

ОСОБЛИВОСТІ АТАКИ ВІДСІКАННЯ НА ГЕШ-ФУНКЦІЮ «СТРИБОГ»

К. А. Олешко^{1, а}¹ Національний технічний університет України «Київський політехнічний інститут»

Анотація

В роботі представлена побудова атаки відсікання на 4,5 раундовий варіант функції стиснення геш-функції «Стрибог», описаний у стандарті ГОСТ Р 34.11-2012.

Ключові слова: атака відсікання, «Стрибог»

Вступ

Геш-функції відіграють важливу роль в криптографії і використовуються, наприклад, для електронного підпису, аутентифікації, забезпечення цілісності даних. ГОСТ Р 34.11-2012 «Стрибог» – це стандарт гешування Російської Федерації. В даній роботі представлена побудова атаки відсікання [1] на функцію стиснення «Стрибог» зі зменшеною кількістю раундів.

1. Геш-функція «Стрибог»

Стрибог [1] – це сімейство геш-функцій, що включає в себе дві функції: функцію з довжиною вихідного значення в 256 біт і функцію з довжиною вихідного значення в 512 біт. Обидві ці функції мають однакову структуру і відрізняються один від одного лише початковим внутрішнім станом.

У стандарті ГОСТ Р 34.11-2012 значення вектору ініціалізації фіксоване і відображене в стандарті: для геш-функції з розміром вихідного гешу 512 біт це 0^{512} , для геш-функції з розміром вихідного геш-коду 256 біт – $(00000001)^{64}$ (всі байти дорівнюють 1).

Вхідними даними для обох функцій є блок даних довжиною $m = 512$ біт. Повідомлення M розбивається на блоки $M = M_1 || \dots || M_{(k)}$, якщо довжина повідомлення M кратна розміру блоку m , якщо ні, то відбувається доповнення повідомлення M шляхом додавання одиниці і потрібної кількості нулів $M = M || \text{pad}(M)$, $\text{pad}(M) = 10 \dots 0$, $|\text{pad}(M)| < m$.

В стискаючій функції використовується 4 різних перетворення.

1) X -перетворення.

Вхідними даними цього перетворення є дві послідовності по 512 біт. Вихідним – додавання за модулем 2 цих двох послідовностей.

2) S -перетворення.

Функція S є звичайною функцією підстановки. Кожен байт з 512-бітної вхідної послідовності замінюється відповідним байтом з таблиці підстановок π . Таблиця π є константою і може бути записана у вигляді масиву.

3) P -перетворення.

Функція P є функцією перестановки. Для кожної пари байт з вхідної послідовності відбувається заміна одного байта іншим. Таблиця перестановок τ також є константою.

4) L -перетворення.

Дане перетворення являє собою множення 64-бітного вектора на матрицю розміром 64×64 у полі $GF(2)$. У стандарті вона представлена масивом з 64-бітних рядків у шістнадцятковій системі числення.

Значення геш-коду повідомлення M обчислюється з використанням ітераційної процедури. На кожній ітерації обчислення геш-коду використовується функція стиснення:

$$f_{\text{stribog}} : (0, 1)^{512} \times (0, 1)^{512} \times (0, 1)^{512} \rightarrow (0, 1)^{512},$$

значення якої обчислюється за формулою:

$$f_{\text{stribog}}(\text{bits}, h, m) = E(LPS(h \oplus m)) \oplus h \oplus m,$$

де E – це ітеративний блочний шифр:

$$E(K, m) = X[K_{13}]LPSX[K_{12}] \dots LPSX[K_1](m).$$

Значення раундових ключів $K_i \in (0, 1)^{512}$, $i = 1, \dots, 13$ обчислюються наступним чином:

$$K_1 = K;$$

$$K_i = LPS(K_{(i-1)} \oplus C_{(i-1)}), i = 2, \dots, 13.$$

Тут C – це набір 512-бітних значень. Значення C є постійним. bits – лічильник оброблених бітів. h – значення гешу.

Після обробки останнього блоку повідомлення виконується ще два виклики функції стиснення – обидві зі значенням лічильника, що дорівнює 0, а замість повідомлення у першому виклику ставиться bits , а у другому – Σ (сума оброблених біт):

$$h_{(t+1)} = f_{\text{stribog}}(0, h, \text{bits});$$

$$h_{(t+2)} = f_{\text{stribog}}(0, h, \Sigma).$$

Значення, яке отримується після обчислення $h_{(t+2)}$ є остаточним значенням.

