

Імовірності Диференціалів Шифруючих Перетворень із Частковим Забілюванням Ключами

Володимир Полулях, Сергій Яковлев
кафедра математичних методів захисту інформації
Фізико-технічний інститут
НТУУ “Київський політехнічний інститут ім. Ігоря Сікорського”
Київ, Україна
manutdvova@gmail.com, yasv@rl.kiev.ua

The Differential Probabilities of the Encryption Mappings with Partial Key Whitening

Volodymyr Poluliakh, 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
manutdvova@gmail.com, yasv@rl.kiev.ua

Анотація—Розробники легкого шифру GIFT запропонували використовувати часткове забілювання даних із раундовими ключами. У даній роботі розглядається вплив такої модифікації на стійкість шифруючих перетворень до диференціального криптоаналізу.

Abstract—Developers of GIFT lightweight cipher proposed to use a partial key whitening of input data within encryption process. We study the effect of such modification on the security of encryption mappings against differential cryptanalysis.

Ключові слова—блокові шифри; S-блоки; диференціальний криптоаналіз.

Keywords—block ciphers; S-boxes; differential cryptanalysis.

I. ВСТУП

Диференціальний криптоаналіз [1] є одним з найпотужніших методів аналізу симетричних блокових шифрів. Сучасні методи аналітичного доведення стійкості алгоритмів шифрування до диференціального криптоаналізу оцінюють складність проведення атаки через значення певних обчислювальних параметрів раундових перетворень та їх окремих компонент, таких як S-блоки та лінійні перетворення. Зазвичай для підвищення стійкості до даного методу аналізу у блокових шифрах обираються біективні S-блоки (тобто підстановки на

бітових векторах) із мінімально можливими імовірностями диференціалів.

Надзвичайне поширення обчислювальних пристроїв та гаджетів (зокрема, у межах розвитку «Інтернету речей») призвело до бурхливого розвитку так званої «легкої» криптографії – окремого напрямку криптології, яких розглядає питання аналізу та синтезу криптографічних перетворень, оптимізованих під виконання на малопотужних обчислювальних архітектурах. Задля економії обчислень мінімізується кількість вентилів у схемах реалізації нелінійних перетворень; зменшується кількість та розміри S-блоків; суттєво спрощуються лінійні перетворення. Розробники блокового шифру GIFT [2] пропонують на кожному раунді забілювати з ключем тільки половину кожного входу на S-блок, що призводить до суттєвої економії ключового матеріалу та прискорення обчислень.

Однак використання часткового забілювання із раундовими ключами може помітно змінити значення криптографічних параметрів структурних елементів шифру та, відповідно, його оцінок стійкості до відомих методів криптоаналізу. Це питання не досліджувалось у опублікованих джерелах. У даній роботі ми проведемо аналіз поведінки криптографічних параметрів ключезалежних S-блоків (зокрема, розподілів імовірностей

диференціалів та їх максимумів) при накладанні певних обмежень на ключовий простір.

II. НЕОБХІДНІ ТЕРМІНИ ТА ПОЗНАЧЕННЯ

Нехай V_n – простір n -бітових векторів, і бінарні операції \otimes та \circ визначають на V_n структуру абелевих груп $\langle V_n, \otimes \rangle$ та $\langle V_n, \circ \rangle$. Для зручності будемо вважати нульовий вектор нейтральним елементом в обох зазначених групах. В якості \otimes та \circ 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.

Тоді (\circ, \otimes) -диференціалом або змішаним диференціалом функції f називається довільна пара бітових векторів $(\alpha, \beta) \in V_n^2$, для якої існує подія $\alpha \rightarrow_f \beta$ (α переходить у β під дією функції f), що для випадкового значення x – входу функції f виконується рівність $f(x \circ \alpha) = f(x) \otimes \beta$. Іншими словами, β є різницею між виходами функції, якщо на вхід подати два значення із різницею α .

