МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

УДК 621.391:519.2 **DOI:10.30837/rt.2021.1.204.01**

А.М. ОЛЕКСІЙЧУК, д-р техн. наук

УЗАГАЛЬНЕНИЙ ДИФЕРЕНЦІАЛЬНО-ЛІНІЙНИЙ КРИПТОАНАЛІЗ БЛОКОВИХ ШИФРІВ

Вступ

Диференціально-лінійний метод криптоаналізу блокових шифрів запропоновано в 1994 р. [1]. Його сутність полягає у сумісному застосуванні для побудови атаки на шифр високоймовірного диференціалу для перших раундів та високоймовірної лінійної апроксимації для останніх раундів шифрування. Зазначений метод виявляється більш ефективним в порівнянні з (окремо) диференціальним та лінійним методами при застосуванні до багатьох блокових шифрів (див. [1 – 5]), проте його наукове обґрунтування залишається предметом подальших досліджень.

Відомо декілька публікацій [2 – 5], присвячених формалізації диференціально-лінійного методу та з'ясуванню умов, за яких його трудомісткість може бути оцінено математично строго. Певний прогрес в цьому напрямі зроблено протягом останніх років [4, 5], але проблема обґрунтування диференціально-лінійного методу в повному обсязі залишається не вирішеною. Мета статті – викласти перші результати, отримані автором у напрямі вирішення цієї проблеми.

В п. 1 розширюється клас диференціально-лінійних атак на блокові шифри. А саме, розглядаються як розрізнювальні атаки, так і атаки, спрямовані на відновлення одного біту інформації про ключ. При цьому не робиться жодних припущень (як у відомих публікаціях [1 – 5]) про можливість представлення шифру у вигляді певних двох компонент. За допомогою окремих результатів роботи [6] отримано нижні оцінки інформаційної складності зазначених атак, вирази яких залежать від усереднених (за ключами) значень квадратів елементів узагальненої автокореляційної таблиці шифрувального перетворення [7]. На відміну від відомих [1, 2, 4], отримані оцінки інформаційної складності диференціально-лінійних атак не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються, та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою. Для порівняння викладено також евристичний підхід до побудови оцінок інформаційної складності узагальненої диференціально-лінійної атаки, який є загальновизнаним у випадку звичайної розрізнювальної атаки.

В п. 2 у важливому окремому випадку отримано явний вираз середнього значення параметра, який фігурує в зазначених вище оцінках, для випадкової рівноймовірної підстановки на множині повідомлень, що шифруються. Аналогічно диференціальному або лінійному методам криптоаналізу цей результат надає можливість порівнювати диференціально-лінійні властивості бієктивних булевих відображень з аналогічними властивостями "ідеального" криптографічного відображення, тобто випадкової рівноймовірної підстановки.

В п. 3 наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт [4, 6, 8], використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано також нове співвідношення для елементів узагальненої автокореляційної таблиці шифрувального перетворення добутку двох блокових шифрів, яке може бути корисним в подальших дослідженнях. Наприкінці статті сформульовано стислі висновки.

1. Узагальнені диференціально-лінійні атаки на блокові шифри

Для будь-якого натурального n позначимо $\sigma(V_n)$ симетричну групу підстановок на множині $V_n = \{0,1\}^n$. Для будь-яких $\alpha = (\alpha_1,...,\alpha_n)$, $\beta = (\beta_1,...,\beta_n) \in V_n$ покладемо $\alpha\beta = \alpha_1\beta_1 \oplus \cdots \oplus \alpha_n\beta_n$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \dots, \alpha_n \oplus \beta_n)$.

Розглянемо блоковий шифр $\Im$ з множиною відкритих (шифрованих) повідомлень $X = V_n$, множиною ключів $K = V_m$ та сім'єю шифрувальних перетворень $(F_k : k \in K)$.

Узагальнена диференціально-лінійна атака на шифр $\Im$ визначається за допомогою ненульових векторів $a, \alpha, \beta \in V_n$, комутативної групової операції $+$ на множині V_n та зрівноваженої функції $\psi : K \to \{0,1\}$. Вважається, що при проведенні атаки супротивник має доступ до оракула F_k з невідомим (вибраним випадково рівноймовірно з множини K) ключем k. Супротивник генерує незалежні в сукупності випадкові рівноймовірні відкриті тексти $X_1, \dots, X_t \in V_n$ та обчислює за відповідними шифротекстами $F_k(X_i), F_k(X_i \oplus a)$ значення $\nu_i = \alpha F_k(X_i) \oplus \beta F_k(X_i + a)$, $i \in \overline{1,t}$. Мета атаки полягає в тому, щоб відновити значення $\psi(k)$ за послідовністю $\nu_1, \dots, \nu_t$.

Зауважимо, що для побудови ефективних диференціально-лінійних атак слід вибирати вектори a, α, β, операцію $+$ та функцію ψ, виходячи з особливостей будови блокового шифру так, щоб випадкова послідовність $\nu_1, \dots, \nu_t$ містила якомога більше інформації про значення $\psi(k)$. Поряд з тим, для обґрунтування стійкості блокових шифрів відносно диференціально-лінійного методу криптоаналізу можна використовувати нижню оцінку інформаційної складності наведеної атаки, яка не накладає жодних додаткових обмежень на вектори a, α, β, операцію $+$ та функцію ψ. Для того щоб навести зазначену оцінку, розглянемо більш загальну атаку на шифр $\Im$, описану в [6], та скористаємося доведеним там твердженням 1.

