Р. 1—17. ***8.*** *Нариманова Е.В. Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е.В. Нариманова // Вісник Східноукр-го нац-го ун-ту ім. В. Даля. — 2008. — №8(126), ч.1. — С.47—55.* ***9.*** *Информационные технологии и системы в управлении, образовании, науке: Монография / Под ред. проф. В. С. Пономаренко. – Х.: Цифрова друкарня №1, 2013. – 278 с.* ***10.*** *Кобозева А. А. Анализ информационной безопасности / А. А. Кобозева, В .А. Хорошко. — К.: Изд.ГУИКТ, 2009. — 251 с.* ***11.*** *Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер.с англ. Х. Д. Икрамова. — М.: Мир, 2001. — 430 с.* ***12****. Гантмахер Ф. Р. Теория матриц / Ф. Р. Гантмахер. — М.: Наука, 1988. — 552 с.* ***13.*** *Кобозева А. А. Векторная SIGN-чувствительность как основа геометрической модели системы защиты информации / А. А. Кобозева, В. А. Хорошко // Захист інформації. — 2008. — №3. — С. 49—57.*

УДК 004.056.55:519.2

МЕТОДИКА ОБГРУНТУВАННЯ СТІЙКОСТІ НЕМАРКОВСЬКИХ СИМЕТРИЧНИХ БЛОЧНИХ ШИФРІВ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

Сергій Яковлєв

Фізико-технічний інститут, НТУУ «КПІ»

Анотація: ***Запропонована методика оцінювання стійкості немарковських блочних шифрів до диференціального аналізу. Ґрунтуючись на даній методиці, був проведений аналіз низки узагальнених схем Фейстеля.***

Summary: ***We propose a procedure of provable security evaluation of non-Markov ciphers against differential cryptanalysis. Security of some generalized Feistel networks is estimated according to proposed procedure.***

Ключові слова: ***Симетрична криптографія, блочні шифри, диференціальний криптоаналіз, доказова стійкість, узагальнені схеми Фейстеля.***

I Вступ

Задача доказової стійкості блочних шифрів до диференціального аналізу була поставлена Ніберг та Кнудсеном у 1994 році [3]; ними була виведена теоретична верхня межа імовірності існування диференціалів у схемі Фейстеля, виражена через відповідні імовірності раундових функцій. Цей параметр дозволяє оцінити знизу складність проведення диференціальної атаки на довільний шифр, побудований на основі схеми Фейстеля. В подальшому подібні результати були одержані для низки інших ітеративних схем блочного шифрування. Зауважимо, однак, що переважна більшість отриманих оцінок стосувалась марковських шифрів, тобто шифрів, диференціальні імовірності яких були незалежними на кожному раунді. Дослідження доказової стійкості немарковських шифрів до диференціального аналізу вперше було зроблене Ковальчук [6]; нею одержані оцінки стійкості для немарковських схеми Фейстеля та MISTY-схеми.

В даній роботі пропонується загальна методика побудови аналітичної оцінки верхньої межі імовірності існування диференціалів через відповідні параметри раундових функцій. Ця методика базується на принципах, які використовувались при доведенні результатів попередніх дослідників, однак вона дозволяє оцінювати немарковські шифри та будувати аналітичні оцінки автоматично, що виявляється дуже корисним для оцінки стійкості складних схем шифрування, для яких традиційний математичний підхід вимагав би розглядання великої кількості різних випадків. Наприкінці ми покажемо застосування методики, що пропонується, для оцінювання стійкості деяких узагальнених схем Фейстеля до диференціального аналізу.

Зауважимо, що при аналізі марковських шифрів наведена методика може бути майже покроково перенесена для побудови оцінки теоретичної стійкості до лінійного криптоаналізу.

II Необхідні теоретичні відомості

Нехай M – множина відкритих текстів, C – множина шифртекстів, K – множина ключів.

Шифруюче перетворення – це функція вигляду

$$F : M \times K \to C,$$

яка задовольняє такій умові: для кожного фіксованого значення $k \in K$ перетворення $y = F(x,k) = F_k(x)$ є бієктивним. Надалі ми розглядаємо лише той випадок, коли множини M та C є просторами V_q двійкових векторів довжини q. Зауважимо, що це справедливо для переважної більшості сучасних алгоритмів шифрування.

