МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИММЕТРИЧНЫХ ШИФРОВ

УДК 621.391:519.2

ШВИДКИЙ ІМОВІРНІСНИЙ АЛГОРИТМ ОЦІНЮВАННЯ ВІДСТАНІ МІЖ ЗРІВНОВАЖЕНОЮ БУЛЕВОЮ ФУНКЦІЄЮ ТА МНОЖИНОЮ *k*-ВИМІРНИХ ФУНКЦІЙ

С.М. КОНЮШОК, А.М. ОЛЕКСІЙЧУК, А.Ю. СТОРОЖУК

Запропоновано поліноміальний імовірнісний алгоритм обчислення значень нижніх меж відносної відстані між зрівноваженою булевою функцією від n змінних, що задається за допомогою оракула, та множиною *k*-вимірних функцій. Показано, що при малих значеннях k цей алгоритм може бути ефективно використано на практиці для аналізу кореляційних властивостей функцій ускладнення потокових шифрів.

Ключові слова: нелінійний криптоаналіз, кореляційна атака, *k*-вимірна функція, ймовірнісний алгоритм, обґрунтування стійкості потокових шифрів.

ВСТУП

Як відомо, необхідною умовою стійкості синхронних потокових шифрів відносно кореляційних атак є неможливість наближення функцій ускладнення, що використовуються в їхніх конструкціях, більш просто збудованими функціями. Найвідомішими прикладами булевих функцій, які мають просту аналітичну будову, є афінні функції, а також функції, що залежать від малої кількості змінних. Більш широкий клас утворюють так звані *k*-вимірні функції, тобто булеві функції від довільної кількості n змінних, що є лінійно еквівалентними функціями від фіксованого числа $k < n$ змінних. Дослідженню властивостей таких функцій, зокрема, як можливих наближень довільних булевих функцій, присвячено роботи [1–7]. Відомі також різноманітні атаки на генератори гами потокових шифрів, функції ускладнення яких є *k*-вимірними або близькими до таких [8–11].

Для обґрунтування стійкості потокових шифрів відносно зазначених атак треба обчислювати або оцінювати знизу відстань між заданою булевою функцією та множиною всіх *k*-вимірних функцій від n змінних. Зауважимо, що ця задача є нетривіальною навіть при $k = 2$, якщо n є достатньо великим числом (наприклад, $n \geq 64$). Головна причина труднощів полягає в надвеликій кількості *k*-вимірних функцій від n змінних, перелічення яких у реальному часі (при зазначених n) є практично неможливим. Зменшити перебір дозволяють теореми 4 і 5 в [2] (або теорема 1 в [7]), проте і в цьому випадку алгоритм обчислення значення відстані між довільною булевою функцією та множиною *k*-вимірних функцій від n змінних вимагає, щонайменше, $2^{k(n-k)}$ операцій.

У даній статті пропонується ймовірнісний алгоритм обчислення значень нижніх меж шуканої відстані, складність якого залежить лінійно від n (та поліноміально від величин, обернених до точності та імовірності помилки алгоритму). Зазначений алгоритм базується на розвитку ідей робіт [12–15], остання з яких присвячена розв'язанню задачі оцінювання відстані в окремому випадку $k = 1$. Наведено результати моделювання запропонованого алгоритму, які дозволяють стверджувати про можливість його застосування на практиці під час дослідження кореляційних властивостей функцій ускладнення потокових шифрів.

ПОСТАНОВКА ЗАДАЧІ ТА ОСНОВНІ ТЕОРЕТИЧНІ РЕЗУЛЬТАТИ

Нижче використовуються такі позначення:

V_n – векторний простір двійкових векторів довжини n;

$V_n^* = V_n \setminus \{0\}$;

$F_{n\times k}$ – множина матриць розміру $n \times k$ над полем $F = \mathbf{GF}(2)$;

B_n – множина булевих функцій від n змінних;

$d(f,g) = 2^{-n} |\{x \in V_n : f(x) \neq g(x)\}|$ – відносна відстань між функціями $f, g \in B_n$;

$d(f,U) = \min\limits_{g\in U} d(f,g)$ – відносна відстань між функцією $f \in B_n$ та множиною $U \subseteq B_n$;

$\hat{f}(\alpha) = 2^{-n} \sum\limits_{x\in V_n} (-1)^{f(x)\oplus \alpha x}$, $\alpha \in V_n$ – нормовані коефіцієнти Уолша-Адамара функції $f \in B_n$.

