

Побудова Оцінок Стійкості SP-мереж Спеціального Виду до Диференціального Криптоаналізу

Олексій Якимчук, Сергій Яковлєв
кафедра математичних методів захисту інформації
Фізико-технічний інститут
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Київ, Україна
salol1d2323@gmail.com, yasv@rl.kiev.ua

Security Evaluation of Special Type SP-networks Against Differential Cryptanalysis

Oleksii Yakymchuk, Serhii Yakovliev
Department of Mathematical Methods of Information Security
Institute of Physics and Technology
National Technical University of Ukraine “Igor Sikorsy Kyiv Polytechnic Institute”
Kyiv, Ukraine
salol1d2323@gmail.com, yasv@rl.kiev.ua

Анотація—У роботі розглядаються SP-мережі, які використовують додавання за модулем у ключовому суматорі. Наводяться аналітичні верхні межі для імовірностей диференціальних характеристик таких SP-мереж за операціями побітового, поблокового та модульного додавання. Одержані оцінки обчислюються через певні специфічні параметри S-блоків шифру.

Abstract—We consider SP-networks with modular key addition in this work. We present analytic upper bounds for the probabilities of differential characteristics of such SP-networks with respect to bit-wise (XOR), block-wise and modular additions. Obtained bounds are expressed through specific parameters of cipher's S-boxes.

Ключові слова—диференціальний криптоаналіз, розподіли диференціалів, диференціальні характеристики, SP-мережа

Keywords—differential cryptanalysis, distributions of differentials, differential characteristics, SP-network

I. ВСТУП

Диференціальний криптоаналіз є одним з найпотужніших методів криптоаналізу блокових шифрів. Стійкість до диференціального криптоаналізу наразі є необхідною вимогою до усіх нових алгоритмів шифрування. В наш час існує добре розвинена формальна теорія диференціального криптоаналізу, яка дозволяє оцінювати складність проведення диференціальної атаки для широких класів різних схем блокового шифрування.

Найбільш детально досліджені так звані марковські шифри (відносно операції побітового додавання). Для різних схем шифрування побудовано оцінки практичної та доказової стійкості до диференціального аналізу. [2-4]

Додавання за модулем 2^n є дуже привабливою операцією з точки зору криптографії. З одного боку, вона доступна майже в усіх сучасних обчислювальних архітектурах на рівні інструкцій процесору, тобто її реалізація є швидкою та ефективною. З іншого боку, модульне додавання має аналітичний опис як булева функція високого степеня нелінійності – і, таким чином, використання модульного додавання робить залежності між бітами шифротексту, відкритого тексту та ключа дуже складними для криптографічного аналізу.

Однак використання додавання за модулем разом із іншими алгебраїчними операціями перетворює більшу частину шифрів у немарковські. Відповідно, наявна формальна теорія диференціального криптоаналізу не застосовна для проведення оцінювання стійкості. Таким чином, разом із очевидним підвищенням складності аналізу використання модульного додавання парадоксально унеможливує гарантованість такої складності – в першу чергу через відсутність методів побудови оцінок стійкості.

Вперше деякі оцінки практичної стійкості до диференціального криптоаналізу для схем Фейстеля із модульним додаванням у ключовому суматорі були

одержані в [1]; в цій роботі розглядались для диференціальні характеристики відносно побітового додавання, що зумовлено структурою схеми Фейстеля. У даній роботі розглядається інший широко вживаний клас блокових шифрів, SP-мережі, із модульним додаванням у ключовому суматорі. Для шифрів даного виду побудовано аналітичні верхні межі для диференціальних характеристик відносно трьох різних алгебраїчних операцій та показано, через які параметри S-блоків шифру обчислюються такі оцінки.

II. НЕОБХІДНІ ТЕРМІНИ ТА ПОЗНАЧЕННЯ

Нехай V_n – простір n -бітових векторів, і бінарні операції \otimes, \bullet визначають на V_n структури абелевих груп.