Імовірністю диференціала $DP^f_{\circ\otimes}(\alpha, \beta)$ відносно операцій \otimes та \circ називається усереднена за усіма можливими значеннями x сума

$$DP^f_{\circ\otimes}(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [f(x \circ \alpha) = f(x) \otimes \beta].$$

Тут і далі ми використовуємо символ [...] (так звані дужки Айверсона) як позначення індикатора події, записаної в дужках: 1, якщо подія істинна, та 0, якщо хибна.

Максимумом диференціальної імовірності функції f є величина $MDP_{\circ\otimes}(f) = \max_{\alpha \neq 0, \beta} DP^f_{\circ\otimes}(\alpha, \beta)$.

Шифруючим перетворенням f_k з ключем k називається відображення $f_k : V_n \times K \rightarrow V_n$, K – простір ключів. При фіксованому ключі k шифруючому перетворенню відповідає деяка булева функція. Отже для нього справедливим є означення імовірності диференціалу

$$DP^f_{\circ\otimes}[k](\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [f_k(x \circ \alpha) = f_k(x) \otimes \beta].$$

Для того, щоб провести атаку, нам потрібно знайти імовірності диференціалів та обрати диференціали з високою імовірністю. Але, оскільки ці імовірності залежать від ключа, потрібно знати ключ, щоб знайти диференціали з високою імовірністю, аби побудувати атаку, що знаходить цей ключ. Щоб розірвати дану логічну петлю, ми користуємося гіпотезою про стохастичну еквівалентність ключів – вважаємо, що розподіли при різних значеннях ключа приблизно однакові. Тому для оцінки складності проведення диференціальної атаки будемо використовувати середню імовірність диференціалу

$$EDP^f_{\circ\otimes}(\alpha, \beta) = \frac{1}{2^{2n}} \sum_{x \in V_n} \sum_{k \in K} [f(x \otimes \beta) = f(x) \otimes \beta],$$

у якості основного параметру. Відповідно, гарантована складність проведення атаки визначається максимумом середньої імовірності диференціалу

$$MEDP_{\circ\otimes}(f_k) = \max_{\alpha \neq 0, \beta} EDP^f_{\circ\otimes}(\alpha, \beta),$$

і саме цей параметр є основною чисельною характеристикою, що визначає стійкість шифру до диференціального криптоаналізу, оскільки мінімальна складність атаки буде обернено пропорційна до неї.

Для побудови оцінок значення $MEDP$ зручно виявилось поняття середньою за ключами імовірності диференціалу у точці x , запропоноване Л.В.Ковальчук [3]:

$$DP^f_{\circ\otimes}(x, \alpha, \beta) = \frac{1}{2^n} \sum_{k \in K} [f_k(x \circ \alpha) = f_k(x) \otimes \beta].$$

Максимум середньої за ключами імовірності диференціалу у точці x – це величина

$$MDP_{\circ\otimes}(f_k) = \max_{\alpha \neq 0, \beta, x} DP^f_{\circ\otimes}(x, \alpha, \beta).$$

Через очевидне співвідношення $MDP \geq MEDP$ можна використовувати верхні оцінки для MDP (які зазвичай простіше обчислювати) для оцінювання гарантованої складності проведення диференціального криптоаналізу.

У 1993 р. С. Лай, Дж. Мессі та Ш. Мерфі розробили першу формальну теорію стійкості до диференціального криптоаналізу яка ґрунтувалася на концепції марковського шифру [4]. Шифруюче перетворення f_k називається марковським відносно операцій \circ, \otimes , якщо

$$\begin{aligned} \forall x \forall \alpha \forall \beta : DP^f_{\circ\otimes}(x, \alpha, \beta) &= DP^f_{\circ\otimes}(0, \alpha, \beta) \\ \Rightarrow DP^f_{\circ\otimes}(x, \alpha, \beta) &= EDP^f_{\circ\otimes}(\alpha, \beta). \end{aligned}$$

Таким чином, для марковських перетворень значення імовірностей диференціалів у довільній точці рівні між собою; відповідно, імовірності диференціалів раундових перетворень марковських блокових шифрів не залежать від того, що відбулось на попередніх раундах.

Сформулюємо декілька властивостей шифруючих перетворень спеціального виду [3-4].