Функція $g \in B_n$ називається *k-вимірною*, якщо вона може бути подана у вигляді $g(x) = \varphi(xA)$, $x \in V_n$, де $\varphi \in B_k$, $A \in F_{n\times k}$, $k \in \overline{0,n-1}$ [3, 4].

Позначимо $B_{n,k}$ множину всіх *k*-вимірних функцій від n змінних. На підставі теореми 1 в [7] відносна відстань між функцією $f \in B_n$ та множиною $B_{n,k}$ визначається за формулою

$$d(f, B_{n,k}) = 1/2 \cdot \left(1 - \max_{H\in L_{n,k}} l_f(H)\right), \qquad (1)$$

де максимум береться за всіма k-вимірними підпросторами H векторного простору V_n,

$$l_f(H) = 2^{-k} \sum_{s \in V_k} \left| \sum_{x \in H} \hat{f}(x)(-1)^{\alpha_s x} \right|, \qquad (2)$$

а $\{\alpha_s : s \in V_k\}$ є системою представників усіх суміжних класів простору V_n по підпростору $H^{\perp}$, дуальному до H.

Припустимо, що f є зрівноваженою функцією, тобто задовольняє умову $\hat{f}(0) = 0$. Позначимо H^* довільний підпростір, на якому досягається максимум значень (2) у правій частині рівності (1) та зафіксуємо $n \times k$ -матрицю A, стовпці якої утворюють базис підпростору H^*. Тоді рівність (1) можна записати у вигляді

$$d(f, B_{n,k}) = 1/2 \cdot (1 - l_{f,A}), \qquad (3)$$

де

$$l_{f,A} = 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \hat{f}(Ay)(-1)^{sy} \right|. \qquad (4)$$

Припустимо зараз, що зрівноважена функція f задається за допомогою оракула, тобто певного алгоритму, що дозволяє обчислювати значення $f(x)$ для довільного вхідного набору $x \in V_n$. Треба розробити алгоритм, який обчислює для будь-яких $k \in \overline{1, n-1}$, $\varepsilon, \delta \in (0,1)$ статистичну верхню оцінку параметра (4) з точністю ε та надійністю не менше $1 - \delta$, тобто таке випадкове значення $\theta \in (0,1)$, що задовольняє умову

$$\mathbf{P}\{l_{f,A} \le \theta + \varepsilon\} \ge 1 - \delta. \qquad (5)$$

При цьому вимагається, щоб для будь-якого фіксованого k обчислювальна складність алгоритму поліноміально залежала від n, ε^{-1} та δ^{-1}.

Для викладення алгоритму, що пропонується, введемо низку позначень та доведемо одну теорему.

Зафіксуємо натуральне число $t > k$ та позначимо X випадкову матрицю з рівномірним розподілом ймовірностей на множині $F_{t \times n}$. Розглянемо випадкові величини

$$\xi_a(X) = \frac{1}{2^t - 1} \sum_{u \in V_t^*} (-1)^{f(uX) \oplus ua}, \; a \in V_t, \qquad (6)$$

$$\eta_B(X) = 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \xi_{By}(X)(-1)^{sy} \right|, \; B \in F_{t \times k}. \qquad (7)$$

Назвемо матрицю $B \in F_{t \times k}$ *спеціальною ступеневою*, якщо транспонована до неї матриця має вигляд

$$B^T = \begin{pmatrix} 0 \ldots 0 & \overset{i_1}{1} * \ldots * & 0 & * \ldots * & \overset{i_2}{0} * \ldots * & \overset{i_r}{0} * \ldots * \\ 0 \ldots 0 & 0 & 0 \ldots 0 & 1 * \ldots * & 0 * \ldots * & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 \ldots 0 & 0 & 0 \ldots 0 & 0 & 0 \ldots 0 & 1 * \ldots * \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 \ldots 0 & 0 & 0 \ldots 0 & 0 & 0 \ldots 0 & 0 \; 0 \ldots 0 \end{pmatrix},$$

де $*$ означає довільний елемент поля F, $1 \le i_1 < \ldots < i_r \le t$. Добре відомо (див., наприклад, [16], с. 149), що будь-яка матриця $B \in F_{t \times k}$ є стовпцево еквівалентною єдиній спеціальній ступеневій матриці, тобто існує точно одна зазначена матриця $\tilde{B}$, яка пов'язана з B співвідношенням $\tilde{B} = BU$, де U — оборотна матриця порядку k над полем F.

