Оцінки Імовірностей Диференціалів Безключової R-Схеми Блокового Шифрування

Євсюкова Яна, Яковлєв Сергій
кафедра математичних методів захисту інформації
Фізико-технічний інститут
НТУУ "Київський політехнічний інститут ім. Ігоря Сікорського"
Київ, Україна
yanayevsyukova@mail.ru, yasv@rl.kiev.ua

Estimations of Differential Probabilities of Unkeyed R-Scheme of Block Encryption

Yana Yevsyukova, Serhii Yakovliev
Dept. of Mathematical Methods of Information Security
Institute of Physics and Technology
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
yanayevsyukova@mail.ru, yasv@rl.kiev.ua

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

***Abstract*—Block encryption R-scheme is one of the analog of wide known Feistel scheme. We present analytic bounds for differential probabilities of three-round keyless R-scheme, expressed with corresponding parameters of its round mappings.**

Ключові слова—блокові шифри; R-схема; диференціальний криптоаналіз; легка криптографія.

Keywords—block ciphers; R-scheme; differential cryptanalysis; lightweight cryptography.

I. Вступ

Диференціальний [3] та лінійний [4] 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 [1] Лі та Ванг 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. А.Канто та ін. [2] 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 диференціальної імовірності через відповідні параметри її раундових функцій.

II. 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) [7]. Визначимо ці два параметри формально.

Нехай V_n – множина всіх n-бітових векторів і F – це відображення з V_n на V_n. Для будь-якої пари різниць (a,b) з V_n^2 визначимо множину

$$D_F(a \to b) = \left\{ x \in F_n^2 \mid F(x \oplus a) \oplus F(x) = b \right\}.$$

Комірка з індексом (a,b) в таблиці розподілів диференціалів F тоді відповідає потужності множини $D_F(a \to b)$; позначимо її як $\delta_F(a,b)$.

Диференціальна рівномірність F – це величина

$$\delta(F) = max_{a \neq 0, b}\, \delta F(a,b).$$

Максимальна імовірність диференціалу *MDP* пов'язана із диференціальною рівномірністю очевидним чином: $MDP(F) = \delta(F)/2^n$. Для будь-яких перетворень F справедлива оцінка $\delta(F) \geq 2$. Функції F, для яких виконується рівність, називаються майже досконалими нелінійними функціями (almost perfect nonlinear mappings, APN). [8]

Перетворення Уолша відображення F – це функція

$$\lambda : V_n^2 \times V_n^2 \to Z$$

$$(a,b) \mapsto \lambda_F(a,b) = \sum_{x \in V} (-1)^{b \cdot F(x) \oplus a \cdot x},$$

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

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

Дійсно, з точністю до множника 2^n нелінійність відповідає імовірності неспівпадіння значення функції F та її найкращої лінійної апроксимації:

$$Pr_X\left[b \cdot F(x) + a \cdot X = 1\right] = \frac{1}{2^n}\left(2^{n-1} - \frac{1}{2}\sum_{x \in F_n^2} (-1)^{b \cdot F(x) \oplus a \cdot x}\right) =$$

$$= \frac{1}{2}\left(1 - \frac{\lambda_F(a,b)}{2^n}\right)$$

Варто зауважити, що для будь-якої фіксованої вихідної маски $b \in V_n$ функція $a \mapsto \lambda_F(a,b)$ 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. Діаграму обчислення R-схеми представлено на рис. 1. Властивості R-схеми як шифруючого перетворення, кожен раунд якого параметризовано ключем, разом із властивостями деяких інших фейстель-подібних схем були досліджені у [5, 6] – зокрема, у [5] були одержані аналітичні оцінки для імовірностей диференціалів та лінійних потенціалів. У даній роботі розглядаються три раундові R-схеми без ключів.

