УДК 003.26

ОЦІНКИ НЕЛІНІЙНОСТЕЙ БЕЗКЛЮЧОВОЇ R-СХЕМИ БЛОКОВОГО ШИФРУВАННЯ

Я. В. Євсюкова[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

R-схема блокового шифрування є одним з аналогів популярної схеми Фейстеля. У даній роботі одержано аналітичні оцінки для нелінійностей трираундової безключової R-схеми через відповідні параметри її раундових функцій.

Ключові слова: блокові шифри; R-схема; лінійний криптоаналіз; легка криптографія

Вступ

Диференціальний [1] та лінійний [2] криптоаналіз є двома потужними методами аналізу симетричних блокових шифрів. Стійкість до даних методів є обов'язковою вимогою для усіх сучасних алгоритмів шифрування. Природний спосіб оцінювання стійкості шифрів до диференціального та лінійного криптоаналізу полягає у дослідженні максимальних ймовірностей диференціалів (потенціалів лінійних наближень) шифруючих перетворень, усереднених по усіх можливих ключах. Однак цей підхід не застосовний для випадку ітеративних безключових перетворень, які останнім часом широко використовуються у легкій криптографії для побудови надійних та ефективно обчислюваних нелінійних відображень (наприклад, S-блоків). У цьому випадку для забезпечення стійкості необхідно гарантувати невеликі значення диференціальних імовірностей та лінійних потенціалів перетворення в цілому. Встановлювати ці параметри шляхом безпосередньої перевірки можна лише для перетворень із невеликим розміром блоку. Тому дуже слушними стають аналітичні методи оцінювання криптографічних параметрів ітеративних безключових перетворень через відповідні параметри їх складових елементів. У роботі [3] одержали аналітичні оцінки для диференціальних імовірностей та лінійних потенціалів для трираундової безключової схеми Фейстеля; ці оцінки побудовані на основі значень диференціальних імовірностей та лінійних потенціалів раундових перетворень (S-блоків) схеми Фейстеля. [4] покращили ці оцінки та поширили їх на трираундову схему MISTY. У даній роботі буде розглянуто ще одну модифікацію схеми Фейстеля – так звану R-схему. Для трираундової безключової R-схеми із певними додатковими умовами будуть одержані оцінки нелінійностей через відповідні параметри її раундових функцій.

[a] yanayevsyukova@mail.ru

1. Необхідні терміни та позначення

У роботі розглядаються S-блоки, що мають однакову кількість вхідних та вихідних бітів. Стійкість до диференціального та лінійного криптоаналізу визначається максимальним значенням у таблиці розподілів диференціалів (таблиці лінійних апроксимацій відповідно) [5]. Визначимо ці два параметри формально. Перетворення Уолша відображення F – це функція

$$\lambda : V_n^2 \times V_n^2 \to Z$$
$$(a, b) \longmapsto \lambda_F(a, b) = \sum_{x \in V} (-1)^{b \cdot F(x) \oplus a \cdot x}$$

де крапкою позначено скалярний добуток бітових векторів. *Нелінійність* F – це величина

$$\alpha(F) = \max_{a,b \in V_n^2, b \neq 0} |\lambda_F(a, b)|$$

Варто зауважити, що для будь-якої фіксованої вихідної маски $b \in V_n$ функція $a \longmapsto \lambda_F(a, b)$ відповідає перетворенню Уолша n-змінної булевої функції $b \cdot F(x)$, що є лінійною комбінацією координатних функцій F.

R-схема блокового шифрування є одним з аналогів широко розповсюдженої схеми Фейстеля. Властивості R-схеми як шифруючого перетворення, кожен раунд якого параметризовано ключем, разом із властивостями деяких інших фейстель-подібних схем були досліджені у [6] та [7] – зокрема, у [6] були одержані аналітичні оцінки для імовірностей диференціалів та лінійних потенціалів. У даній роботі розглядаються трираундові R-схеми без ключів.

2. Нелінійність для трираундової R-схеми

Одержані оцінки нелінійності для трираундової R-схеми базуються на розгляданні окремих різниць, для яких вхідна різниця одного з раундових S-блоків дорівнює нулю.

Теорема 1. *Нехай S_1, S_2 та S_3 – це три n-бітні S-блоки (не обов'язково різні), F – це $2n$-бітова*

функція, побудована за структурою трираундової R-схеми із відображеннями S_1, S_2 та S_3 в якості раундових перетворень. Тоді для будь-яких a, b та c з F_2^n маємо:

1) *Якщо S_1 та S_2 – бієктивні, то* $\lambda_F(0||a,b||c) = \lambda_{S_2}(a, a \oplus b) \times \lambda_{S_3}(a, b \oplus c)$
2) *Якщо S_1 та S_2 – бієктивні, то* $\lambda_F(a||0,b||c) = \lambda_{S_1}(b, a \oplus c) \times \lambda_{S_3}(a, c)$
3) *Якщо S_1 – бієктивний, то* $\lambda_F(a||b,c||c) = \lambda_{S_1}(a, b) \times \lambda_{S_2}(b, c)$

