

ДИФЕРЕНЦІАЛЬНІ ВЛАСТИВОСТІ ІТЕРАТИВНИХ ПЕРЕТВОРЕНЬ З ОДНАКОВИМИ КЛЮЧАМИ

Б. Ю. Пясецький¹

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

Анотація

У даній роботі досліджується поведінка диференціалів ітеративних двораундових перетворень із однаковими раундовими ключами. Експериментально показано, що такі перетворення втрачають властивість марковості, однак для деяких форм раундової функції вони можуть зберігати окремі властивості модельних шифрів – зокрема, значення середніх імовірностей диференціалів.

Ключові слова: S-блок, диференціальний аналіз, DDT, раундові ключі.

Вступ

У диференціальному та лінійному криптоаналізі сучасних блокових шифрів використовують стандартне модельне припущення, що раундові ключі є випадковими, рівноімовірними та незалежними. Але на практиці ключі не завжди є випадковими і незалежними. Питання, наскільки працює дане модельне припущення у випадках, коли раундові ключі явно не є незалежними, залишається відкритим й досі. Рюмен та Демен [1, 2] дослідили асимптотичні розподіли диференціальних імовірностей та лінійних потенціалів марковських шифрів із зафіксованими ключами та показали, що значення середніх імовірностей будуть параметрами відповідних граничних розподілів для імовірностей диференціалів таких перетворень. Лі та Вань [3] знайшли найкращу диференціальну рівномірність та лінійність для 3-х раундів шифрування схемою Фейстеля із константними ключами, тобто ключами із максимально нерівноімовірними розподілами.

Питання адекватності припущення про незалежність раундових ключів слабо досліджено у відкритих джерелах. У даній роботі буде експериментально показано, як впливають однакові раундові ключі на властивості диференціалів деяких стандартних перетворень.

1. Терміни, означення та основна теорія

Диференціалом булевої функції $f : V_n \rightarrow V_n$, де V_n – простір двійкових векторів довжини n , будемо називати пару двійкових векторів (a, b) , $a, b \in V_n$, для яких існує значення x таке, що виконується співвідношення $f(x \oplus a) \oplus f(x) = b$. Тоді імовірність

диференціалу (a, b) булевої функції f дорівнює

$$DP^f(a, b) = \overline{\sum_x [f(x \oplus a) \oplus f(x) = b]},$$

де $\overline{\sum_x}$ – усереднена сума по всіх x , а $[P]$ – дужки Айверсона: $[P] = 1$, якщо P істинне, та 0, якщо P – хибне.

Введемо додаткове позначення для максимумів імовірностей диференціалів:

$$MDP(f) = \max_{a \neq 0, b} DP^f(a, b).$$

На практиці зручно представляти диференціальні імовірності булевої функції у спеціальній матриці.

Таблиця розподілів диференціалів (англ. *difference distribution table*) – матриця розмірності $2^n \times 2^n$, елементами якої є імовірності DP^f . Така матриця позначається як $DDT^f = ||DP^f(a, b)||$, $a, b \in V_n$.

Для булевої функції, параметризованої ключем $f_k : V_n \times K \rightarrow V_n$, (де K – множина ключів) означення диференціальних імовірностей змінюється. Середньою за ключами імовірністю диференціала (a, b) булевої функції f_k є

$$EDP^{f_k}(a, b) = \overline{\sum_k \sum_x DP[k](a, b)}.$$

Відповідно, максимальна середня імовірність диференціала (a, b) булевої функції f_k дорівнює

$$MEDP(f_k) = \max_{a \neq 0, b} EDP^{f_k}(a, b).$$

Складність проведення диференціальних атак обернено пропорційна до значення $MEDP$; таким чином, для оцінки стійкості блокових шифрів до диференціального аналізу потрібно обчислювати або оцінювати зверху максимальні середні імовірності диференціалів криптографічних перетворень.

Також будемо користуватись означенням середньої за ключами імовірності диференціалу у точці x ,

введене Ковальчук [4]:

$$DP^{f_k}(x, a, b) = \sum_k [f_k(x \oplus a) \oplus f_k(x) = b],$$

та її максимуму

$$MDP(f_k) = \max_{a \neq 0, b, x} DP^{f_k}(x, a, b).$$

Для відображень, параметризованих ключами, елементами матриці DDT^{f_k} покладемо середні імовірності EDP^{f_k} .

Функція $f_k : V_n \times K \rightarrow V_n$ називається *марковським перетворенням* [5, 4], якщо значення середніх за ключами диференціальних імовірностей не залежать від точки входу, тобто

$$\forall x : DP^{f_k}(x, a, b) = DP^{f_k}(0, a, b).$$

Якщо ж дана умова не виконується, то функція f_k є немарковською.

2. Постановка задачі та результати дослідження

Класичним модельним припущенням у криптоаналізі ітеративних блокових шифрів є випадковість, незалежність та рівноімовірність раундових ключів. Однак для більшості сучасних шифрів схеми генерування раундових ключів не гарантують ані випадковість, ані незалежність раундових ключів. Наприклад, в AES [6] наступні раундові ключі є складними перетвореннями від попередніх, а в шифрі «Калина» [7] ключі непарних раундів є простими циклічними зсувами ключів парних раундів.