Ітеративний r-раундовий блочний шифр E – перетворення виду $E: V_q \times K^r \to V_q$, що є композицією *r* шифруючих перетворень:

$$E = F_{k_1}^{(1)} \circ F_{k_2}^{(2)} \circ \ldots \circ F_{k_r}^{(r)}.$$

Функції $F_{k_i}^{(i)}$ будемо називати *раундовими перетвореннями*, а змінні k_i – *раундовими ключами.* Тут і надалі вважається, що раундові ключі $(k_1, k_2, \ldots, k_r)$ є випадковими, незалежними та рівномірно розподіленими в ключовому просторі.

Якщо $Y = E_k(X)$, то пов'яжемо із шифром *E* послідовність проміжних значень $(X_0, X_1, \ldots, X_r)$, де $X_0 = X$, $X_i = F_{k_i}^{(i)}(X_{i-1})$, $Y = X_r$.

Нагадаємо основні означення диференціального криптоаналізу [1].

Диференціал (звичайної) булевої функції f – пара двійкових векторів (α, β) така, що виконується співвідношення $f(z \oplus \alpha) \oplus f(z) = \beta$. Ми будемо також позначати диференціал символом $\alpha \underset{f}{\to} \beta$ або просто $\alpha \to \beta$, якщо функція зрозуміла з контексту.

Імовірність диференціалу (α, β) *функції f* – величина

$$d^f(\alpha, \beta) = \frac{1}{2^q} \sum_{z \in V_q} [f(z \oplus \alpha) \oplus f(z) = \beta],$$

де $[A = B]$ дорівнює 1, якщо $A = B$, та 0, якщо $A \neq B$ (так звані *дужки Айверсона*).

Ми будемо казати, що диференціал є *неможливим*, якщо імовірність його існування дорівнює нулю. Диференціал виду $(0,0)$ будемо називати *тривіальним*; імовірність тривіального диференціалу дорівнює 1. Всі інші диференціали будемо називати *нетривіальними*.

Для функцій, що параметризовані ключем, диференціали розглядаються в кожній точці окремо:

Середня за ключами імовірність диференціалу (α, β) *функції* f_k *в точці z* – величина

$$d^{f_k}(z, \alpha, \beta) = \frac{1}{|K|} \sum_{k \in K} [f_k(z \oplus \alpha) \oplus f_k(z) = \beta].$$

Середня імовірність диференціалу (α, β) *функції* f_k – величина

$$d^{f_k}(\alpha, \beta) = \frac{1}{2^q} \sum_{z \in V_q} d^{f_k}(z, \alpha, \beta).$$

Диференціальна характеристика r-раундового ітеративного блочного шифру E – послідовність $\Omega = (\omega_0, \omega_1, \ldots, \omega_r) \in (V_q \setminus \{0\})^{r+1}$ така, що (ω_{i-1}, ω_i) – диференціал раундової функції $F_{k_i}^{(i)}$. Загалом, диференціальною характеристикою може бути довільна послідовність ненульових двійкових векторів потрібної довжини.

Середня за ключами ймовірність диференціальної характеристики (у точці X_0) визначається як

$$DP(\Omega, X_0) = d^{F_{k_1}^{(1)}}(X_0, \omega_0, \omega_1) \cdot d^{F_{k_2}^{(2)}}(X_1, \omega_1, \omega_2) \cdot \ldots \cdot d^{F_{k_r}^{(r)}}(X_{r-1}, \omega_{r-1}, \omega_r).$$

Імовірність диференціалу (ω_0, ω_r) шифру *E* тоді обчислюється через імовірності всіх можливих відповідних диференціальних характеристик:

$$d^{E_k}(z, \omega_0, \omega_r) = \sum_{\omega_1 \neq 0, \ldots, \omega_{r-1} \neq 0} DP(\Omega, z).$$

Перетворення називається *марковським*, якщо імовірності кожного диференціалу на кожному раунді не залежать від точки входу, тобто $d^{f_k}(z, \alpha, \beta) = d^{f_k}(0, \alpha, \beta) = d^{f_k}(\alpha, \beta)$. В цьому випадку імовірність

диференціальної характеристики розбивається у добуток незалежних диференціальних імовірностей кожного раунду, що суттєво спрощує аналіз. Для немарковських перетворень пораундові диференціальні імовірності є залежними, оскільки на значення кожного X_i впливають усі попередні точки входу та раундові ключі.

