# Асимтотичні Розподіли Імовірностей Змішаних Диференціалів Випадкових S-Блоків

Всеволод Бахтігозін, Сергій Яковлєв
кафедра математичних методів захисту інформації
Фізико-технічний інститут
Національній технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Київ, Україна
seba.bakh@gmail.com, yasv@rl.kiev.ua

# Asymptotic Distributions of Mixed-Type Differential Probabilities of Random S-Boxes

Vsevolod Bakhtigozin, 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
seba.bakh@gmail.com, yasv@rl.kiev.ua

***Анотація*—У роботі наводяться асимптотичні розподіли ймовірностей диференціалів випадкових перестановок за різними груповим операціями на вході та на виході (побітове та модульне додавання); також знайдено довірчий інтервал для ймовірностей диференціалів такого типу.**

***Abstract*—We present asymptotic distributions of probabilities of random permutation differentials with respect to different group operations for inputs and outputs (bitwise and modular additions are considered). Also we provide confidence interval for such mixed-type differential probabilities.**

***Ключові слова—диференціальний криптоаналіз, розподіли диференціалів***

***Keywords—differential cryptoanalysis, distributions of differentials***

## I. Вступ

Диференціальний криптоаналіз є одним з найпотужніших методів криптоаналізу симетричних блокових шифрів. Сучасні методи доведення стійкості алгоритмів шифрування до диференціального криптоаналізу фактично зводять відповідні оцінки стійкості до певних обчислювальних параметрів раундових перетворень та їх окремих компонент, таких як S-блоки (див., наприклад, [1-4]). Зазвичай для підвищення стійкості до даного методу аналізу у блокових шифрах обираються бієктивні S-блоки (тобто підстановки на бітових векторах) із мінімально можливими імовірностями диференціалів.

У роботах [5,6] було досліджено асимптотичні розподіли ймовірностей диференціалів випадкових перестановок за різними груповими операціями, а саме побітового додавання (XOR), додавання за модулем та множення за модулем. Зокрема, було показано, що імовірності таких диференціалів підкорюються розподілам Пуассона із різними параметрами (1/2 для побітового додавання та 1 для інших операцій, які розглядались). Також були побудовані довірчі інтервали для диференціалів за кожною операцією та показано, що диференціали за побітовим додаванням мають в цілому суттєво більші імовірності.

Однак для деяких класів блокових шифрів оцінки доказової стійкості до диференціального аналізу будуються через значення імовірностей змішаних диференціалів, в яких різниці на вході та на виході S-блоку обчислюються за різними операціями (див., зокрема, [7-9]). У даній роботі ми розглянемо асимптотичні розподіли імовірностей диференціалів найпоширенішого змішаного типу, в яких різниці обчислюються за побітовим та модульним додаванням. Буде доведено, що імовірності змішаних диференціалів асимптотично підкорюються розподілу Пуассона із параметрами 1 або ½. Також для довільного розміру S-блоку нами буде одержано довірчій інтервал для диференціальних імовірностей змішаного типу.

## II. Необхідні терміни та позначення

Нехай $V_n$ – простір $n$-бітових векторів, і бінарна операція $\otimes$ визначає на $V_n$ структуру абелевої групи. В якості $\otimes$ ми будемо розглядати, зокрема, операції $\oplus$ (побітове додавання) та + (додавання за модулем $2^n$); в останньому випадку бітові вектори трактуються як цілі невід'ємні числа у двійковому записі.

Позначимо через $\pi$ деяку підстановку на $V_n$. *Диференціалом* $\pi$ називається довільна пара бітових векторів $(\alpha, \beta)$, які трактуються як різниці на вході та на виході $\pi$ за операцією $\otimes$:

$$u \otimes v^{-1} = \alpha \Rightarrow \pi(u) \otimes (\pi(v))^{-1} = \beta,$$

де $\alpha, \beta, u, v \in V_n$, $\otimes$ – групова операція, обернені елементи обчислюються за цією операцією. *Імовірністю диференціала* $(\alpha, \beta)$ називається величина

$$DP^{\pi}_{\otimes}(\alpha,\beta) = Pr_{x \in V_n}\{\pi(x \otimes \alpha) = \pi(x) \otimes \beta\}.$$