Загальна атака (d-го порядку, $d = 1, 2, \dots$) на шифр $\Im$ будується на основі пари відображень $\varphi : X^d \times X^d \to Z$, $\psi : K \to S'$, де Z, S' – скінченні множини, відображення φ є відмінним від константи, а відображення ψ задовольняє умові $|\psi^{-1}(s')| = |K| \cdot |S'|^{-1}$ для будь-якого $s' \in S'$. Вважається, що на множині K задано рівномірний розподіл ймовірностей, а на множині X^d – певний розподіл $P^{(d)}$. При проведенні атаки супротивник має доступ до оракула F_k з невідомим (вибраним випадково рівноймовірно з множини K) ключем k. Супротивник генерує незалежні в сукупності набори відкритих повідомлень $X_i = (X_{i,1}, \dots, X_{i,d})$, кожен з яких розподілений за законом $P^{(d)}$, отримує набори $F_k(X_i) = (F_k(X_{i,1}), \dots, F_k(X_{i,d}))$ та обчислює значення $Z_i = \varphi(X_i, F_k(X_i))$, $i \in \overline{1,t}$. Мета супротивника – відновити значення $\psi(k)$ за відомою послідовністю $Z^{(t)} = Z_1, \dots, Z_t$.

Наступна лема дозволяє оцінити інформаційну складність наведеної атаки.

Лема 1 [6]. Найменший обсяг даних, необхідних для проведення описаної загальної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{(1-\delta)\log|S'| - h(\delta)}{|K|^{-1} \sum_{k \in K} \Delta(P_k)} \ln 2, \qquad (1)$$

де

$$\Delta(P_k) = |Z|^{-1} \sum_{z \in Z} (|Z| P^{(d)}\{\varphi(X, F_k(X)) = z\} - 1)^2, \qquad (2)$$

$h(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$, а $X = (X_1, \dots, X_d)$ є випадковим вектором, розподіленим на множині X^d за законом $P^{(d)}$, $F_k(X) = (F_k(X_1), \dots, F_k(X_d))$, $k \in K$.

Доведемо зараз наступне твердження.

Твердження 1. Найменший обсяг даних, необхідних для проведення на шифр $\Im$ диференціально-лінійної атаки (на основі векторів a, α, β, операції $+$ та функції ψ) з імовірністю

помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{(1-\delta-h(\delta))\ln 2}{|K|^{-1}\sum\limits_{k\in K}(2\mathbf{P}_X\{\alpha F_k(X)=\beta F_k(X+a)\}-1)^2}, \tag{3}$$

де X – випадковий вектор з рівномірним розподілом ймовірностей на множині V_n.

Доведення. Помітимо, що диференціально-лінійна атака на шифр $\Im$ є окремим випадком наведеної вище загальної атаки при $d=2$, $S'=Z=\{0,1\}$, $\varphi((x,x'),(y,y'))=\alpha y \oplus \beta y'$, $x,x',y,y' \in V_n$ та розподілі ймовірностей $P^{(d)}$, що є рівномірним на множині $\{(x, x+a): x \in V_n\}$. Оскільки при цьому

$$\Delta(P_k)=|Z|^{-1}\sum_{z\in Z}(|Z|P^{(d)}\{\varphi(X, F_k(X))=z\}-1)^2 =$$

$$=(2\mathbf{P}_X\{\alpha F_k(X)=\beta F_k(X+a)\}-1)^2,$$

то нерівність (3) є безпосереднім наслідком нерівності (1). Твердження доведено.

Поряд із наведеною вище диференціально-лінійною атакою, спрямованою на відновлення значення $\psi(k)$ (тобто одного біту інформації про ключ) за випадковою послідовністю $\nu_i = \alpha F_k(X_i) \oplus \beta F_k(X_i + a)$, $i \in \overline{1,t}$, розглянемо також розрізнювальну атаку на шифр $\Im$, яка має за мету відрізнити цей шифр від суто випадкової підстановки на множині V_n шляхом аналізу послідовності ν_i, $i \in \overline{1,t}$. Зауважимо, що саме такі атаки (в окремому випадку $\alpha = \beta$) розглядаються в переважній більшості робіт, присвячених диференціально-лінійному криптоаналізу (див., наприклад, [2, 4, 5]).

Для того щоб навести нижню оцінку інформаційної складності розрізнювальної диференціально-лінійної атаки, розглянемо спочатку більш загальну атаку на шифр $\Im$, описану в [6].

Нехай Φ – випадкове відображення, яке з ймовірністю $1/2$ є випадковою рівноймовірною підстановкою на множині $X = V_n$ (гіпотеза H_0) або випадковим рівноймовірним шифрувальним перетворенням шифру $\Im$ (гіпотеза H_1). Розрізнювальна атака на шифр $\Im$ будується на основі відмінної від константи функції $\varphi: X^d \times X^d \to Z$ та розподілу ймовірностей $P^{(d)}$ на множині X^d і спрямована на те, щоб розрізнити гіпотези H_0 та H_1 за відомою реалізацією випадкової послідовності $Z^{(t)} = Z_1, \ldots, Z_t$, де $Z_i = \varphi(X_i, \Phi(X_i))$, а $X_i = (X_{i,1}, \ldots, X_{i,d})$ є незалежними наборами відкритих повідомлень, кожен з яких розподілений за законом $P^{(d)}$, $\Phi(X_i) = (\Phi(X_{i,1}), \ldots, \Phi(X_{i,d}))$, $i \in \overline{1,t}$.

Наступна лема містить нижню оцінку інформаційної складності цієї атаки.

Лема 2 [6]**.** Найменший обсяг даних, необхідних для проведення зазначеної розрізнювальної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{2(1-h(\delta))\ln 2}{|K|^{-1}\sum\limits_{k\in K}\Delta(P_k)+|\sigma(V_n)|^{-1}\sum\limits_{F\in\sigma(V_n)}\Delta(P_F)}, \tag{4}$$

де $\Delta(P_k)$ визначається за формулою (2), а $\Delta(P_F)$ – за аналогічною формулою, яка отримується з формули (2) шляхом заміни у ній F_k на $F \in \sigma(V_n)$.