Позначимо $\tilde{F}_{t \times k}$ множину усіх спеціальних ступеневих матриць розміру $t \times k$ над F та покладемо

$$\theta(X) = \max_{B \in \tilde{F}_{t \times k}} \{\eta_B(X)\}. \qquad (8)$$

Теорема 1. Нехай $k \in \overline{1, n-1}$, $\varepsilon, \delta \in (0,1)$ і $2^t \ge 2^k \varepsilon^{-2} \delta^{-1}$. Тоді для випадкової величини $\theta = \theta(X)$ виконується нерівність (5).

Д о в е д е н н я. Перш за все, переконаємося у справедливості такої нерівності:

$$|l_{f,A} - \eta_{XA}(X)| \le \left(\sum_{y \in V_k^*} (\hat{f}(Ay) - \xi_{XAy}(X))^2 \right)^{1/2}. \qquad (9)$$

Дійсно, на підставі формул (4), (6) та нерівності між середнім арифметичним і середнім квадратичним

$$\left| l_{f,A} - \eta_{XA}(X) \right| =$$

$$= \left| 2^{-k} \sum_{s \in V_k} \left(\left| \sum_{y \in V_k^*} \hat{f}(Ay)(-1)^{sy} \right| - \left| \sum_{y \in V_k^*} \xi_{XAy}(X)(-1)^{sy} \right| \right) \right| \le$$

$$\le 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right| \le$$

$$\le \left(2^{-k} \sum_{s \in V_k} \left(\sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right)^2 \right)^{1/2}. \qquad (10)$$

Далі,

$$2^{-k} \sum_{s \in V_k} \left(\sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right)^2 =$$

$$= 2^{-k} \sum_{y_1, y_2 \in V_k^*} \left(\hat{f}(Ay_1) - \xi_{XAy_1}(X) \right) \left(\hat{f}(Ay_2) - \xi_{XAy_2}(X) \right) \times$$

$$\times \sum_{s \in V_k} (-1)^{s(y_1 \oplus y_2)} = \sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)^2.$$

Підставляючи зазначений вираз у формулу (10), отримаємо нерівність (9).

Покажемо зараз, що

$$\mathbf{P}_X\{|l_{f,A} - \eta_{XA}(X)| > \varepsilon\} \le 2^{k-t} \varepsilon^{-2}. \qquad (11)$$

Дійсно, на підставі формули (9) та нерівності Маркова справедливі такі оцінки:

$$\mathbf{P}_X\{|l_{f,A} - \eta_{XA}(X)| > \varepsilon\} \le$$

$$\le \mathbf{P}_X \left\{ \sum_{y \in V_k^*} (\hat{f}(Ay) - \xi_{XAy}(X))^2 > \varepsilon^2 \right\} \le$$

$$\le \varepsilon^{-2} \sum_{y \in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{XAy}(X))^2. \qquad (12)$$

Далі, безпосередньо з формули (6) випливає, що для будь-якого $y \in V_k^*$ математичне сподівання випадкової величини $\xi_{XAy}(X)$ дорівнює $\hat{f}(Ay)$. Отже,

$$\sum_{y\in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{XAy}(X))^2 =$$

$$= \sum_{y\in V_k^*} \mathbf{E}(\xi_{XAy}(X) - \mathbf{E}(\xi_{XAy}(X))^2 = \sum_{y\in V_k^*} \mathbf{D}(\xi_{XAy}(X)) =$$

$$= \frac{1}{(2^t-1)^2} \sum_{y\in V_k^*} \mathbf{D}\left(\sum_{u\in V_t^*} (-1)^{f(uX)\oplus uX(Ay)} \right) =$$

$$= \frac{1}{(2^t-1)^2} \sum_{y\in V_k^*} \sum_{u\in V_t^*} \mathbf{D}\left((-1)^{f(uX)\oplus uX(Ay)}\right),$$