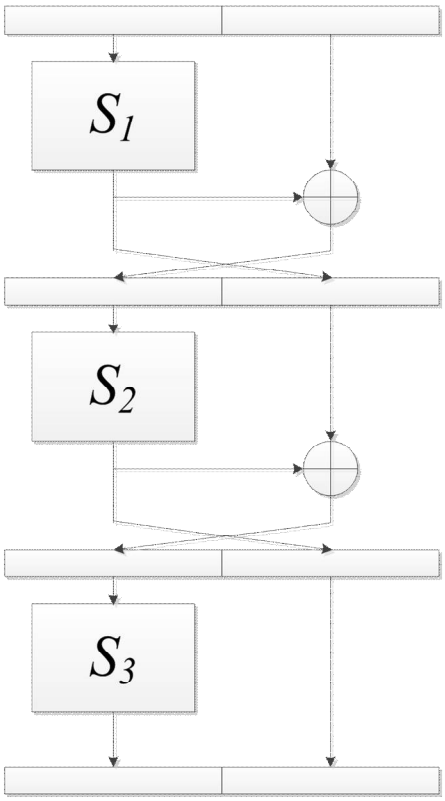

Рис. 1. Діаграма трираундової R-схеми блокового шифрування. В останньому раунді не використовується додавання частин блоку між собою.

III. Диференціальна рівномірність для трираундової R-схеми

Одержані оцінки диференціальної рівномірності 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 V_n маємо:

1) якщо S_1 – бієктивний, то

$$\delta_F(0 \,||\, a,b \,||\, c) = \delta_{S_2}(a, b \oplus c) \times \delta_{S_3}(b \oplus c, c)$$

2) якщо S_2 – бієктивний, то

$$\delta_F(b \,||\, a,c \,||\, c) = \delta_{S_1}(b,a) \times \delta_{S_3}(a,c)$$

3) якщо S_3 – бієктивний, то

$$\delta_F(a \,||\, b,c \,||\, 0) = \delta_{S_1}(a,c) \times \delta_{S_2}(b \oplus c, c).$$

Доведення: Для вектору $x \in V_n^2$ позначимо через x_L та x_R його ліву та праву частини відповідно. Розглянемо проходження різниці входів x та $x \oplus (0 \,||\, a)$ через функцію F таким чином, щоб одержати на виході різницю $(b \,||\, c)$.

Випадок 1:

Перший раунд:

$$(x_R \oplus S_1(x_L), S_1(x_L)) \oplus (x_R \oplus a \oplus S_1(x_L), S_1(x_L)) = [a,0].$$

Другий раунд:

$$\begin{aligned}
&(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L)), S_2(x_R \oplus S_1(x_L))) \oplus \\
&\oplus (S_1(x_L) \oplus S_2(x_R \oplus a \oplus S_1(x_L)), S_2(x_R \oplus a \oplus \\
&\oplus S_1(x_L))) = \\
&= (S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus a \oplus S_1(x_L)), \\
&S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus a \oplus S_1(x_L))) = \\
&= [b \oplus c, b \oplus c]
\end{aligned}$$

Третій раунд:

$$\begin{aligned}
&(S_2(x_R \oplus S_1(x_L)) \oplus S_3(S_1(x_L) \oplus S_2(x_R \oplus \\
&\oplus S_1(x_L))), S_3(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L)))) \oplus \\
&\oplus (S_2(x_R \oplus a \oplus S_1(x_L)) \oplus S_3(S_1(x_L) \oplus S_2(x_R \oplus \\
&\oplus a \oplus S_1(x_L))), S_3(S_1(x_L) \oplus S_2(x_R \oplus a \oplus S_1(x_L)))) = \\
&= (S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus a \oplus S_1(x_L)) \oplus \\
&\oplus S_3(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L))) \oplus S_3(S_1(x_L) \oplus \\
&\oplus S_2(x_R \oplus a \oplus S_1(x_L))), S_3(S_1(x_L) \oplus S_2(x_R \oplus \\
&\oplus S_1(x_L))) \oplus S_3(S_1(x_L) \oplus S_2(x_R \oplus a \oplus S_1(x_L)))) = [b,c]
\end{aligned}$$

