УДК 003.26:519.21

ПАРАМЕТРИ, ЯКІ ХАРАКТЕРИЗУЮТЬ СТІЙКІСТЬ S-БЛОКІВ ДО АНАЛІЗУ УСІЧЕНИХ ДИФЕРЕНЦІАЛІВ

О. П. Якимчук[1, a], С. В. Яковлєв[1]

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

Анотація

У даній роботі представлено формалізацію підходу до криптоаналізу на основі усічених диференціалів за схемою, аналогічною до класичного диференціального криптоаналізу. Було запропоновано параметр стійкості та його уточнення. Представлено результати практичної перевірки параметру, які показали його не інформативність у загальному випадку, але уточнений параметр показав кращі результати під час практичної перевірки, тому його можна рекомендувати для оцінки імовірності усіченого диференціалу. Також наведено деякі характеристики та властивості уточненого параметру.

Ключові слова: диференціальний криптоаналіз, усічені диференціали, імовірність диференціалу

Вступ

Вперше криптоаналіз на основі усічених диференціалів був запропонований Ларсом Кнудсеном 1994 року [1]. Якщо звичайний диференціальний криптоаналіз досліджує повну різницю між двома текстами, то аналіз, що використовує усічені диференціали, враховує відмінності між текстами, які визначаються лише частково. На сьогодні існує декілька прикладів успішного застосування диференціальних атак на основі усічених диференціалів до існуючих шифрів або їх модифікацій: атака на перші 6 раундів шифру `DES` [1], атака на 5 раундів шифру `Salsa20` [2], атака на шифр `KLEIN` [3] та ін.

Не зважаючи на успішні випадки практичного застосування цього методу, на сьогодні не існує формальної теорії, яка описує криптоаналіз на основі усічених диференціалів. У даній роботі наводиться формалізація цього методу та практична оцінка адекватності формалізації.

1. Необхідні терміни та означення

Позначимо $V_n = \{0,1\}^n$ – простір усіх бітових векторів довжини n. Такі вектори також можна називати текстами. Потужність множини V_n:

$$|V_n| = 2^n.$$

Диференціал функції f – пара довільних двійкових векторів (α, β). Для диференціалу (α, β) позначимо символом $\alpha \underset{f}{\to} \beta$ (або просто $\alpha \to \beta$, якщо функція зрозуміла з контексту) подію $f(z \oplus \alpha) = f(z) \oplus \beta$, що індукується випадковою величиною $z \in_R V_n$.

В цій роботі розглядається одна операція додавання за модулем 2 (`XOR`, $\oplus$); проте в загальному випадку можна розглядати дві окремих операції, кожна з яких визначає структуру абелевої групи з нейтральним елементом на V_n, для вхідних та вихідних різниць.

Роль функції f виконує S-блок. *S-блок* – це бієктивне перетворення вигляду $f : V_n \to V_n$. Традиційно S-блоки задаються таблицями підстановки.

Для кожного диференціалу певної функції (перетворення) є параметр, який характеризує ефективність цього диференціалу – імовірність диференціалу.

Імовірність диференціалу (α, β) перетворення S – величина:

$$DP^S(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [S(x \oplus \alpha) = S(x) \oplus \beta],$$

де $[P]$ - дужки Айверсона:

$$[P] = \begin{cases} 1, \text{якщо твердження } P \text{ – істинне;} \\ 0, \text{якщо твердження } P \text{ – хибне.} \end{cases}$$

У багатьох випадках зручно розглядати множину

$$D^S(\alpha, \beta) = \{x \in V_n : S(x \oplus \alpha) = S(x) \oplus \beta\}.$$

Тоді можна сказати, що $DP^S(\alpha, \beta) = \frac{1}{2^n} |D^S(\alpha, \beta)|$.

