УДК 004.056.53

МЕТОДИКИ АНАЛИЗА БЛОКОВ НЕЛИНЕЙНОЙ ЗАМЕНЫ ПРИ АТАКАХ ДИФФЕРЕНЦИАЛЬНОГО АНАЛИЗА

Дакуо Ж. -М. Н. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»),

Научный руководитель – кандидат технических наук Таранов С. В. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В ходе работы были исследованы две атаки дифференциального криптоанализа с внедрением адаптивной ошибки на примере легковесного шифра DES Light: внедрение нулевой ошибки и атака на таблицы замены. Были предложены способы противодействия этим атакам для блочных легковесных шифров.

Введение. Повсеместное распространение в настоящее время получили умные устройства, для их защиты из-за ограниченности ресурсов необходимо прибегать к использованию легковесных шифров, например, DES Light. На данный момент нет эффективных способов противостоять угрозе дифференциального криптоанализа с внедрением ошибки (DFA). В работе предлагается рассмотреть две атаки. В рам ках работы разработаны методики по защите и анализу S-box’a.

Основная часть. Развитие современных технологий увеличивает арсенал злоумышленников, позволяя им создавать и атаковать слабые места криптографических устройств. Были рассмотрены две атаки: внедрение «нулевой ошибки» и внедрение ошибки в S-box шифра DES L. Первая ошибка показала, что, внедряя ошибку, которая вызывает обнуление части шифр-текста, перед сложением оного с последним раундовым ключом, можно получить весь раундовый ключ, что в дальнейшем позволит получить Мастер-ключ. Вторая ошибка вызывает коллизии в выходных значениях S-box, что, в свою очередь, вносит неравномерность в распределение выходных значений дифференциалов, что влечёт за собой уязвимость шифра к дифференциальному криптоанализу. Для минимизации рисков в связи с эксплуатацией этих двух уязвимостей предлагается использовать: новый S-box, разработанный на основе bent-функции, устойчивой к внедрению функциональных ошибок; использование «дифференциальной защиты», которая будет чувствительна к изменению напряжения в сети криптографического устройства (используются катушки); создание системы обнаружения помех CED, которая сможет отследить полное состояние устройства в реальном времени.

Выводы. В ходе работы над статьей были разобраны два примера различных атак DFA и разработаны способы противодействия им. Каждый из них имеет свои достоинства и может быть использован для устранения уязвимостей умных устройств в зависимости от имеющихся ресурсов. В дальнейшем планируется рассмотреть другие атаки DFA, а также других представителей легковесной криптографии.

Дакуо Ж.-М. Н. (автор)

Таранов С. В. (научный руководитель)