УДК 004.056.5

МЕТОДЫ ЗАЩИТЫ АЛГОРИТМА BelT ОТ АТАК С ВНЕДРЕНИЕМ ОШИБОК

А.С. Герасимов, К.Е. Макаренко
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе исследуется уязвимость алгоритма блочного шифрования BelT к атакам с внедрением ошибок. Рассмотрен математический принцип дифференциальной атаки на последний раунд шифрования BelT-128, позволяющий восстановить секретный ключ по четырем успешным внедрениям ошибок. Выполнена оценка вычислительной сложности. Проанализированы методы защиты аппаратных реализаций.
Ключевые слова: BelT, атаки по сторонним каналам, внедрение ошибок, fault injection, дифференциальный анализ.

A METHODS OF PROTECTING THE BELT ALGORITHM FROM ATTACKS WITH FAULTS

A.S. Gerasimov, K.E. Makaranka
Educational Institution «Belarusian State University of Informatics and Radio Electronics», Minsk, Belarus

Abstract. The paper investigates the vulnerability of the BelT block encryption algorithm to error injection attacks. It considers the mathematical principle of a differential attack on the last round of BelT-128 encryption, which allows for the recovery of the secret key based on four successful error injections. The computational complexity is evaluated. The methods for protecting hardware implementations are analyzed.
Keywords: BelT, side-channel attacks, error injection, fault injection, and differential analysis.

Введение

Алгоритм блочного шифрования BelT утвержден в качестве государственного стандарта Республики Беларусь СТБ 34.101.31-2020 [1]. BelT используется в смарт-картах, токенах, модулях безопасности. При атаке с внедрением ошибок злоумышленник воздействует на устройство, вызывая сбой в вычислениях, и по разности правильного и ошибочного результатов восстанавливает ключ. В 2015 году исследователи из Университета Пассау, Германия, опубликовали работу, в которой показали, что BelT уязвим к таким атакам [2]. Для BelT-128 требуется 4 успешных внедрений ошибок. Это означает, что при физическом доступе к устройству злоумышленник может легко восстановить ключ. В данной работе продемонстрируем математический принцип атаки с внедрением ошибок на BelT-128 и предложим решение данной проблемы.

Основная часть

Атака основана на дифференциальном анализе ошибок. Рассмотрим последний (8-й) раунд шифрования BelT-128. В этом раунде используются два ключевых слова θ_7 и θ_8 (32 бита каждое). В BelT-128 выполняется соотношение $\theta_7 = \theta_3$, $\theta_8 = \theta_4$ [1].

В позицию L_1 (рисунок 1) внедряется ошибка f_1, которая может изменить произвольное количество битов в 32-разрядном слове. Наблюдая правильный шифротекст Y и ошибочный шифротекст Y', можно получить значения f_1 и разность на выходе.

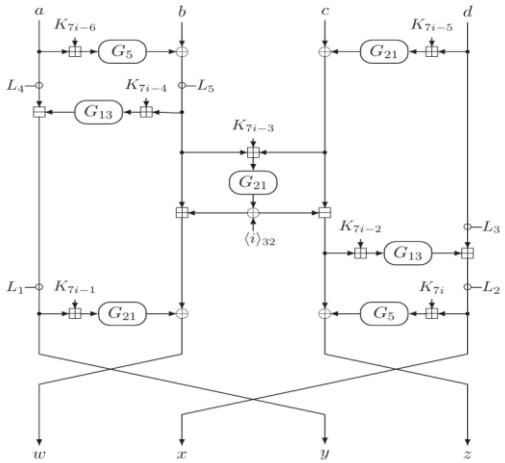

Схема алгоритма BelT
The scheme of the BelT algorithm

Пусть:
$Y = (w, x, y, z)$ – правильный шифротекст (4 слова по 32 бита);
$Y' = (w', x', y', z')$ – ошибочный шифротекст
L_1 – значение в точке внедрения ошибки;
$f_1 = y \oplus y'$ – значение ошибки (наблюдаемая разность);
$\Delta w = w \oplus w'$ – разность на выходе в позиции w.
Получаем уравнение:

$$G_{21}(L1 \boxplus \theta_7) \oplus G_{21}((L1 \oplus f1) \boxplus \theta_7) = \Delta w \qquad (1)$$

Все величины в уравнении (1), кроме θ_7, известны. $L_1 = y, f_1 = y \oplus y'$, $\Delta w = w \oplus w'$ из правильного и ошибочного шифртекстов.