(\circ, \bullet) -диференціалом булевої функції $f: V_n \rightarrow V_n$ називається пара векторів $(\alpha, \beta) \in V_n^2$. Імовірністю диференціалу (α, β) називається величина:

$$DP_{\circ, \bullet}^f(\alpha, \beta) = \sum_x [f(x \circ \alpha) = f(x) \bullet \beta],$$

де $\sum_x = \frac{1}{2^n} \sum_x$ – середня сума, $[P]$ – дужки Айверсона,

які визначаються так: $[P] = \begin{cases} 1, & \text{якщо } P \text{ – істинне;} \\ 0, & \text{якщо } P \text{ – хибне.} \end{cases}$

Якщо функція $f_k: V_n \times K \rightarrow V_n$ – булева функція, параметризована певними ключами, то імовірність диференціалу такої функції в точці x визначається як

$$DP_{\circ, \bullet}^{f_k}(x, \alpha, \beta) = \sum_k [f_k(x \circ \alpha) = f_k(x) \bullet \beta].$$

r -раундовою SP-мережею називається перетворення $E: V_n \times K^r \rightarrow V_n$, що є композицією r раундових шифруючих перетворень виду $F_k(x) = L(S_k(x))$ (див. рис. 1), де L – лінійне відносно визначеної операції перетворення. Далі усюди вважається, що ключі раундів обираються незалежно та рівномірно з множини ключів K . У даній роботі розглядається спеціальний клас SP-мереж виду $F_k(x) = L(S(x+k))$, де $+$ – додавання за модулем 2^n , S – нелінійне перетворення (S-блоки), L – лінійне перетворення.

Диференціальною характеристикою називається послідовність ненульових векторів $\Omega = (\omega_0, \omega_1, \dots, \omega_r)$, $\omega_i \in V_n, \omega_i \neq 0, i = 1, \dots, r$. Ця послідовність розглядається як набір різниць між проміжними шифротекстами раундових перетворень.

Імовірністю диференціальної характеристики називається величина:

$$DCP_{\circ}^E(\Omega, x_0) = \sum_{k_1} \sum_{k_2} \dots \sum_{k_r} \prod_{i=1}^r [F_{k_i}(x_{i-1} \circ \omega_{i-1}) = F_{k_i}(x_{i-1}) \circ \omega_i].$$

Нехай $n = m \cdot u$ та $V_n = (V_u)^m$. Далі будемо розглядати різниці відносно трьох операцій над даною множиною векторів:

- $+$: операція додавання за модулем 2^n , враховується біт переносу: $x, k \in V_n$:
 $x + k = (x_1 + k_1, x_2 + k_2 + \mu_2, \dots, x_m + k_m + \mu_m)$,
де $\mu_{i+1} = \left\lfloor \frac{x_i + k_i + \mu_i}{2^u} \right\rfloor$, $\mu_1 = 0$, $i = \overline{1, r-1}$,
 $\mu_i, x_i, k_i \in V_u, i = \overline{1, r}$.
- \oplus : операція побітового додавання, без біту переносу.
- $[+]$: додавання за модулем 2^u , $x, k \in V_n$:
 $x + k = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$, $x_i, k_i \in V_u$,
 $i = \overline{1, r}$ (покоординатне додавання).

III. ОЦІНКИ ІМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛІВ ШИФРУЮЧИХ ПЕРЕТВОРЕНЬ СПЕЦІАЛЬНОГО ВИГЛЯДУ

Розглянемо шифруюче перетворення $F_k = S(x+k)$, де ключ додається за модулем 2^n , а функція S – композиція m незалежних s -блоків $s_1(x_1), s_2(x_2), \dots, s_m(x_m)$, (див. рис. 1). Знайдемо аналітичні оцінки імовірностей диференціалів даного перетворення відносно наведених трьох операцій.

