УДК 003.26:519.21

ПАРАМЕТР, ЯКИЙ ХАРАКТЕРИЗУЄ СТІЙКІСТЬ S-БЛОКІВ ДО АНАЛІЗУ УСІЧЕНИХ ДИФЕРЕНЦІАЛІВ

Якимчук Олексій, Яковлєв Сергій

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

Анотація

У даній роботі представлено формалізований підхід до криптоаналізу на основі усічених диференціалів за схемою, аналогічною до класичного диференціального криптоаналізу. Запропоновано параметр стійкості для S-блоків, який характеризує стійкість до атак на основі усічених диференціалів, досліджено деякі його властивості та розглянуто поведінку цього параметру для деяких S-блоків із гарантованим рівнем стійкості до диференціальних атак.

Abstract

We present formalized approach for truncated differential cryptanalysis in a way similar to classical differential cryptanalysis. We propose an S-box parameter which designates a security against truncated differential attacks, study some properties of this parameter and show its behavior for some S-boxes with guaranteed security against differential attacks.

Вступ

Вперше криптоаналіз на основі усічених диференціалів був запропонований Ларсом Кнудсеном у 1994 році [1]. Якщо звичайний диференціальний криптоаналіз досліджує повну різницю між двома відкритими текстами під час шифрування, то аналіз, що використовує усічені диференціали, враховує відмінності між текстами, які визначаються лише частково. Існує декілька прикладів успішного застосування атак на основі усічених диференціалів до існуючих шифрів або їх модифікацій [3-4].

Не зважаючи на відносно успішні випадки практичного застосування даного методу, на сьогодні не існує формальної теорії, яка описує криптоаналіз на основі усічених диференціалів та дозволяє проводити оцінку стійкості конкретних шифрів до нього. У даній роботі представлено формалізований підхід до використання усічених диференціалів на основі шаблонів (бітових масок) та запропоновано параметр стійкості для S-блоків, який потенційно дозволяє оцінювати стійкість шифрів до даного класу атак.

Необхідні терміни та позначення

Позначимо через $V_n = \{0,1\}^n$ простір усіх двійкових векторів довжини n. *Диференціалом* функції $f : V_n \to V_n$ називають пару довільних двійкових векторів (α, β), $\alpha, \beta \in V_n$, з якою пов'язують подію $f(z \oplus \alpha) = f(z) \oplus \beta,$ що індукується випадковою величиною $z \in_R V_n$. Вектори α та β диференціалу трактуються як різниці між парами вхідних та вихідних значень функції f.

У даній роботі розглядаються бієктивні S-блоки, тобто булеві функції виду $S : V_n \to V_n$, які є бієктивними відображеннями. У сучасних шифрах S-блоки зазвичай мають невеликий розмір (n = 4 або n = 8) та задаються таблично.

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] – так звані дужки Айверсона: [P] дорівнює одиниці, якщо твердження P істинне, інакше [P] дорівнює нулю. У багатьох випадках зручно також розглядати множини

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

Тоді можна сказати, що $DP^S(\alpha,\beta)=2^{-n}\cdot\left|D^S(\alpha,\beta)\right|$.

Розглянемо простір усіх можливих формальних векторів довжини n з елементами з множини $\{0,1,*\}$, який позначимо як V_n^*. Два вектори $\alpha,\beta\in V_n^*$ будемо трактувати як маски для вхідних та вихідних різниць: якщо в масці на деякій позиції стоїть 0, то і в різниці на відповідній позиції стоїть 0, якщо 1 – то і в різниці 1; якщо ж в масці на певній позиції стоїть *, то в різниці на цій позиції може бути як 0, так і 1 (нам не важливо, чи змінилось щось на заданій позиції). Кожній масці $\alpha\in V_n^*$ у відповідність можна представити множину $\Delta(\alpha)$ усіх різниць $\alpha'\in V_n\setminus\{0\}$, які відповідають даній масці; для нульової маски покладемо $\Delta(0)=\{0\}$.

Пара (α,β), $\alpha,\beta\in V_n^*$, називається *усіченим диференціалом* булевої функції. Усічені диференціали застосовуються для передбачення лише декількох бітів вихідної різниці, що потенційно дозволяє будувати більш точні та потужні розпізнавачі для шифруючих перетворень (зокрема, блокових шифрів).

Параметр стійкості до атак на основі усічених диференціалів

Безпосередньо з означення випливає, що для аналізу усічених диференціалів треба розглядати таку подію: пара входів із різницею з множини $\Delta(\alpha)$, переходить у пару виходів, різниця яких відповідає заданій масці β. Також потрібно гарантувати, що для будь-якої вхідної різниці з множини $\Delta(\alpha)$ ми отримаємо очікувані значення на заданих позиціях вихідної різниці, і коректно означити імовірність такої події. Відповідно, визначимо імовірність переходу від вхідної маски α до вихідної маски β таким чином:

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

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

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

Введена таким чином імовірність дозволяє перенести увесь апарат диференціального криптоаналізу на аналіз усічених диференціалів – зокрема, усі наявні методи пошуку диференціалів із високими імовірностями для побудови атаки на ітеративні блокові шифри. Варто зауважити, що введена імовірність *TDP* (на відміну від імовірності диференціалу *DP*) є лише нижньою оцінкою для істинних значень імовірностей усічених диференціалів, оскільки для конкретного диференціалу імовірність може перевищувати значення *TDP* (що буде показано нижче). Так само нульове значення *TDP* не означає, що відповідні диференціали неможливі, оскільки *TDP* розглядає усі диференціали, які відповідають заданим маскам у сукупності. Однак величина *TDP* покаже гарантовану імовірність такого переходу; відповідно, якщо *TDP* буде великою, то шифруюче перетворення є нестійким до аналізу усічених диференціалів.

