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.

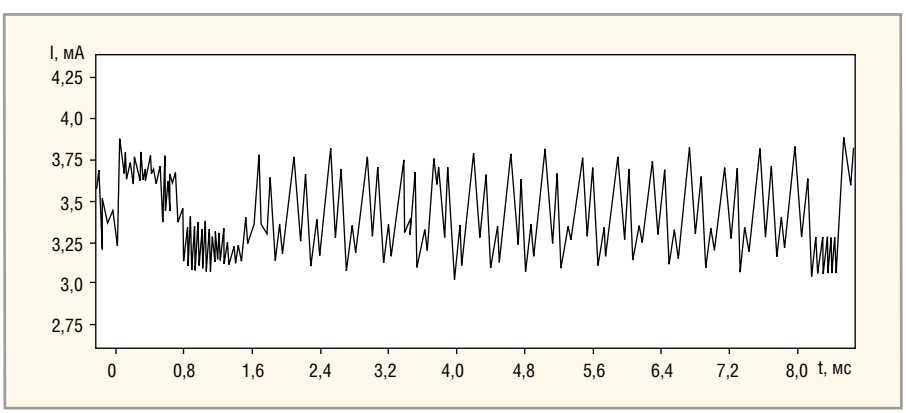

Рис. 1. SPA-атака криптографического алгоритма шифрования DES

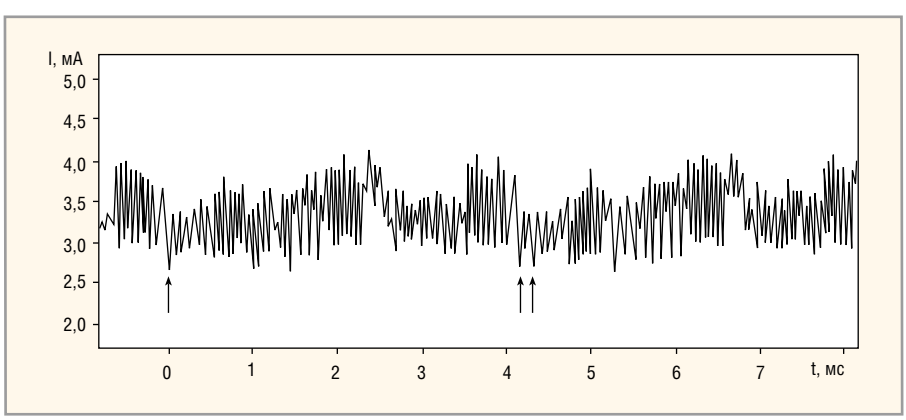

Рис. 2. 2-й и 3-й раунды SPA-атаки криптографического алгоритма шифрования DES

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, процессором 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.

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. Резко нарастающий фронт в корреляционном следе в начале 10-го раунда подтверждает правильное определение 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.

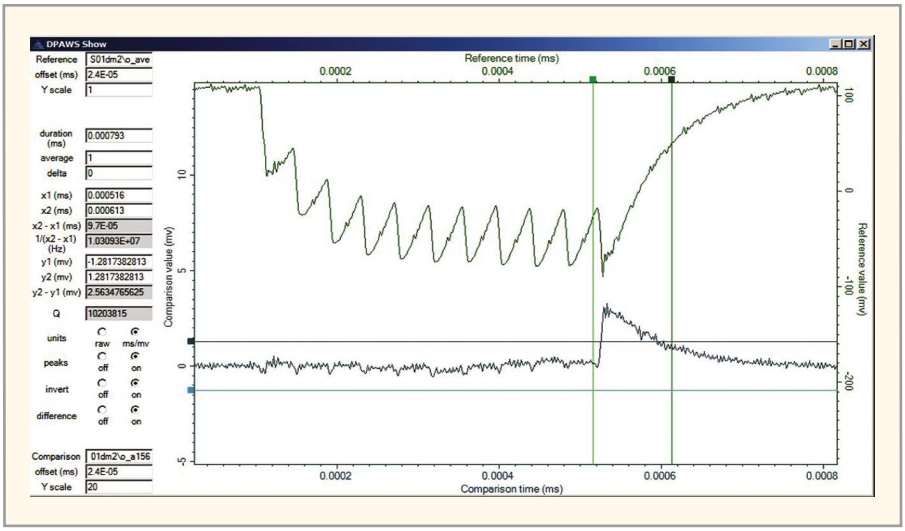

Рис. 3. DPA-атака при реализации шифрования AES-128

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.

