepsilon^{-1} + 2^{-n} \sum_{\substack{y \in V_n: \\ \xi(y) > \frac{1}{2}\mathrm{E}\xi(Y)}} \left(P_Z\{f(y \oplus Z) = f(Z)\}\right)^m ,$$

де $M_Y = \left\{f(Y \oplus Z_s) = f(Z_s), s \in \overline{1,m}, \xi(Y) > \frac{1}{2}\mathrm{E}\xi(Y)\right\}$.

При цьому на підставі леми 5 та нерівності (10) для будь-якого $y \in V_n$ такого, що $\xi(y) > \frac{1}{2}\mathrm{E}\xi(Y)$, справедливі такі нерівності:

$$\mathrm{P}_Z\{f(y \oplus Z) \neq f(Z)\} = \sum_{\substack{\alpha \in V_n: \\ y\alpha = 1}} |\hat{f}(\alpha)|^2 \geq \xi(y) > \frac{\varepsilon}{4} .$$

З останніх двох співвідношень отримаємо кінцеву оцінку параметра (9):

$$2^t \mathrm{P}_{Y,Z_1,\ldots,Z_m}\left\{f(Y\oplus Z_s)=f(Z_s),\, s\in\overline{1,m}\right\}\le$$

$$\le 2^t(8\varepsilon^{-1}\theta^2+(1-\varepsilon/4)^m).$$

Таким чином, ймовірність помилки алгоритму не перевищує значення (8), що й треба було довести.

Для завершення доведення теореми залишається зауважити, що на підставі лем 8 та 10 ймовірність помилки другого роду Алгоритму реалізації методу не перевищує $\max\{p_1, p_2\}$, де

$$\begin{aligned} p_1 &= 2^{1-c}+(k+1)(1-\theta^2)^m 2^{k+c-1},\\ p_2 &= 2^{k+c}(8\varepsilon^{-1}\theta^2+(1-\varepsilon/4)^m). \end{aligned} \qquad (11)$$

Вважаючи у формулах (11) $\theta^2=2^{-t-3}\,\varepsilon\,\delta$, $m=2^{t+4}t\,\varepsilon^{-1}\delta^{-1}$, де $\delta\in(0,1/2)$, отримаємо, що

$$p_1 \le 2^{1-c}+1/2\cdot(k+1)\exp\{k+c-\theta^2 m\}=$$

$$=2^{1-c}+1/2\cdot e^{-c}(k+1)e^{-k}<$$

$$<2^{1-c}+1/2\cdot 2^{-c}=5\cdot 2^{-c-1},$$

$$p_2=2^{k+c}(8\varepsilon^{-1}\theta^2+(1-\varepsilon/4)^m)=$$

$$=\delta+2^{k+c}(1-\varepsilon/4)^m<\delta+2^{k+c}\exp\{-m\varepsilon/4\}=$$

$$=\delta+2^{k+c}\exp\{-4t2^t\delta^{-1}\}<\delta+2^{k+c}\exp\{-8t2^t\}<$$

$$<\delta+\exp\{t-8t2^t\}<\delta+\exp\{-7t2^t\}<\delta+\exp\{-7c2^c\}.$$

Отже, ймовірність помилки другого роду Алгоритму реалізації методу не перевищує $\max\{5\cdot 2^{-c-1},\ \delta+\exp\{-7c2^c\}\}$.

Теорему повністю доведено.

Результати моделювання запропонованого методу. Для оцінки ефективності методу на практиці, наведений вище алгоритм реалізації методу був реалізовані програмно та застосовані для розпізнавання k-вимірності фільтрувальної функції f шифру Decim^{v2} [16].

Decim^{v2} – це синхронний потоковий шифр з довжиною ключа, яка дорівнює 80 бітів та вектором ініціалізації довжиною 64 біт. Decim^{v2} на сьогодні стандартизований [17]. В структурі Decimv2 можливо виділити (див. рис. 1): регістр зсуву з лінійним зворотним зв'язком довжиною 192 біти, нелінійну функцію f для генерації двійкової послідовності, функцію вибірки ABSG та буфер, що призначений для забезпечення безперервної видачі бітів гами (оскільки функція ABSG не забезпечує систематичну видачу бітів).