Таким чином, вектор $x = (x_L, x_R)$ задовольняє рівнянню

$$F(x_L \,\|\, x_R) \oplus F(x_L \,\|\, (x_R \oplus a)) = b \,\|\, c$$

тоді і тільки тоді, коли:

$$\begin{aligned}
&S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus a \oplus S_1(x_L)) \oplus S_3(S_1(x_L) \oplus \\
&\oplus S_2(x_R \oplus S_1(x_L))) \oplus S_3(S_1(x_L) \oplus S_2(x_R \oplus a \oplus S_1(x_L))) = \\
&= b, \\
&S_3(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L))) \oplus S_3(S_1(x_L) \oplus \\
&\oplus S_2(x_R \oplus a \oplus S_1(x_L))) = c,
\end{aligned}$$

тобто

$$\begin{aligned}
&S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus a \oplus S_1(x_L)) = b \oplus c, \\
&S_3(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L))) \oplus S_3(S_1(x_L) \oplus \\
&\oplus S_2(x_R \oplus a \oplus S_1(x_L))) = c,
\end{aligned}$$

що рівносильне тому, що

$$y_L \in D_{S_2}(a \to b \oplus c),$$

$$y_R \in S_2(y_L) \oplus D_{S_3}(b \oplus c \to c),$$

якщо S_1 – бієктивний.

Таким чином доведено, що існує $\delta_{S_2}(a, b \oplus c)$ значень x_R та для кожного з них $\delta_{S_3}(b \oplus c, c)$ значень x_L, таких що x досягає різниці.

Випадок 2:

Розглянемо проходження різниці входів x та $x \oplus (b \,||\, a)$ через функцію F таким чином, щоб одержати на виході різницю $(c \,||\, c)$.

Аналогічно, бачимо, що вектор $x = (x_L, x_R)$ задовольняє рівнянню

$$F(x_L \,||\, x_R) \oplus F((x_L \oplus b) \,||\, (x_R \oplus a)) = c \,||\, c$$

тоді і тільки тоді, коли:

$$\begin{aligned}
&S_1(x_L) \oplus S_1(x_L \oplus b) = a, \\
&S_3(S_1(x_L) \oplus S_2(x_R \oplus S_1(x_L))) \oplus S_3(S_1(x_L \oplus b) \oplus \\
&\oplus S_2(x_R \oplus a \oplus S_1(x_L \oplus b))) = c,
\end{aligned}$$

що рівносильно системі

$$\begin{aligned}
&x_L \in D_{S_1}(b \to a), \\
&x_R \in S_1(x_L) \oplus D_{S_3}(a \to c),
\end{aligned}$$

якщо S_2 – бієктивний.

Випадок 3:

Розглянемо проходження різниці входів x та $x \oplus (a \,||\, b)$ через функцію F таким чином, щоб одержати на виході різницю $(c \,||\, 0)$

Аналогічно, бачимо, що вектор $x = (x_L, x_R)$ задовольняє рівнянню

$$F(x_L \,||\, x_R) \oplus F((x_L \oplus a) \,||\, (x_R \oplus b)) = c \,||\, 0$$

тоді і тільки тоді, коли:

$$S_1(x_L) \oplus S_1(x_L \oplus a) = c,$$
$$S_2(x_R \oplus S_1(x_L)) \oplus S_2(x_R \oplus b \oplus S_1(x_L \oplus a)) = c,$$

що рівносильно

$$x_L \in D_{S_1}(a \to c),$$
$$x_R \in S_1(x_L) \oplus D_{S_2}(b \oplus c \to c),$$

якщо S_3 – бієктивний.

Основний результат щодо оцінки диференціальної рівномірності без ключової R-схеми подамо у вигляді такої теореми.

