УДК 004.056.55:519.2

СТІЙКІСТЬ ШИФРУ AES ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ ВІДНОСНО АЛЬТЕРНАТИВНИХ АЛГЕБРАЇЧНИХ ОПЕРАЦІЙ

Сергеєв Станіслав, Яковлєв Сергій

Фізико-технічний інститут, КПІ ім. Ігоря Сікорського

Анотація

Досліджується стійкість блокового шифру AES до диференціального криптоаналізу, який використовує побудовані спеціальним чином алгебраїчні операції, альтернативні операції побітового додавання у скінченному полі характеристики 2. Розглянуто 64 альтернативні операції та показано, що відносно майже всіх таких операцій гарантована стійкість шифру AES до диференціального криптоаналізу знижується.

Abstract

We study a security of AES cipher against differential cryptanalysis with respect to specific operations, which are similar to bitwise addition (XOR) in finite Galois field of characteristics 2. We consider 64 of such operations and show that AES guaranteed security against differential cryptanalysis in almost all cases is lowered.

Вступ

Диференціальний криптоаналіз є одним з найпотужніших методів криптоаналізу блокових шифрів; стійкість до диференціального криптоаналізу наразі є необхідною умовою для усіх алгоритмів шифрування. Для національного стандарту шифрування США, шифру AES [1], теоретична та практична стійкість до диференціального аналізу відносно операції побітового додавання була забезпечена параметрами S-блоків та раундового лінійного перетворення [2].

У роботі [3] було запропоновано новий підхід до диференціального криптоаналізу SP-мереж, в якому замість побітового додавання розглядаються спеціальні алгебраїчні операції на множині двійкових векторів. У даній роботі буде проведено аналіз стійкості шифру AES до диференціального криптоаналізу відносно деяких з таких операцій.

Необхідні терміни та визначення

У подальшому використовуються такі терміни та позначення.

Нехай $V_n = \{0,1\}^n$ – векторний простір всіх бітових векторів довжини *n*. На множині V_n визначено дві операції $\circ, +$, кожна з яких задає структуру абелевої групи.

Диференціалом булевої функції $f : V_n \to V_n$ відносно операцій $(\circ,+)$ (або просто $(\circ,+)$-диференціалом) називається довільна пара двійкових векторів (*a, b*).

Імовірність $(\circ,+)$-диференціала (*a, b*) булевої функції *f* (або просто диференціальна імовірність) визначається за формулою

$$d^{f}_{\circ,+}(a,b) = \frac{1}{2^n}\sum_{x}[\,f(x \circ a) + (f(x))^{-1} = b\,],$$

де [A] – індикатор події A (1, якщо A виконується, та 0, якщо ні), а через $(f(x))^{-1}$ позначено елемент, обернений до $f(x)$ відносно операції +. Позначимо також $MDP_{\circ,+}(f) = \max\limits_{a\neq 0,b} d^{f}_{\circ,+}(a,b)$ – максимум диференціальної імовірності функції *f*.

Для шифруючих перетворень (булевих функцій, параметризованих ключами) диференціальні імовірності розглядаються усереднено за усіма ключами. У цьому

випадку усереднена величина *MDP* є основним параметром стійкості до диференціального криптоаналізу, оскільки складність проведення атаки буде обернено пропорційна до неї; відповідно, чим більшою є *MDP*, тим менш стійким є шифр, та навпаки.

Блоковий шифр AES [1] побудовано на основі структури SP-мережі. Він складається з декількох раундів шифрування (від 10 до 14), на кожному з яких виконується нелінійна заміна байтів стану (процедура SubBytes) та лінійне перемішування байтів стану (процедури ShiftRows та MixColumns). S-блок *s* для процедури SubBytes було підібрано таким чином, щоб його *MDP* відносно операції побітового додавання $\oplus$ був мінімально можливий: 4/256. Процедура MixColumns побудована як множення векторів із байтів стану на спеціальну матрицю, при цьому всі операції виконуються у скінченному полі *GF*(256).

Теоретична стійкість шифру AES була доведена у [2], де показано, що складність будь-якої диференціальної атаки на AES буде щонайменше 2^{96} операцій шифрування. В подальшому ці оцінки були ще покращені.

Альтернативні операції для диференціального криптоаналізу

У [3] було запропоновано провадити диференціальний криптоаналіз SP-мереж відносно спеціально побудованих операцій, які зберігають деякі властивості операції побітового додавання. Головна ідея полягає у виборі таких операцій, відносно яких процедура MixColumns залишається лінійною. Якщо при цьому диференціальні імовірності S-блоків відносно таких операцій збільшуються, то загальна аналітична оцінка стійкості шифру до диференціального криптоаналізу знижується – відповідно, знижується й рівень безпеки шифру.

Будемо позначати через $\circ$ довільну операцію із описаними вище властивостями. Методика побудови таких операцій наведена у [4] та більш детально – у [3].

Диференціальний криптоаналіз відносно операції $\circ$ може провадитись у двох можливих сценаріях.