Змішаним, або $(+,\oplus)$-диференціалом $\pi$, будемо називати пара бітових векторів $(\alpha, \beta)$, які трактуються як різниці на вході та виході за різними операціями: для двох вхідних значень $u, v$

$$(u - v) \bmod 2^n = \alpha,\ \pi(u) \oplus \pi(v) = \beta.$$

Імовірністю $(+,\oplus)$-диференціалу називається величина

$$DP^{\pi}_{+,\oplus}(\alpha,\beta) = Pr_{x \in V_n}\{\pi(x + \alpha) = \pi(x) \oplus \beta\}.$$

Аналогічним чином визначаються $(\oplus,+)$-диференціали підстановки $\pi$ та їх імовірності $DP^{\pi}_{\oplus,+}$.

Нехай $a = ord\alpha$, $b = ord\beta$, де $(\alpha, \beta)$ – довільний диференціал. Ймовірність такого диференціалу залежить лише від порядків елементів у групах, які визначаються відповідними операціями [5]:

$$p_t(a,b) = Pr_{\pi}\{2^n \cdot DP^{\pi}(\alpha,\beta) = t\}.$$

Для абелевої групи $\langle V_n, \otimes \rangle$ визначимо такі множини:

$$E_{\delta} = \{(u,v) \mid u \otimes v^{-1} = \delta\}$$

– множина пар елементів, які мають різницю $\delta$ за відповідною операцією, та

$$A_{uv} = \{\pi \mid (\pi(u), \pi(v)) \in E_{\delta}\}$$

– множина перестановок, що відображає пару елементів $(u,v)$ у пару елементів, яка належить множини $E_{\delta}$.

## III. Асимптотичні розподіли імовірностей змішаних диференціалів

Розглянемо довільний диференціал $(\alpha, \beta)$, де $\alpha, \beta \neq 0$, $a = ord\alpha$, $b = ord\beta$. Імовірність $p_t(a,b)$ визначається як $p_t(a,b) = P_t/2^n!$, де $P_t$ – кількість перестановок, які відображають рівно t елементів з множини $E_{\alpha}$ у множину $E_{\beta}$.

У роботі [5] було показано, що

$$P_t = \sum_{i=0}^{2^n - t} (-1)^i C^i_{t+i} S_{t+i},$$

де $S_k = \sum_{Y \subseteq E_{\alpha}, |Y|=k} \left| \bigcap_{uv \in Y} A_{uv} \right|$.

Наведений вище вираз для $S_k$ стає надзвичайно складним для $a$ і $b$ більше 2. Розглянемо інший вираз, визначений не в термінах пар елементів, а в термінах окремих елементів. Нехай $Y \subseteq E_{\alpha}$, $|Y| = k$, тоді кількість окремих елементів $p(Y)$ у множині $Y$ буде знаходитись у межах від $k$ (всі елементи утворюють єдиний цикл) до $2k$ (жоден окремий елемент не утворює двох диференціалів). Розглянемо функцію:

$$\varphi(k,j) = \sum_{Y \subseteq E_{\alpha}, |Y|=k, p(Y)=j} \left| \{\pi \mid \pi(Y) \subseteq E_{\beta}\} \right|.$$

Тоді вираз для $S_k$ приймає наступний вигляд:

$$S_k = \sum_{j=k}^{2k} \varphi(k,j)$$

В цій сумі домінуючим додатком є $\varphi(k,2k)$. Якщо $j \neq 2k$, маємо два випадки:

1) $ord\alpha = 2$ – таких елементів всього два: 0 та $2^{n-1}$, причому перше значення відповідає тривіальному диференціалу, який має константний розподіл. Оскільки $b = 2$ для будь-якого диференціалу, то одержуємо ситуацію, яка була повністю досліджена у [5, 6]. Зокрема, було показано, що величина $2^n DP(\alpha,\beta)$ має розподіл Пуассона з параметром 1/2

2) $ord\alpha \neq 2$ – в цьому випадку маємо дві пари елементів $(x, y)$, $(y, z) \subseteq E_{\alpha}$, причому $x \neq z$ (інакше це попередній випадок, оскільки тоді $ord\alpha = 2$) Але тоді маємо

$$\pi(x) \oplus \pi(y) = \pi(y) \oplus \pi(z) = \beta.$$

Отже, $\pi(x) \oplus \pi(z) = 0$, що можливо тільки при $x = z$; маємо протиріччя, а тому одна з цих пар не належить $E_{\beta}$. Отже, доданків такого виду у $S_k$ не міститься взагалі.

