Список использованных источников
1. Никульченко М.Ф., Исмагилова А.С. Анализ защищенности и обнаружения атак с помощью уязвимости протокола SMB // Защита информации. Инсайд. 2020. № 5 (95). С. 52-56.

Никульченко Максим Филиппович, аспирант ФГБОУ ВО «Башкирский государственный университет», E-mail: RQWZ@protonmail.com
Исмагилова Альбина Сабирьяновна, доктор физико-математических наук, доцент, заведующий кафедрой управления информационной безопасностью ФГБОУ ВО «Башкирский государственный университет», E-mail: IsmagilovaAS@yandex.ru

УДК 004.056.5

МОДЕЛИРОВАНИЕ И ИЗМЕРЕНИЕ ЭНЕРГОПОТРЕБЛЕНИЯ УСТРОЙСТВА ПРИ ВЫПОЛНЕНИИ ШИФРА AES

Е.А. Маро
Южный федеральный университет, г. Таганрог

Ключевые слова: энергопотребление устройств, криптографический алгоритм, Advanced Encryption Standard (AES)

Метод анализа побочных каналов криптографических устройств заключается в поиске математической зависимости в параметрах функционирования шифрующего устройства, например, времени вычислений, энергопотреблении, электромагнитном и акустическом излучении. Целью работы является теоретический и экспериментальный анализ трасс энергопотребления устройств при выполнении криптографических алгоритмов. Для реализации поставленной задачи был смонтирован аппаратный стенд на основе платы Arduino Nano, выполняющей алгоритм шифрования AES в различных вариантах реализации, и высокоточного осциллографа RIGOL DS1054. Моделирование трасс энергопотребления проводилось в программном обеспечении ELMO [1]. В результате работы сформирована модель трассы энергопотребления при выполнении шифра AES (рисунок 1) и получены трассы для устройства Arduino Nano.

Проведенное моделирование и выполненные на аппаратном стенде измерения энергопотребления позволяют оценить число инструкций, содержащих информацию о защищаемых данных (секретном ключе) на основе выполнения t-теста (с пороговым значением |4.5|) для фиксированного и случайных открытых текстов. В Таблице 1 представлены результаты моделирования утечек первого порядка по побочным каналам для нескольких реализаций шифра AES.

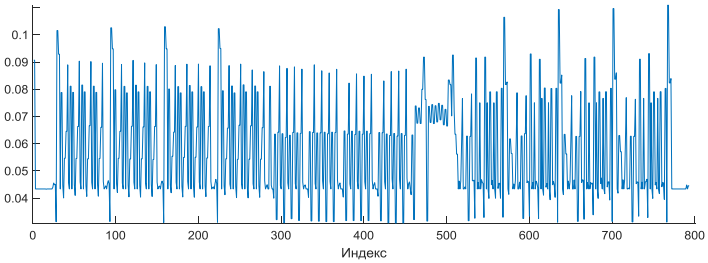

Рисунок 1 – Модель трассы энергопотребления при выполнении одного раунда шифрования AES в ELMO

Таблица 1 – Результаты моделирования утечек по побочным каналам для различных реализаций шифра AES

Вариант реализации шифра AES	**Общее число инструкций**	**Число инструкций с выявленными утечками по энергопотреблению**
AES (1 раунд)	741	514
AESMasked_R1	451	83
MBedAES	2402	1755

По результатам сравнения трасс энергопотребления одного раунда шифра AES построен график, отображающий результаты Fix vs Random теста энергопотребления для инструкций (рисунок 2).

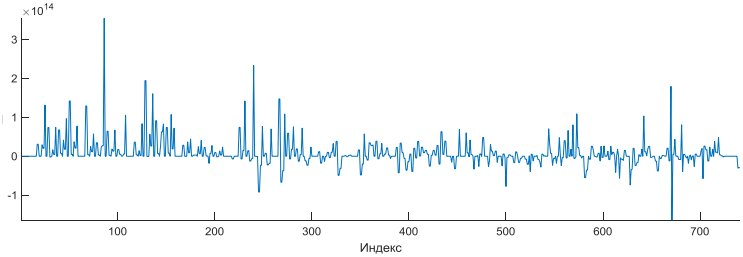

Рисунок 2 – Результат Fix vs Random теста для инструкций

Работа выполнена при поддержке Российского научного фонда (номер проекта 19-71-00041).

Список использованных источников

1. McCann D., Oswald E., Whitnall C. Towards Practical Tools for Side Channel Aware Software Engineering: 'Grey Box' Modelling for Instruction Leakages. USENIX Security Symposium, 2017, pp. 199-216.

Маро Екатерина Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий. E-mail: eamaro@sfedu.ru.