Differential fault-analysis of GOST 28147 block cipher implementations

Yaroslav Reshetar[1], Yaroslav Sovyn[2]

Protection of Information Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12,
[1]E-mail: j_reshetar@ukr.net

[2]E-mail: sovynjarosl@gmail.com

In practice, most cryptographic devices are subject to possible external influences from unauthorized users. In such cases, the device behavior is critical for maintaining the confidentiality of a key (secret) information and can be used for cryptanalysis.

Regardless of the implementation form, cryptographic device provides several internal and external impact factors. The external factors such as power supply and clocking allows to generate these parameters that lead to failures in cryptographic computations [1]. In addition to external means there is a possibility to change internal intermediate states of registers and RAM cells direct using modern equipment with IC depackaging.

In this report we presents a successful attack on symmetric block cipher GOST 28147 implementations with fault induced during the last round computations.

Adapted to GOST 28147 attack model (Figure 1) involves the construction of difference distribution tables for each S-box. Since standard defines 4-bit substitution tables there are generally 16 possible combinations. Moreover, unlike DES algorithm, GOST 28147 has addition modulo 2^{32} with round key operation, so we need to consider carry to more significant bits. As a result, for the adder block difference distribution tables has been constructed that take into account all 256 possible combinations for 4-bit (R, K) values.

The general idea of the attack is that not all ΔS_{in} are possible, because of specific ΔS_{out} and also for particular ΔR (Figure. 1). So we can discard possible key bits according to the expected differences.

Implementation of the algorithmic part of attack confirms the possibility to recover last round key by analyzing between 9-15 faulty ciphertexts without knowing plaintexts.

Thus GOST 28147 encryption algorithm, as other block ciphers with Feistel structure, seems to be vulnerable to fault analysis. The adapted model for the last round, that allowed to recover 32-bit key for a reasonable number of faulty ciphertexts could be extended to the last few rounds to extract the entire key.

Диференційний криптоаналіз реалізацій алгоритму ГОСТ 28147 через атаки виклику помилок

Ярослав Решетар[1], Ярослав Совин[2]

Кафедра захисту інформації,
Національний університет "Львівська політехніка",
УКРАЇНА, м. Львів, вул. С. Бандери, 12,
[1]E-mail: j_reshetar@ukr.net

[2]E-mail: sovynjarosl@gmail.com

У доповіді представлено модель успішної атаки на останній раунд реалізацій алгоритму симетричного блокового шифрування згідно ДСТУ ГОСТ 28147:2009 шляхом спричинення помилок в ході обчислень. Програмна реалізація алгоритму атаки підтверджує можливість відновлення раундового ключа за допомогою 9-15 спотворених шифротекстів.

Ключові слова – симетричний криптоалгоритм, крипто аналіз, атаки виклику помилок, некоректні шифротексти.

I. Вступ

На практиці криптографічні пристрої підлягають можливості сторонніх впливів з боку несанкціонованих користувачів. В таких випадках поведінка системи є критичною щодо збереження конфіденційності ключової (секретної) інформації, тобто може бути використана для криптоаналізу.

II. Атаки виклику помилок

Реалізація криптографічних пристроїв, як правило, виконана у формі одного кристалу ІС, з внутрішньою структурою, що може містити елементи ПЗП та ОЗП, регістри, блоки вводу-виводу, тощо.

Незалежно від форми реалізації криптографічний пристрій передбачає декілька внутрішніх та зовнішніх факторів для стороннього впливу. До зовнішніх факторів належать загальнодоступні (умовно) кола живлення та тактування, а також зовнішні виводи ІС.

Зовнішній контроль над схемами живлення та синхронізації дозволяє генерувати такі їх параметри, що приводитимуть до внутрішніх збоїв в криптографічних обчисленнях [1]. Зовнішні виводи ІС можуть також слугувати засобом для спричинення помилок в роботі криптопроцесора, зокрема шляхом встановлення їх у відповідні значення.

Окрім зовнішніх засобів для впливу сучасне обладнання дозволяє провести розпакування частини корпусу ІС і отримати доступ до внутрішньої структури пристрою, зокрема за допомогою недорогого фото-оптичного обладнання.

У таких випадках атакуючий, крім можливості спостереження загальної архітектури пристрою частково може змінювати вміст деяких компонентів, спричиняючи помилку наступних обчислень.

III. Аналіз некоректних шифротекстів та відновлення ключа

Можливість успішного криптоаналізу за допомогою атак виклику помилок для симетричних криптосистем вперше було представлено у статті [2] для алгоритму DES. Для відновлення ключових даних було використано модель диференційної атаки, що передбачає отримання на основі одного блоку відкритого тексту двох текстів, з та без помилки.

Криптографічний алгоритм блокового шифрування згідно ДСТУ ГОСТ 28147:2009 має 32-раундову структуру з мережею Фейстеля та 256-бітним секретним ключем [X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0] [3]. Раундові ключі є 32-бітними частинами цілого ключа і використовуються в послідовності $X_0 \ldots X_7$, $X_0 \ldots X_7$, $X_0 \ldots X_7$, $X_7 \ldots X_0$.