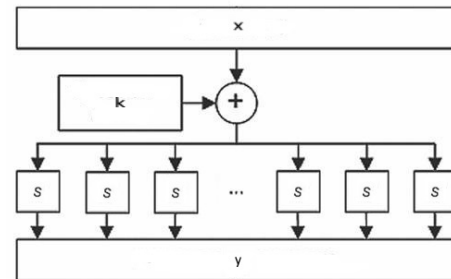


Рис. 1. Шифруюче перетворення F .

A. Дослідження $DP_{+,+}^{F_k}(x, \alpha, \beta)$

З означення імовірності диференціалу випливає

$$DP_{+,+}^{F_k}(x, \alpha, \beta) = \sum_k [F_k(x + \alpha) = F_k(x) + \beta] = \sum_k [S((x + \alpha) + k) = S(x + k) + \beta].$$

Для переходу до покоординатних додавань u -бітових слів введемо змінні для бітів переносу, які виникають під час виконання обчислень:

$$\hat{\mu}_{i+1} = \left\lfloor \frac{x_i + \alpha_i + k_i + \mu_i}{2^u} \right\rfloor, \quad \mu_{i+1} = \left\lfloor \frac{x_i + k_i + \mu_i}{2^u} \right\rfloor,$$

$$\varepsilon_{i+1} = \left\lfloor \frac{s_i(x_i + k_i + \mu_i) + \beta_i + \varepsilon_i}{2^u} \right\rfloor,$$

де $\hat{\mu}_0 = 0$, $\mu_0 = 0$, $\varepsilon_0 = 0$, $x_i, k_i, \alpha_i, \beta_i \in V_u$, $i = \overline{0, m-1}$.
Відповідно, можемо записати:

$$\begin{aligned} & \sum_k [S((x + \alpha) + k) = S(x + k) + \beta] = \\ & = \prod_{i=1}^m \sum_{k_i} [s_i(x_i + \alpha_i + k_i + \hat{\mu}_i) = s_i(x_i + k_i + \mu_i) + \beta_i + \varepsilon_i], \end{aligned}$$

оскільки всі s-блоки незалежні між собою. Виконавши заміну $u_i = x_i + k_i + \mu_i$, $i = 1, \dots, m$, одержимо таку рівність:

$$\prod_{i=1}^m \sum_{k_i} [s_i(x_i + \alpha_i + k_i + \hat{\mu}_i) = s_i(x_i + k_i + \mu_i) + \beta_i + \varepsilon_i] = \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i]. \quad (1)$$

Із визначення бітів переносу випливає, що $\hat{\mu}_i \geq \mu_i$.
Неважко також показати, що $\hat{\mu}_i = 2$ лише у випадку, коли $\mu_i = 1$. Відповідно, значення різниці $\hat{\mu}_i - \mu_i \in \{0, 1\}$.

Для наочності розглянемо останній множник з отриманого добутку (1):

$$\begin{aligned} & \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i] = \\ & = \prod_{i=1}^{m-1} \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i] \times \\ & \times \sum_{k_m} [s_m(u_m + \alpha_m + \hat{\mu}_m - \mu_m) = s_m(u_m) + \beta_m + \varepsilon_m]. \end{aligned}$$

Зауважимо, що u_m є функцією від k_m та, коли k_m пробігає усі можливі значення, u_m також пробігає усі можливі значення. Отже, останній множник за визначенням дорівнює $DP_{+,+}^{s_m}(\alpha_m + \hat{\mu}_m - \mu_m, \beta_m + \varepsilon_m)$. Однак $\hat{\mu}_m, \mu_m, \varepsilon_m$ є функціями від усіх попередніх частин ключа, тому уся сума не розпадається на добуток незалежних сум по кожній частині ключа. Втім, можна замінити точне значення диференціальної імовірності на оцінку:

$$\begin{aligned} & \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i] \leq \\ & \leq \prod_{i=1}^{m-1} \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i] \times \\ & \times \max_{\alpha, \varepsilon \in \{0,1\}} DP_{+,+}^{s_m}(\alpha_m + \mu, \beta_m + \varepsilon). \end{aligned}$$