де остання рівність випливає з того, що доданки в сумі під знаком дисперсії є попарно незалежними випадковими величинами. Нарешті, використовуючи тривіальну оцінку $\mathbf{D}\left((-1)^{f(uX)\oplus uX(Ay)}\right) \le 1$, $u \in V_t^*$, $y \in V_k^*$, отримаємо, що

$$\sum_{y\in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{XAy}(X))^2 \le \frac{2^k-1}{2^t-1} \le 2^{k-t}.$$

Звідси на підставі формули (12) випливає нерівність (11).

Для завершення доведення залишається зауважити, що $\eta_B(X) = \eta_{BU}(X)$ для будь-яких матриці $B \in F_{t\times k}$ та оберненої матриці $U \in F_{k\times k}$. Отже, згідно з формулою (8), $\theta(X) \ge \eta_B(X)$ для довільної (а не тільки спеціальної ступеневої) матриці $B \in F_{t\times k}$. Зокрема, подія $\{l_{f,A} > \theta(X) + \varepsilon\}$ тягне подію $\{l_{f,A} > \eta_{XA}(X) + \varepsilon\}$, звідки на підставі нерівності (11) випливає, що

$$\mathrm{P}_X\{l_{f,A} > \theta(X) + \varepsilon\} \le \mathrm{P}_X\{l_{f,A} > \eta_{XA}(X) + \varepsilon\} \le$$

$$\le \mathrm{P}_X\{|l_{f,A} - \eta_{XA}(X)| > \varepsilon\} \le 2^{k-t}\varepsilon^{-2}.$$

Таким чином, за виконанням умови $2^t \ge 2^k \varepsilon^{-2}\delta^{-1}$ справедлива нерівність (5).

Теорему доведено.

Наведемо зараз ймовірнісний **алгоритм обчислення нижніх меж параметра (3).**

Вхід: зрівноважена функція $f \in B_n$, задана за допомогою оракула; числа $k \in \overline{1,n-1}$, $\varepsilon, \delta \in (0,1)$.

1. Покласти

$$t = k + \left\lceil \log(\varepsilon^{-2}\delta^{-1}) \right\rceil, \qquad (13)$$

згенерувати випадкову рівноймовірну булеву $t\times n$-матрицю X та обчислити значення функції $f_X(u) = f(uX)$, $u \in V_t$.

2. Обчислити значення (6) за допомогою алгоритму швидкого перетворення Адамара.

3. Для кожної матриці $B \in \tilde{F}_{t\times k}$:

– за відомими значеннями (6) обчислити значення функції

$$h(y) = \begin{cases} \xi_{By}(X), \text{ якщо } y \in V_k^*; \\ 0, \text{ якщо } y = 0; \end{cases}$$

– обчислити значення

$$\hat{h}(s) = \sum_{y\in V_k^*} \xi_{By}(X)(-1)^{sy}, \ s \in V_k$$

за допомогою алгоритму швидкого перетворення Адамара;

– покласти $\eta_B(X) = 2^{-k} \sum_{s\in V_k} |\hat{h}(s)|$.

4. Покласти $\theta(X) = \max_{B\in\tilde{F}_{t\times k}} \{\eta_B(X)\}$.

Результат: випадкове число

$$\Delta(f, B_{n,k}) = 1/2 \cdot (1 - (\theta(X) + \varepsilon)),$$

що задовольняє умову

$$\mathrm{P}_X\{d(f, B_{n,k}) \ge \Delta(f, B_{n,k})\} \ge 1 - \delta.$$

Коректність алгоритму випливає з наведеної вище теореми.

Для оцінювання трудомісткості алгоритму доведемо допоміжне твердження.

Лема. Для будь-яких натуральних $k < t$ справедлива нерівність

$$|\tilde{F}_{t\times k}| \le c(k+1)\max\{2^{k^2}, 2^{k(t-k)}\},$$

де $c^{-1} = \prod_{i=1}^{\infty}(1 - 2^{-i})$.

