УДК 681.3.06
Мариняк А.В. ст.гр. КСМзм - 52
Тернопільська академія народного господарства

ПРОГРАМНИЙ ЗАСІБ ПОПЕРЕДНЬОЇ ОБРОБКИ РЕЗУЛЬТАТІВ ЕКСПЕРИМЕНТАЛЬНОГО ВИМІРЮВАННЯ ТРЕКІВ ЕНЕРГОСПОЖИВАННЯ ДЛЯ ПРОВЕДЕННЯ КРИПТОАТАКИ

Науковий керівник: д.т.н., проф. Курітник І.П.

На даний час, атаки енергоспоживання (Power Analysis) були виділені як клас криптографічних атак на пристрої криптографічного захисту інформації. Атаки енергоспоживання - це підклас атак побічних каналів витоку інформації (Side Channel Attacks). В їх основі лежить експлуатація характеристик виконання операцій апаратно-реалізованого алгоритму криптографічного захисту інформації.

В той час як класичні методи криптоаналізу, де криптоаналітик використовує тільки інформацію відомого входу та/або виходу алгоритму. Атаки енергоспоживання експлуатують відмінності в енергоспоживанні виконання криптографічного алгоритму протягом криптографічних перетворень. За допомогою такого аналізу, криптоаналітик може довідатися про секретний ключ шифрування, що зберігається в середині пристрою [1]. Особливо уразливими проти цього виду атак є інтелектуальні картки (smartcards - смарткартка). Це викликано переважно тим, що смарткартки мають зовнішнє джерело живлення, що дає криптоаналітику можливість отримати треки енергоспоживання картки під час проведення нею криптографічних перетворень [1].

Для проведення даного виду атаки криптоаналітику необхідно [1]: пристрій для роботи зі смарткарткою та пристрій для вимірювання енергоспоживання.

На даний час широко розвинулися методи криптографічних атак на базі енергоспоживання на криптографічні пристрої, де реалізовано асиметричні чи симетричні блочні криптоалгоритми, в той час як немає систематичних досліджень можливості проведення таких атак на потокові шифри, основою яких є LFSR (регістр зсуву з лінійними зворотними зв'язками) [2].

В [2] вперше проведено експериментальні дослідження по успішному проведенні атаки аналізу енергоспоживання базованого на вагах Хемінга на простий потоковий шифр базований на LFSR з відомим поліномом зворотних зв'язків та без відомого поліному. Результати дослідження показують, що ефективність атаки аналізу енергоспоживання з використанням ваг Хемінга залежить від наступних факторів [2]:

1. точності виміряних треків енергоспоживання;
2. методу попередньої обробки отриманих треків енергоспоживання;
3. методу додаткової обробки обчислених ваг Хемінга.

Автором розроблено програмний засіб, що реалізує метод попередньої обробки отриманих треків енергоспоживання, використання якого відповідно автоматизує проведення криптографічної атаки. В основі реалізованого програмного засобу лежить алгоритм, наведений в [2].

Література.

1. James Alexander Muir. Techniques of side channel cryptanalysis // University of Waterloo. Dept. of Combinatorics and Optimization, 2001
2. Широчин В.П., Васильцов І.В. Карпінський Б.З. Hemming Weight Power Analysis of LFSR-based Stream Ciphers // Матеріали VIII міжнародної науково-технічної конференції CADSM 2005, 23-26 лютого, 2005, Львів-Поляна, Україна, ст.168-171.