Вважаючи у формулюванні леми 2 $d=2$, $Z=\{0,1\}$, $\varphi((x,x'),(y,y'))=\alpha y \oplus \beta y'$, $x,x',y,y' \in V_n$, та визначаючи $P^{(d)}$ як рівномірний розподіл ймовірностей на множині

$\{(x, x+a): x \in V_n\}$, отримаємо наступне твердження, яке встановлює нижню межу інформаційної складності розрізнювальної диференціально-лінійної атаки, що будується на основі ненульових векторів $a, \alpha, \beta \in V_n$ та операції $+$.

Твердження 2. Найменший обсяг даних, необхідних для проведення на шифр $\Im$ диференціально-лінійної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності (4), де

$$\Delta(P_k) = (2\mathbf{P}_X\{\alpha F_k(X) = \beta F_k(X+a)\} - 1)^2, \tag{5}$$

$$\Delta(P_F) = (2\mathbf{P}_X\{\alpha F(X) = \beta F(X+a)\} - 1)^2, \tag{6}$$

а X є випадковим вектором із рівномірним розподілом ймовірностей на множині V_n.

На завершення цього пункту розглянемо традиційну розрізнювальну диференціально-лінійну атаку на шифр $\Im$, яка будується на основі ненульових векторів a, α, β, що задовольняють умові

$$\mathbf{P}_{x,k}\{\alpha F_k(x) = \beta F_k(x+a)\} \geq 1/2 \cdot (1+\varepsilon), \tag{7}$$

де x і k є незалежними випадковими векторами з рівномірними розподілами ймовірностей на множинах X і K відповідно, $\varepsilon \in (0, 1/2)$. Вважається, що при проведенні атаки супротивник має доступ до оракула F, який з імовірністю $1/2$ є реалізацією випадкової рівноймовірної підстановки на множині V_n (гіпотеза H_0) і з такою ж ймовірністю співпадає з шифрувальним перетворенням F_k шифру $\Im$ при невідомому ключі k, вибраному випадково рівноймовірно з множини K (гіпотеза H_1). Мета атаки полягає в тому, щоб розрізнити зазначені гіпотези. Для цього супротивник генерує незалежні в сукупності випадкові рівноймовірні вхідні повідомлення $X_1, \ldots, X_t \in V_n$, обчислює за відповідними вихідними повідомленнями $F(X_i), F(X_i + a)$ значення $\nu_i = \alpha F(X_i) \oplus \beta F(X_i + a)$, $i \in \overline{1,t}$, та перевіряє умову $\nu_1 + \cdots + \nu_t > C$ (для заздалегідь визначеної величини $C > 0$). Якщо ця умова виконується, то приймається гіпотеза H_0; інакше приймається гіпотеза H_1.

Визначимо умови, за яких наведена атака є успішною, та оцінимо її трудомісткість. Перш за все, доведемо таку лему.

Лема 3. Середнє значення ймовірності $\mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\}$ за всіма підстановками $F \in \sigma(V_n)$ дорівнює $1/2$, якщо $\alpha \neq \beta$ та $1/2 \cdot (1 - (2^n - 1)^{-1})$, якщо $\alpha = \beta$.

Доведення. Помітимо, що

$$\frac{2}{2^n!}\sum_{F \in \sigma(V_n)} \mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\} - 1 = \frac{1}{2^n!}\sum_{F \in \sigma(V_n)} 2^{-n} \sum_{x \in V_n} (-1)^{\alpha F(x) \oplus \beta F(x+a)} =$$

$$= \frac{1}{2^n!} 2^{-n} \sum_{x \in V_n} \sum_{\substack{y,z \in V_n: \\ y \neq z}} |\{F \in \sigma(V_n): F(x) = y, F(x+a) = z\}| (-1)^{\alpha y \oplus \beta z} =$$

$$= \frac{1}{2^n(2^n - 1)} \sum_{\substack{y,z \in V_n: \\ y \neq z}} (-1)^{\alpha y \oplus \beta z} = \frac{1}{2^n(2^n - 1)} \left(0 - \sum_{y \in V_n} (-1)^{(\alpha \oplus \beta) y} \right).$$

При цьому останній вираз дорівнює 0, якщо $\alpha \neq \beta$ та $-(2^n - 1)^{-1}$, якщо $\alpha = \beta$. Лему доведено.

З опису наведеної атаки випливає, що випадкова послідовність $\nu_i = \alpha F(X_i) \oplus \beta F(X_i + a)$, $i \in \overline{1,t}$, яку спостерігає супротивник, є схемою Бернуллі з ймовір-

ністю успіху $p_F = 1 - \mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\}$. При цьому на підставі леми 3 число $\frac{1}{2^n!}\sum_{F\in\sigma(V_n)} p_F$ майже не відрізняється від $1/2$ (при $n \geq 64$), в той час як за умови (7) число $\frac{1}{|K|}\sum_{k\in K} p_{F_k}$ не перевищує $1/2\cdot(1-\varepsilon)$. Зазначений факт дозволяє прийняти такі припущення, аналогічні відомим гіпотезам про розрізненість та, відповідно, стохастичну еквівалентність ключів у статистичних атаках на блокові шифри (див., наприклад, [9, 10]).

Припущення 1. За умови справедливості гіпотези H_0 для кожного $F \in \sigma(V_n)$ виконується рівність $p_F = 1/2$.

Припущення 2. За умови справедливості гіпотези H_1 для кожного $k \in K$ виконується нерівність $p_{F_k} \leq 1/2\cdot(1-\varepsilon)$.

Використовуючи стандартні міркування із застосуванням нерівності Гефдінга [11], отримаємо наступне твердження, яке встановлює оцінку трудомісткості наведеної атаки.