Лема 1. Нехай $f_k(x) = S(x \circ k)$, де $S : V_n \rightarrow V_n$ – S-блок. Тоді f_k – марковське відносно \circ, \otimes та

$$\forall x : DP^f_{\circ\otimes}(x, \alpha, \beta) = DP^S_{\circ\otimes}(\alpha, \beta).$$

Лема 2. Нехай $f_k(x) = S(x \otimes k)$. Тоді f_k – не марковське відносно \circ, \otimes , але

$$\begin{aligned} \forall x : DP^f_{\circ\otimes}(x, \alpha, \beta) &= DP^S_{\circ\otimes}(\alpha'_x, \beta), \\ \text{де } \alpha'_x &= (x \circ \alpha) \otimes x^{-1}. \end{aligned}$$

III. АНАЛІТИЧНА ОЦІНКА ЗМІН СЕРЕДНІХ ЗА КЛЮЧАМИ ЙМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛІВ З ОБМЕЖЕННЯМИ НА КЛЮЧОВИЙ ПРОСТІР

Розглянемо (\otimes, \otimes) -диференціал параметризованої функції f_k . Введемо обмеження на ключовий простір: будемо вважати, що ключі обираються з деякої множини $K \subset K'$. Потрібно з'ясувати як зміняться значення математичного очікування імовірності диференціалу f_k .

Нехай EDP' – середня за ключами імовірність (\otimes, \otimes) -диференціалу перетворення зі зменшеним ключовим простором.

Лема 3. Нехай $f_k(x) = S(x \otimes k)$, $x \in V_n$, $k \in K'$, $K' \subset V_n$. Тоді

$$EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta) = DP^S_{\otimes\otimes}(\alpha, \beta).$$

Доведення: за визначенням маємо

$$\begin{aligned} EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta) &= \\ &= \frac{1}{2^n} \sum_{x \in V_n} \frac{1}{|K'|} \sum_{k \in K'} [f_k(x \otimes \alpha) = f_k(x) \otimes \beta] = \\ &= \frac{1}{2^n} \sum_{x \in V_n} \frac{1}{|K'|} \sum_{k \in K'} [S(x \otimes \alpha \otimes k) = S(x \otimes k) \otimes \beta] \end{aligned}$$

Оскільки операція \otimes утворює абелеву групу та k пробігає всі можливі значення, то й $x \otimes k$ також пробігає всі можливі значення. Отже можемо зробити заміну $x \otimes k = u$ Звідси:

$$\begin{aligned} &\frac{1}{2^n} \sum_{x \in V_n} \frac{1}{|K'|} \sum_{k \in K'} [S(x \otimes \alpha \otimes k) = S(x \otimes k) \otimes \beta] = \\ &= \frac{1}{2^n} \sum_{x \in V_n} \frac{1}{|K'|} \sum_{k \in K'} [S(u \otimes \alpha) = S(u) \otimes \beta] = \\ &= \frac{1}{|K'|} \sum_{k \in K'} \frac{1}{2^n} \sum_{u \in V_n} [S(u \otimes \alpha) = S(u) \otimes \beta] = \\ &\frac{1}{|K'|} \sum_{k \in K'} DP^S_{\otimes\otimes}(\alpha, \beta) = DP^S_{\otimes\otimes}(\alpha, \beta), \end{aligned}$$

за означенням.

Отже, навіть з обмеженнями на ключовий простір шифр зберігає деякі властивості маркових шифруючих перетворень. Однак, як буде показано далі, значення імовірностей диференціалів у точках в загальному випадку не зберігається – тобто, при обмеженнях на ключовий простір шифри можуть втратити властивість марковості. Для шифрів, які є немарковськими, в окремих випадках (для деяких диференціалів) значення середньої імовірності може зберегтись – однак більш ніж для половини диференціалів імовірності змінюються.

IV. АНАЛІЗ РОЗПОДІЛІВ ЙМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛІВ У ТОЧКАХ ДЛЯ ДЕЯКИХ НЕЛІНІЙНИХ ПЕРЕТВОРЕНЬ

Розглянемо два типи раундових перетворень: $F_k = S(x \oplus k)$, $G_k = S(x + k)$. Слід зазначити, що в роботі

розглядаються тільки $(+, +)$ - та (\oplus, \oplus) -диференціали, але операції в диференціалах та операція забілювання з ключем різні.