Доведення. З означення множини $\tilde{F}_{t\times k}$ випливає, що $|\tilde{F}_{t\times k}| = \sum_{i=0}^{k} \begin{bmatrix} t \\ i \end{bmatrix}$, де

$$\begin{bmatrix} t \\ i \end{bmatrix} = \frac{(2^t-1)(2^{t-1}-1)\cdots(2^{t-i+1}-1)}{(2^i-1)(2^{i-1}-1)\cdots(2-1)}$$

є число i-вимірних підпросторів простору V_t, $i \in \overline{0,t}$. Використовуючи оцінку $\begin{bmatrix} t \\ i \end{bmatrix} \le c \cdot 2^{i(t-i)}$, $i \in \overline{0,t}$, отримаємо, що

$$|\tilde{F}_{t\times k}| = \sum_{i=0}^{k} \begin{bmatrix} t \\ i \end{bmatrix} \le c \sum_{i=0}^{k} 2^{i(t-i)} \le c(k+1)2^{t^2/4}.$$

Нехай $t \le 2k$. Тоді в силу наведеної нерівності $|\tilde{F}_{t\times k}| \le c(k+1)2^{k^2}$. Якщо ж $t > 2k$, то

$$\begin{bmatrix} t \\ i \end{bmatrix} \le \begin{bmatrix} t \\ k \end{bmatrix} \le c \cdot 2^{k(t-k)}$$

для кожного $i \in \overline{0,k}$ і, отже, $|\tilde{F}_{t\times k}| \le c(k+1)2^{k(t-k)}$. Таким чином, у будь-якому випадку виконується нерівність

$$|\tilde{F}_{t\times k}| \le c(k+1)\max\{2^{k^2}, 2^{k(t-k)}\},$$

що й треба було довести.

Теорема 2. Трудомісткість наведеного алгоритму в найгіршому випадку дорівнює

$$T_{n,k}(\varepsilon,\delta) =$$

$$= O\left(2^k(k + \varepsilon^{-2}\delta^{-1})(n\varepsilon^{-2}\delta^{-1} + k^2\max\{2^{k^2}, \varepsilon^{-2k}\delta^{-k}\})\right). \qquad (14)$$

Доведення. На кроці 1 потрібно виконати $O(2^t tn)$ операцій (булевого додавання та звернення до функції f), а на кроці 2 – $O(2^t t)$ операцій (додавання та віднімання цілих чисел). Далі, для кожної фіксованої матриці $B \in \tilde{F}_{t\times k}$ на кроці 3 потрібно виконати $O(2^k tk)$ таких самих операцій. Отже, на підставі леми трудомісткість кроку 3 складає

$$O(2^k tk\,|\,\tilde{F}_{t\times k}\,|) = O(2^k tk^2 \max\{2^{k^2}, 2^{k(t-k)}\}).$$

Нарешті, трудомісткість четвертого кроку є $O(|\,\tilde{F}_{t\times k}\,|) = O(\max\{2^{k^2}, 2^{k(t-k)}\})$. Підсумовуючи отримані оцінки, з урахуванням рівності (13) отримаємо формулу (14).

Теорему доведено.

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ ЗАПРОПОНОВАНОГО АЛГОРИТМУ

У табл. 1 показано чисельні значення двійкового логарифму виразу під знаком O у правій частині рівності (14). Як видно з таблиці, із збільшенням параметра k чи зменшенням параметра ε трудомісткість алгоритму досить швидко зростає. Навпаки, помітне збільшення параметра n практично не впливає на зростання трудомісткості алгоритму.

Таблиця 1

Чисельні оцінки трудомісткості алгоритму ($\delta = 0{,}0625$)

ε \ k	2		3		4	
1/2	20,3663	21,2143	22,7665	23,1536	30,0931	30,0987
1/4	25,0112	25,5962	30,2263	30,2647	36,0238	36,0252
1/8	30,3247	30,5878	38,1766	38,1791	46,0056	46,0057
n	64	128	64	128	64	128

У табл. 2, 3 показано результати застосування запропонованого алгоритму при $k = 2$ до функцій від 64 та 11 змінних відповідно. Обчислення проводилися на ЕОМ з процесором Intel Core i7 (1,6 ГГц) та обсягом оперативної пам'яті 4 Гб RAM (DDR3) на базі Windows 7 (використовувався пакет прикладних програм Maple 13.0). Середній час роботи комп'ютерної програми складає 804,5 секунди при $n = 64$ та 652,1 секунди при $n = 11$.