Твердження 3. Нехай виконуються умова (7) та припущення 1 і 2. Тоді при $C = t/2\cdot(1+\varepsilon/2)$, $t = \left\lceil 8\varepsilon^{-2}\ln(\delta^{-1})\right\rceil$, $\delta \in (0,\, 1/2)$ наведена атака дозволяє відрізнити блоковий шифр $\mathfrak{I}$ від випадкової рівноймовірної підстановки на множині V_n із середньою ймовірністю помилки не вище ніж δ за $O(t)$ операцій.

Зауважимо, що твердження 3 встановлює верхню оцінку трудомісткості описаної розрізнювальної атаки на шифр $\mathfrak{I}$ за умови припущень 1 і 2, в той час як твердження 2 визначає нижню оцінку трудомісткості будь-якої розрізнювальної диференціально-лінійної атаки на шифр $\mathfrak{I}$ без жодного евристичного припущення. Згідно з твердженням 3 трудомісткість наведеної атаки обернено пропорційна параметру $(2\mathbf{P}_{x,k}\{\alpha F_k(x) = \beta F_k(x+a)\} - 1)^2$, який не перевищує середнє арифметичне значення чисел (5) за всіма $k \in K$.

2. Аналітичний вираз середнього значення параметра, що характеризує диференціально-лінійні властивості випадкової рівноймовірної підстановки

Розглянемо практично важливий випадок, в якому операція $+$ співпадає з покоординатним булевим додаванням $\oplus$ на множині V_n, та отримаємо в цьому випадку явний вираз параметра $\overline{\Delta}_a(\alpha,\beta) = |\sigma(V_n)|^{-1}\sum_{F\in\sigma(V_n)}\Delta(P_F)$, де $\Delta(P_F)$ визначається за формулою (6). Доведемо наступне твердження.

Твердження 4. Справедливі рівності

$$\overline{\Delta}_a(\alpha,\beta) = 2^{1-n} + \frac{(3\cdot 2^n - 6)}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha = \beta; \tag{8}$$

$$\overline{\Delta}_a(\alpha,\beta) = 2^{-n} - \frac{1}{2^n(2^n-1)} + \frac{2^n-6}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha \neq \beta. \tag{9}$$

Доведення. На підставі формули (6)

$$\Delta(P_F) = \left(2^{-n}\sum_{x\in V_n}(-1)^{\alpha F(x)\oplus\beta F(x\oplus a)}\right)^2 =$$

$$= 2^{-2n}\sum_{(x,\,x')\in V_n\times V_n}(-1)^{\alpha(F(x)\oplus F(x'))\oplus\beta(F(x\oplus a)\oplus F(x'\oplus a))} = S_1 + S_2 + S_3,$$

де S_1, S_2 та S_3 позначають суми зазначених виразів за всіма парами (x, x'), що належать множинам $M_1 = \{(x, x') \in V_n \times V_n : x' = x\}$, $M_2 = \{(x, x') \in V_n \times V_n : x' = x \oplus a\}$ та $M_3 = \{(x, x') \in V_n \times V_n : x' \notin \{x, x \oplus a\}\}$ відповідно.

Позначимо $\overline{S}_l$ середнє значення суми S_l за всіма підстановками $F \in \sigma(V_n)$, $l = 1, 2, 3$. Тоді

$$\overline{\Delta}_a(\alpha, \beta) = \overline{S}_1 + \overline{S}_2 + \overline{S}_3. \tag{10}$$

При цьому

$$\overline{S}_1 = 2^{-n}, \tag{11}$$

$$\overline{S}_2 = 2^{-2n} \sum_{x \in V_n} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{(\alpha \oplus \beta)(F(x) \oplus F(x \oplus a))} = 2^{-n}, \text{ якщо } \alpha = \beta.$$

Нехай $\alpha \neq \beta$. Тоді

$$|\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{(\alpha \oplus \beta)(F(x) \oplus F(x \oplus a))} =$$

$$= \frac{1}{2^n!} \sum_{\substack{(y,z) \in V_n \times V_n: \\ y \neq z}} \sum_{\substack{F \in \sigma(V_n): \\ F(x)=y, \\ F(x \oplus a)=z}} (-1)^{(\alpha \oplus \beta)(y \oplus z)} =$$

$$= \frac{1}{2^n(2^n - 1)} \sum_{\substack{(y,z) \in V_n \times V_n: \\ y \neq z}} (-1)^{(\alpha \oplus \beta)(y \oplus z)} = -\frac{1}{2^n - 1},$$

де остання рівність випливає зі співвідношення ортогональності для характерів (див., наприклад, [12]). Отже, у випадку, що розглядається, маємо $\overline{S}_2 = 2^{-2n} \sum_{x \in V_n} \frac{-1}{2^n - 1} = -\frac{1}{2^n(2^n - 1)}$.

Таким чином, отримаємо кінцевий вираз:

$$\overline{S}_2 = 2^{-n}, \text{ якщо } \alpha = \beta; \ \overline{S}_2 = -\frac{1}{2^n(2^n - 1)}, \text{ якщо } \alpha \neq \beta. \tag{12}$$

Обчислимо зараз значення суми

$$\overline{S}_3 = 2^{-2n} \sum_{(x, x') \in M_3} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{\alpha(F(x) \oplus F(x')) \oplus \beta(F(x \oplus a) \oplus F(x' \oplus a))}.$$

З означення множини M_3 випливає, що

$$T \stackrel{\text{def}}{=} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{\alpha(F(x) \oplus F(x')) \oplus \beta(F(x \oplus a) \oplus F(x' \oplus a))} =$$

$$= \frac{1}{2^n(2^n - 1)(2^n - 2)(2^n - 3)} \sum_{(y_1, y_2, y_3, y_4) \in R_n} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)},$$

де R_n позначає множину, що складається з усіх четвірок попарно різних двійкових векторів довжини n.