Аналогічним чином можна оцінювати множник за множником від m -того до першого та за індукцією побудувати загальну оцінку добутку (1) зверху:

$$\begin{aligned} & \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \alpha_i + \hat{\mu}_i - \mu_i) = s_i(u_i) + \beta_i + \varepsilon_i] \leq \\ & \leq \prod_{i=1}^m \max_{\alpha, \varepsilon \in \{0,1\}} DP_{+,+}^{s_i}(\alpha_i + \mu, \beta_i + \varepsilon). \end{aligned}$$

Отже, маємо

$$DP_{+,+}^{F_k}(x, \alpha, \beta) \leq \prod_{i=1}^m \max_{\mu, \varepsilon \in \{0,1\}} DP_{+,+}^{s_i}(\alpha_i + \mu, \beta_i + \varepsilon).$$

B. Дослідження $DP_{\oplus, \oplus}^{F_k}(x, \alpha, \beta)$

З означення імовірності диференціалу випливає

$$\begin{aligned} DP_{\oplus, \oplus}^{F_k}(x, \alpha, \beta) &= \sum_k [F_k(x \oplus \alpha) = F_k(x) \oplus \beta] = \\ &= \sum_k [S((x \oplus \alpha) + k) = S(x + k) \oplus \beta]. \end{aligned}$$

У даному випадку для переходу до по координатних додавань необхідно ввести такі змінні для бітів переносу:

$$\mu_{i+1} = \left\lfloor \frac{(x_i \oplus \alpha_i) + k_i + \mu_i}{2^u} \right\rfloor, \quad \eta_{i+1} = \left\lfloor \frac{x_i + k_i + \eta_i}{2^u} \right\rfloor,$$

де так само $\mu_0 = 0$, $\eta_0 = 0$, $x_i, k_i, \alpha_i, \beta_i \in V_u$, $i = \overline{0, m-1}$.
Відповідно, одержимо

$$\begin{aligned} & \sum_k [S((x \oplus \alpha) + k) = S(x + k) \oplus \beta] = \\ &= \prod_{i=1}^m \sum_{k_i} [s_i(x_i \oplus \alpha_i + k_i + \mu_i) = s_i(x_i + k_i + \eta_i) \oplus \beta_i]. \end{aligned}$$

Введемо нові змінні $\hat{\alpha}_i$ такі, що $x_i + \hat{\alpha}_i = x_i \oplus \alpha_i$ для кожного $i = \overline{1, m}$. Також виконаємо заміну: $u_i = x_i + k_i + \eta_i$. Одержимо:

$$\begin{aligned} & \prod_{i=1}^m \sum_{k_i} [s_i(x_i \oplus \alpha_i + k_i + \mu_i) = s_i(x_i + k_i + \eta_i) \oplus \beta_i] = \\ &= \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \hat{\alpha}_i + \mu_i - \eta_i) = s_i(u_i) \oplus \beta_i]. \end{aligned}$$

В цьому випадку $\mu_i, \eta_i \in \{0, 1\}$ і певної залежності між їх значеннями нема, тому $\mu_i - \eta_i \in \{-1, 0, 1\}$. Звідси перетвореннями, які є аналогічними наведеним у попередньому випадку, одержуємо нерівність

$$DP_{\oplus, \oplus}^{F_k}(x, \alpha, \beta) \leq \prod_{i=1}^m \max_{\mu \in \{-1, 0, 1\}} DP_{+, \oplus}^{s_i}(\hat{\alpha}_i + \mu, \beta_i).$$

Треба зауважити, що в цьому випадку $\hat{\alpha} = \hat{\alpha}(x, \alpha)$.

