

УДК 004.056.55:519.2

ОБЧИСЛЕННЯ ВЕРХНІХ МЕЖ ДИФЕРЕНЦІАЛЬНИХ ІМОВІРНОСТЕЙ ДЛЯ ДЕЯКИХ КЛАСІВ БЛОЧНИХ ШИФРІВ

Яковлев Сергей, Доброногов Євген

НТУУ «КПІ», Фізико-технічний інститут

Анотація

Пропонується метод обчислення верхніх меж диференціальних імовірностей для класу немарковських схем Фейстеля, що дозволяє встановити теоретичну стійкість шифрів даного класу до диференціального криптоаналізу.

Abstract

We propose a new technique for estimating upper bounds of differential probabilities for class of non-Markov Feistel networks. These results allow to claim provable security against differential cryptanalysis for ciphers from this class.

Вступ

Стійкість до диференціального криптоаналізу в наш час є необхідною вимогою для будь-якого блочного шифру. Однак існуючих аналітичних методів досі недостатньо для обґрунтування теоретичної (доказової) стійкості довільного алгоритму шифрування. В даній роботі пропонується метод обчислення параметрів стійкості до диференціального криптоаналізу для широкого класу немарковських схем Фейстеля.

Необхідні терміни та позначення

Нехай V_q – простір q -бітних векторів, K – простір ключів. Розглянемо шифруюче перетворення $f_k : V_q \times K \rightarrow V_q$. Диференціалом такої функції називатимемо довільну пару векторів $(\alpha, \beta) \in (V_q)^2$. Імовірність диференціала (α, β) в точці x визначається як

$$d^{f_k}(x; \alpha, \beta) = \frac{1}{|K|} \sum_k [f_k(x \oplus \alpha) \oplus f_k(x) = \beta],$$

де через $[X]$ позначено індикатор події X , \oplus – операція побітового додавання.

Максимальна диференціальна імовірність $MDP(f) = \max_{x, \alpha \neq 0, \beta} d^{f_k}(x; \alpha, \beta)$ характеризує стійкість шифруючого перетворення до диференціального криптоаналізу.

Ітеративний блочний шифр є композицією декількох шифруючих перетворень (раундів):

$$E_k(x) = F_{k_r}^{(r)}(F_{k_{r-1}}^{(r-1)}(\dots F_{k_1}^{(1)}(x)\dots)).$$

Тут $k = (k_1, k_2, \dots, k_r)$ – послідовність раундових ключів; ми вважаємо, що всі раундові ключі є випадковими, рівноімовірними та незалежними один від одного. Імовірність r -раундового диференціала (α, β) шифру E в точці x будемо позначати через $d^{[r]}(x; \alpha, \beta)$.

Одна із найпоширеніших схем побудови ітеративних шифрів є схема Фейстеля. В даній роботі ми розглядаємо наступний клас схем Фейстеля. Нехай $q = 2n$, $n = u \cdot t$.

- 1) Кожен раунд шифрування має вид $F_k(x, y) = (y, x \oplus f_k(y))$, де $x, y \in V_n$.
- 2) Раундова функція $f_k : V_n \times K \rightarrow V_n$ має вид $f_k(x) = L(S(x \otimes k))$, де L – лінійне (відносно \oplus) перетворення, $S = (s_1, \dots, s_m)$, $s_i : V_u \rightarrow V_u$ – S-блоки (нелінійні перетворення), а \otimes – деяка операція, що задає на V_n структуру абелевої групи та зберігає блокову структуру векторів.

На рис. 1 представлена діаграма двох раундів схеми Фейстеля.

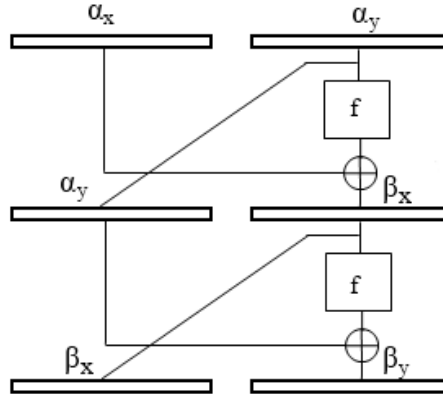


Рисунок 1 – Двораундова схема Фейстеля і відповідні диференціали

Метод оцінювання верхніх меж диференціальних імовірностей

Для обчислення величини MDP потрібно перебрати три q -бітні параметри, що для сучасних шифрів ($q = 64, 128, 256$) є надважкою задачею. Для алгоритму шифрування Camellia Ліам Келіхер запропонував метод обрахунку та алгоритм знаходження верхньої межі для MDP , який дозволяє суттєво спростити обчислення. Метод Келіхера із відповідними уточненнями може бути застосований для довільної марковської схеми Фейстеля; запропонований Келіхером алгоритм є доволі складним, оскільки використовує декілька нетривіальних «трюків», направлених на істотне зменшення обчислювальної складності.