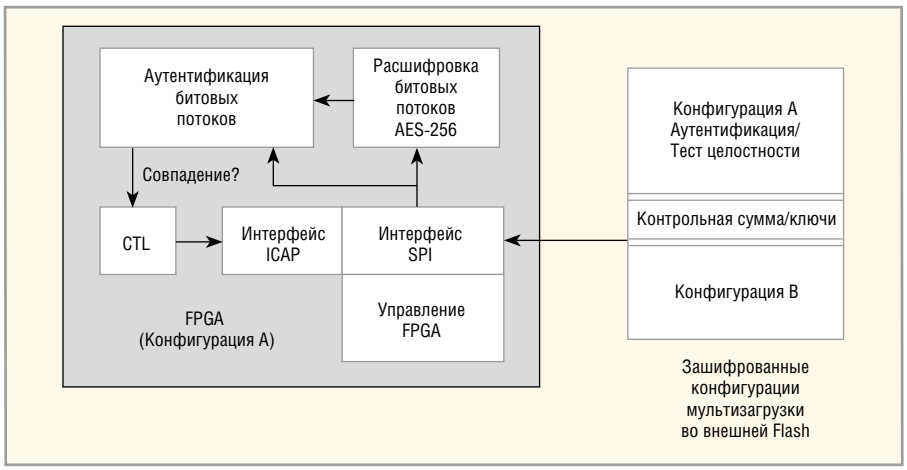

Рис. 4. Схема мультизагрузки с аутентификацией битовых потоков в ПЛИС

2. ПЛИС с битовыми потоками шифрования (FPGA Xilinx Virtex II/4/5/6, Spartan-6, Altera Stratix II/III/IV/V, Actel ProASIC3, LatticeECP, использующие AES-128 или AES-256-шифрования). Аутентификация и криптографические проверки целостности битовых потоков во время функционирования ПЛИС не поддерживаются.

3. FPGA без криптографических функций (Xilinx Spartan-3).

Большинство семейств ПЛИС с архитектурой FPGA базируются на использовании в качестве логических блоков ячеек статической оперативной памяти (SRAM) и требуют конфигурирования после включения питания (для этого служат специализированные внешние ПЗУ). При этом проекты, реализованные на FPGA, уязвимы для копирования, поскольку конфигурационный поток данных может быть перехвачен в момент загрузки при старте системы и использован для несанкционированного повторения проекта. Некоторые семейства FPGA для защиты от этого могут использовать кодированный конфигурационный поток. Но для этого нужна дополнительная операция записи в энергонезависимую память FPGA декодирующего ключа, что, как правило, требует использования дополнительного оборудования. К тому же микросхемы, поддерживающие кодированную конфигурацию, дороги. Более того, это шифрование не решает всех проблем безопасности. Следует отметить, что используемое ПЛИС программное обеспечение само по себе не является безопасным. Чтобы быть безопасным, оно должно быть запущено аппаратно корнем доверия.

При разработке средств обеспечения конфигурационной конфиденциальности, аутентификации и целостности битовых потоков в ПЛИС необходимо учитывать следующие факторы: разные уровни производительности внешних средств и собственно ПЛИС; жёсткие ограничения по стоимости; большое количество постоянно эволюционирующих стандартов; необходимость обеспечения защиты данных интегральной системы управления данными при функционировании в инфраструктуре ИТ-системы.

Защита информации может осуществляться с помощью программных и аппаратных средств. Обычно первый вариант кажется более простым и привлекательным, однако из-за большого объёма вычислений в алгоритмах шифрования/дешифрования применение программных средств ограничивается случаями, когда система рассчитана на одного пользователя/клиента.

Для аутентификации и поддержания целостности битовых потоков шифрования, а также защиты от обратного проектирования после копирования конфигурации может использоваться схема мультизагрузки нескольких конфигураций в FPGA, использующая её внешние и внутренние порты (см. рис. 4), как это делается, например, в Xilinx Spartan-6. Аутентификация битовых потоков в такой структуре осуществляется параллельно с работой основного приложения. Проверки целостности битовых потоков и конфигурационной конфиденциальности осуществляются с помощью интерфейса ICAP.

Однако большинство семейств FPGA не имеет возможности использовать кодированный конфигурационный поток. Для таких семейств ПЛИС эффективным средством защиты проектов от копирования является использование микросхем специальной памяти. Наилучшее решение по применению энергонезависимых ОЗУ ПЛИС для хранения ключа дешифрования заключается в использовании технологии Antifuse, обеспечивающей высокую надёжность и мощные ресурсы трассировки, не требующей конфигурационного ПЗУ и не предусматривающей чтение данных при загрузке ПЛИС.

Шагом вперёд для ускорения работы реализуемых алгоритмов по сравнению с программными средствами при реализации систем защиты информации является использование настраиваемых аппаратных средств.