C. Дослідження $DP_{[+], [+]}^{F_k}(x, \alpha, \beta)$

З означення імовірності диференціалу випливає

$$\begin{aligned} DP_{[+], [+]}^{F_k}(x, \alpha, \beta) &= \sum_k [F_k(x[+] \alpha) = F_k(x)[+] \beta] = \\ &= \sum_k [S((x[+] \alpha) + k) = S(x + k)[+] \beta]. \end{aligned}$$

Для переходу до по координатних додавань вводимо нові змінні для бітів переносу:

$$\mu_{i+1} = \left\lfloor \frac{x_i + \alpha_i + k_i + \mu_i}{2^u} \right\rfloor, \quad \eta_{i+1} = \left\lfloor \frac{x_i + k_i + \eta_i}{2^u} \right\rfloor,$$

де знову $\mu_0 = 0$, $\eta_0 = 0$, $x_i, k_i, \alpha_i, \beta_i \in V_u$, $i = \overline{0, m-1}$.
Відповідно, врахувавши, що на рівні u -бітових слів

операція $[+]$ перетворюється у звичайне додавання за модулем 2^u , одержуємо

$$\begin{aligned} & \sum_k [S((x[+] \alpha) + k) = S(x + k)[+] \beta] = \\ & = \prod_{i=1}^m \sum_{k_i} [s_i(x_i + \alpha_i + k_i + \mu_i) = s_i(x_i + k_i + \eta_i) + \beta_i] . \end{aligned}$$

Виконавши стандартну заміну $u_i = x_i + k_i + \eta_i$, отримаємо

$$\begin{aligned} & \prod_{i=1}^m \sum_{k_i} [s_i(x_i + \alpha_i + k_i + \mu_i) = s_i(x_i + k_i + \eta_i) + \beta_i] = \\ & = \prod_{i=1}^m \sum_{k_i} [s_i(u_i + \alpha_i + \mu_i - \eta_i) = s_i(u_i) + \beta_i] . \end{aligned}$$

Так як і в пункті А: $\mu_i \geq \eta_i$, тому $\mu_i - \eta_i \in \{0, 1\}$. Звідси перетвореннями, аналогічними до попередніх, одержуємо оцінку

$$DP_{[+], [L]}^{F_k}(x, \alpha, \beta) \leq \prod_{i=1}^m \max_{\mu \in \{0, 1\}} DP_{+, +}^{s_i}(\alpha_i + \mu, \beta_i) .$$

IV. ОЦІНКИ ІМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛЬНИХ ХАРАКТЕРИСТИК SP-МЕРЕЖ СПЕЦІАЛЬНОГО ВИГЛЯДУ

Розглянемо блоковий шифр із структурою SP-мережі та раундовим перетворенням виду $F_k(x) = L(S(x + k))$ (див. рис. 2).

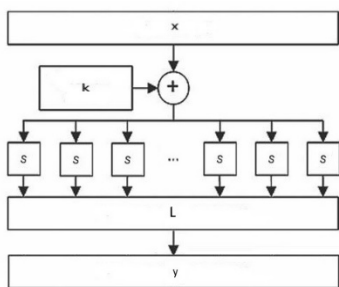


Рис. 2. Один раунд SP-мережі.

При розгляданні різниць відносно операцій \oplus та $[+]$ даний шифр буде немарковським, а при розгляданні різниць відносно операції $+$ імовірності диференціалів не обчислюються явним чином через параметри S-блоків. Однак у [1] доведено оцінку для імовірностей диференціальних характеристик, яка застосовна до будь-якого ітеративного шифру: $\forall x_0 \in V_n, \forall \Omega$:

$$DCP_{\circ, \oplus}^E(\Omega, x_0) \leq \prod_{i=1}^r \max_z DP_{\circ, \oplus}^F(z, \omega_{i-1}, \omega_i) . \quad (2)$$

Застосувавши нерівність (2) до SP-мереж описаного типу, можна одержати аналітичні оцінки імовірностей диференціальних характеристик через параметри S-блоків, які розглядались у попередньому розділі.