В даній роботі ми пропонуємо узагальнення методу Келіхера для описаного в попередньому розділі класу немарковських схем Фейстеля.

Основою методу є ітеративний обрахунок верхньої межі для довільного r -раундового диференціалу, тобто визначення масиву $UB^{[r]}$, що задовольняє властивості $\forall x, \alpha, \beta : d^E(x; \alpha, \beta) \leq UB^{[r]}(\alpha, \beta)$; тоді $MDP(E) \leq \max_{\alpha \neq 0, \beta} UB^{[r]}(\alpha, \beta)$. Бачимо, що знаходження такої верхньої межі дозволяє нам нехтувати параметром x , що вже значно спрощує обчислення.

Для довільної схеми Фейстеля масив $UB^{[r]}$ обчислюється за такими формулами:

$$UB^{[2]}(\alpha, \beta) = UB^f(\alpha_y, \alpha_x \oplus \beta_x) \cdot UB^f(\beta_x, \alpha_y \oplus \beta_y),$$

$$UB^{[r]}(\alpha, \beta) = \sum_{\gamma_x \in V_n} UB^{[r-1]}(\alpha, (\gamma_x, \beta_x)) \cdot UB^f(\beta_x, \gamma_x \oplus \beta_y),$$

де $\alpha = (\alpha_x, \alpha_y)$, $\beta = (\beta_x, \beta_y)$, а UB^f – масив верхніх меж диференціальних імовірностей раундової функції f , який обчислюється окремо.

Оскільки α та β є n -бітними векторами, де для сучасних шифрів $n \geq 32$, безпосереднє обчислення масиву $UB^{[r]}$ вимагає пам'яті та часу, які далеко виходять за рамки можливого. Тому ми скористаємось запропонованим Келіхером підходом із використанням шаблонів.

Кожен вектор $x \in V_n$ ми розглядаємо як вектор $x \in (V_u)^m$ та співставляємо йому вектор-шаблон $\hat{x} \in V_m$, де i -тий біт $\hat{x}_i = 1$, якщо i -та координата $x_i \neq 0$, та $\hat{x}_i = 0$, якщо $x_i = 0$. Для векторів $y \in V_{2n}$ шаблон будується таки само чином для кожної половини. Тоді, враховуючи структуру раундової функції f , замість обчислення масиву $UB^{[r]}$ для всіх векторів α та β ми можемо обчислювати цей масив лише для шаблонів $\hat{\alpha}$ та $\hat{\beta}$. При використанні шаблонів масив $UB^{[r]}$ матиме розміри $2^{2m} \times 2^{2m}$, де для сучасних шифрів $m = 4$ або 8 . Практичні розрахунки для модифікованого алгоритму ГОСТ показують, що зберігання масиву $UB^{[r]}$ вимагає до 40 Гб пам'яті, а повне обчислення значень верхніх меж диференціальних імовірностей для одного раунду безпосередньо за вказаними формулами потребує 3-4 години роботи персонального комп'ютеру.

Наведемо точні формули для обчислення матриці UB^f за допомогою шаблонів. Позначимо через $T: V_n \rightarrow V_m$ оператор, що співставляє вектор та його шаблон: $Tx = \hat{x}$. Маємо:

$$UB^f(\hat{\alpha}, \hat{\beta}) = \max_{\hat{\gamma} \in W(\hat{\beta})} UB^S(\hat{\alpha}, \hat{\gamma}),$$

де $W(\hat{\beta}) = \{\hat{\gamma} \mid \exists x: Tx = \hat{\gamma}, T(L(x)) = \hat{\beta}\}$, а масив UB^S визначається як

$$UB^S(\hat{\alpha}, \hat{\beta}) = \begin{cases} p^{wt(\hat{\alpha})}, & \hat{\alpha} = \hat{\beta} \\ 0, & \hat{\alpha} \neq \hat{\beta} \end{cases}$$

Тут p – максимальна диференціальна імовірність серед усіх S-блоків s_i , $wt(\cdot)$ – вага Хемінга (кількість одиничних біт вектору).

Зауважимо, що представлений метод після незначних модифікацій може бути застосований до багатьох інших схем шифрування, таких як MISTY-схема, R-схема, узагальнені схеми Фейстеля тощо. Також (з точністю до заміни позначень) описаний метод може бути використаний для визначення стійкості описаного класу блочних шифрів до лінійного криптоаналізу.

Список використаних джерел:

1. Keliher Liam. Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers [електронний ресурс] / L. Keliher. – Режим доступу: <http://ijns.femto.com.tw/contents/ijns-v5-n2/ijns-2007-v5-n2-p167-175.pdf>