Перейдемо до оцінки величини $\varphi(k,2k)$. Побудова перестановок $\pi(Y) \subseteq E_{\beta}$ відбувається у такий комбінаторний спосіб. Існує $2^n$ способів відобразити перший елемент однієї пари із різницею $\alpha$; другий елемент

ції пари після цього відображається однозначно. Для наступної пари маємо вже $2^n - 2$ способів побудови образу, і так далі, доки не отримаємо $k$ пар для диференціалу $(\alpha, \beta)$. Елементи, які залишились, можна довільно відобразити $(2^n - 2k)!$ способами. Таким чином, кількість перестановок $\pi$: $\pi(Y) \subseteq E_\beta$ дорівнює

$$\prod_{i=0}^{k-1}(2^n - 2i)(2^n - 2k)! =$$
$$= \left(\frac{2^n}{2}\right)^{\underline{k}} 2^k (2^n - 2k)! \approx 2^{nk}(2^n - 2k)!$$

Відповідно, кількість множин $Y \subseteq E_\alpha$, $|Y| = k$ оцінюється у такий спосіб: першу пару можна вибрати $2^n$ способами, другу – $(2^n - 3)$ способами (оскільки не можна вибирати пари, суміжні з вже обраними) і т.д. Кількість множин $Y \subseteq E_\alpha$, $|Y| = k$, дорівнює

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^n - 3i) = \frac{1}{k!}\left(\frac{2^n}{3}\right)^{\underline{k}} 3^k \approx \frac{2^{nk}}{k!}$$

(Відповідні апроксимації наведено у [6].)

Тоді вираз для $\varphi(k,2k)$ приймає вигляд:

$$\varphi(k,2k) = 2^{nk}(2^n - 2k)!\frac{2^{nk}}{k!} \approx \frac{2^n!\,2^{2nk}}{k!\,2^{2nk}}.$$

Підставляючи це в формулу для $S_k$, а потім і для $P_t$, остаточно одержуємо:

$$P_t = \sum_{i=0}^{2^n - t}(-1)^i C_{t+i}^i \frac{2^n!}{(t+i)!} =$$
$$= \sum_{i=0}^{2^n - t}(-1)^i \frac{(t+i)!\,2^n!}{i!\,t!\,(t+i)!} =$$
$$= \frac{2^n!}{t!}\sum_{i=0}^{2^n - t}\frac{(-1)^i}{i!} \approx \frac{2^n!}{t!}e^{-1}$$

Звідси $p_t(a,b) = e^{-1}/t$, тобто імовірності $(+,\oplus)$-диференціалів для випадкової перестановки підкорюються розподілу Пуассона з параметром $1$ – так само, як і імовірності $(+,+)$-диференціалів.

Зауважимо, що одержані асимптотичні оцінки залишаються вірними і для $(\oplus,+)$-диференціалів через природну відповідність: будь-якому $(\oplus,+)$-диференціалу $(\alpha, \beta)$ перестановки $\pi(x)$ відповідає $(+,\oplus)$-диференціал $(\beta, \alpha)$ зворотної перестановки $\pi^{-1}(x)$; оскільки розподіли диференціалів обчислюються на множині всіх перестановок, то асимптотичні розподіли означених диференціалів будуть співпадати. Оскільки ж асимптотичні розподіли всіх $(+,\oplus)$-диференціалів $(\beta, \alpha)$ при $\mathrm{ord}\beta \neq 2$ однакові, то вони будуть однаковими й для всіх $(\oplus,+)$-диференціалів $(\alpha, \beta)$.

## IV. Довірчі інтервали для імовірностей змішаних диференціалів

Побудова довірчого інтервалу для імовірностей $(+,\oplus)$-диференціалів (а також для $(\oplus,+)$-диференціалів) відбувається в майже такий само спосіб, як і побудова довірчого інтервалу для $(+,+)$-диференціалів, описаного у [5].

