УДК 519.257

АТАКА ЗБОЇВ НА ARX-КРИПТОСИСТЕМУ HIGHT ТА ЇЇ ЕФЕКТИВНІСТЬ

Блинов Сергій, Яковлєв Сергій

Фізико-технічний інститут, КПІ ім. Ігоря Сікорського

Анотація

Запропоновано атаку збоїв на блоковий шифр HIGHT, яка використовує модель фіксованого збою. Експериментально показано, що поведінка збоїв у даному шифрі носить нерівномірний характер, що не дозволяє використовувати наявний статистичний апарат для відновлення ключів, однак певні особливості розподілу збоїв дозволяють суттєво звузити множину можливих значень, а за повторення атаки – повністю відновити ключ шифрування.

Abstract

We propose a fault attack on HIGHT cipher based on fixed faults model. We experimentally show that faults inside this cipher are non-uniform, so one cannot use an existing statistical methods for key recovery. However, some properties of fault distribution allow to significantly reduce a set of possible keys (up to full recover with attack repeating).

Вступ

Розвиток алгоритмів «легкої» криптографії (англ. lightweight cryptography), призначених для використання у малопотужних пристроях, зазвичай вимагає економії на усіх обчислювальних ресурсах; тому в рамках даного напрямку широкого розвитку набули так звані ARX-криптосистеми (від англ. Add-Rotation-XOR) – алгоритми, які для обчислення використовують лише операції модульного та побітового додавання, а також циклічного зсуву двійкових векторів. Використання простих перетворень, які доступні на рівні базових інструкцій процесорів, суттєво пришвидшує шифрування даних, водночас достатній рівень захисту забезпечується за рахунок комбінування різних алгебраїчних операцій.

Атаки за побічними каналами напрямлені не на власне криптоалгоритми, а на їх реалізації у певних обчислювальних середовищах. Вони поділяються на пасивні, які одержують інформацію з побічних каналів (час виконання, споживана потужність тощо) та активні, які втручаються у роботу пристроїв та вносять збої у процес шифрування. Такі атаки є критичними для малопотужних пристроїв через обмеженість ресурсів, які можна виділити для захисту. Тому для алгоритмів легкої криптографії необхідно проводити обов'язковий аналіз стійкості до атак за побічними каналами.

Дана робота присвячена модельному дослідженню стійкості ARX-криптосистеми HIGHT до атак збоїв. Розглядаються поширені моделі зловмисника та різні сценарії проведення атаки, ефективність яких перевіряється експериментально.

Необхідні теоретичні відомості

Шифр HIGHT є блоковим шифром з ARX-дизайном, розробленим Корейською агенцією національної безпеки [1] та стандартизованим ISO [2]. Він перетворює 64-бітовий блок даних за допомогою 128-бітового ключа, виконуючи 32 раунди шифрування. Далі будуть використовуватись такі позначення.

Відкритий текст та шифротекст розглядаються як конкатенація восьми байтів і позначаються відповідно $P = P_0 \|...\| P_6 \| P_7$ та $C = C_0 \|...\| C_6 \| C_7$. Проміжні значення представлені аналогічно: $X_i = X_{i,0} \|...\| X_{i,6} \| X_{i,7}$ для $i = 0,\ldots,31$. Ключ шифрування (masterKey) розглядається як конкатенація 16 байтів, з яких генеруються вісім забілюючих ключів WK та 128 раундових ключі SK.

Раундове перетворення визначається такими співвідношеннями:

$$X_{i+1,j-1} = X_{i,j} \oplus (f_0(X_{i,j+1}) + SK_{i,j+1}),\ j = 0,4;$$
$$X_{i+1,j-1} = X_{i,j} + (f_1(X_{i,j+1}) \oplus SK_{i,j+1});\ j = 2,6.$$

де f_0 та f_1 – певні перетворення (див. детальніше [1]). Схема раундової функції наведена на рис. 1. На початку та наприкінці шифрування окремі чотири байти вхідного тексту та, відповідно, шифротексту додатково забілюються ключами WK.

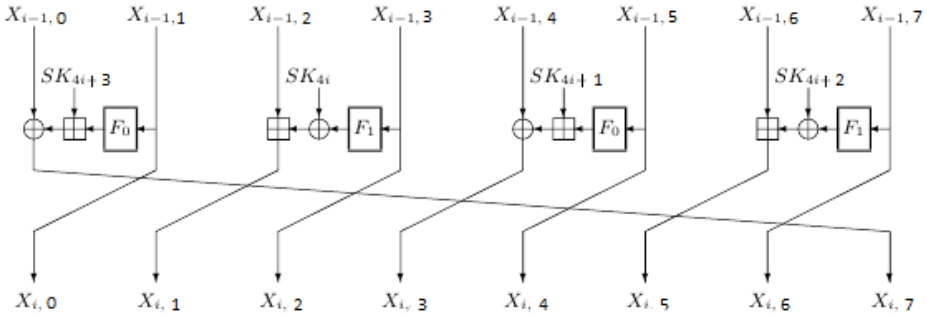

Рисунок 1 – Раундове перетворення шифру HIGHT

Блокова структура раундової функції спрощує аналіз, оскільки в цьому випадку можна перебирати раундові ключі окремо, по кожному з яких є відносно невелика кількість варіантів.