У даній роботі ми дослідимо, як впливає така залежність на поведінку імовірностей диференціалів ітеративного шифру, на прикладі крайової ситуації, коли раундові ключі повністю співпадають. Для цього проведемо порівняльний аналіз диференціальних властивостей двораундових перетворень $G_k(x) = F_k(F_k(x))$ (з однаковими раундовими ключами) та $H_{k_1, k_2}(x) = F_{k_2}(F_{k_1}(x))$ (із двома незалежними раундовими ключами), а також порівняння властивостей цих перетворень з властивостями одного раунду $F_k(x)$. У якості раундових функцій будемо розглядати типову конструкцію «замішування із ключем + нелінійне перетворення»; три традиційні форми такого раунду позначимо так:

- 1) $F_k^{(1)}(x) = S(x \oplus k)$;
- 2) $F_k^{(2)}(x) = S(x) \oplus k$;
- 3) $F_k^{(3)}(x) = S(x \oplus k) \oplus k$.

Відповідно, верхні індекси у функцій G та H позначатимуть, яку форму раундового перетворення було використано.

У якості нелінійного перетворення S розглядалися восьмибітові S -блоки: S -блок шифру AES, чотири S -блоки шифру «Калина», другий S -блок шифру Aria [8], S -блок шифру «Кузнечик» [9] та S -блок шифру STB [10].

Для імовірностей диференціалів відображень, які розглядаються, мають місце аналітичні співвідношення. Оскільки усі функції $F_k^{(i)}$ та $H_{k_1, k_2}^{(i)}$ є марковськими перетвореннями, то для них виконується:

- $DDT^{F_k^{(i)}} = DDT^S$;
- $DDT^{H_{k_1, k_2}} = DDT^S \times DDT^S$.

Нам цікаво як будуть поводити себе диференціальні імовірності при двох шифруваннях на однакових раундових ключах, в порівнянні з одним шифруванням та двома шифруваннями на незалежних раундових ключах.

Для функцій G_k , H_{k_1, k_2} були розглянуті всі випадки в залежності від функції F_k^i , $i = 1, 3$. Було доведено, що для всіх функцій F_k^i при фіксованому S -блоці матриці DDT^F є ідентичними, звідки випливає, що матриці DDT^H також ідентичні.

Експериментальним чином було встановлено, що функція G_k є немарковським перетворенням. Шляхом безпосередніх обчислень імовірностей диференціалів в різних точках x для функції $F_k^{(1)}$ та другого S -блоку «Калини» було отримано:

$$DP^{G_k}(00000000, 00001101, 00010101) = 1/2^8,$$

$$DP^{G_k}(00000001, 00001101, 00010101) = 2/2^8,$$

що суперечить означенню марковського перетворення. Також обчислення показали, що для функцій $F_k^{(1)}$ та $F_k^{(2)}$ таблиці середніх імовірностей DDT^G та DDT^H є ідентичними.

Для усіх зазначених функцій та S -блоків було знайдено такі величини:

- $MEDP$ для усіх функцій;
- $\# \uparrow$ – кількість диференціалів (a, b) , імовірність яких збільшилась;
- $\# \downarrow$ – кількість диференціалів (a, b) , імовірність яких зменшилась;
- $\# =$ – кількість диференціалів (a, b) , імовірність яких залишилась незмінною;
- $\max \uparrow$ – максимальне збільшення імовірності диференціалу;
- $\max \downarrow$ – максимальне зменшення імовірності диференціалу.

У таблиці 1 показано, як змінюється максимальна середня імовірність диференціалу. У таблицях 2, 3, 4 представлені відмінності між DDT^G , DDT^F та DDT^H .

Табл. 1. Значення величини $2^8 \cdot MEDP$ для функцій $F_k^{(i)}$ та $G_k^{(i)}$, $i = 1, 3$

S -блок	$F_k^{(i)}$	$G_k^{(1)}, G_k^{(2)}$	$G_k^{(3)}$	$H_{k_1, k_2}^{(i)}$
AES	4	1,297	18	1,297
Калина 1	8	1,453	10	1,453
Калина 2	8	1,406	12	1,406
Калина 3	8	1,422	12	1,422
Калина 4	8	1,422	10	1,422
Кузнечик	8	1,562	12	1,562
STB	8	1,547	10	1,547
Aria	4	1,281	10	1,281

З проведених експериментальних обчислень випливає, що середні за ключами імовірності диференціалів відображень G та H співпадають для раундових функцій типу (1) та (2), в той час як для функції типу (3) таблиці DDT функцій G та H відрізняється суттєво. З іншого боку, двораундове відображення G