Для геш-функції Стрибог довжиною в 512 біт отримується на останньому кроці геш-значення залишається незмінним. Для геш-функції Стрибог із вихідною

^аkostia070694@gmail.com

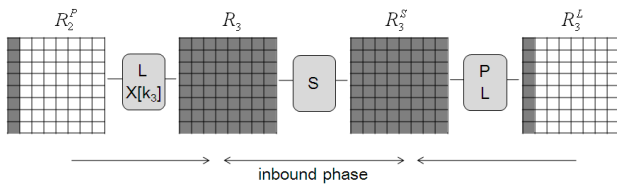


Рис. 1. Схематичне зображення внутрішньої фази атаки на 4,5 раундову функцію стиснення ГОСТ Р. Активні байти стану виділені чорним.

довжиною в 512 біт додається ще один крок: від отриманого на останньому кроці геш-значення береться 256 найбільш значущих бітів, що і представляють собою вихід геш-функції.

2. Атака відсікання на функцію стиснення алгоритму ГОСТ Р 34.11-2012, зменшену до 4,5 раундів [2]

Атака відсікання – це метод аналізу геш-функцій, яка вперше була запропонована Менделем і ін [1]. Зазвичай вона складається з внутрішньої фази і подальшої зовнішньої фази.

В атаці відсікання блочний шифр E насамперед поділяється на три субшифри $E = E_{fw} \circ E_{in} \circ E_{bw}$, де E_{in} – внутрішня частина, а E_{fw} і E_{bw} разом складають зовнішню частину.

На першому кроці внутрішньої фази ми починаємо з 8-байтної різниці одночасно на стадіях R_2^P та R_3^L і просуваємося вперед і назад до R_3 і R_3^S відповідно (див. рис. 1). Згідно властивостям поширення різниці операції L (оскільки L – це лінійне перетворення, визначена вхідна різниця в L призводить до певної вихідної різниці), ми отримуємо повністю активний стан як в, R_3 так і в R_3^S .

На другому кроці внутрішньої фази ми виконуємо пошук відповідності на рівні S в r_3 з метою пошуку відповідного поєднання вхідних / вихідних різниць.

Варто відзначити, що всього існує 2^{128} різних диференціальних шляхів, і ми можемо отримати не більше 2^{128} актуальних значень для R_3 і R_3^S . Оскільки k_3 може мати будь-яке значення, максимальна кількість стартових точок дорівнює $2^{128+512} = 2^{640}$.

В зовнішній фазі використовуються стартові точки, знайдені на внутрішній фазі, і обробляється їх значення в прямому і зворотному напрямку. Різниця в R_2^P і R_3^L призводить до різниць тільки в перших стовпчиках в R_1 і R_5^P відповідно. Можна легко сконструювати колізію для функції стиснення ГОСТ Р, усіченої до 4,5 раунду, використовуючи значення, згенеровані на попередньому кроці. Оскільки

$$h' = m \oplus E(k, m) \oplus h,$$

для ідентичних значень h і k одна і та ж різниця для m і $E(k, m)$ завжди призводить до колізії. Для пари значень, згенерованих на зовнішній фазі, різниця еквівалентна для m і $E(k, m)$ з імовірністю 2^{-64} . Отже, ми повинні згенерувати близько 2^{64} стартових точок для конструювання колізії. Трудомісткість цього становить близько 2^{64} [2].

Висновки

В даній роботі була представлена побудова атаки відсікання на функцію стиснення діючого стандарту РФ «Стрибог» зі зменшеною до 4,5 кількістю раундів. Трудомісткість побудованої атаки на 4,5 раундову геш-функцію «Стрибог» становить близько 2^{64} .

Перелік використаних джерел

1. Riham AlTawy, Aleksandar Kircanski, Amr M. Youssef 1. Rebound attacks on Stribog — 2013. — 2-9 с.
2. Zongyue Wanga, Hongbo Yub, Xiaoyun Wangb 2. Cryptanalysis of GOST R Hash Function — 2013. — 3-7 с.