Загальна схема атаки

Основні принципи диференціальних атак збоїв для фейстель-подібних схем були сформульовані Біхамом та Шаміром [3] та в подальшому покращені Рівайном [4] при побудові атаки на шифр DES. Аналітик має доступ до шифруючого пристрою і використовує коректні та пошкоджені під час шифрування шифртексти від одного відкритого тексту, знання якого при цьому не вимагається. На основі одержаного статистичного матеріалу будуються розпізнавачі для правильних значень раундових ключів, які після цього вже знаходяться (зазвичай, перебором).

Для атаки на шифр HIGHT розглядається модель із фіксованим збоєм: аналітик може спотворювати один байт проміжного шифротексту, позиція якого йому відома, але невідоме спотворене значення. Порівняння коректних та збитих шифротекстів у 0, 2, 4 та 6 байтах шифротексту дає змогу відновити правильні значення ключів забілювання та раундових ключів за допомогою функцій розпізнавання

$$g^j(WK, SK) = (\overline{C_j} \oplus (f_0(\overline{C_{j+1}} \oplus WK) + SK)) \oplus (C_j \oplus (f_0(C_{j+1} \oplus WK) + SK)),\ j = 0,4,$$
$$g^j(WK, SK) = (\overline{C_j} - (f_1(\overline{C_{j+1}} - WK) \oplus SK)) \oplus (C_i - (f_1(C_{j+1} - WK) \oplus SK)),\ j = 2,6,$$

які отримано з аналітичного виду останнього раунду шифрування (тут C – правильний шифротекст, $\overline{C}$ – збитий шифротекст). Для правильних значень ключів поведінка функцій розпізнавання очікується суттєво нерівноімовірною, а для неправильних – значно ближчою до рівноімовірного.

Опишемо покроково алгоритм атаки.

1) Згенерувати N шифротекстів та N відповідних збитих шифротекстів. Збиті шифротексти одержуються за рахунок одного спотвореного байту проміжного шифротексту із фіксованою позицією (номер раунду, номер байту у блоці).

2) Для кожного кандидата у пару ключів (WK, SK) обчислити вибірковий розподіл значень функцій розпізнавання g^j

3) Перевірити, чи має g^j очікуваний розподіл. Якщо так, то даний кандидат є правильною парою ключів.

Оскільки на практиці теоретичний розподіл функцій g^j фактично невідомий, оскільки залежить від характеру збою та внутрішньої структури шифру (його пошук становить окрему цікаву задачу), то для кожного байту будемо перевіряти евклідову відстань до рівномірного розподілу:

$$d(WK,SK)=\sum_{x=0}^{256}\left(\frac{\#(g^j(WK,SK)=x)}{N}-\frac{1}{256}\right)^2$$

Експериментальні результати

Для проведення експериментів було реалізовано модель шифру із відповідними функціями збоїв та розпізнавання (використовувалась мова Java, ключі, тексти та збої генерувались за допомогою класу SecureRandom). Описаний сценарій атаки перевірено на 1000 випадкових ключах шифрування, для кожного з яких генерувалось 1000 пар випадкових правильних та збитих шифротекстів.

Виявилось, що навіть через лавинні ефекти, тобто змішування спотворених байтів між собою під час шифрування, розподіл функцій розпізнавання не був настільки нерівноімовірним, щоб гарантувати для правильних значень раундових ключів максимальну евклідову відстань від рівноімовірного розподілу. Однак для правильних кандидатів евклідова відстань знаходилась у діапазоні $0.00090 < d(\mathrm{WK,SK}) < 0{,}00110$. Експериментально встановлено, що використовуючи дане обмеження, можна за допомогою одного збою щонайменше втричі зменшити кількість кандидатів; відповідно, при послідовному повторенні атаки з декількома різними збоями (приблизно 10-16 повторів) можна відновити правильні раундові ключі або звузити множину їх можливих значень, після якої відновлення ключа шифрування можна виконати безпосередньо перебором.

Відповідно, для захисту від атак збоїв реалізації шифру HIGHT повинні контролювати коректність обчислень щонайменше на 16 останніх раундах шифрування.

Висновки

У даній роботі було запропоновано атаку збоїв на шифр HIGHT, яка використовує байтові випадкові помилки у внутрішніх раундах шифрування. Обрана модель є не дуже жорсткою для аналітика, проте дозволяє ефективно зменшувати множину значень ключа шифрування. Експериментально встановлено, що байтові збої у шифрі HIGHT носять нерівноімовірний характер, що не дає змогу перенести атаку Рівайна на даний шифр; однак аналіз цього розподілу дозволяє суттєво зменшувати кількість кандидатів у правильні ключі. Описаний сценарій атаки дозволяє за рахунок 10-16 повторних запусків відновити ключ шифрування.

Список використаних джерел:

1. Hong D. et al. HIGHT: A New Block Cipher Suitable for Low-Resource Device. // Proceedings of CHES 2006. – LNCS. – vol. 4249. – Springer, 2006. – pp. 46-59.

2. Information technology – Security techniques – Encryption – Part 3: Block ciphers. ISO/IEC 18033-3.

3. Biham E., Shamir A. Differential fault analysis of secret key cryptosystems // Proceedings of CRYPTO'97. – LNCS. – vol.1294. – Springer, 1997. – pp. 513-525.

4. Rivain M. Differential Fault Analysis on DES Middle Rounds // Proceedings of CHES 2009. – LNCS. – vol. 5747. – Springer, 2009. – pp. 457-469.