У табл. 2 наведено значення

$$\Delta(f, B_{n,2}) = 1/2 \cdot (1 - (\theta(X) + \varepsilon))$$

статистичних нижніх оцінок параметра $d(f, B_{n,2})$, отримані за допомогою запропонованого алгоритму для двох функцій вигляду

$$f(x) = f(x_1, x_2) = g(x_1, x_2) h_1(x_2) \oplus$$

$$\oplus\,(g(x_1, x_2) \oplus 1) h_2(x_2),\ x = (x_1, x_2) \in V_{n_1} \times V_{n_2},$$

де $g(x_1, x_2) = (\alpha_1 x_1)(\alpha_2 x_1)$ – двовимірна функція, що не залежить суттєво від останніх n_2 змінних (α_1 та α_2 є різними ненульовими булевими векторами довжини n_1, а $\alpha_i x_1$ означає булевий скалярний добуток векторів α_i та $x_1 \in V_{n_1}$, $i = 1, 2$); h_1 та h_2 – довільні булеві функції від n_2 змінних, що задовольняють умову $wt(h_1) = 2^{-n_2}(2^{n_2+1} - 3m)$, $wt(h_2) = 2^{-n_2} m$, де m – ціле число таке, що $2^{n_2} < 3m < 2^{n_2+1}$. Як показує прямий підрахунок, у цьому випадку

$$wt(f) = 1/4 \cdot wt(h_1) + 3/4 \cdot wt(h_2) = 1/2,$$

$$d(f, g) = 1/4 \cdot (1 - wt(h_1)) + 3/4 \cdot wt(h_2) =$$

$$= 1/4 + 1/2 \cdot (1 - wt(h_1)).$$

Отже, f є зрівноваженою функцією від $n = n_1 + n_2$ змінних, що знаходиться від множини $B_{n,2}$ на відносній відстані не більше, ніж

$$\Delta^*(f, B_{n,2}) =$$

$$= \min\{1/4 + 1/2 \cdot (1 - wt(h_1)),\ 3/4 - 1/2 \cdot (1 - wt(h_1))\}. \quad (15)$$

Параметр m у таблиці задає функції h_1 та h_2 за правилом:

$$h_1(x_2) = 1 \ \Leftrightarrow\ |x_2| < 2^{n_2+1} - 3m,$$

$$h_2(x_2) = 0 \ \Leftrightarrow\ |x_2| < 2^{n_2} - m,$$

де $|x_2|$ – двійкове ціле число, що відповідає вектору $x_2 \in V_{n_2}$. Значення t і $\theta(X)$ обчислені, відповідно, на кроках 1 і 4 алгоритму, а в останній колонці таблиці показано значення параметра (15).

Таблиця 2

Статистичні нижні оцінки параметра $d(f, B_{n,2})$ ($n_1 = 20$, $n_2 = 44$, $\varepsilon = 1/4$, $\delta = 0{,}0625$, $t = 10$)

Номер експерименту	m	$\theta(X)$	$\Delta(f, B_{n,2})$	$\Delta^*(f, B_{n,2})$
1	$(2^{44} + 5)/3$	0,5010	0,1245	0,25
2		0,5010	0,1245	
3		0,5191	0,1155	
4		0,5308	0,1096	
5		0,5020	0,1240	
6	$(2^{45} - 5)/3$	0,5020	0,1240	0,25
7		0,5059	0,1221	
8		0,5010	0,1245	
9		0,5020	0,1240	
10		0,5073	0,1213	