Розглянемо два вектори $\alpha, \beta \in V_n$ як маски вхідних та вихідних різниць; пара (α, β) називається *усіченим диференціалом*. Усічені диференціали застосовуються для передбачення декількох нульових бітів вихідної різниці, що потенційно дозволяє будувати більш точні та потужні розпізнавачі для блокових шифрів. Принцип роботи цих масок наступний: якщо в масці на деякій позиції стоїть 0, то і в різниці на цій самій позиції повинен бути 0; якщо в масці на деякій позиції стоїть 1, то в різниці на цій самій позиції може бути або 0, або 1. Таким чином, кожній масці у відповідність можна представити множину різниць, які можливі при цій масці. Визначимо цю

[a] oleksii.yakymchuk@gmail.com

множину таким чином:

$$\Delta(\alpha) = \{\alpha' \in V_n \setminus \{0\} : \alpha' \vee \alpha = \alpha\}.$$

2. Параметр стійкості на основі безпосереднього означення

Безпосередньо з ідей усіченого диференціального криптоаналізу випливає, що для аналізу усічених диференціалів треба розглядати подію, що пара входів, різниця яких задовольняє заданій масці α, переходить у пару виходів, різниця яких відповідає заданій масці β. Відповідно, визначимо імовірність цієї події таким чином:

$$TDP^S(\alpha,\beta) = \frac{1}{2^n}\sum_{x\in V_n}[\exists\alpha' \in \Delta(\alpha), \exists\beta' \in \Delta(\beta) : S(x\oplus\alpha') = S(x)\oplus\beta'].$$

Дану імовірність, за аналогією до класичної імовірності диференціалу, можна представити через таку множину двійкових векторів у чисельнику:

$$TD^S(\alpha,\beta) = \{x \in V_n | \exists\alpha' \in \Delta(\alpha), \exists\beta' \in \Delta(\beta) : S(x\oplus\alpha') = S(x)\oplus\beta'\}.$$

Таким чином, отримуємо альтернативну формулу для обчислення імовірності усіченого диференціалу:

$$TDP^S(\alpha,\beta) = 2^{-n}|TD^S(\alpha,\beta)|.$$

Для перевірки цього параметру спробуємо обрахувати його для 4-бітових S-блоків, запропонованих у роботі [4]. Розрахунки показують, що цей параметр не адекватно характеризує імовірність усіченого диференціалу та, відповідно, не може бути застосований для криптоаналізу.

Для ілюстації розглянемо такий приклад. Візьмемо S-блок

$$(7, 9, 4, D, 0, 2, C, B, A, 8, 1, 6, E, 5, F, 3),$$

тут значення наведено в шістнадцятковій системі числення. Для цього S-блоку обраховано значення потужностей множини TD^S для усіх можливих усічених диференціалів. Для маски вхідної різниці $\alpha = 7 = 0111_2$ ми отримали результати, представлені в таблиці 1. У таблиці значення маски β представлено в шістнадцятковій системі числення, проте надалі ми будемо використовувати двійкову.

В таблиці наведено потужність множини $TD^S(\alpha,\beta)$ для кожного значення β; імовірністю буде число з таблиці поділене на $2^4 = 16$. Як можемо бачити, в таблиці є декілька варіантів β, при яких $TDP^S(0111_2,\beta) = 1$, наприклад, $\beta = A_{16} = 1010_2$ та $\beta = D_{16} = 1101_2$. Таким чином, маємо подію, що два тексти з маскою різниці 0111 на вході, після застосування до них S-блоку, дають різницю з маскою 1010 на виході з імовірністю 1, тобто завжди. Така ж ситуація і з вихідною маскою різниці 1101. Тобто можна стверджувати, що два тексти з маскою різниці 0111 на вході, після застосування до них S-блоку, одночасно дають різницю з масками 1010 та 1101. Виходячи з наших позначень, це можливо і породжує наступну подію: два тексти з маскою різниці 0111 на вході, після застосування до них S-блоку, завжди дають різницю з маскою 1000 (ми порівняли побітово дві вихідні маски, і на місцях, де біти різні записали 0). Але це суперечить результатам наших розрахунків, оскільки з таблиці 1 ми можемо обрахувати імовірність усіченого диференціалу $(0111, 1000)$ і вона дорівнює $\frac{1}{4}$.