Так, за означенням маємо

$$\begin{aligned} & DCP_{+, +}^E(\Omega, x_0) = \\ & = \sum_{k_1} \sum_{k_2} \dots \sum_{k_r} \prod_{i=1}^r [F_{k_i}(x_{i-1} + \omega_{i-1}) = F_{k_i}(x_{i-1}) + \omega_i] , \end{aligned}$$

де r – кількість раундових перетворень в SP-мережі.

За нерівністю (2) маємо

$$\begin{aligned} & DCP_{+, +}^E(\Omega, x_0) \leq \prod_{i=1}^r \max_x DP_{+, +}^F(x, \omega_{i-1}, \omega_i) = \\ & = \prod_{i=1}^r \max_x DP_{+, +}^{s_k}(x_i, \omega_{i-1}, L^{-1}(\omega_i)), \hat{\omega}_i = L^{-1}(\omega_i) \end{aligned}$$

Для вектору $\forall \omega_i \in \Omega: \forall i = 1, \dots, r$, позначимо його координати $\omega_i = (\omega_i^{(1)}, \omega_i^{(2)}, \dots, \omega_i^{(m)})$. Враховуючи оцінки, одержані у попередньому розділі, остаточно маємо для усіх характеристик Ω та початкових точок x_0 :

$$DCP_{+, +}^E(\Omega, x_0) \leq \prod_{i=1}^r \prod_{j=1}^m \max_{\mu, \varepsilon \in \{0, 1\}} DP_{+, +}^{s_j^{(i)}}(\omega_j^{(i-1)} + \mu, \omega_i^{(j)} + \varepsilon) .$$

Аналогічно одержимо нерівності й для диференціальних характеристик відносно інших операцій:

$$DCP_{\oplus, \oplus}^E(\Omega, x_0) \leq \prod_{i=1}^r \prod_{j=1}^m \max_{\mu \in \{-1, 0, 1\}} DP_{+, \oplus}^{s_j^{(i)}}(\omega_j^{(i-1)} + \mu, \omega_i^{(j)}) ,$$

$$DCP_{[+], [L]}^E(\Omega, x_0) \leq \prod_{i=1}^r \prod_{j=1}^m \max_{\mu \in \{0, 1\}} DP_{+, +}^{s_j^{(i)}}(\omega_j^{(i-1)} + \mu, \omega_i^{(j)}) .$$

ВИСНОВКИ

У даній роботі розглянуто SP-мережі із додаванням за модулем у ключовому суматорі. Для таких блокових шифрів побудовано аналітичні верхні межі для імовірностей диференціальних характеристик відносно побітового, поблокового та модульного додавання. Одержані оцінки використовують специфічні параметри S-блоків та можуть застосовуватись для чисельного визначення імовірностей характеристик, які визначають практичну стійкість блокових шифрів до диференціального криптоаналізу.

Результати даної роботи є першими кроками до побудови загальної формальної теорії диференціального криптоаналізу блокових шифрів із ключовими суматорами неблокової структури.

ЛІТЕРАТУРА REFERENCES

- [1] A. N. Alekseychuk, L. V. Kovalchuk. "Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis" [Online]. – Available at: <https://eprint.iacr.org/2011/489>
- [2] Kanda M. "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function" // Proceedings of Selected Areas in Cryptography (SAC 2000). – Springer Verlag, 2001. – P. 324 – 338.
- [3] K. Nyberg, L.R. Knudsen. "Provable Security Against a Differential Attack". – Journal of Cryptology. – Vol.8. – No.1. – 1995.
- [4] S. Park et al. "On the security of Rijndael-like structures against differential and linear cryptanalysis" // Advances in Cryptology (ASIACRYPT 2002). – LNCS, vol. 2501. – 2002. – pp. 176-191.