Доведення: Для вектору $x \in V_n^2$ позначимо через x_L та x_R його ліву та праву частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||a)$ через функцію F таким чином, щоб одержати на виході пару $(b||c)$.Доведемо наведену границю для третього випадку Теореми 1; інші випадки доводяться аналогічно.
Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $x_L = S_1^{-1}(x_R \oplus z)$, та

$$\lambda_F(a||b,c||c) =$$
$$= \sum_{(x_R,x_L)\in(F_2^n)^2} (-1)^{a\cdot x_L \oplus b\cdot x_R \oplus c\cdot S_2(x_R \oplus S_1(x_L))}) =$$
$$= \sum_{(x_R,x_L)\in(F_2^n)^2} (-1)^{a\cdot x_L \oplus b\cdot x_R \oplus c\cdot S_2(z)} =$$
$$= \sum_{(x_R,x_L)\in(F_2^n)^2} (-1)^{a\cdot x_L \oplus b\cdot z \oplus b\cdot S_1(x_L) \oplus c\cdot S_2(z)} =$$
$$= \sum_{(x_R,x_L)\in(F_2^n)^2} (-1)^{a\cdot x_L \oplus b\cdot S_1(x_L)}.$$
$$\cdot \sum_{(x_R,x_L)\in(F_2^n)^2} (-1)^{b\cdot z \oplus c\cdot S_2(z)} =$$
$$= \lambda_{S_1}(a,b) \times \lambda_{S_2}(b,c)$$

Теорема 2. *Нехай S_1 , S_2, та S_3 – це три n-бітні S-блоки (не обов'язково різні), F – це 2n-бітова функція, побудована за структурою трираундової R-схеми із відображеннями S_1 , S_2, та S_3 в якості раундових перетворень. Тоді:*

$$\alpha(F) \geq \max(\alpha(S_2)\alpha_{min}(S_3)),$$
$$\alpha(S_1)\alpha_{min}(S_3)), \alpha(S_1)\alpha_{min}(S_2))),$$

де $\alpha_{min}(F) = \min_{b\in F_2^n, b\neq 0} \; max_{a\in F_2^n} |\lambda_F(a,b)|$
Більш того,

1) *Якщо S_1 – перестановка, то*
$$\alpha(F) \geq \alpha(S_2)\alpha_{min}(S_3)$$
2) *Якщо S_2 – перестановка, то*
$$\alpha(F) \geq \alpha(S_3)\alpha_{min}(S_1^{-1})$$
3) *Якщо S_3 – перестановка, то*
$$\alpha(F) \geq \alpha(S_2)\alpha_{min}(S_1)$$

Доведення: Даний результат є прямим наслідком Теореми 1. Розглянемо пару масок (α, β), на якому S_2 досягає нелінійності: $\alpha(S_2) = \alpha_{S_2}(\alpha, \beta)$
Оберемо $a = \alpha$ та якщо $b = \alpha \oplus \beta$, тоді для будь-яких $\gamma \in F_2^n$

$$|\lambda_F(0||\alpha, (\alpha \oplus \beta)||\gamma)| = \lambda(S_2) \times |\lambda_{S_3}(\alpha, \alpha \oplus \beta \oplus \gamma)|$$

Розглянемо пару масок (α, β), на якому S_1 досягає нелінійності: $\alpha(S_1) = \alpha_{S_1}(\alpha, \beta)$
Оберемо $a = \alpha$ та якщо $b = \beta$, тоді для будь-яких $\gamma \in F_2^n$

$$|\lambda_F(\alpha||\beta, \gamma||\gamma)| = \lambda(S_1) \times |\lambda_{S_2}(\beta, \gamma)|$$

Розглянемо пару масок (α, β), на якому S_3 досягає нелінійності: $\alpha(S_3) = \alpha_{S_3}(\alpha, \beta)$
Оберемо $a = \alpha$ та якщо $c = \beta$, тоді для будь-яких $\gamma \in F_2^n$

$$|\lambda_F(\alpha||0, \gamma||\beta)| = \lambda(S_3) \times |\lambda_{S_1}(\gamma, \alpha \oplus \beta)|$$

Можемо вибрати для γ значення, яке максимізує $|\lambda_{S_1}(\gamma, \alpha \oplus \beta)|$. Це значення завжди більше або дорівнює $\alpha_{min}(S_1^{-1})$, коли S_1 – бієктивний.

Висновки

У даній роботі було проведено аналіз безключової R-схеми блокового шифрування. Одержано аналітичні оцінки для нелінійностей R-схеми, виражені через відповідні параметри її раундових перетворень (S-блоків).

Дані результати можуть бути використані для побудови надійних алгоритмів легкої криптографії з ефективною реалізацією.

Перелік використаних джерел

1. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—EUROCRYPT'93 — LNCS, vol. 765, pp. 386–397. Springer (1994)
2. Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems", in. Journal of Cryptology. — 1991.–V.4.–№1.–P.3–72.
3. Li, Y., Wang, Constructing S-boxes for Lightweight Cryptography with Feistel Structure. In: Cryptographic Hardware and Embedded Systems 2014. —
4. Anne Canteaut, Sebastien Duval, and Gaetan Leurent, "Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version)" 2015. — Режим доступа: `http://eprint.iacr.org/2015/711.pdf`.
5. Heys Howard M. "A Tutorial on Linear and Differential Cryptanalysis" — Режим доступа: `http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf`
6. Y. Kaneko, F. Sano, K. Sakurai, "On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions" — Proc. of SAC'97. – Springer, 1997.
7. Henri Gilbert and Marine Minier, "New Results on the Pseudorandomness of Some Blockcipher Constructions" — FSE 2001. – LNCS vol.2355.–Berlin:Springer, 2002.–pp.248-266.