Для знаходження виразу параметра T скористаємося методом включення-виключення [13]. На множині "предметів" V_n^4 задамо властивості $\{i, j\}$, де $1 \le i < j \le 4$. За означенням "предмет" $y = (y_1, y_2, y_3, y_4) \in V_n^4$ володіє властивістю $\{i, j\}$, якщо $y_i = y_j$. Позначимо також $\omega(y) = (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)}$ вагу "предмету" y. Тоді значення T є пропорційним сумарній

вазі “предметів”, які не володіють жодною із зазначених властивостей. Отже, на підставі формули включення-виключення маємо

$$T = \frac{1}{2^n(2^n-1)(2^n-2)(2^n-3)} \sum_{k=0}^{6} (-1)^k T_k , \qquad (13)$$

де

$$T_0 = \sum_{y \in V_n^4} \omega(y) , \; T_k = \sum_{\{i_1, j_1\}, \ldots, \{i_k, j_k\}} M(A_{i_1, j_1}, \ldots, A_{i_k, j_k}) ,$$

і в останній формулі підсумування відбувається за всіма сполученнями з k властивостей $\{i_1, j_1\}, \ldots, \{i_k, j_k\}$, а $M(A_{i_1, j_1}, \ldots, A_{i_k, j_k})$ позначає сумарну вагу “предметів”, які володіють цими властивостями, $1 \le k \le 6$.

Для обчислення значення T за формулою (13) розглянемо декілька випадків.

Випадок 1: $k = 0$. Згідно із співвідношенням ортогональності для характерів маємо $T_0 = \sum_{y \in V_n^4} \omega(y) = \sum_{y \in V_n^4} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)} = 0$.

Випадок 2: $k = 1$. Тоді для будь-якої властивості $\{i, j\}$ справедлива рівність $M(A_{i,j}) = \sum_{\substack{y \in V_n^4: \\ y_i = y_j}} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)} = 0$, в чому неважко переконатися, розглядаючи усі можливі значення i та j. Звідси випливає, що $T_1 = 0$.

Випадок 3: $k = 2$. Існує тільки три сполучення $\{\{i_1, j_1\}, \{i_2, j_2\}\}$ таких, що $M(A_{i_1, j_1}, A_{i_2, j_2})$ може бути відмінним від нуля, а саме, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 2\}, \{3, 4\}\}$, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 3\}, \{2, 4\}\}$, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 4\}, \{2, 3\}\}$. При цьому, як показує безпосередня перевірка, $M(A_{1,2}, A_{3,4}) = 2^{2n}$, $M(A_{1,3}, A_{2,4}) = M(A_{1,4}, A_{2,3}) = 2^{2n}$, якщо $\alpha = \beta$; $M(A_{1,3}, A_{2,4}) = M(A_{1,4}, A_{2,3}) = 0$, якщо $\alpha \ne \beta$. Звідси випливає, що $T_2 = 3 \cdot 2^{2n}$, якщо $\alpha = \beta$ та $T_2 = 2^{2n}$, якщо $\alpha \ne \beta$.

Випадок 4: $k = 3$. В цьому випадку існує точно 4 сполучення $\{\{i_1, j_1\}, \{i_2, j_2\}, \{i_3, j_3\}\}$ таких, що $M(A_{i_1, j_1}, A_{i_2, j_2}, A_{i_3, j_3}) = 0$, а саме, $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, $\{\{1, 2\}, \{1, 4\}, \{2, 4\}\}$, $\{\{1, 3\}, \{1, 4\}, \{3, 4\}\}$, $\{\{2, 3\}, \{2, 4\}, \{3, 4\}\}$. Для решти сполучень по k кожен “предмет” $y = (y_1, y_2, y_3, y_4)$, що володіє властивістю, яка визначається цим сполученням, задовольняє умові $y_1 = y_2 = y_3 = y_4$. Звідси випливає, що для такого сполучення $M(A_{i_1, j_1}, A_{i_2, j_2}, A_{i_3, j_3}) = 2^n$. Таким чином, $T_3 = 2^n \left(\binom{6}{3} - 4 \right) = 16 \cdot 2^n$.

Випадок 5: $k \in \{4, 5, 6\}$. В цьому випадку для будь-якого “предмету”, що володіє властивостями $\{i_1, j_1\}, \ldots, \{i_k, j_k\}$, виконуються рівності $y_1 = y_2 = y_3 = y_4$. Отже, $M(A_{i_1, j_1}, \ldots, A_{i_k, j_k}) = 2^n$ і $\sum_{k=4}^{6} (-1)^k T_k = 2^n \left(\binom{6}{4} - \binom{6}{5} + \binom{6}{6} \right) = 10 \cdot 2^n$.

Підставляючи вирази, отримані у випадках 1 – 5, у формулу (13), знайдемо, що

$$T = \frac{3 \cdot 2^{2n} - 6 \cdot 2^n}{2^n(2^n-1)(2^n-2)(2^n-3)} , \text{ якщо } \alpha = \beta ;$$

$$T = \frac{2^{2n} - 6 \cdot 2^n}{2^n(2^n-1)(2^n-2)(2^n-3)} , \text{ якщо } \alpha \ne \beta .$$

Звідси, використовуючи формулу $\overline{S}_3 = 2^{-2n} \sum_{(x,\,x')\,\in M_3} T$, отримаємо кінцевий вираз:

$$\overline{S}_3 = \frac{(3\cdot 2^n - 6)}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha = \beta;\ \overline{S}_3 = \frac{2^n - 6}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha \neq \beta. \qquad (14)$$

Нарешті, використовуючи формули (10) – (12), (15), отримаємо формули (8), (9). Твердження доведено.