Позначимо $DP(\pi) = max_{\alpha,\beta\neq 0} DP^{\pi}_{+,\oplus}(\alpha,\beta)$. Знайдемо обмеження для $DP(\pi)$ з асимптотичною ймовірністю 1. Визначимо величину

$$\theta_t(\pi) = \frac{1}{(2^n - 1)^2}\sum_{\alpha\neq 0}\sum_{\beta\neq 0} I\left(2^n \cdot DP(\alpha,\beta) = t\right),$$

що є часткою вхідних/вихідних різниць, які справедливі рівно для $t$ пар входів (виходів), $0 \le t \le 2^n$. Маємо, що $M\theta_t(\pi) \sim e^{-1}/t!$

Покладемо $\Omega^{(t)} = (2^n - 1)^2\theta_t(\pi)$, а також $\Omega = \Omega^{(2B_n)}$, де

$$B_n = \frac{\ln N^2}{\ln\ln N^2},\ N = 2^n - 1$$

Тоді $M\Omega = (2^n - 1)^2 M\theta_{2B_n}(\pi) \sim N^2 e^{-1}/(2B_n)!$

Використаємо формулу Стірлінга для асимптотичної оцінки факторіалу:

$$(2B_n)! \sim \left(\frac{2B_n}{e}\right)^{2B_n} \cdot \sqrt{2\pi \cdot 2B_n} =$$
$$= \frac{(\ln N^2)^{2\ln N^2/\ln\ln N^2}}{((e/2)\ln\ln N^2)^{2B_n}} 2\sqrt{\pi B_n},$$

де $(\ln N^2)^{2\ln N^2/\ln\ln N^2} = \left(e^{\ln\ln N^2}\right)^{2\ln N^2/\ln\ln N^2} = N^2$

Звідси

$$M\Omega \sim N^2\frac{e^{-1}}{N^4}((e/2)\ln\ln N^2)^{2\ln N^2/\ln\ln N^2}\frac{1}{2\sqrt{\pi B_n}} =$$
$$= \frac{e^{-1}}{2\sqrt{\pi B_n}}\left(\frac{((e/2)\ln\ln N^2)^{2/\ln\ln N^2}}{(N^2)^{1/\ln N^2}}\right)^{\ln N^2} =$$
$$= \frac{e^{-1}}{2\sqrt{\pi B_n}}\left(\frac{((e/2)\ln\ln N^2)^{2/\ln\ln N^2}}{e}\right)^{\ln N^2}.$$

Вираз в дужках позначимо через $y(N)$. Можна показати, що $y(N) \le 1$. Отже,

$$M\Omega \sim \frac{e^{-1}}{2\sqrt{\pi B_n}} y(N)^{\ln N^2} = o(1),$$

при $n \to \infty$. Відповідно, при $2B_n = o(2^{n/2})$ маємо

$$M\Omega^{(t)} = M\Omega/(2B_n)^{t-2B_n}.$$

Таким чином, середня кількість нетривіальних диференціалів, імовірність яких більша або рівна за $2B_n/2^n$, дорівнює

$$\sum_{t \geq B_n} M\Omega^{(t)} \leq \sum_{t \geq B_n} \frac{M\Omega}{(2B_n)^{t-2B_n}} = M\Omega \sum_{i \geq 0} \frac{1}{(2B_n)^i} =$$

$$= \frac{M\Omega}{1 - 1/(2B_n)} \sim M\Omega = o(1)$$

Ймовірність $DP(\pi) \geq B_n/2^{n-1}$ менше за середню кількість диференціалів із імовірністю $t/2^n \geq 2B_n/2^n$. Звідси випливає, що

$$Pr\left\{DP(\pi) \geq \frac{B_n}{2^{n-1}}\right\} = o(1), \text{ ч.т.}$$

Таким чином, величина $DP(\pi)$ для змішаних диференціалів майже напевно лежить у межах від 0 до $2B_n/2^n$.

## V. Перевірка швидкості збіжності

Швидкість збіжності імовірностей диференціалів до їх асимптотичних розподілів була оцінена експериментально для перестановок розміру від 4 до 10 бітів.