Оцінка стійкості немарковського шифру до диференціального аналізу визначається величиною

$$MDP(E) = \max_{\alpha \neq 0, \beta, z} d^E(z, \alpha, \beta).$$

Наведемо декілька властивостей диференціалів, справедливих для довільної функції f_k [1,2,4,5]:

а) $d^{f_k}(z,0,\beta) = [\beta = 0]$;

б) $d^{f_k}(z,\alpha,0) = [\alpha = 0]$, якщо f_k бієктивна при кожному значенні ключа;

в) $\forall \alpha \forall z : \sum_{\beta} d^{f_k}(z,\alpha,\beta) = 1$;

г) $\forall \beta \forall z : \sum_{\alpha} d^{f_k}(z,\alpha,\beta) = 1$, якщо f_k бієктивна при кожному значенні *k*.

Також ми будемо користуватись лемою, що була доведена у [6].

Лема 1. Для *r*-раундової диференціальної характеристики $\Omega = (\omega_0, \omega_1, ..., \omega_r)$ ітеративного шифру E_k виконується нерівність:

$$\forall z : DP(\Omega, z) \le \prod_{i=1}^{r} \max_x d^{F_{k_i}^{(i)}}(x, \omega_{i-1}, \omega_i).$$

III Методика оцінювання верхніх меж імовірностей диференціалів

Розглянемо деякий *r*-раундовий ітеративний шифр *E* та його диференціал (ω_0, ω_r); імовірність цього диференціалу обчислюється через суму імовірностей всіх диференціальних характеристик $\Omega = (\omega_0, \omega_1, ..., \omega_r)$ за всіма проміжними значеннями ω_i, $i = \overline{1, r-1}$. Для оцінки імовірності кожної характеристики необхідно розглянути всі диференціали $\omega_{i-1} \to \omega_i$ на кожному раунді. Такі переходи можуть бути виражені через деяку множину параметрів, що відповідають відомим значенням (ω_0, ω_r), та деяку множину змінних, які відповідають невідомим проміжним значенням характеристики.

Назвемо раундовий диференціал $\omega_{i-1} \xrightarrow[f]{} \omega_i$ *регулярним відносно змінної* β, якщо або ω_{i-1}, або ω_i виражаються через β та виконується умова $\sum_{\beta} d^f(\omega_{i-1}, \omega_i) = 1$. Аналогічно можна визначити і регулярні раундові диференціали функцій, параметризованих ключем.

Нехай $A = \{a_1, ..., a_l\}$ – множина відомих параметрів, $B = \{b_1, ..., b_s\}$ – множина змінних сумування. Для довільної диференціальної характеристики $\Omega = (\omega_0, \omega_1, ..., \omega_r)$ шифру *E* маємо:

$$\omega_0 = \omega_0(A),\ \omega_r = \omega_r(A),$$
$$\omega_i = \omega_i(A, B),\ i = \overline{1, r-1}.$$

Звідси ми можемо виразити імовірність диференціалу (ω_0, ω_r):

$$d^E(X_0, \omega_0, \omega_r) = \sum_{\omega_1, \omega_2, ..., \omega_{r-1}} DP(\Omega, X_0) = \sum_{b_1} ... \sum_{b_s} DP(\Omega, X_0),$$

де суми обчислюються по всіх змінних $b_i \in B$.

Очевидно, що залежно від значень констант із множини *A* деякі переходи в диференціальній характеристиці можуть тривіалізуватись, а деякі змінні з множини *B* – приймати лише фіксовані значення. Якщо тривіалізується диференціал, що є регулярним відносно деякої змінної $b \in B$, то ця змінна може приймати лише одне значення і, таким чином, сумування по ній зникає.

Позначимо через $u(A)$ кількість нетривіальних раундових диференціалів у характеристиці Ω після підстановки значень параметрів з множини *A*, а через $v(A,B)$ – кількість змінних сумування з множини *B*, що не приймають фіксованих значень після підстановки значень параметрів з множини *A*. Тоді має місце така теорема.