Табл. 3 демонструє результати застосування алгоритму до функції від 11 змінних, яка використовується в алгоритмі шифрування Achterbahn-128/80 [17]:

$$G(x_1, ..., x_{11}) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_9 \oplus x_{11} \oplus$$
$$\oplus x_2 x_{10} \oplus x_2 x_{11} \oplus x_4 x_8 \oplus x_5 x_6 \oplus x_6 x_8 \oplus x_6 x_{10} \oplus x_6 x_{11} \oplus$$
$$\oplus x_7 x_8 \oplus x_8 x_9 \oplus x_8 x_{10} \oplus x_9 x_{10} \oplus x_9 x_{11} \oplus x_1 x_2 x_8 \oplus$$
$$\oplus x_1 x_4 x_{10} \oplus x_1 x_4 x_{11} \oplus x_1 x_8 x_9 \oplus x_1 x_9 x_{10} \oplus x_1 x_9 x_{11} \oplus$$
$$\oplus x_2 x_3 x_8 \oplus x_2 x_4 x_8 \oplus x_2 x_4 x_{10} \oplus x_2 x_4 x_{11} \oplus x_2 x_7 x_8 \oplus$$
$$\oplus x_2 x_8 x_{10} \oplus x_2 x_8 x_{11} \oplus x_2 x_9 x_{10} \oplus x_2 x_9 x_{11} \oplus x_3 x_4 x_8 \oplus$$
$$\oplus x_3 x_8 x_9 \oplus x_4 x_7 x_8 \oplus x_4 x_8 x_9 \oplus x_5 x_6 x_8 \oplus x_5 x_6 x_{10} \oplus$$
$$\oplus x_5 x_6 x_{11} \oplus x_6 x_8 x_{10} \oplus x_6 x_8 x_{11} \oplus x_7 x_8 x_9 \oplus x_8 x_9 x_{10} \oplus$$
$$\oplus x_8 x_9 x_{11} \oplus x_1 x_2 x_3 x_8 \oplus x_1 x_2 x_7 x_8 \oplus x_1 x_3 x_5 x_8 \oplus x_1 x_3 x_8 x_9 \oplus$$
$$\oplus x_1 x_4 x_8 x_{10} \oplus x_1 x_4 x_8 x_{11} \oplus x_1 x_5 x_7 x_8 \oplus x_1 x_7 x_8 x_9 \oplus x_1 x_8 x_9 x_{10} \oplus$$
$$\oplus x_1 x_8 x_9 x_{11} \oplus x_2 x_3 x_4 x_8 \oplus x_2 x_3 x_5 x_8 \oplus x_2 x_4 x_7 x_8 \oplus x_2 x_4 x_8 x_{10} \oplus$$
$$\oplus x_2 x_4 x_8 x_{11} \oplus x_2 x_5 x_7 x_8 \oplus x_2 x_8 x_9 x_{10} \oplus x_2 x_8 x_9 x_{11} \oplus x_3 x_4 x_8 x_9 \oplus$$
$$\oplus x_4 x_7 x_8 x_9 \oplus x_5 x_6 x_8 x_{10} \oplus x_5 x_6 x_8 x_{11},\ (x_1, ..., x_{11}) \in V_{11}.$$

Обчислення відносної відстані $d(G, B_{n,2})$ за формулою (1) показує, що її точне значення дорівнює 0,4375. При цьому час обчислення складає 3020 секунд, що приблизно в 5 разів переви-

щує середній час оцінювання цього параметра з точністю $\varepsilon = 1/8$ та надійністю $1 - \delta \geq 0{,}75$ (див. табл. 3).

Таблиця 3

Статистичні нижні оцінки параметра $d(G, B_{n,2})$ ($n = 11$, $\varepsilon = 1/8$, $\delta = 0{,}25$, $t = 10$)

Номер експерименту	$\theta(X)$	$\varnothing(G, B_{n,2})$
1	0,2517	0,3316
2	0,1881	0,3434
3	0,1881	0,3434
4	0,1266	0,3742
5	0,1881	0,3434
6	0,2512	0,3119
7	0,2498	0,3126
8	0,1891	0,3429
9	0,1891	0,3429
10	0,2507	0,3121

Для підвищення точності оцінок, наведених у табл. 2 і табл. 3, слід зменшити значення ε, що призведе до збільшення часу виконання алгоритму. Наприклад, при $\varepsilon = 1/8$ нижня оцінка параметра $d(f, B_{n,2})$ становить приблизно 0,1871, при цьому середній час роботи комп'ютерної програми складає майже 4 години.