Наведемо деякі алгебраїчні властивості параметру *TDP*:

1) Якщо $\beta\in\{0,*\}^n$, то $TDP^S(0,\beta)=1$, інакше $TDP^S(0,\beta)=0$. Ця властивість випливає з наявності тривіального диференціалу (0, 0), який завжди має імовірність 1.

2) $TDP^S(\alpha,**...*)=1$. Очевидно, що маска **…* накриває усі можливі маски, тому для довільного α та довільного входу *x* вихідна різниця точно буде відповідати **…*.

3) Якщо $\alpha\in\{0,1\}^n$, то $TDP^S(\alpha,\beta)\geq\max\limits_{\alpha'\in\Delta(\alpha),\beta'\in\Delta(\beta)} DP^S(\alpha',\beta')$. Дійсно, в цьому випадку множина $\Delta(\alpha)$ складається, фактично, з одного вектору, а маска α і є єдиною

можливою вхідною різницею, в той час як кількість можливих вихідних різниць не зменшується. Якщо ж $\alpha, \beta \in \{0,1\}^n$, то $TDP^S(\alpha,\beta) = DP^S(\alpha,\beta)$, оскільки в цьому випадку усічений диференціал збігається з класичним.

Поведінку введеного параметру проілюструємо на прикладі S-блоку K1 з [2], який задається перестановкою K1 = (7, 9, 4, D, 0, 2, C, B, A, 8, 1, 6, E, 5, F, 3) (у шістнадцятковому представленні). Частину обчислень наведено у таблиці 1.

Для випадків, коли $|\Delta(\alpha)| > 3$, усі значення $TDP^S(\alpha,\beta)$ виявились нульовими; це можна пояснити тим, що умова виконання події в *TDP* дуже строга для S-блоків невеликого розміру. Для випадків, коли потужність множини $\Delta(\alpha)$ дорівнює 2 або 3, імовірність усічених диференціалів приймає значення від 0 до 0,5; для більшості з них $TDP^S(\alpha,\beta) = 0$, однак є достатньо диференціалів із ненульовими *TDP*. Як можна побачити з таблиці 1, встановити пряму залежність між значенням *TDP* та імовірностями звичайних диференціалів, які відповідають заданим усіченим, доволі важко: *TDP* може бути як більше, так і менше, а іноді навіть точно співпадає із значенням імовірності диференціалу. Це свідчить, в першу чергу, про те, що шифри із гарантованою стійкістю проти класичного диференціального криптоаналізу можуть виявитись нестійкими до атак на основі усічених диференціалів в межах запропонованого формалізованого методу.

Таблиця 1 – Значення *TDP* та *TD* деяких усічених диференціалів S-блоку K1.

(α,β)	$\max_{\alpha'\in\Delta(\alpha),\beta'\in\Delta(\beta)} DP^S(\alpha',\beta')$	$TDP^S(\alpha,\beta)$	$TD^S(\alpha,\beta)$
(001*, 10*1)	0,125	0,125	{0111, 1010}
(001*, 11**)	0,25	0,125	{0110, 1011}
(001*, 1***)	0,25	0,5	{0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011}
(001*, *101)	0,25	0	∅
(001*, *10*)	0,25	0,0625	{0001}

Висновки

У роботі запропоновано формалізований підхід до побудови усічених диференціалів на основі шаблонів, які розглядають також обов'язкові зміни у різницях текстів. Запропоновано параметр стійкості для S-блоків, який дозволяє проводити побудову усічених диференціалів із гарантованою імовірністю появи. Показано, що для конкретного S-блоку значення запропонованого параметру слабко пов'язані із імовірностями диференціалів, тому стійкість шифру до класичного диференціального криптоаналізу не може свідчити про стійкість до аналізу усічених диференціалів.

Список використаних джерел

1. Lars Knudsen. Truncated and Higher Ordered Differentials. / Knudsen L. – International Workshop on Fast Software Encryption (FSE), 1994. – 196‑211 с.

2. Яковлєв Сергій Володимирович. Збалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ 28147-89 / Яковлєв С. В. – Інформаційні технології та комп'ютерна інженерія, 2009. – №1(14). – 48-55 с.

3. Paul Crowley. Truncated differential cryptanalysis of five rounds of Salsa20 [Електронний ресурс] / Crowley P. – 2005. – Режим доступу до ресурсу: https://eprint.iacr.org/2005/375.pdf.

4. An Improved Truncated Differential Cryptanalysis of KLEIN [Електронний ресурс] / S.Rasulzadeh, Z. Ahmadian, M. Salmasizadeh, M. Reza Aref. – 2014. – Режим доступу до ресурсу: https://eprint.iacr.org/2014/485.pdf.