Теорема 1. Нехай *E* – *r*-раундовий ітеративний шифр із раундовими перетвореннями $F_i(x,k)$, $i=\overline{1,r}$, і $p=\max\limits_i MDP(F_i)$. Нехай довільна диференціальна характеристика Ω цього шифру виражається через множину констант *A* та множину змінних *B*, причому кожен раундовий диференціал є регулярним відносно деякої змінної множини *B*. Тоді має місце така оцінка:

$$\forall x\forall\alpha\neq 0\forall\beta:\quad d^E(x,\alpha,\beta)\le\max_A\{p^{u(A)-v(A,B)}\}=p^{\min\limits_A\{u(A)-v(A,B)\}}.$$

Доведення. За означенням множин *A* та *B* ми можемо виразити імовірність довільного диференціала шифру *E* таким чином.

$$d^E(X_0,\omega_0,\omega_r)=\sum_{b_1}\ldots\sum_{b_s}DP(\Omega,X_0)=\sum_{b_1}\ldots\sum_{b_s}d^{F^{(1)}_{k_1}}(X_0,\omega_0,\omega_1)\cdot\ldots\cdot d^{F^{(r)}_{k_r}}(X_{r-1},\omega_{r-1},\omega_r).$$

де $X_0=x$, $X_i=F^{(i)}(X_{i-1},k_i)$.

Оскільки значення кожного X_i залежить від усіх попередніх точок входу та раундових ключів, верхню оцінку ми повинні будувати від останнього раунду до першого: оцінюючи величину $d^{F^{(r)}_{k_r}}(X_{r-1},\omega_{r-1},\omega_r)$ деяким константним значенням, ми виносимо його із суми і можемо аналітично представляти та оцінювати імовірності передостаннього раунду, і так далі.

Зафіксуємо значення параметрів з множини *A* та викреслимо з множини *B* всі змінні, значення яких також зафіксувались; в результаті ми одержали $u=u(A)$ нетривіальних раундових диференціалів та $v=v(A,B)$ змінних сумування. Впорядкуємо змінні множини *B* за появою їх у диференціальній характеристиці: $B=\{b_1,\ldots,b_v\}$, де змінна b_1 з'являється в описі раундових диференціалів першою, b_2 – наступною і т.д. Введемо додаткові позначення:

u_v – кількість переходів, що залежать від змінної b_v;

u_{v-1} – кількість переходів, що залежать від змінної b_{v-1} та не залежать від змінної b_v;

u_{v-2} – кількість переходів, що залежать від змінної b_{v-2} та не залежать від змінних b_v та b_{v-1};

…

u_1 – кількість переходів, що залежать від змінної b_1 та не залежать від змінних b_2, b_3, …, b_v;

u_0 – кількість переходів, що не залежать від змінних множини *B*.

Очевидно, що $u=u_0+u_1+u_2+\ldots+u_v$.

Зафіксуємо довільну вхідну точку *x* та обчислимо верхню оцінку імовірності диференціалу (ω_0,ω_r) через суму імовірностей всіх диференціальних характеристик, для яких він є обвідним (ми розглядаємо лише такі диференціальні характеристики Ω, для яких $DP(\Omega,x)\neq 0$). Для цього будемо оцінювати диференціальні імовірності на кожному раунді шифрування, починаючи з останнього. Розглянемо *i*-тий раунд та відповідний перехід $\omega_{i-1}\to\omega_i$. Маємо такі можливі випадки:

1) Раунд виявився тривіальним. В цьому випадку $d^{F^{(i)}_{k_i}}(X_{i-1},\omega_{i-1},\omega_i)=1$.

2) Раунд виявився нетривіальним, але він не залежить від змінних множини *B*. В цьому випадку $d^{F^{(i)}_{k_i}}(X_{i-1},\omega_{i-1},\omega_i)\le MDP(F^{(i)}_{k_i})\le p$

3) Раунд виявився нетривіальним і залежним від *B*. Нехай b_s – змінна з максимальним індексом, від якої залежить $\omega_{i-1}\to\omega_i$. Тоді:

– якщо серед попередніх раундів є інші залежні від b_s, то ми можемо стверджувати, що $d^{F_{k_i}^{(i)}}(X_{i-1},\omega_{i-1},\omega_i) \le MDP(F_{k_i}^{(i)}) \le p$.

– якщо ж даний раунд є останнім залежним від b_s, то в силу регулярності переходу відносно b_s виконується рівність $\sum_{b_s} d^{F_{k_i}^{(i)}}(X_{i-1},\omega_{i-1},\omega_i) = 1$.