Отже, ми не можемо використовувати такий параметр для побудови розпізнавача шифруючого перетворення від випадкової функції.

3. Уточнений параметр стійкості для аналізу усічених диференціалів

Розвинемо нашу ідею для внесення адекватності в наш параметр оцінки імовірності усіченого диференціалу, переформулюючи його.

Введемо нове означення для імовірності усіченого диференціалу таким чином:

$$TDP^S(\alpha,\beta) = \frac{1}{2^n}\sum_{x\in V_n}[\forall\alpha' \in \Delta(\alpha), \exists\beta' \in \Delta(\beta) : S(x\oplus\alpha') = S(x)\oplus\beta'].$$

Тут квантор $\exists$ біля різниці α' замінено на квантор $\forall$, щоб для будь-якої вхідної різниці з множини $\Delta(\alpha)$ можна було гарантувати нулі на певних позиціях у вихідній масці з деякою імовірністю.

Тепер ми можемо змінити і означення множини TD:

$$TD^S(\alpha,\beta) = \{x \in V_n | \forall\alpha' \in \Delta(\alpha), \exists\beta' \in \Delta(\beta) : S(x\oplus\alpha') = S(x)\oplus\beta'\}.$$

Визначення імовірності усіченого диференціалу через потужність множини TD залишається незмінним.

Цей підхід показав кращі результати; розглянемо їх детальніше на конкретному прикладі. Для перевірки візьмемо 8-бітовий S-блок π_0 зі специфікації шифру `Калина` [5]. Побудуємо таблицю, де для усіх можливих пар масок (α,β), $\alpha,\beta \in V_8$, буде обраховано:

- $DP^S(\alpha,\beta)$,
- $\max_{\alpha'\in\Delta(\alpha),\beta'\in\Delta(\beta)} DP^S(\alpha',\beta')$,
- $TDP^S(\alpha,\beta)$,
- $TD^S(\alpha,\beta)$.

Перше, що видно з результатів – це те, що для $\alpha = 0$ результати усіх $TDP^S(0,\beta) = 0$, окрім $\beta = 0$ та $\beta = 11111111_2$, що є очікувано, оскільки нульова різниця вхідних текстів може породити лише нульову різницю вихідних текстів, яка включається в маску 11111111_2. Наступною тривіальною властивістю є те, що для будь-якого α при $\beta = 11111111_2$ імовірність усіченого диференціалу (α,β) дорівнює одиниці, що також є очікувано, оскільки будь-яка різниця вхідних текстів може породити будь-яку різницю вихідних текстів.

Якщо розглянути окремо α такі, що $|\Delta(\alpha)| = 1$, то «новий» підхід ніяк не відрізняється від підходу, описаного в попередньому розділі, оскільки в цьому випадку квантор $\forall$ не надає ніяких додаткових обмежень. В такому випадку множина $TD^S(\alpha,\beta)$ буде

Табл. 1. Результати обчислення потужності множини TD^S для усічених диференціалів виду $(7, \beta)$ для обраного S-блоку

β	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\lvert TD^S(\alpha,\beta)\rvert$	0	4	8	16	8	14	12	16	4	14	16	16	14	16	16	16

Табл. 2. Частина результатів розрахунку параметрів для S-блоку π_0 зі специфікації шифру `Калина`

(α,β)	$\lvert D^S(\alpha,\beta)\rvert$	$\lvert TD^S(\alpha,\beta)\rvert$	$TD^S(\alpha,\beta)$
$(00000011_2, 00011111_2)$	2	4	$[70_{16}, 71_{16}, 72_{16}, 73_{16}]$
$(00000011_2, 00111111_2)$	2	8	$[04_{16}, 05_{16}, 06_{16}, 07_{16}, 70_{16}, 71_{16}, 72_{16}, 73_{16}]$

складатися з усіх векторів, які, маючи різницю α на вході, породжують хоча б одну з різниць з множини $\Delta(\beta)$. Слід зауважити, що усі α для яких $|\Delta(\alpha)| = 1$, характеризуються тим, що у них вага – 1. Для таких випадків $TDP^S(\alpha,\beta) \in [\frac{2}{2^8}, \frac{148}{2^8}]$ для S-блоку, який розглядається.