В ході експерименту було згенеровано 100 000 випадкових перестановок відповідного розміру, на основі яких обчислено вибіркові розподіли кожного диференціала. Для перевірки збіжності обчислювалось середньоквадратична відстань (СКВ) між вибірковим розподілом та розподілом Пуассона із параметром 1. Для оцінки швидкості розглядались максимальне та середнє по всіх диференціалах значення середньоквадратичної відстані. Результати обчислень наведені на рис 1,2.

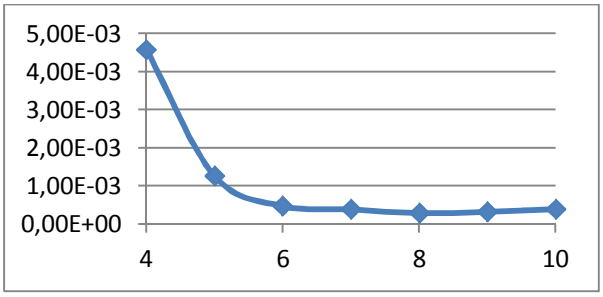


Рис. 1. Максимальне значення СВК імовірностей по всіх диференціалах

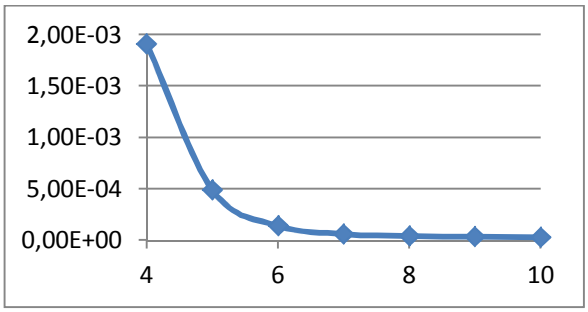


Рис. 2. Середнє значення СВК імовірностей по всіх диференціалах

## VI. Висновки

У даній роботі було розглянуто асимптотичні розподіли імовірностей диференціалів найпоширенішого змішаного типу, в яких різниці обчислюються за операцією модульного додавання на вході та операцією побітового додавання на виході або навпаки. Було встановлено, що ймовірності диференціалів такого типу асимптотично підкорюються розподілу Пуассона з параметром 1, окрім класу диференціалів із вхідною різницею $\alpha = 2^{n-1}$, для яких відповідний параметр розподілу Пуассона становить ½. Також було знайдено довірчій інтервал для диференціалів змішаного типу і показано, що майже завжди значення імовірностей таких диференціалів не дуже великі. Одержані аналітичні твердження були перевірені експериментально; результати експериментів показали, що вже для 6-бітових S-блоків середньоквадратичне відхилення розподілів від асимптотичних не перевищує $10^{-4}$.

Одержані результати можуть бути використані для побудови адекватних моделей та оцінювання стійкості до диференціального криптоаналізу немарковських блокових шифрів із різними алгебраїчними операціями у раундових перетвореннях та ключову суматорі.

## Література References


[1] K. Nyberg, Provable Security Against a Differential Attack / K. Nyberg, L.R. Knudsen // Journal of Cryptology. – Vol.8. – No.1. – 1995.

[2] C. Adams, Designing S-boxes resistant to differential cryptanalysis [електронний ресурс] / C. Adams, St. Tavares. – Режим доступу :

[14] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.2536

[3] S. Park, On the security of Rijndael-like structures against differential and linear cryptanalysis / S. Park, S.H. Sung, S. Chee, E.-J. Yoon, J. Lim // Advances in Cryptology, ASIACRYPT 2002. – LNCS, vol. 2501. – Berlin: Springer, 2002. – pp. 176-191.

[4] S. Park, Improving the upper bound on the maximum differential and the maximum linear hull probability for the SPN structures and AES / S. Park, J. Sung, S. Lee, J. Lim // Fast Software Encryption. – FSE'03, Proceedings. – Springer Verlag, 2003. – P. 247 – 260.

[5] P. M. Hawkes and L. J. O'Connor, "XOR and NON-XOR Differential Probabilities" in Lecture Notes in Computer Science, May 1999, 10.1007/3-540-48910-X_19

[6] J.L. Massey, Nomination of SAFER++ as candidate algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE). / J.L. Massey, G.H. Khachatrian, M.K. Kuregian. – Primitive submitted to NESSIE by Cylink Corp. – 2000.