3. Співвідношення між параметрами, що характеризують диференціальні, лінійні та диференціально-лінійні властивості блокових шифрів

Для будь-якої комутативної групової операції $+$ на множині V_n та довільної підстановки $f \in \sigma(V_n)$ визначимо матриці $C_f = (C_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $L_f = (L_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $D_{f,+} = (D_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$ та $A_{f,+} = (A_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$, вважаючи

$$C_f(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\alpha f(x)\oplus\beta x},\ \alpha,\beta\in V_n, \qquad (15)$$

$$L_f(\alpha,\beta) = (2\mathbf{P}_X\{\alpha X = \beta f(X)\} - 1)^2,\ \alpha,\beta\in V_n, \qquad (16)$$

$$D_{f,+}(\alpha,\beta) = \mathbf{P}_X\{f(X+\alpha)\oplus f(X) = \beta\},\ \alpha,\beta\in V_n, \qquad (17)$$

$$A_{f,+}(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\beta(f(x+\alpha)\oplus f(x))},\ \alpha,\beta\in V_n, \qquad (18)$$

де у виразах (16) і (17) X позначає випадковий вектор з рівномірним законом розподілу на множині V_n. Матриці (15) і (16) співпадають (з точністю до нормуючих множників) з кореляційною матрицею [14] і таблицею розподілу кореляційної імунності [15] підстановки f відповідно, а матриці (17) і (18) (у випадку, коли $+ = \oplus$) – відповідно з таблицею розподілу різниць і таблицею розподілу автокореляції підстановки f [15]. (Декілька інша термінологія використовується в [4, 7], де матриця (2), з точністю до співмножника 2^{-n}, називається таблицею лінійних апроксимацій, а матриця (5) – автокореляційною таблицею підстановки f).

Нехай $\mathfrak{I}$ – блоковий шифр з множиною відкритих (шифрованих) повідомлень V_n, множиною ключів K та сім'єю шифрувальних перетворень $(F_k : k \in K)$. Тоді матриці $C_{\mathfrak{I}}$, $L_{\mathfrak{I}}$, $D_{\mathfrak{I},+}$ та $A_{\mathfrak{I},+}$ визначаються як середні арифметичні за всіма $k\in K$ значення матриць C_{F_k}, L_{F_k}, $D_{F_k,+}$ та $A_{F_k,+}$ відповідно.

Загальновідомо, що максимальні елементи матриць $L_{\mathfrak{I}}$ та $D_{\mathfrak{I},+}$, що містяться в їх рядках та стовпцях з ненульовими номерами, характеризують стійкість шифру $\mathfrak{I}$ відносно лінійного та диференціального методів криптоаналізу відповідно. При цьому на підставі твердження 3 спроможність цього шифру протистояти наведеній вище диференціально-лінійній атаці (у випадку $\alpha = \beta$) характеризується максимальним значенням квадратів елементів матриці $A_{\mathfrak{I},+}$, які містяться у її рядках та стовпцях з ненульовими номерами.

Відзначимо взаємозв'язок між матрицями (15) – (18).

Перш за все, безпосередньо з формул (15), (16) випливає рівність

$$L_f(\alpha,\beta) = C_f(\beta,\alpha)^2,\ \alpha,\beta\in V_n. \qquad (19)$$

Далі, позначимо $H_n = ((-1)^{\alpha\beta})_{\alpha,\beta\in V_n}$ матрицю Адамара абелевої групи $(V_n,\oplus)$, $\Pi_f = (\delta(f(\alpha),\beta))_{\alpha,\beta\in V_n}$ – підстановочну матрицю, що відповідає підстановці $f\in\sigma(V_n)$ (тут і

далі δ позначає символ Кронекера: $\delta(f(\alpha),\beta)=1$, якщо $f(\alpha)=\beta$; $\delta(f(\alpha),\beta)=0$ – у протилежному випадку). Справедливі такі рівності:

$$C_f = 2^{-n} H_n \Pi_f^{\,T} H_n,\ D_{f,\oplus} = 2^{-n} H_n L_f H_n, \tag{20}$$

перше з яких випливає безпосередньо з наведених означень, а друге – доведено в [16]. З першої формули (20) випливає, що матриця C_f є ортогональною. Отже, на підставі рівностей (17) та (19) матриці L_f та D_f є двічі стохастичними.

Справедливі також наступні рівності, що пов'язують між собою матриці (3), (4) та (5) у випадку $+=\oplus$ [15]:

$$A_{f,\oplus} = D_{f,\oplus} H_n = H_n L_f. \tag{21}$$

У загальному випадку справедлива рівність

$$A_{f,+} = D_{f,+} H_n, \tag{22}$$

яка доводиться шляхом безпосередньої перевірки.

Безпосередньо з формул (21), (22) випливає наступна лема.

Лема 4. Нехай $\mathfrak{I}$ є блоковим шифром з множиною відкритих (шифрованих) повідомлень V_n. Тоді $A_{\mathfrak{I},+} = D_{\mathfrak{I},+} H_n$ і $A_{\mathfrak{I},\oplus} = D_{\mathfrak{I},\oplus} H_n = H_n L_{\mathfrak{I}}$.

Матричні співвідношення (8) дозволяють швидко отримати один з основних результатів роботи [4], оригінальне доведення якого є більш складним.

Для будь-яких підстановок $f, g \in \sigma(V_n)$ позначимо $f \circ g$ їх композицію: $(f \circ g)(x) = f(g(x))$, $x \in V_n$. Слідуючи [4], назвемо ці підстановки диференціально (лінійно) незалежними, якщо $D_{f\circ g} = D_g D_f$ ($L_{f\circ g} = L_g L_f$). Зауважимо, що на підставі другої рівності (21) диференціальна незалежність підстановок на множині V_n рівносильна їх лінійній незалежності (див. твердження 2 в [4]).