1) За припущення, що раундові ключі шифрування *k* відносяться до множини так званих «слабких» ключів, тобто для довільного вектору *x* виконується рівність $x \circ k = x \oplus k$. У даному випадку стійкість до диференціального криптоаналізу буде визначатись величиною $MDP_{\circ,\circ}(s)$.

У [3] показано, що множина слабких ключів $W_\circ = \{k \mid \forall x : x \circ k = x \oplus k\}$ утворює лінійний підпростір простору V_n; більш того, розмірність цього простору $d = \dim(W_\circ)$ задовольняє нерівностям $2 - (n \bmod 2) \le d = \dim(W_\circ) \le n - 2$. Відповідно, чим більша розмірність у $W_\circ$, тим більше імовірність потрапити на слабкі ключі.

2) Для довільних ключів із збереженням операції $\oplus$ у ключовому суматорі. У даному випадку стійкість шифру до диференціального криптоаналізу буде визначатись величиною $MDP_{\oplus,\circ}(s)$.

Експерименти

Для оцінювання стійкості шифру AES до диференціального криптоаналізу нами був побудований ряд альтернативних операцій із наведеними вище властивостями. Для аналізу обирались операції із максимально можливим простором слабких ключів. Оскільки для S-блоку шифру AES маємо $n = 8$, тому максимальна можлива розмірність простору слабких ключів $W_\circ$ $d = 6$. У [5] показано, що існує лише 64 операції, які задовольняють цій вимозі.

Для кожної з побудованих операцій були обчислені значення $MDP_{\oplus,\circ}(s)$ та $MDP_{\circ,\circ}(s)$ S-блоку шифру AES, які порівнювались із значенням $MDP_{\oplus,\oplus}(s)$ = 0,015625. Одержано такі результати:

1. Величина $MDP_{\oplus,\circ}(s)$ відносно 63-х операцій дорівнює 6/256 = 0,0234375.
2. Величина $MDP_{\oplus,\circ}(s)$ відносно однієї операції дорівнює 4/256 = 0,015625.
3. Величина $MDP_{\circ,\circ}(s)$ відносно 55-ти операцій дорівнює 8/256 = 0,03125.
4. Величина $MDP_{\circ,\circ}(s)$ відносно 8-ми операцій дорівнює 10/256 = 0,0390625.
5. Величина $MDP_{\circ,\circ}(s)$ відносно однієї операції дорівнює 4/256 = 0,015625.

Отже, бачимо, що лише для однієї операції максимальна диференціальна імовірність не збільшується (власне, ця операція є побітовим додаванням $\oplus$). Відносно всіх інших операцій маємо збільшення значення *MDP* щонайменше у півтори рази. Відповідно, при другому сценарію проведення аналізу складність проведення диференціальної атаки (теоретична оцінка стійкості згідно [2]) становить щонайменше $(6/256)^{-16} \approx 2^{86}$ операцій шифрування, що на 10 порядків менше за попередні оцінки. За першим сценарієм оцінка повинна складати $(10/256)^{-16} \approx 2^{75}$ операцій шифрування, однак дана оцінка буде виконуватись лише за умови, що всі раундові ключі будуть слабкими; імовірність такої події потрібно оцінювати окремо, з урахуванням процедури генерування раундових ключів.

Висновки

У даній роботі було розглянуто нещодавно запропонований підхід до проведення диференціального криптоаналізу SP-мереж за допомогою алгебраїчних операцій спеціального виду. Було побудовано 64 такі операції для поля *GF*(256) із найбільш прийнятними криптографічними параметрами, після чого було оцінено величини диференціальних імовірностей S-блоку шифру AES відносно даних операцій. Показано, що для деяких операцій гарантована стійкість шифру AES до диференціального криптоаналізу зменшується щонайменше на 10 порядків (тобто у тисячу разів). Хоча такі уточнені оцінки стійкості все одно гарантують стійкість AES, результати дослідження говорять про необхідність ретельного аналізу захищеності алгоритмів шифрування відносно різних модифікацій диференціального криптоаналізу та формулювання відповідних вимог до складових шифрів, зокрема, S-блоків.

Список використаних джерел:

1. Advanced Encryption Standard. [електронний ресурс]. – Режим доступу : http://csrc.nist.gov/archive/aes

2. Park S. 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.

3. Blondeau C. Differential Attacks: Using Alternative Operations [електронний ресурс] / C. Blondeau, R. Civino, M. Sala. – Режим доступу : https://eprint.iacr.org/2017/610.pdf

4. Calderini M. Elementary abelian regular subgroups as hidden sums forcryptographic trapdoors [електронний ресурс] / M. Calderini, M. Sala. – Режим доступу : https://arxiv.org/pdf/1702.00581.pdf

5. Сергеєв С.О. Використання альтернативних алгебраїчних операцій для диференціального криптоаналізу SP-мереж // Матеріали конференції «Теоретичні і прикладні проблеми фізики, математики та інформатики» (м. Київ, 26-27 квітня 2018 р.). – Том 2. – К.: ВПІ ВПК «Політехніка», 2018. – С. 75-77.