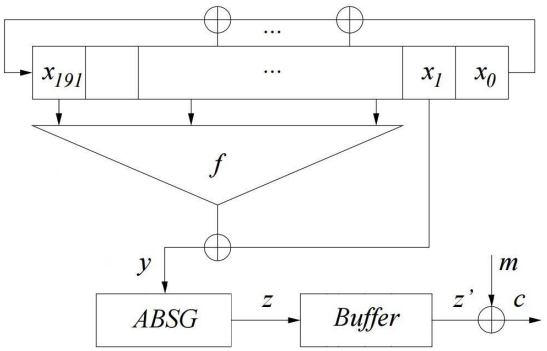

Рис. 1. Структурна схема шифру Decim^{v2}

Як зазначено в [17], функція f може бути означена таким чином

$$f(x_0,\ldots,x_{191})=\begin{cases}0, \textit{ якщо } S \bmod 4<2,\\ 1, \textit{ в іншому випадку}\end{cases},$$

де $S=1+x_{13}+x_{28}+x_{45}+x_{54}+x_{65}+x_{104}+x_{111}+$ $+x_{144}+x_{162}+x_{172}+x_{178}+x_{186}+x_{191}$.

Як видно з опису шифру Decim^{v2}, функція f має 192 змінних серед яких 13 є суттєвими, а, отже, k не перевищує 13.

Експерименти проведені з використанням пакета прикладних програм Maple на ПЕОМ типу Intel(R) Core(TM) i7-3770K 3,5 GHz, 8 Gb RAM у середовищі операційної системи Windows 7 та наступним чином.

Фіксувалися значення вхідних даних k, ε та δ (від якого безпосередньо залежить ймовірність помилки другого роду та значення p_0 ймовірності помилки першого роду тесту, яке дозволяє обчислити значення параметрів $c=-\log_2(p_0)$ та $t=k+c$), що задає значення $m=2^{t+4}t\,\varepsilon^{-1}\delta^{-1}$. Під час проведення обчислювального експерименту значення ε, δ та p_0 були обрані рівними 0,125.

Слід зауважити, що для моделювання випадкових рівноймовірних матриці X та векторів $Z_{1j},\ldots,Z_{mj}$ застосовувалась випадкова послідовність достатньо високої якості, що була сформована та протестована заздалегідь.

Кількість запусків обрана рівною 150 для кожного значення k від 1 до 13, щоб кількість відхилених вірних гіпотез H_0 (або H_1) не перевищувала 12,5% з надійністю не меншою 0,9973 (див., наприклад, [18], с. 99 – 100).

Як видно з таблиці 1, тест жодного разу не припустився помилки 1 роду, а ймовірність помилки 2 роду не перевищила 8%, що відповідає вихідним параметрам тесту, крім того, середній час перевірки гіпотези H_0 значно перевищує відповідний показник

для H_1, що пов'язано з необхідністю виконання кроку 2 вдосконаленого тесту k-вимірності в повному обсязі для кожного $j \in \overline{1,l}$ для перевірки гіпотези H_0.

Таблиця 1.

Результати дослідження функції f

k	$2^k k^2 \varepsilon^{-1}$	Кількість прийнятих гіпотез		Середній час перевірки гіпотези, сек.	
		H_0	H_1	H_0	H_1
1	16	0	150	–	0,04
2	128	0	150	–	0,07
3	576	0	150	–	0,11
4	2048	0	150	–	0,18
5	6400	0	150	–	0,30
6	18432	0	150	–	0,58
7	50176	0	150	–	1,06
8	131072	0	150	–	2,09
9	331776	0	150	–	4,21
10	819200	0	150	–	8,41
11	1982464	6	144	7071,48	17,41
12	4718592	12	138	12948,79	35,32
13	11075584	150	0	24687,61	–

Таким чином, вдосконалений тест може бути ефективно застосований на практиці до розпізнавання k-вимірності булевих функцій (зокрема, від десятків чи сотен змінних), які використовуються в сучасних симетричних криптосистемах.

Література

[1] *Chuan-Kun Wu* Boolean Functions and Their Applications in Cryptography / Chuan-Kun Wu, Dengguo Feng. Springer-Verlag Berlin Heidelberg, 2016, p. 267.

[2] *Логачев, О. А.* Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. М. : МЦНМО, 2004. 470 с.

[3] *Gopalan, P.* Testing Fourier dimensionality and sparsity / P. Gopalan, R. O'Donnel, A. Servedio, A. Shpilka, K. Wimmer // SIAM J. on Computing. 2011. V. 40(4). P. 1075–1100.

[4] *Gopalan, P.* A Fourier-analytic approach to Reed-Muller decoding / P. Gopalan // Annual IEEE Symp. on Foundation in Computer Science. – FOCS 2010, Proceedings. Berlin. Springer-Verlag. 2010. P. 685–694.