Бачимо, що кожна змінна b_s, з якою пов'язані u_s диференціальних переходів, $u_s - 1$ раз вносить в оцінку диференціальної імовірності множник *p*; останній, u_s -тий перехід знищується завдяки зовнішній сумі по всіх значеннях b_s. Додатково ми також маємо u_0 множників *p* від нетривіальних раундів, що не залежать від змінних $\{b_i\}$.

Остаточно можемо записати:

$$d^E(x,\omega_0,\omega_r) \le p^{u_0+(u_1-1)+(u_2-1)+\ldots+(u_v-1)} = p^{u-v},$$

звідки й випливає твердження теореми. Теорему доведено.

Користуючись результатами теореми, можна описати методику побудови верхньої межі диференціальної імовірності ітеративного блочного шифру. Побудова виконується в такі кроки.

1) Перебираються такі можливі значення параметрів множини *A*, що приводять до всіх можливих варіантів тривіалізації диференціальних переходів всередині шифру; зазвичай замість повного перебору всіх можливих значень потрібно розглянути лише випадки, коли змінна дорівнює нулю, не дорівнює нулю та/або дорівнює комбінації інших змінних, що приводить до появи тривіальних диференціалів у характеристиці.

2) Для кожного варіанту тривіалізації обчислюється відповідна величина $p^{u(A)-v(A,B)}$.

3) Максимальна з обчислених величин і буде верхньою межею для диференціальних імовірностей шифру.

Ця методика дозволяє автоматизувати побудову оцінок стійкості до диференціального аналізу. В наступному розділі ми покажемо застосування методики до деяких класів узагальнених схем Фейстеля.

Необхідно зауважити, що для марковських шифрів ця методика повністю (с точністю до позначень) переноситься на побудову аналітичних оцінок верхніх меж імовірностей лінійних апроксимацій, що характеризують стійкість блочних шифрів до лінійного криптоаналізу. Для немарковських шифрів такий перенос наразі неможливий через відсутність повної та адекватної формальної теорії стійкості немарковських шифрів до лінійного криптоаналізу.

IV Оцінка стійкості деяких узагальнень схеми Фейстеля

В даному розділі ми наведемо результати аналізу деяких узагальнень схеми Фейстеля, що лягли в основу таких шифрів, як Skipjack, CAST-256, SMS4 та низки інших. Подібні узагальнення виникли наприкінці 80-х – початку 90-х років як спроба масштабування існуючих алгоритмів шифрування (збільшення оброблюваного блоку даних) із збереженням «елементної бази» – раундових функцій ускладнення.

Ми будемо називати *узагальненою схемою Фейстеля* ітеративну схему шифрування, в якій вхідний блок даних розбивається на *m* окремих частин (підблоків) по *n* біт кожна, а раундові перетворення використовують одну чи декілька бієктивних ключезалежних перетворень *n* в *n* біт. В наявних алгоритмах шифрування зазвичай $m = 4$, $n = 16$ або 32.

Skipjack-подібна схема шифрування є узагальненою схемою Фейстеля, що складається з раундів такого виду:

$$F_k(x_0,x_1,\ldots,x_{m-2},x_{m-1}) = (x_1 \oplus f_k(x_0), x_2,\ldots,x_{m-1},f_k(x_0))$$

Далі ми для зручності вважаємо, що на кожному раунді використовується одна й та сама функція *f*.

Розглянемо *r*-раундову Skipjack-подібну схему (вважаємо, що $r > m$). Із кожною її диференціальною характеристикою $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ можна пов'язати таку послідовність *n*-бітних змінних $a_0, a_1, \ldots, a_{r+m-1}$, що будуть виконуватись співвідношення

$$\omega_i = (a_{i+m-1} \oplus a_i, a_{i+1},\ldots,a_{i+m-2},a_{i+m-1}),$$

$$d^{F_k}(X_i,\omega_i,\omega_{i+1}) = d^{f_k}(X_i^{(0)}, a_i \oplus a_{i+m-1}, a_{i+m}),\ i = \overline{0, r-1}.$$

Тут $X_i = (X_i^{(0)}, X_i^{(1)}, ..., X_i^{(m-1)})$, і кожне $X_i^{(j)}$ є *n*-бітним вектором.