Для експериментальних обчислень було обрано 8-бітні бієктивні S-блоки: S-блок американського стандарту шифрування AES [5] та чотири S-блоки національного стандарту шифрування України ДСТУ 7624:2014 (шифр «Калина») [6]. Усі обчислення були проведені у спеціальному обчислювальному середовищі, написаному мовою C++.

Обмеження на ключовий простір накладається шляхом скорочення довжини ключа до 4-х біт. Таким чином потужність $|K| = 2^8$, для обмеженої множини $|K'| = 2^4$. Розподіли середніх за ключами ймовірностей диференціалів із забілюванням ключами довжини 8 бітів порівнюється з розподілами середніх за ключами ймовірностей диференціалів у випадках, коли з ключем замішуються тільки старші або молодші 4 біти (порядок бітів – big-endian).

Ще однією статистичною характеристикою, яка оцінювалася у ході експерименту, було *середньоквадратичне відхилення* середніх імовірностей диференціалів

$$\sigma = \sqrt{\frac{1}{2^8} \sum_{\alpha \neq \beta} (EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta) - EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta))^2},$$

де \otimes – операція $+$ або \oplus .

Для аналізу змін у розподілах додатково розглянемо такі множини, які показують випадки, коли середня імовірність диференціалів збільшилась або зменшилась:

$$\Delta^+ = \{(\alpha, \beta) | EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta) > EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta)\},$$

$$\Delta^- = \{(\alpha, \beta) | EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta) < EDP'^{f_k}_{\otimes\otimes}(\alpha, \beta)\}.$$

Статистичні характеристики розподілів $DP'^{F_k}_{++}$ для перетворень, які побудовані на основі S-блоку шифру AES та матриць підстановок шифру «Калина», наведено у таблиці I. У таблиці II наведено аналогічні статистичні дані про розподіли.

Максимуми $DP'^{F_k}_{++}$ зросли рівно у 8 разів для S-блоку AES та підстановок π_0 та π_1 шифру «Калина»; для підстановок π_2 , π_3 шифру «Калина» збільшення склало 6,86 разів. Майже у всіх випадках збільшилися $MEDP'^{F_k}_{++}$ (окрім забілювання з молодшими бітами AES). Приблизно для половини диференціалів значення EDP' збільшилось, а для інших диференціалів залишилось незмінним.

ТАБЛИЦЯ I. СТАТИСТИЧНІ ПАРАМЕТРИ $DP'^{F_k}_{++}$

Забілені Біти	$MDP'^{F_k}_{++}$	$MEDP'^{F_k}_{++}$	$ \Delta^+ $	σ
AES				
Всі	0.0234375	0.0195312	–	–

Старші	0.1875	0.0214844	28258	0.0021117
Молодші	0.1875	0.0195312	30488	0.001666
π_0				
Всі	0.0234375	0.015625	—	—
Старші	0.1875	0.0214844	28400	0.002079
Молодші	0.1875	0.03125	30154	0.001675
π_1				
Всі	0.0234375	0.0136719	—	—
Старші	0.1875	0.0205078	28324	0.0021032
Молодші	0.1875	0.0195312	30286	0.0016819
π_2				
Всі	0.0273438	0.015625	—	—
Старші	0.1875	0.0239258	28270	0.002112
Молодші	0.1875	0.0273438	30160	0.0016698
π_3				
Всі	0.0234375	0.0234375	—	—
Старші	0.1875	0.0234375	25381	0.0021032
Молодші	0.25	0.0292969	23870	0.0016819