Применение технологии FlashLock позволяет исключить различные варианты клонирования, копирования, обратного проектирования и т.д., ликвидировать возникающие проблемы защиты данных, с которыми сталкиваются проектировщики, использующие устройства, базирующиеся на технологии SRAM. Пользователю предоставляется возможность перепрограммировать ПЛИС, используя известный ему ключ защиты. 128-битный ключ операции AES-шифрования FlashLock используется для расшифровки и проверки подлинности входящих зашифрованных данных конфигурации, используемых для обновления конструкции ПЛИС.

Алгоритм работы проекта программирования секретного ключа с использованием операции шифрования FlashLock для схемы ПЛИС Microsemi SoC Products Group, включающей наборы ПЛИС фирмы Actel семейств ProASIC3, IGLOO, Fusion и SmartFusion, обеспеченных корнем доверия для поддержания необходимого уровня безопасности конструкции, приведён на рисунке 5.

Режим FlashLock обеспечивает дополнительный уровень проектной безопасности. После начального программирования конфигурации битового потока с использованием открытого текста, Lock-биты безопасности устанавливаются так, что ни один из ресурсов FPGA нельзя перепрограммировать. 128-битный код пароля блока FlashLock (см. рис. 5) запрограммирован в устройстве таким образом, чтобы предотвратить любые изменения, вносимые после введения пароля. Имеется возможность запрограммировать ПЛИС для предотвращения клонирования схемы, а также вме-

шательства по беспроводной сети. Для этого в настройках безопасности программируется 128-битный ключ дешифрования AES и устанавливается 128-битный FlashLock-пароль. В том случае, если часть ПЛИС не перепрограммируется, флэш-FPGA преобразуется в одноразовое программируемое устройство путём настройки первого Lock-бита безопасности и отключения перепрограммирования всех ресурсов FPGA. Функция совпадения FlashLock-пароля отключена.

Таким образом, эффективная поддержка зашифрованных битовых потоков для криптографической защиты данных в ПЛИС обеспечивается операцией шифрования FlashLock, запрещающей считывание или модификацию проекта после программирования.

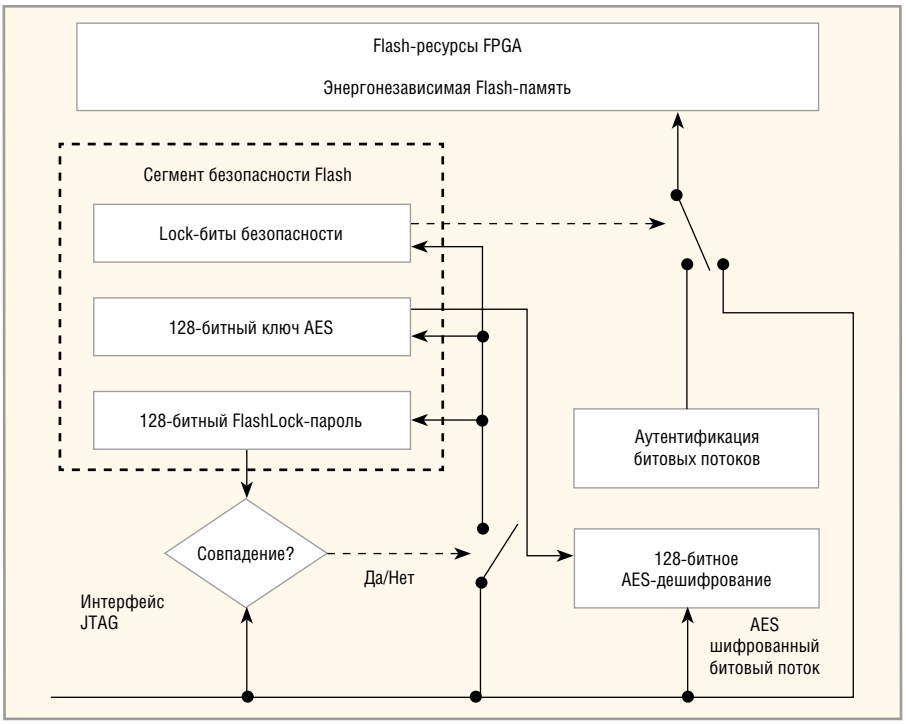

Рис. 5. Алгоритм работы проекта программирования секретного ключа для ПЛИС

Литература

1. *Chari S., Jutla C., Rao J., Rohatgi P.* Towards Sound Approaches to Counteract Power-Analysis Attacks // Advances in Cryptology. CRYPTO. Springer, 1999. Vol. 1666. P. 398–412.
2. *Kocher P.* Differential Power Analysis. CRYPTO. Springer-Verlag, 1999.
3. *Velegalati R., Yalla P.* Differential Power Analysis Attack on FPGA Implementation of AES. Technicalreport. http://bass.gmu.edu.
4. *Kocher P.* Timing attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems. CRYPTO. Springer-Verlag, 1996.
5. *McGrath Gartner D.* ASIC design starts to fall by 22% in 2009. EE Times. www.eetimes.com.