[5] *Lechner, R. L.* Harmonic analysis of switching functions / R. L. Lechner // Recent Developments in Switching Theory. New-York. Academic Press. 1971. P. 122–228.

[6] *Dawson, E.* Construction of correlation immune Boolean functions / E. Dawson, C.K. Wu // Information and Communication Security, Proceedings. Berlin. Springer-Verlag. 1997. P. 170–180.

[7] *Алексеев, Е. К.* О некоторых мерах нелинейности булевых функций / Е. К. Алексеев // Прикладная дискретная математика. 2011. № 2(12). С. 5–16.

[8] *Daemen, J.* Resynchronization weaknesses in synchronous stream ciphers / J. Daemen, R. Govaerts, J. Vandewalle // Advances in Cryptology – EUROCRYPT'93, Proceedings. Berlin. Springer-Verlag. 1993. P. 159–167.

[9] *Golić, J.* On the resynchronization attack / J. Golić, G. Morgari // Fast Software Encryption. – FSE'03, Proceedings. Berlin. Springer-Verlag. 2003. P. 100–110.

[10] *Алексеев, Е. К.* Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной / Е. К. Алексеев // Сборник статей молодых ученых факультета МВК МГУ, 2011. В. 8. С. 114–123.

[11] *Алексейчук, А. Н.* Усовершенствованный тест k-мерности для булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2013. Т. 49. № 2. С. 27–35.

[12] *Levin L.A.* Randomness and non-determinism / Levin L.A. // J. of Symbolic Logic. – 1993. – Vol. 58. – № 3. – P. 1102 – 1103.

[13] *Alon N.* Testing Reed-Muller codes / Alon N., Kaufman T., Krivelevich M., Litsyn S., Ron D. // IEEE Trans. on Inform. Theory. – 2005. – Vol. 51(11). – P. 4032 – 4039.

[14] *Bhattacharyya A.* Optimal testing of Reed-Muller codes / Bhattacharyya A., Kopparty S., Schoenebeck G., Sudan M., Zuckerman D. // Proc. of the 51st Annual IEEE Symposium on Fundations of Computer Sci. – Las Vegas, Nevada, Oct. 23 – 26, 2010. – P. 488 – 497.

[15] *Ященко В.В.* О критерии распространения для булевых функций и бент-функциях / Ященко В.В // Проблемы передачи информации. – 1997. – Т. 33. – № 1. – С. 75 – 86.

[16] *Berbain C.* Decim^{v2} / Berbain C., Billet O., Canteaut A., Courtois N., Debraize B., Gilbert H., Goubin L., Gouget A., Granboulan L., Lauradoux C., Minier M., Pornin T., Sibert H. // URL: https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/BBC08b.pdf (last access: 25.05.18).

[17] ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers, 2011. – 92 p.

[18] *Ширяев А.Н.* Вероятность / А.Н. Ширяев. В 2-х кн. – 3-е изд., перераб. и доп. – М.: МЦНМО, 2004. – Кн. 1. – 520 с.

Надійшла до редколегії 25.12.2018

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника інституту (з наукової роботи) Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Галузь наукових інтересів – криптографічні властивості булевих функцій.

УДК 621.391:519.2

Конюшок С. Н. **Метод распознавания k-мерности булевых функций, заданных с помощью оракулов** / С. Н. Конюшок // Прикладная радиоэлектроника: научный журнал. – 2018. – Том 17, №. 3, 4. – С. 168–175.

Предложен вероятностный метод распознавания k-мерности булевых функций, заданных с помощью оракулов, имеющий меньшую трудоемкость и характеризующийся меньшей вероятностью ошибки первого рода (при той же верхней границе вероятности ошибки второго рода) по сравнению с аналогичным ранее известным методом.

Ключевые слова: проверка свойств булевых функций, вероятностный метод, k-мерная функция, преобразование Уолша-Адамара.

Табл. 01. Іл. 01. Библиогр.: 18 назв.

UDC 621.391:519.2

Koniushok S. M. **The method for recognizing the k-dimensionality of Boolean functions given by the oracles** / S. M. Koniushok // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 168–175.

A probabilistic method of recognizing k-dimensionality of Boolean functions given by means of oracles is proposed. The proposed method has less time complexity and less likely to be characterized by a less first kind error probability (at the same upper bound of the second kind error probability) compared to the previously known method.

Keywords: testing properties of Boolean functions, probabilistic method, k-dimensional function, Walsh–Hadamard transform.

Tab. 01. Fig. 01. Ref.: 18 items.