Вміст проміжних та кінцевих регістрів раундів визначається такими виразами:

$$R_j = (11 <<< S((R_{j-1} + K_j) \bmod 2^{32})) \oplus L_{j-1},$$

$$L_j = R_{j-1}, \text{ при j=1..31}$$

$$R_{32} = R_{31}$$

$$L_{32} = (11 <<< S((R_{31} + K_{32}) \bmod 2^{32})) \oplus L_{31},$$

де L_j, R_j відповідно старші та молодші 32-біти результату раундової функції.

Припустимо, що в регістр R_{31} вноситься спотворення ΔR_{31}, тоді

$$L'_{32} = (11 <<< S((R_{31} \oplus \Delta R_{31} + K_{32}) \bmod 2^{32})) \oplus L_{31}.$$

Просумувавши за модулем два ліві частини коректного та спотвореного шифротекстів отримаємо:

$$(L_{32} \oplus L'_{32}) >>> 11 = S(S_{вх}) \oplus S(S'_{вх}), \text{ де}$$

$$S_{вх} = (R_{31} + K_{32}) \bmod 2^{32}$$

$$S'_{вх} = (R_{31} \oplus \Delta R_{31} + K_{32}) \bmod 2^{32}$$

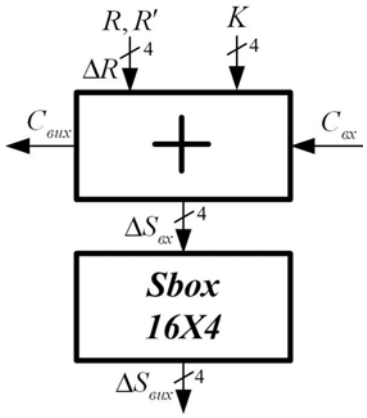
Таким чином, $(L_{32} \oplus L'_{32}) >>> 11 = \Delta S_{вих}$. Враховуючи, що блок заміни складається з 8-ми незалежних 4-бітних таблиць отримаємо $\Delta S_{вих}$ для кожної таблиці.

Адаптована до ГОСТ 28147 модель атаки (рис. 1) передбачає побудову таблиць розподілу диференціалів для кожного блоку заміни. Оскільки стандарт визначає 4-бітні таблиці заміни загалом можлива комбінація 16 пар $S_{вх}, S'_{вх}$. Крім того, на відміну від алгоритму DES, сумування регістру R з раундовим ключем відбувається за модулем 2^{32}, тому необхідно враховувати переноси у старші розряди. Як наслідок, для блоку сумування побудовано додаткові таблиці розподілу диференціалів $\Delta R \Rightarrow \Delta S_{вх}$, що враховують всі можливі 256 комбінацій 4-бітних значень (R, K).

Суть атаки полягає в тому, що не всі $\Delta S_{вх}$ можливі, по-перше для конкретних таблиці заміни та $\Delta S_{вих}$, по-друге для конкретного ΔR (рисунок). Ключі знаходяться шляхом перебору можливих гіпотез, що задовільняють систему рівнянь:

$$\begin{cases} (R + K + C) \bmod 2^4 = S_{вх} \\ (R' + K + C') \bmod 2^4 = S'_{вх} \end{cases}$$

Якщо визначити єдиний варіант 4-біт ключа неможливо, використовується наступна пара $(\Delta R, \Delta S_{вих})$.



Модель диференційної атаки для 4-біт ключа

Для перевірки практичних результатів, було реалізовано алгоритмічну частину атаки з генерацією випадкових спотворень в одному з розрядів регістра R_{31}. Програма аналізу знаходила останній раундовий ключ (X_0) за допомогою 9-15 спотворених шифротекстів. Відновлення раундового ключа дозволяє перейти до результатів попередніх ітерацій і поступово відновити весь ключ (7 останніх раундів).

Висновок

Реалізації алгоритму симетричного блокового шифрування згідно ДСТУ ГОСТ 28147:2009 можуть бути вразливими до аналізу некоректних шифротекстів, спричинених апаратними збоями атак виклику помилок. Наведена адаптована модель атаки останнього раунду дозволяє відновити 32-біти ключа за прийнятної кількості спотворених шифротекстів.

Проведені дослідження підтвердили можливість розширення моделі до декількох останніх раундів.

Література

[1] Zhou Y., Feng D. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing [Електронний ресурс] // Proc. of National Institute of Standardization: Physical Security Testing Workshop, Hawaii, September 26-29, 2005 – режим доступу до публ. http://eprint.iacr.org/2005/388.

[2] Biham, E., Shamir, A. Differential Fault Analysis of Secret Key Cryptosystem. // In: Kaliski Jr., B.S. (ed.) CRYPTO 1997, Springer, Heidelberg – LNCS, vol. 1294, pp. 513–525.

[3] Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования: ДСТУ ГОСТ 28147:2009. – [Чинний від 2009-02-01]. – К.: Держспоживстандарт України, 2008. – 28 с. – (Національний стандарт України).