Табл. 2. Зміни в $DDT^{G_k^{(i)}}$ відносно $DDT^{F_k^{(i)}}$, $i = 1, 2$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,281	-3,156	32640	32385
Калина 1	1,391	-7,062	36345	28680
Калина 2	1,359	-7,062	36070	28955
Калина 3	1,391	-7,125	36179	28846
Калина 4	1,359	-7,219	36177	28848
Кузнечік	1,562	-7,203	37725	27300
STB	1,453	-7,359	36980	28045
Aria	1,281	-3,156	32640	32385

Табл. 3. Зміни в $DDT^{G_k^{(3)}}$ відносно $DDT^{F_k^{(3)}}$

S-блок	max $\uparrow \cdot 2^8$	# =	# $\uparrow$	# $\downarrow$
AES	16	29516	15828	19681
Калина 1	10	29694	16763	18568
Калина 2	12	29637	16687	18701
Калина 3	12	29857	16511	18657
Калина 4	10	30091	16527	18407
Кузнечік	10	30083	16999	17943
STB	10	29866	16863	18296
Aria	10	29605	15856	19564

також за властивостями відрізняється й від одного раунду F : як видно з таблиці 2, для S -блоків AES та Aria кількості елементів DDT^G , які збільшились та зменшились, приблизно однакові, в той час, коли для всіх інших S -блоків кількість елементів, які зросли, більша приблизно на 7 тисяч. Таблиця 3 показує нам, що $DDT^{F_k^{(3)}}$ незначно відрізняється від $DDT^{G_k^{(3)}}$, так як майже половина елементів таблиці залишилась незмінною, а інша частина майже порівну розділилась між елементами, які зросли та зменшились, коли сама зміна в елементах не є занадто значною.

У підсумку можемо стверджувати, що ітеративне перетворення з однаковими раундовими ключами втрачає властивість марковості, а тому до нього не може бути застосовна існуюча формальна теорія диференціального криптоаналізу. Однак для деяких форм раундових функцій перетворення з однаковими ключами може зберігати окремі властивості перетворень з незалежними ключами, зокрема, значення середніх імовірностей диференціалів.

Висновки

У даній роботі досліджувалась поведінка диференціалів ітеративних двораундових перетворень із однаковими раундовими ключами для перевірки стандартного модельного припущення у криптоаналізі блокових шифрів про незалежність раундових ключів. Експериментально показано, що такі перетворення втрачають властивість марковості, однак для деяких форм раундової функції вони можуть зберігати окремі властивості модельних шифрів – зокрема, значення середніх імовірностей диференціалів.

Криптографічні властивості ітеративних перетворень із однаковими або, у більш загальному випадку, залежними раундовими ключами вимагають подальших аналітичних та експериментальних досліджень.

Табл. 4. Зміни в $DDT^{H_{k_1,k_2}^{(3)}}$ відносно $DDT^{G_k^{(3)}}$

S-блок	max $\uparrow \cdot 2^8$	max $\downarrow \cdot 2^8$	# $\uparrow$	# $\downarrow$
AES	1,297	-16,969	39317	25708
Калина 1	1,453	-9,109	39225	25800
Калина 2	1,375	-11	39302	25722
Калина 3	1,422	-11	39489	25536
Калина 4	1,422	-9,156	39276	25749
Кузнечік	1,562	-10,053	39223	25802
STB	1,547	-9,219	39301	25724
Aria	1,281	-9,141	39159	25866

Перелік використаних джерел

1. Daemen Joan, Rijmen Vincent. Probability distributions of correlation and differentials in block ciphers // Journal of Mathematical Cryptology. — 2007. — Vol. 1, no. 3. — P. 221 – 242.
2. Daemen Joan, Rijmen Vincent. Statistics of Correlation and Differentials in Block Ciphers. — 2008. — Access mode: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.4898>.
3. Li Y., Wang M. Constructing S-boxes for Lightweight Cryptography with Feistel Structure // Cryptographic Hardware and Embedded Systems – CHES 2014 / Ed. by Lejla Batina, Matthew Robshaw. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — P. 127–146.
4. Ковальчук Л. В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25 – 27 октября 2006 г. — 2007. — С. 595–599.
5. Lai Xuejia, Massey James L., Murphy Sean. Markov Ciphers and Differential Cryptanalysis // Advances in Cryptology — EUROCRYPT '91 / Ed. by Donald W. Davies. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1991. — P. 17–38.
6. FIPS PUB 197 : Advanced Encryption Standard. — 2001.
7. Oliynykov Roman, Gorbenko Ivan, Kazymyrov Oleksandr et al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. — Cryptology ePrint Archive, Report 2015/650. — 2015. — <https://eprint.iacr.org/2015/650>.
8. New Block Cipher: ARIA / Daesung Kwon, Jaesung Kim, Sangwoo Park et al. // Information Security and Cryptology - ICISC 2003 / Ed. by Jong-In Lim, Dong-Hoon Lee. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2004. — P. 432–445.
9. Информационная технология. Криптографическая защита информации. Блочные шифры : ГОСТ 34.12-2018. — 2018.
10. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности : СТБ 34.101.31-2011. — 2011.