Наступна лема є матричним аналогом теореми 2 в [4].

Лема 5. Якщо підстановки $f, g \in \sigma(V_n)$ є диференціально (лінійно) незалежними, то $A_{f\circ g} = A_g L_f$.

Доведення. Дійсно, $A_{f\circ g} = D_{f\circ g} H_n = D_g D_f H_n = D_g H_n (2^{-n} H_n) D_f H_n = A_g L_f$. Лему доведено.

За означенням [9] блоковий шифр $\mathfrak{I}$ називається марковським (відносно операції $\oplus$), якщо для будь-яких $x, \alpha, \beta \in V_n$ виконується рівність $D_{f,\oplus}(\alpha,\beta) = \mathbf{P}_k\{F_k(x\oplus\alpha) \oplus F_k(x) = \beta\}$.

Якщо $\mathfrak{I}_1$ і $\mathfrak{I}_2$ – блокові шифри з множиною відкритих (шифрованих) повідомлень V_n та сім'ями шифрувальних перетворень $(F'_{k'} : k' \in K')$ і $(F''_{k''} : k'' \in K'')$ відповідно, то їх добуток $\mathfrak{I} = \mathfrak{I}_1 \mathfrak{I}_2$ визначається як блоковий шифр з сім'ю шифрувальних перетворень $(F_k : k \in K)$, де $K = K' \times K''$, $F_k(x) = F''_{k''}(F'_{k'}(x))$, $x \in V_n$, $k = (k', k'') \in K$.

Твердження 5. Нехай $\mathfrak{I} = \mathfrak{I}_1 \mathfrak{I}_2$, де $\mathfrak{I}_2$ є марковським шифром. Тоді $A_{\mathfrak{I},+} = A_{\mathfrak{I}_1,+} L_{\mathfrak{I}_2}$.

Доведення. З марковості шифру $\mathfrak{I}_2$ випливає рівність $D_{\mathfrak{I},+} = D_{\mathfrak{I}_1,+} D_{\mathfrak{I}_2,\oplus}$. Звідси, використовуючи лему 2, отримаємо, що

$$A_{\mathfrak{I},+} = D_{\mathfrak{I},+} H_n = D_{\mathfrak{I}_1,+} D_{\mathfrak{I}_2,\oplus} H_n = (D_{\mathfrak{I}_1,+} H_n)(2^{-n} H_n D_{\mathfrak{I}_2,\oplus} H_n) = A_{\mathfrak{I}_1,+} L_{\mathfrak{I}_2}.$$

Твердження доведено.

Розглянемо більш загальні (в порівнянні з числами (18)) параметри, введені в [7], які визначають стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу. А саме, для будь-яких $f \in \sigma(V_n)$, $a \in V_n$ позначимо $\Delta_{f,+,a}$ матрицю з елементами

$$\Delta_{f,+,a}(\alpha,\beta)=2^{-n}\sum_{x\in V_n}(-1)^{\alpha f(x)\oplus\beta f(x+a)},\ \alpha,\beta\in V_n. \qquad (23)$$

Зауважимо, що $\Delta_{f,+,a}(\alpha,\alpha)=A_{f,+}(a,\alpha)$. В роботі [7] набір, що складається з чисел (23) за всіма $a\in V_n$ (для випадку $+=\oplus$), названо узагальненою автокореляційною таблицею підстановки f.

Якщо $\mathfrak{I}$ – блоковий шифр з множиною відкритих (шифрованих) повідомлень V_n та сім'єю шифрувальних перетворень $(F_k: k\in K)$, то на підставі твердження 3 його стійкість відносно наведеної в п. 1 диференціально-лінійної атаки визначається параметром

$$(2\mathbf{P}_{x,k}\{\alpha F_k(x)=\beta F_k(x+a)\}-1)^2=\left(|K|^{-1}\sum_{k\in K}(\Delta_{F_k,+,a}(\alpha,\beta))^2\right).$$

Отримаємо представлення цього параметра для шифру $\mathfrak{I}$, що є добутком двох довільних шифрів.

Твердження 6. Нехай $\mathfrak{I}=\mathfrak{I}_1\mathfrak{I}_2$, де $\mathfrak{I}_1$ і $\mathfrak{I}_2$ – блокові шифри з множиною відкритих (шифрованих) повідомлень V_n та сім'ями шифрувальних перетворень $(F'_{k'}: k'\in K')$ і $(F''_{k''}: k''\in K'')$ відповідно. Тоді для будь-яких $a\in V_n$, $k=(k',k'')\in K'\times K''$ справедлива рівність $\Delta_{F_k,+,a}=C_{F''_{k''}}\Delta_{F'_{k'},+,a}(C_{F''_{k''}})^T$, де матриця $C_{F''_{k''}}$ визначається згідно з формулою (15).

Доведення. Для будь-яких підстановок $f_1, f_2\in\sigma(V_n)$ має місце рівність

$$C_{f_2\circ f_1}=C_{f_2}C_{f_1}, \qquad (24)$$

справедливість якої випливає з формули $\Pi_{f_2\circ f_1}=\Pi_{f_1}\Pi_{f_2}$ та першої рівності (20).