З позицій описаної в попередньому розділі методики для довільного диференціала (ω_0, ω_r) маємо множину відомих параметрів $A = \{a_0, a_1, ..., a_{m-1}, a_r, a_{r+1}, ..., a_{r+m-1}\}$ та множину змінних сумування $B = \{a_m, a_{m+1}, ..., a_{r-1}\}$, причому імовірність цього диференціалу буде обчислюватись таким чином:

$$d^{E_K}(X_0, \omega_0, \omega_r) = \sum_B \prod_{i=0}^{r-1} d^{f_k}(X_i^{(0)}, a_i \oplus a_{i+m-1}, a_{i+m}).$$

Оскільки всі раундові диференціали є регулярними відносно деяких змінних з множини *B*, то ми можемо використовувати описану вище методику для побудови аналітичної верхньої межі диференціальних імовірностей Skipjack-подібної схеми.

Позначимо $p = MDP(f)$. За допомогою спеціального програмного забезпечення була знайдена мінімальна кількість раундів шифрування, необхідна для того, щоб імовірності диференціалів не перевищували межі в p^u для $u = 2,3,...,m$. Ці результати подані у таблиці 1.

Таблиця 1 – Кількість раундів, необхідна для досягнення заданої верхньої межі диференціальної імовірності.

	p^2	p^3	p^4	p^5
$m = 2$	$r = 3$ *(4 випадки)*			
$m = 3$	$r = 5$ *(12 випадків)*	$r = 7$ *(25 випадків)*		
$m = 4$	$r = 7$ *(33 випадки)*	$r = 10$ *(98 випадків)*	$r = 13$ *(299 випадків)*	
$m = 5$	$r = 9$ *(88 випадків)*	$r = 13$ *(376 випадків)*	$r = 17$ *(1649 випадків)*	$r = 21$ *(7122 випадки)*

В дужках після значення *r* вказана кількість різних шляхів тривіалізації всередині диференціальної характеристики. Як бачимо, вже для $m = 4$ потрібно розглядати сотні різних випадків, що вкрай ускладнює «ручне» доведення таких тверджень.

Наведена в таблиці 1 кількість раундів є дійсно мінімально необхідною; під час аналізу для меншої кількості раундів були знайдені диференціали, імовірності яких можуть перевищувати вказану межу. Наприклад, при $m = 5$ та $r = 20$ імовірність диференціала $(a,*,*,*,b) \to (0,0,0,0,a)$, де $a \neq 0$, $b \neq 0$, $a \neq b$, а зірочками помічені довільні можливі значення, може теоретично досягати величини p^4, що більше за очікувану верхню межу p^5.

Ґрунтуючись на одержаних даних, ми можемо висунути гіпотезу, що для досягання значення верхньої межі у p^u потрібно щонайменше $r = um - u + 1$ раунд Skipjack-подібної схеми; зокрема, для досягання межі p^m потрібно $r = m^2 - m + 1$ раундів шифрування.

Якщо в схемі використовуються різні раундові функції f_i, то одержані оцінки залишаються в силі, але параметр *p* буде визначатись як максимум поміж раундових функцій: $p = \max_i MDP(f_i)$. Якщо враховувати особливості кожної раундової функції, то можна одержати більш точну оцінку верхньої межі диференціальних імовірностей шифру, однак відповідні аналітичні вирази стають занадто громіздкими.

Одержані результати підтверджують оцінки, знайдені групою корейських дослідників для марковської Skipjack-подібної схеми із чотирма блоками [7].

Наведемо ще три схеми блочного шифрування, аналіз яких практично повністю повторює аналіз Skipjack-подібної схеми.

CAST-подібна схема шифрування є узагальненою схемою Фейстеля, що складається із раундів такого виду:

$$F_k(x_0, x_1, ..., x_{m-2}, x_{m-1}) = (x_1 \oplus f_k(x_0), x_2, ..., x_{m-1}, x_0)$$

Розглянемо *r*-раундову CAST-подібну схему (вважаємо, що $r > m$). Як і в попередньому випадку, із кожною диференціальною характеристикою $\Omega = (\omega_0, \omega_1, ..., \omega_r)$ можна пов'язати таку послідовність *n*-бітних змінних $a_0, a_1, ..., a_{r+m-1}$, що будуть виконуватись співвідношення

$$\omega_i = (a_{i+m-1}, a_i, a_{i+1}, ..., a_{i+m-2}),$$
$$d^{F_k}(X_i, \omega_i, \omega_{i+1}) = d^{f_k}(X_i^{(0)}, a_{i+m-1}, a_i \oplus a_{i+m}),\ i = \overline{0, r-1}.$$
$$d^{E_K}(X_0, \omega_0, \omega_r) = \sum_B \prod_{i=0}^{r-1} d^{f_k}(X_i^{(0)}, a_{i+m-1}, a_i \oplus a_{i+m}).$$