ТАБЛИЦЯ II. СТАТИСТИЧНІ ПАРАМЕТРИ $DP_{\oplus\oplus}^{G_k}$

Забілені Біти	$MDP_{\oplus\oplus}^{G_k}$	$MEDP_{\oplus\oplus}^{G_k}$	$ \Delta^+ $	σ
AES				
Всі	0.0273438	0.0195312	—	—
Старші	0.1875	0.015625	26132	0.002336
Молодші	0.25	0.0205078	24045	0.001842
π_0				
Всі	0.0234375	0.0234375	—	—
Старші	0.25	0.03125	25440	0.0026496
Молодші	0.1875	0.0249023	23905	0.0019236
π_1				
Всі	0.0234375	0.0234375	—	—
Старші	0.1875	0.0234375	25381	0.0021032
Молодші	0.25	0.0292969	23870	0.0016819
π_2				
Всі	0.0273438	0.0234375	—	—
Старші	0.25	0.03125	25439	0.002676
Молодші	0.25	0.0361328	23953	0.0019321
π_3				
Всі	0.0273438	0.0234375	—	—
Старші	0.25	0.0234375	25405	0.0026727
Молодші	0.1875	0.0297852	24082	0.001917

Зауважимо, що множина Δ^- виявилась порожньою: середнє значення імовірностей диференціалів у точках із забілюванням половини бітів виявилось завжди не менше за середнє значення із забілюванням по всій довжині входу. Цікаво, що серед імовірностей, які збереглися, були як нульові, так і ненульові.

Абсолютні значення $MDP_{\oplus\oplus}^{G_k}$ та $MEDP_{\oplus\oplus}^{G_k}$ для усіх S-блоків, які розглядались, більші за відповідні значення $MDP_{++}^{F_k}$ та $MEDP_{++}^{F_k}$; але відносна поведінка при звуженні ключового простору практично така сама: відбувається збільшення значень диференціальних імовірностей більш ніж для половини диференціалів, а також суттєве збільшення максимальних значень.

Відповідно, можна констатувати, що загалом стійкість шифруючих перетворень, які розглядались, до

диференціального криптоаналізу при частковому забілюванні ключами понизилась у порівнянні із повним забілюванням. Таким чином, при використанні даного підходу при синтезі блокових шифрів необхідно після побудови щонайменше проводити окреме незалежне оцінювання стійкості до статистичних методів криптоаналізу.

ВИСНОВКИ

У даній роботі розглянуто новий підхід для побудови алгоритмів шифрування легкої криптографії, в якому запропоновано використовувати часткове забілювання вхідних даних із ключами. Такий підхід дозволяє зменшити витрати на генерування раундових ключів та відповідні вимоги до генераторів випадкових бітів. У роботі проаналізовано стійкість шифруючих перетворень із частковим забілюванням до диференціального криптоаналізу. Показано, що для марковських шифруючих перетворень зменшення ключового простору зберігає значення середніх імовірностей диференціалів, однак може не зберігати імовірності диференціалів у окремих точках. Для немарковських шифруючих перетворень імовірності диференціалів суттєво підвищуються, тобто загальна стійкість до диференціального криптоаналізу падає. Таким чином, при застосуванні даного підходу необхідно проводити окремий додатковий аналіз стійкості до відомих методів криптоаналізу.

Одержані результати можуть бути використані для подальшої модифікації існуючих шифрів та при розробці нових алгоритмів легкої криптографії.

ЛІТЕРАТУРА REFERENCES

- [1] Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems", in: *Journal of Cryptology*. – 1991. – V. 4. – № 1. – P. 3 – 72.
- [2] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo "GIFT: A Small Present" [Online] // LASEC, Switzerland, 2017. – <https://eprint.iacr.org/2017/622.pdf>.
- [3] Ковальчук Л.В. «Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа» // Математика и безопасность информационных технологий. Материалы конференции (25 – 27 октября 2006 г.) – М.: МЦНМО, 2007. – С. 595 – 599.
- [4] Lai X. Markov ciphers and differential cryptanalysis / X. Lai, J.L. Massey, S. Murphy. // *Advances in Cryptology – EUROCRYPT'91, Proceedings*. – Springer Verlag, 1991. – pp. 17-38.
- [5] Advanced Encryption Standard. [електронний ресурс]. – Режим доступу : <http://csrc.nist.gov/archive/aes>
- [6] Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.