У більшості інших випадків, не описаних вище, $TDP^S(\alpha,\beta) = 0$, проте розглянемо випадки, коли це не так. Для цих випадків, коли імовірність усіченого диференціалу не дорівнює нулю, характерною ознакою є вага маски α, яка рівна або 2, або 3, та має місце правило «домінуючої» β. Розглянемо дію цього правила на одному з таких усічених диференціалів. Як ми бачимо з результатів в таблиці 2 для маски β, в якої зафіксовано три нульових елементи, ми отримуємо множину можливих відкритих текстів потужності 4, яка складається з таких елементів: 70_{16}, 71_{16}, 72_{16}, 73_{16}. Для β з двома фіксованими нульовими елементами на місцях, що співпадають з нульовими елементами попередньої β, множина $TD^S(\alpha,\beta)$ містить вісім елементів, чотири з яких співпадають з елементами множини відкритих текстів для $\beta = 00011111_2$. Враховуючи наші позначення, ми можемо стверджувати, що маска 00111111_2 «домінує» над маскою 00011111_2 (включає в себе цю маску). Це і отримано в результатах, оскільки

$$TDP^S(03_{16}, 3F_{16}) = \frac{8}{2^8} > TDP^S(03_{16}, 1F_{16}) = \frac{4}{2^8},$$

та $TD^S(03_{16}, 1F_{16}) \subset TD^S(03_{16}, 3F_{16})$.

Також слід зауважити, що в будь-якому випадку, коли $TDP^S(\alpha,\beta) > 0$, то $TDP^S(\alpha,\beta) > DP^S(\alpha,\beta)$. Нажаль, порівняння $TDP^S(\alpha,\beta)$ з величиною $\max_{\alpha'\in\Delta(\alpha),\beta'\in\Delta(\beta)} DP^S(\alpha',\beta')$ зробити не можна, оскільки, за результатами розрахунків, не виявлено ніякої залежності між цими величинами.

У випадках, коли даний метод дає ненульову нижню оцінку імовірності усіченого диференціалу, вона виходить більшою за імовірність звичайного диференціалу, що потенційно дозволяє будувати більш ефективні атаки.

Висновки

У даній роботі проведено формалізацію теорії диференціального аналізу на основі усічених диференціалів, а саме представлено параметр стійкості, який характеризує імовірність усіченого диференціалу. Запропоновано два варіанти такого параметру, один з яких виявився не інформативним. Для іншого параметру, побудованого на основі попереднього, наведено деякі характеристики та властивості та показано, що він може використовуватись для побудови атак на основі усічених диференціалів. Дана ідея формалізації теорії стійкості до криптоаналізу на основі усічених диференціалів не є виключною та єдиною можливою, але перспективна з точки зору побудови аналітичних оцінок стійкості шифрів до певних класів атак.

Перелік використаних джерел

1. Knudsen L. Truncated and Higher Ordered Differentials. — International Workshop on Fast Software Encryption (FSE). — 1994. — №1008. — С. 196–211.
2. Crowley P. Truncated differential cryptanalysis of five rounds of Salsa20 — 2005. — Режим доступу: `https://eprint.iacr.org/2005/375.pdf`.
3. Rasoolzadeh S. An Improved Truncated Differential Cryptanalysis of KLEIN — 2014. — Режим доступу: `https://eprint.iacr.org/2014/485.pdf`.
4. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ 28147-89 — Інформаційні технології та комп'ютерна інженерія. — 2009. — №1(14). — С. 48–55.
5. A New Encryption Standard of Ukraine: The Kalyna Block Cipher — 2015. — Режим доступу: `https://eprint.iacr.org/2015/650.pdf`.