Альтернативна CAST-подібна схема шифрування є узагальненою схемою Фейстеля, що складається із раундів такого виду:

$$F_k(x_0, x_1, ..., x_{m-2}, x_{m-1}) = (x_1, x_2, ..., x_{m-1}, x_0 \oplus f_k(x_1))$$

Для такої схеми та відповідної послідовності $a_0, a_1, ..., a_{r+m-1}$ виконуються співвідношення

$$\omega_i = (a_i, a_{i+1}, ..., a_{i+m-2}, a_{i+m-1}),$$
$$d^{F_k}(X_i, \omega_i, \omega_{i+1}) = d^{f_k}(X_i^{(1)}, a_{i+1}, a_i \oplus a_{i+m}),\ i = \overline{0, r-1}.$$
$$d^{E_K}(X_0, \omega_0, \omega_r) = \sum_B \prod_{i=0}^{r-1} d^{f_k}(X_i^{(1)}, a_{i+1}, a_i \oplus a_{i+m}).$$

Нарешті, *узагальнена MISTY-подібна схема шифрування* є узагальненою схемою Фейстеля, що складається із раундів такого виду:

$$F_k(x_0, x_1, ..., x_{m-2}, x_{m-1}) = (x_1, x_2, ..., x_{m-1}, x_1 \oplus f_k(x_0))$$

Для такої схеми та відповідної послідовності $a_0, a_1, ..., a_{r+m-1}$ виконуються співвідношення

$$\omega_i = (a_i, a_{i+1}, ..., a_{i+m-2}, a_{i+m-1}),$$
$$d^{F_k}(X_i, \omega_i, \omega_{i+1}) = d^{f_k}(X_i^{(0)}, a_i, a_{i+1} \oplus a_{i+m}),\ i = \overline{0, r-1}.$$
$$d^{E_K}(X_0, \omega_0, \omega_r) = \sum_B \prod_{i=0}^{r-1} d^{f_k}(X_i^{(0)}, a_i, a_{i+1} \oplus a_{i+m}).$$

Розрахунки показали, що оцінки верхніх меж диференціальних імовірностей CAST-подібної, альтернативної CAST-подібної та узагальненої MISTY-подібної схем шифрування повністю повторюють відповідні оцінки для Skipjack-подібної схеми, що пояснюється бієктивністю функції f та однотипністю виразів для $d^{E_K}(X_0, \omega_0, \omega_r)$.

V Висновки

В роботі була запропонована методика побудови аналітичної оцінки верхньої межі імовірності існування нетривіальних диференціалів ітеративних блочних шифрів через відповідні параметри раундових функцій. Така оцінка дозволяє оцінити знизу складність проведення диференціальної атаки на шифр. Перевагами запропонованої методики є її застосовність до немарковських шифрів та можливість автоматичної побудови оцінок для складних схем шифрування. Для марковських шифрів методика може бути перенесена на оцінювання стійкості до лінійного криптоаналізу.

Також в роботі розглянута низка узагальнених схем Фейстеля, для яких були одержані верхні межі диференціальних імовірностей та обчислена кількість раундів, необхідна для заданого рівня стійкості шифру до диференціального аналізу.

Література: ***1.*** *Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.* ***2.*** *Lai X., Massey J.L., Murphy S., Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17-38.* ***3.*** *Nyberg K., Knudsen L.R. Provable Security Against a Differential Attack // Journal of Cryptology, Vol.8, no.1 (1995).* ***4.*** *Matsui M., On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis – IEICE Trans. Fundamentals, vol. E82-A – 1999 – #1 – P. 117-122.* ***5.*** *Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.* ***6.*** *Ковальчук Л. В., Шерстюк А. О. Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2 // Прикладная радиоэлектроника. – №3. – 2009. – С. 15–27.* ***7.*** *Hong S., Sung J., Lee S., Lim J., Kim J. Provable Security for 13-round Skipjack-like Structure // Information Processing Letters, 2001.*