В цілому, отримані результати показують, що при малих значеннях k запропонований алгоритм може бути ефективно використано на практиці для аналізу кореляційних властивостей функцій ускладнення потокових шифрів.

Литература

[1] *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.

[2] *Canteaut A.* On the correlations between a combining function and function of fewer variables / A. Canteaut // The 2002 IEEE Information Theory Workshop, Proceedings. Berlin. Springer-Verlag. 2002. – P. 78–81.

[3] *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.

[4] *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.

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

[6] *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.

[7] *Алексейчук А. Н.* Алгебраически вырожденные приближения булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2014. Вып. 50. № 5 (в печати).

[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. – Вып. 8. – С. 114–123.

[11] *Алексейчук А. Н.* Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А. Н. Алексейчук, С. Н. Конюшок, А.Ю. Сторожук // Прикладная радиоэлектроника. 2014. – Вып. 176. – С. 13–21.

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

[13] *Bshouty N.* More efficient PAC-learning of DNF with membership queries under the uniform distribution / N. Bshouty, J. Jackson, C. Tamon // Proc. 12th Annual Conf. on Comput. Learning Theory, 1999. – P. 286–295.

[14] *Алексейчук А.Н.* Быстрый алгоритм статистического оценивания максимальной несбалансированности билинейных аппроксимаций булевых отображений / А.Н. Алексейчук, А.С. Шевцов // Прикладная дискретная математика. 2011. – № 3(13). – С. 5–11.

[15] *Алексейчук А.Н.* О статистических свойствах нелинейности сужений булевых функций на случайно выбранное подпространство / А.Н. Алексейчук, С.Н. Конюшок // Прикладная дискретная математика. 2012. – Вып. 1(15). – С. 5–10.

[16] *Глухов М.М.* Алгебра / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. – Учеб. в 2-х т., Т. 1. – М.: Гелиос АРВ, 2003. – 336 с.

[17] *Gammel B.M.* Achterbahn-128/80 / B.M. Gammel, R. Gottfert, O. Kniffler // eSTREAM, ECRYPT Stream Cipher Ptoject, Report 2006/001, 2006.

Надійшла до редколегії 4.06.2014

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник (з навчальної та наукової роботи) начальника Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: криптографічні властивості булевих функцій.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: теоретична криптографія.

Сторжук Артем Юрійович, аспірант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: прикладна криптографія.

УДК 621.391:519.2

Быстрый вероятностный алгоритм оценивания расстояния между уравновешенной булевой функцией и множеством *k*-мерных функций / С.М. Конюшок, А.Н. Алексейчук, А.Ю. Сторожук // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 186–191.

Предложен полиномиальный вероятностный алгоритм вычисления значений нижних границ относительного расстояния между уравновешенной булевой функцией от *n* переменных, заданной с помощью оракула, и множеством *k*-мерных функций. Показано, что при малых значениях *k* этот алгоритм может быть эффективно использован на практике для анализа корреляционных свойств функций усложнения поточных шифров.

Ключевые слова: нелинейный криптоанализ, корреляционная атака, *k*-мерная функция, вероятностный алгоритм, обоснование стойкости поточных шифров.

Табл.: 3. Библиогр.: 17 назв.

UDC 621.391:519.2

Fast probabilistic algorithm for distance evaluation between balanced Boolean function and set of *k*-dimensional functions / S.N. Konyushok, A.N. Alekseychuk, A.Yu. Storozhuk // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 186–191.

A polynomial probabilistic algorithm for computing the values of lower bounds of the relative distance between a balanced Boolean function in *n*-variables (defined by an oracle) and a set of *k*-dimensional functions is proposed. It is shown that for small values of *k* this algorithm can be efficiently used in practice to analyze the correlation properties of Boolean functions used in stream ciphers.

Keywords: non-linear cryptanalysis, correlation attack, *k*-dimensional function, probabilistic algorithm, stream ciphers resistance proof.

Tab.: 3. Ref.: 17 items.