Уравнение (1) позволяет отфильтровать возможные значения θ_7. Для каждого из 2^{32} возможных значений θ (от 0 до 2^{32}-1) вычислим левую часть уравнения и сравним с правой частью Δw. Из θ, при которых выполняется равенство, будет составлено множество отобранных кандидатов как Θ_7. Аналогично для θ_8.

При внедрении ошибки в позицию L_2 (соответствующую x) и анализе разности $\Delta z = z \oplus z'$ получаем уравнение для θ_8:

$$G_{13}(L_2 \boxplus \theta_8) \oplus G_{13}((L_2 \oplus f_2) \boxplus \theta_8) = \Delta z \quad (2)$$

где $f_2 = x \oplus x'$, $L_2 = x$.

Аналогичные процедуры выполняются для последнего раунда расшифрования, что позволяет восстановить θ_1 и θ_2. В результате получаем, что атака с внедрением ошибок позволяет восстановить ключ BelT-128 за 4 успешных внедрения ошибок.

Решением проблемы предложим два метода защиты аппаратных реализаций BelT [3]. Первый – временная избыточность, заключающаяся в выполнении каждой критической операции дважды, между вызовами которых вставляется случайная задержка, результаты которых сравниваются. Из-за случайной задержки нарушитель не может рассчитать точное время вызова. Второй – добавление битов четности к ключам и промежуточным значениям для обнаружения изменений. К каждому 32-разрядному ключевому слову добавляются 4 контрольных бита – по одному на каждый байт. Бит четности для байта вычисляется как XOR всех его битов. При каждой загрузке ключа устройство пересчитывает контрольные биты и сравнивает с сохраненными.

Заключение

Алгоритм BelT, являющийся стандартом Республики Беларусь, уязвим к атакам с внедрением ошибок. Для восстановления ключа достаточно 4 успешных внедрений ошибок. Уязвимость обусловлена отсутствием в стандарте требований к защите аппаратных реализаций от физических атак. При сертификации средств КЗИ на соответствие СТБ необходимо включать требования по защите от атак по сторонним каналам, включая атаки с внедрением ошибок.

Список использованных источников

1. СТБ 34.101.31-2020. (2020) *Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности.* Минск, Госстандарт.

2. Jovanovic P., Polian I. (2015) Fault-based Attacks on the Bel-T Block Cipher Family. *Design, Automation & Test in Europe Conference & Exhibition (DATE).* 601-604.

3. Boneh D., DeMillo R., Lipton R. (2001) On the Importance of Elimination Errors in Cryptographic Computations. *Journal of Cryptology*. 14, 101–119.

References

1. STB 34.101.31-2020. (2020) Information Technologies and Security. Algorithms for Encryption and Integrity Control. Minsk, Gosstandart (in Russian).

2. Jovanovic P., Polian I. (2015) Fault-based Attacks on the Bel-T Block Cipher Family. *Design, Automation & Test in Europe Conference & Exhibition (DATE),* 601-604.

3. Boneh D., DeMillo R., Lipton R. (2001) On the Importance of Elimination Errors in Cryptographic Computations. *Journal of Cryptology*. 14, 101–119.

Сведения об авторах

Герасимов А.С., магистр, старший преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.gerasimov@bsuir.by.

Макаренко К.Е., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», makarenkokirilka05@gmail.com.

Information about the authors

Gerasimov A.S., master, senior lecture, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.gerasimov@bsuir.by.

Makaranka K.E., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", makarenkokirilka05@ gmail.com.