Защита данных в ИТ-системах

Владимир Вычужанин (г. Одесса, Украина)

Защита данных является обязательной задачей при разработке архитектуры ИТ-систем. Существуют разнообразные способы защиты информации, но любой из них вместе с преимуществами имеет недостатки. Поэтому необходимо постоянно совершенствовать методы защиты информации, обеспечивая их соответствие современным критериям безопасности.

В настоящее время защита данных в ИТ-системах осуществляется за счёт совместного использования аппаратных и программных средств. При этом аппаратные средства зачастую разрабатываются отдельно и нуждаются в защите от компрометации, т.к. вполне возможно, например, копирование ключей или алгоритмов защиты, что позволяет злоумышленникам получать несанкционированный доступ к защищаемой информации. Особенное значение такая защита приобретает при использовании устройства в ИТ-системе, разрабатываемой и используемой сторонними организациями и лицами в неконтролируемой разработчиками обстановке.

В условиях широкого распространения криптостойких методов шифрования данных особого внимания заслуживают меры противодействия попыткам дистанционного взлома криптографических модулей ИТ-систем, цель которых – определение типов защиты и считывание паролей при анализе работы действующей защищённой системы (т.н. косвенные атаки).

Одним из видов таких атак является анализ потребляемой мощности [1], при котором злоумышленник исследует энергопотребление аппаратного устройства защиты данных – криптографического модуля, например, смарт-карты. Чем более изолированную и узкую функцию выполняет модуль, тем успешнее может быть атака, бесконтактно извлекающая криптографические ключи и другую секретную информацию.

К пассивным атакам на энергопотребление относятся простые и дифференциальные (SPA (Single Power Analysis) и DPA (Differential Power Analysis) [2, 3], атаки во времени [4] и атаки по электромагнитному излучению. SPA-атаки позволяют выделить значимые флуктуации питания. DPA-атака использует статистический анализ результатов тысячи транзакций и технику коррекции ошибок для выделения информации, связанной с секретными ключами.

Следует отметить, что переменное энергопотребление электронными устройствами вызвано различием энергопотребления при выполнении, например, процессорами различных команд, что, в свою очередь, определяется неодинаковым количеством переключений его транзисторов. В результате на графике энергопотребления можно идентифицировать команды или группы команд.

Для противостояния прямым атакам используются криптографические алгоритмы с высокой криптостойкостью, например, DES или AES. На рисунках 1 и 2 проиллюстрировано применение SPA-атаки при криптографическом алгоритме DES-операции, выполняемой в обычной смарт-карте. Рисунок 1 демонстрирует операцию шифрования, включая начальное перемешивание, 16 DES-раундов и конечное перемешивание. На рисунке 2 приведены 2-й и 3-й раунды SPA-атаки при анализе криптографического алгоритма DES.

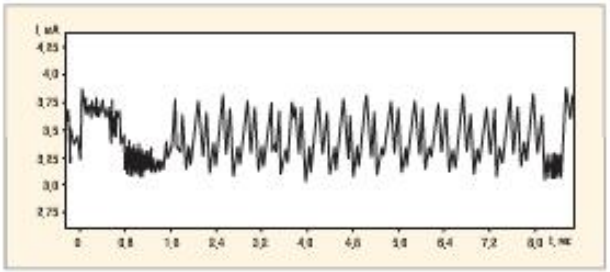

Рис. 1. SPA-атака криптографического алгоритма шифрования DES

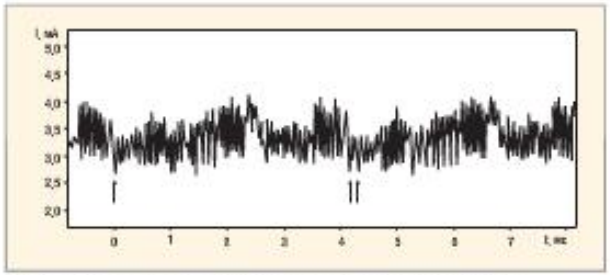

Рис. 2. 2-й и 3-й раунды SPA-атаки криптографического алгоритма шифрования DES

На рисунке 3 изображена DPA-атака при реализации AES-128 шифрования [5]. Верхний график соответствует среднему значению потребляемой мощности смарт-карты при 10 000 операциях шифрования с одиннадцатью тактовыми циклами, необходимыми для выполнения операции AES-шифрования. Нижняя кривая показывает корреляцию энергетических следов предсказания в начале 10-го раунда при правильном предположении ключевого байта. Чтобы извлечь весь 16-байтовый ключ достаточно менее чем 5 мс вычислений фактического криптографического времени наблюдений и одной минуты анализа на ПК.

Фактически единственным методом защиты от таких атак является конструктивное решение криптографического модуля, которое не позволяет их производить. Однако нужно учитывать, что во многих случаях и криптомодули, и ИТ-системы в целом строятся на базе ПЛИС, в том числе и со структурой FPGA, большинство из которых позволяют перепрограммировать их внутреннюю структуру, а конфигурационная информация для них хранится во внешних энергонезависимых запоминающих устройствах. В этих случаях возможно осуществить перенос схемы и IP из одной системы в другую простым копированием информации о конфигурации. В таких условиях эксплуатации без адекватной защиты FPGA не может быть обеспечена её эффективная конструкционная безопасность или защита данных от SPA- или DPA-атак. Кроме того, возможна утечка информации на уровне микросхемы ПЛИС за счёт электромагнитных эффектов внутри кристалла и печатной платы. Эффекты перекрёстных помех и задержки сигналов, возникающие в микросхеме ПЛИС, служат источником утечки информации по техническим каналам.

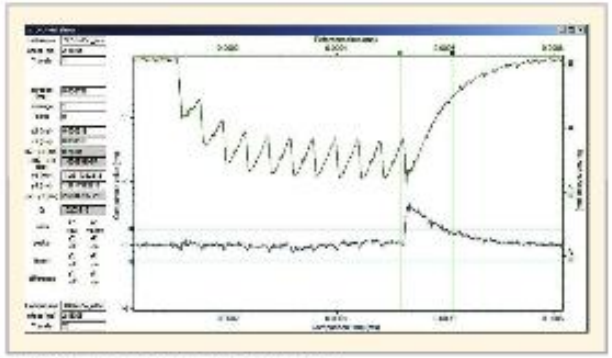

Рис. 3. DPA-атака при реализации шифрования AES-128

Современные FPGA с точки зрения хранения информации можно классифицировать следующим образом:

1. ПЛИС с аутентификацией шифрования (FPGA Xilinx Virtex-6 с обеспечением конфигурационной конфиденциальности, аутентификации и целостности битовых потоков во время включения питания). Аутентификация и криптографические проверки целостности битовых потоков во время функционирования ПЛИС не поддерживаются.