Покладемо $f_1=F'_{k'}$, $f_2=F''_{k''}$, $f=F_k=F''_{k''}\circ F'_{k'}$ та позначимо T_a підстановку, що реалізує зсув на вектор a: $T_a(x)=x+a$, $x\in V_n$. Використовуючи у формулі (23) заміну змінних $x=f^{-1}(y)$, отримаємо, що

$$\Delta_{f,+,a}(\alpha,\beta)=2^{-n}\sum_{y\in V_n}(-1)^{\alpha y\oplus\beta f(f^{-1}(y)+a)}=2^{-n}\sum_{y\in V_n}(-1)^{\alpha y\oplus\beta(f\circ T_a\circ f^{-1})(y)}=C_{f\circ T_a\circ f^{-1}}(\beta,\alpha).$$

Аналогічно отримаємо, що $\Delta_{f_1,+,a}(\alpha,\beta)=C_{f_1\circ T_a\circ f_1^{-1}}(\beta,\alpha)$. Звідси, використовуючи формулу (24), отримаємо рівності:

$$\Delta_{f,+,a}(\alpha,\beta)=(C_{f_2}(C_{f_1}C_{T_a}C_{f_1}^{-1})C_{f_2}^{-1})(\beta,\alpha)=(C_{f_2}\Delta_{f_1,+,a}C_{f_2}^{-1})(\beta,\alpha)=C_{f_2}\Delta_{f_1,+,a}(C_{f_2})^T(\beta,\alpha),$$

з яких на підставі симетричності матриць $\Delta_{f,+,a}$, $\Delta_{f_1,+,a}$ випливає формула (24).

Твердження доведено.

Зауважимо, що отримане твердження надає явний вираз параметра вигляду (23) (а отже, й параметрів вигляду (18)) для довільного блокового шифру $\mathfrak{I}$ в термінах кореляційних матриць перетворень його співмножників $\mathfrak{I}_1$ і $\mathfrak{I}_2$, не використовуючи при цьому жодних додаткових припущень про шифр (на кшталт тих, що робляться в [1 – 5]).

Висновки

1. В роботі отримано нижні оцінки інформаційної складності двох видів диференціально-лінійних атак на блокові шифри, а саме, розрізнювальних атак і атак, спрямованих на відновлення одного біту інформації про ключ. Отримані вирази зазначених оцінок залежать від усереднених (за ключами) значень квадратів елементів узагальнених автокореляційних таблиць шифрувальних перетворень. На відміну від відомих [1, 2, 4], отримані оцінки не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються,

та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою.

2. У важливому окремому випадку отримано явний вираз середнього значення параметра, який фігурує в зазначених вище оцінках, для випадкової рівноймовірної підстановки на множині повідомлень, що шифруються. Аналогічно диференціальному або лінійному методам криптоаналізу цей результат надає можливість порівнювати диференціально-лінійні властивості бієктивних булевих відображень з аналогічними властивостями "ідеального" криптографічного відображення, тобто випадкової рівноймовірної підстановки.

3. Наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт [4, 6, 8], використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано також нове співвідношення для елементів узагальненої автокореляційної таблиці блокового шифру, що є добутком двох довільних шифрів. Це співвідношення не базується на жодних додаткових припущеннях про шифр (на кшталт таких, що робляться в [1 – 5]) та може бути корисним в подальших дослідженнях ефективності диференціально-лінійного методу криптоаналізу.

Список літератури:

1. Langford S., Hellman M. Differential-linear cryptanalysis // Advanced in Cryptology – Crypto 1994, LNCS. Vol. 839. 1994. P. 17 – 25.
2. Biham E., Dunkelman O., Keller N. Enhancing differential-linear cryptanalysis // Advanced in Cryptology – ASIACRYPT 2002, LNCS. Vol. 2401. 2002. P. 254 – 266.
3. Lu J. A methodology for differential-linear cryptanalysis and its applications // Designs, Codes and Cryptography. 2015. Vol. 77. № 1. P. 11 – 48.
4. Blondeau C., Leander G., Nyberg K. Differential-linear cryptanalysis revisited // J. Cryptology. 2017. Vol. 30. № 3. P. 859 – 888.
5. Bar-On A., Dunkelman O., Keller N., Weizman A. DLCT: a new tool for differential-linear cryptanalysis // Cryptology ePrint Archive, Report 2019/256. http://eprint.iacr.org/2019/256.
6. Алексейчук А.Н. Неасимптотические нижние границы информационной сложности статистических атак на симметричные криптосистемы // Кибернетика и системный анализ. 2018. Т. 54. № 1. С. 93 – 104.
7. Nyberg K. The extended autocorrelation and boomerang tables and links between nonlinearity properties of vectorial Boolean functions // Cryptology ePrint Archive, Report 2019/1381. http://eprint.iacr.org/2019/1381.
8. Canteuat A., Koelsch L., Li Ch. [et al.] On the differential-linear connectivity table of vectorial Boolean function // CoRR, abs/190807455. 2019.
9. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. P. 17 – 38.
10. Harpes C., Kramer G.G., Massey J.L. A generalisation of linear cryptoanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology – EUROCRYPT'95, Proceedings. – Springer Verlag, 1995. P. 24 – 38.
11. Hoeffding W. Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc. 1963. Vol. 58. № 301. P. 13 – 30.
12. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. Москва : МЦНМО, 2004. 470 с.
13. Сачков В.Н. Введение в комбинаторные методы дискретной математики. Москва : Наука, 1982. 384 с.
14. Daemen J., Govards R., Vandervalle J. Correlation matrices // Fast Software Encryption – FSE'94, LNCS. Vol. 1008. 1994. P. 275 – 285.
15. Zhang X.-M., Zheng J., Imai H. Relating differential distribution tables to other properties of substitution boxes // Des. Codes Cryptography. 2000. Vol. 19. № 1. P. 45 – 63.
16. Chabaud F., Vaudenay S. Links between differential and linear cryptanalysis // Advanced in Cryptology – EUROCRYPT'94, LNCS. Vol. 950. 1994. P. 356 – 365.

Надійшла до редколегії 03.02.2021

Відомості про автора:

Олексійчук Антон Миколайович – д-р техн. наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ", професор кафедри Кібербезпеки; Україна; e-mail: alex-dtn@ukr.ne