УДК 004.056.53

ПРИМЕНЕНИЕ ВЭЙВЛЕТОВ К АТАКАМ ПО СТОРОННИМ КАНАЛАМ

Р.А. Мостовой, Д.М. Слепцова, Э.Д. Андреев (Санкт-Петербургский Государственный Университет Информационных технологий, Механики и Оптики, Санкт-Петербург)
Научный руководитель – А.Б. Левина (Санкт-Петербургский Государственный Университет Информационных технологий, Механики и Оптики, Санкт-Петербург)

Атаки по сторонни каналам – сравнительно молодая, но очень перспективная область криптоанализа. Такие атаки нацелены на нарушение конфиденциальности информации. Существует множество видов атак, отличающихся методами съема информации из побочных каналов, а также степенью вмешательства в работу системы (в том числе физического). Однако наибольший интерес представляют так называемые пассивные не инвазивные атаки, т.к. они не требуют активного взаимодействия с атакуемой системой и потому не детектируемы. В данной работе были использованы унифицированные трейсы конкурса DPA contest v2.

Природа исследуемого сигнала – энергопотребление платы FPGA при вычислении первого S-Box'а алгоритма AES.

Первой проблемой, с которой приходится столкнуться при анализе сигнала, является привязка исследуемых операций ко времени. В полученном сигнале соответствующие временные промежутки могут быть сдвинуты относительно ожиданий аналитика в силу погрешности устройства для снятия, неравномерной работы жертвы, а также в результате применения мер защиты (рассинхронизация тактового сигнала, добавление случайных пауз в работу программы).

Вторая проблема – зашумленность сигнала.

Третья – недостатки одного из базовых инструментов, используемых в ЦОС – преобразования Фурье, а именно: потеря «временного домена» (невозможность детектирования появления сигнала определенной частоты в определенный промежуток времени), неудовлетворительная применимость к не стационарным сигналам, а в случае с оконным преобразованием (призванным решить описанные проблемы) – деградация разрешения либо по времени, либо по частоте (в зависимости от размеров окна).

Вэйвлетное преобразование способно решить все три описанных проблемы.

Данная работа сфокусирована на вопросе устранения шумов, и ее целями являются: имплементация дискретного вейвлетного преобразования для уменьшения шума сигнала, полученного по сторонним каналам; сравнение различных вейвлет семейств и классических методов уменьшения шума в единых условиях; исследование влияния выбора вейвлет семейства на качество удаления шума.

Вэйвлетное преобразование сводится к построению набора карт вэйвлетных коэффициентов (результата свертки с сигналом) для различных масштабов вейвлета (коэффициента растяжения повременной оси).

Сжатие выполняется за счет введения функции порога, согласно которому коэффициенты делятся на аппроксимации и детали. Вторые можно отбросить (обнулить, жесткая фильтрация) или обнулить с вычитанием их среднего значения из коэффициентов аппроксимаций (обнуление с вычитанием среднего, мягкая фильтрация). Самих типов порога, как и основных вэйвлет-семейств, несколько. При этом в существующих работах довольно слабо освещен вопрос обоснования выбора того или иного семейства и типа порога.

Устранение шума – задача, решаемая при помощи каскадного многоуровневого вэйвлет-преобразования с фильтрацией деталей (сжатием) и последующим обратным преобразованием. Эмпирическим путем было выяснено, что для фильтрации сигналов, представляющих собой энергопотребление вычислительного модуля, наилучшим выбором является порог Донохо-Джонстона с мягкой фильтрацией.

С использованием этого порога было произведено сравнение эффективности шести популярных вэйвлет-семейств: Хаар, Симлет, Добеши, Биортогональные, Койфлеты, Мейер. В качестве показателя эффективности выбрана статистическая вероятность проведения успешной атаки на определенном количестве участвующих в атаке трейсов.

Помимо фильтров шума, использующих вэйвлет-преобразования, в экспериментах, в качестве референсного, использовался распространенный фильтр Калмана.

Полученные результаты показали, во-первых, что на количестве трейсов больше 10^3, все методы фильтрации показывают убедительные результаты – вероятность успешной атаки не ниже 0.8. С другой стороны, максимальной вероятности успешной атаки достигнуть получилось лишь с тремя типами фильтров – Добеши, Симлет и Калмана (в порядке увеличения числа необходимых для этого трейсов). При этом на некотором небольшом промежутке фильтр Калмана показывал результаты даже лучшие (правда, незначительно), чем Симлет.

Полученные результаты являются эмпирическими – возможно, в будущем мы также уделим внимание поиску объяснений для тех или иных характерных точек полученных графиков, однако на данный момент, благодаря этим результатам, определены оптимальные методы фильтрации шумов под задачи наших дальнейших исследований в области пассивных атак по сторонним каналам.

Авторы _____/Мостовой Р.А.
_____/Слепцова Д.М.
_____/Андреев Э.Д.

Научный руководитель _____/Левина А.Б.

Заведующий кафедрой ПБКС _____/Заколдаев Д.А.