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,

$$\delta(F) \geq \delta(S_2) \max(\delta_{\min}(S_3), \delta_{\min}(S_1)),$$

де $\delta_{\min}(S) = \min_{a \neq 0} \max_b \delta_S(a,b)$. Зокрема, якщо S_2 є перестановкою, то

$$\delta(F) \geq \max_{i \neq 2, j \neq 2, i} \max(\delta(S_i)\delta_{\min}(S_j), \delta(S_i)\delta_{\min}(S_2^{-1})) .$$

Якщо S_2 не є перестановкою, то $\delta(F) \geq 2^{n+1}$.

Доведення. Даний результат є прямим наслідком Теореми 1. Доведемо наведену границю для першого випадку Теореми 1; інші випадки доводяться аналогічно.

Розглянемо диференціал (α, β), на якому S_2 досягає диференціальної рівномірності: $\delta(S_2) = \delta_{S_2}(\alpha, \beta)$. Оберемо $a = \alpha$ та якщо $b = \beta \oplus c$; тоді для будь-яких $c \in V_n$

$$\delta_F(0 \,||\, \alpha, (\beta \oplus c) \,||\, (\beta \oplus b)) = \delta(S_2) \times \delta_{S_3}(\beta, \beta \oplus b)$$

Якщо $b \neq \beta \oplus c$, то добуток може бути більше або рівний за $\delta(F)$, або менший. Якщо ж добуток менший, то можна знайти таке значення *b*, щоб максимізувати його.

Тоді можемо вибрати для *b* значення, яке максимізує $\delta_{S_3}(\beta, \beta \oplus b)$. Це значення завжди більше або дорівнює $\delta_{\min}(S_3)$.

Так само розглянемо диференціал (α, β), на якому S_3 досягає диференціальної рівномірності: $\delta(S_3) = \delta_{S_3}(\alpha, \beta)$. Оберемо $\beta = c$ та $b = \alpha \oplus \beta$; тоді для довільного $a \in V_n$:

$$\delta_F(0 \,||\, \alpha, (\beta \oplus \alpha) \,||\, \beta) = \delta_{S_2}(a, \alpha) \times \delta(S_3) .$$

Можемо вибрати для a значення, яке максимізує $\delta_{S_2}(a, \alpha)$. Це значення завжди більше або дорівнює $\delta_{\min}(S_2^{-1})$, коли S_2 бієктивний.

Припустимо тепер, що S_2 не бієктивний. Це означає, що існує деякий ненульовий $a \in V_n$ такий, що $\delta_{S_2}(a,0) \geq 0$. Тоді з першого пункту Твердження 1 випливає, що при $b = c = 0$ співвідношення

$$F(x_L \,||\, x_R) \oplus F(x_L \,||\, (x_R \oplus a)) = (0,0)$$

має $\delta_{S_2}(a,0) \times \delta_{S_3}(0,0) \geq 2 \times 2^n = 2^{n+1}$ розв'язків у V_n^2.

Результати, аналогічні твердженням Теорем 1 та 2, також одержуються для лінійних потенціалів безключової трираундової R-схеми, що дозволяє виводити безпосередні оцінки стійкості до лінійного криптоаналізу.

IV. Висновки

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

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

Література References

[1] Li, Y., Wang, M.: Constructing S-boxes for Lightweight Cryptography with Feistel Structure. In: Cryptographic Hardware and Embedded Systems – CHES 2014, LNCS, vol. 8731, pp. 127–146. Springer (2014).

[2] Anne Canteaut, Sebastien Duval, and Gaetan Leurent "Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version)", Inria, project-team SECRET, France [Online.] – http://eprint.iacr.org/2015/711.pdf

[3] Matsui, M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 386–397. Springer (1994)

[4] Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems", in. Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.

[5] 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.

[6] 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.

[7] Heys Howard M. "A Tutorial on Linear and Differential Cryptanalysis" [Online.] – Available at http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf