Дифференциальный анализ питания. (Differential Power Analysis).

Введение.

Большинство современных криптографических устройств выполнены на полупроводниковых логических элементах, построенных из транзисторов. Электроны, протекающие через кремниевую подложку, когда к транзисторному зазору приложен (снят) заряд, потребляют напряжение и испускают электромагнитное излучение.

Такие атаки, как дифференциальный анализ, позволяют проводить анализ таких устройств. Это не теоретические атаки. Криптографические исследования успешно используют эти атаки для анализа большого числа устройств, основанных на смарт-картах. В то время, как некоторые устройства стойки к Простому Анализу Питания (Simple Power Analysis), очень мало серийно-выпускаемых устройств, противостоящих дифференциальному анализу напряжений. Количество времени, необходимое для атаки зависит от типа атаки (DPA, SPA, и.т.д.) и от самого устройства. SPA атаки обычно занимают несколько секунд на карточку, а DPA атаки могут занимать несколько часов.

Технический обзор.

Базовые концепции новой методики вскрытия были сформулированы в известной работе Пола Кочера (1995 г.) "Криптоанализ на основе таймерной атаки" (Timing Attack Cryptoanalysis), показавшей, что можно вскрывать криптоустройства, просто точно замеряя интервалы времени, которые тем требуются на обработку данных. Криптографические устройства используют секретный ключ для обработки входной информации и/или для предоставления выходной информации. Разработчики протоколов предполагают, что у атакующих имеется входная и выходная информация, а информация о ключе не известна.

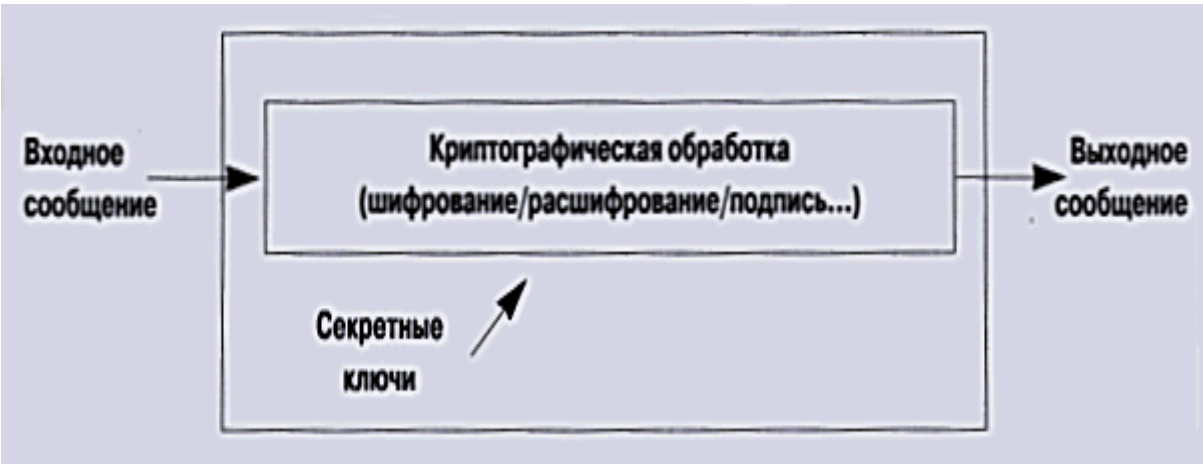


Рис. 1. Традиционные криптографические предположения

Атаки анализом напряжения (и родственные атаки, разработанные Полом Кохэром и Cryptography Research, включая синхронные атаки и дифференциальный анализ напряжения, использующие электромагнитное излучение) работают, потому что другая информация часто доступна атакующим.

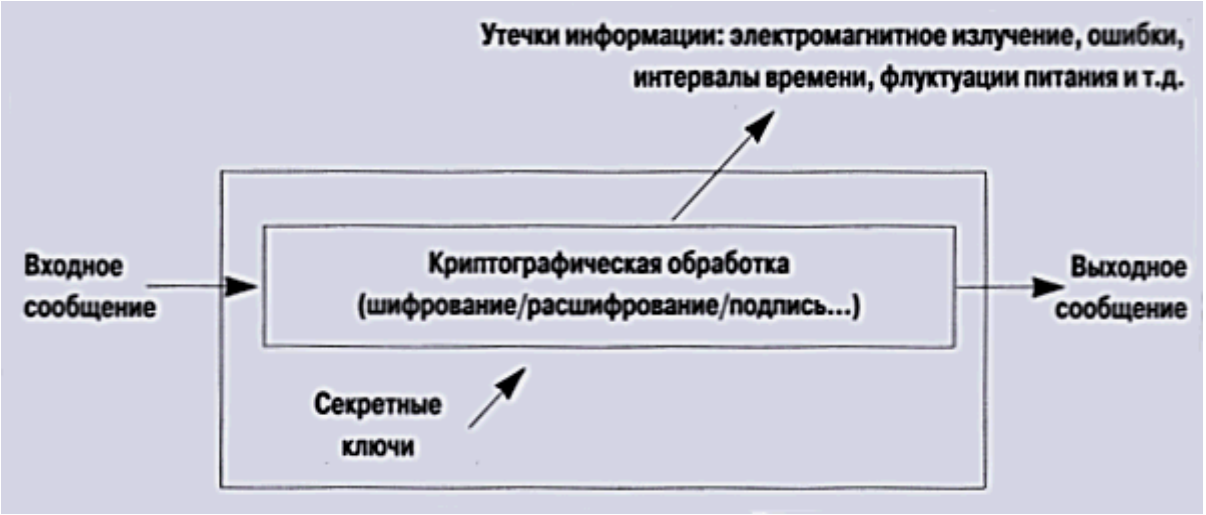
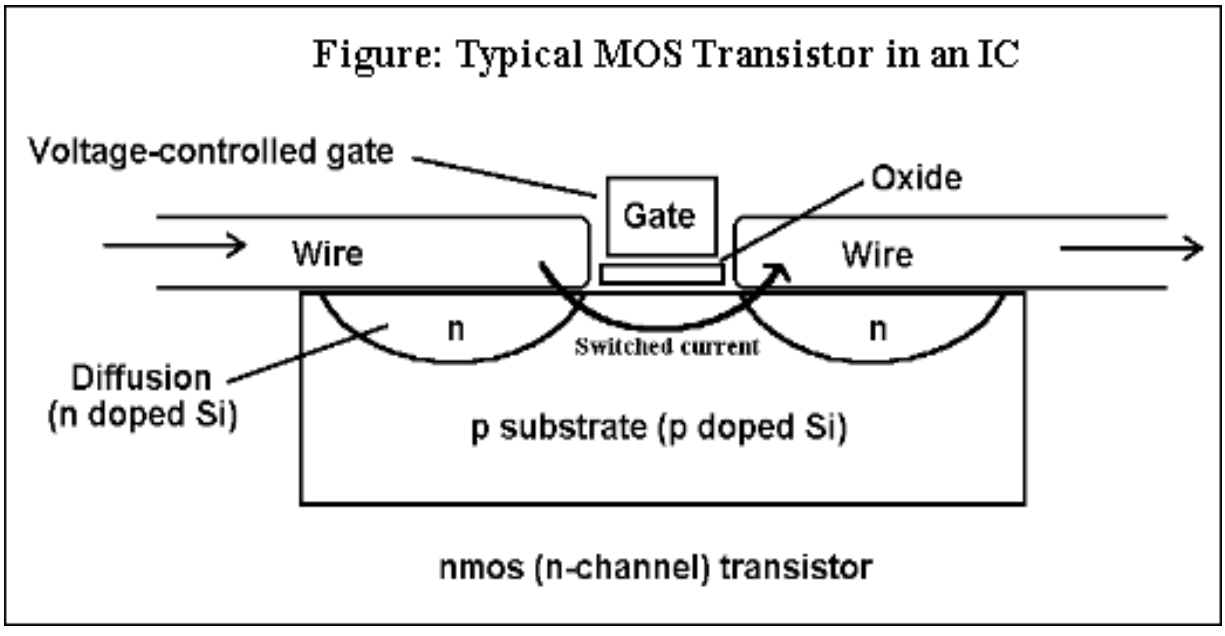


Рис. 2. Действительно доступная информация

Характеристики, необходимые для анализа, могут быть довольно точно измерены при выполнении устройством криптографических операций. В частности, простой амперметр, сконструированный из активной (омической) нагрузки, может быть использован для наблюдения потребления питания.

Изменение питания.

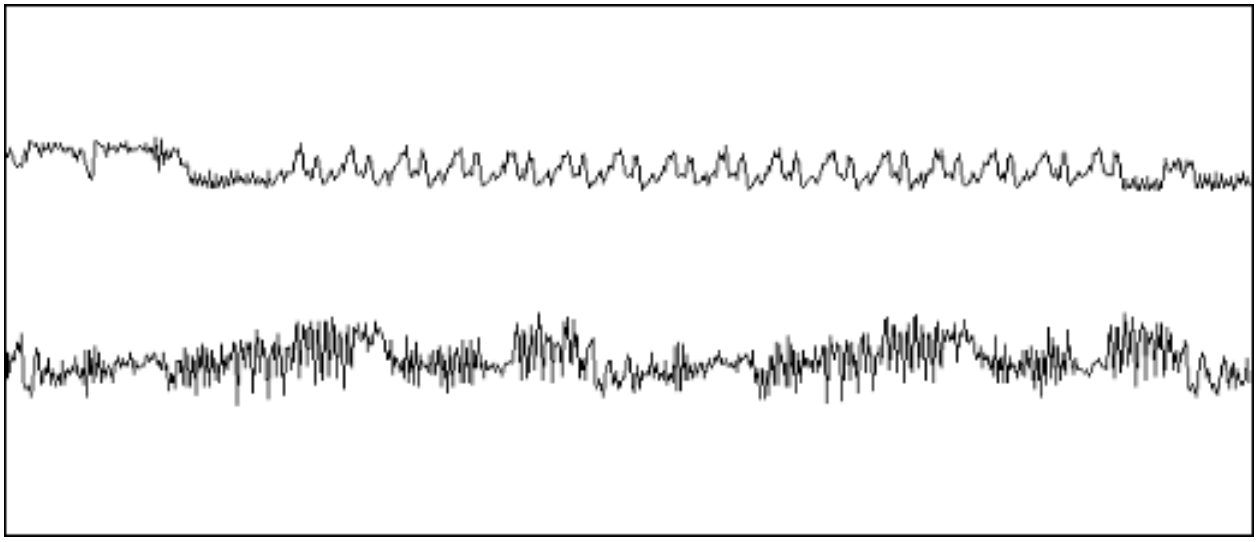
Интегрированная цепь построена из отдельных транзисторов, которые действуют как переключатели, контролирующие питание. Ток протекает через транзисторную подложку, когда к зазору приложен (или отведён) заряд. Этот ток затем доставляет заряд к зазорам других транзисторов, и другая цепь «загружается». Движение электрического заряда расходует питание и производит электромагнитное излучение, и эти два параметра внешне измеримы.



Поэтому, отдельные транзисторы предоставляют внешне наблюдаемое электрическое поведение. Так как микропроцессорные логические области выполняют регулярное переключение, это даёт возможность для лёгкого определения микропроцессорных характеристик (таких как процессорная активность) простым наблюдением потребленя питания. Атаки типа дифференциального анализа питания выполняют более сложную интерпретацию этих данных.

Простой Анализ Питания.*(Simple Power Analysis)*

В атаках простым анализом питания, криптоаналитик непосредственно исследует потребление питания системы. Количество потребляемой мощности изменяется в зависимости от выполняемых микропроцессором инструкций. Большие вычисления, такие как DES раунды, RSA операции и.т.д. могут быть идентифицированы, поскольку операции выполняемые микропроцессором меняются очень сильно в различных частях этих операций. При большом коэффициенте усиления отдельные инструкции могут быть различимы. Простой анализ питания может, например, быть использован для взлома RSA реализаций посредством выявления отличий между операциями умножения и извлечения корня. Аналогично, много DES реализации имеют видимые отличия в перемешиваниях и сдвигах, и могут таким образом быть взломаны, используя SPA. Несмотря на то, что Cryptography Research нашли много смарт-карт, уязвимых к SPA анализу, нет особой сложности, чтобы сделать SPA-устойчивые устройства.



Выше приведённый рисунок иллюстрирует SPA наблюдение простой DES операции, выполненной обычной смарт-картой. Верхняя кривая показывает операцию шифрования, включая начальное перемешивание, 16 DES раундов, и конечное перемешивание. Нижняя кривая детально показывает 2-й и 3-й раунды.

По отдельности эти кривые изображены ниже:

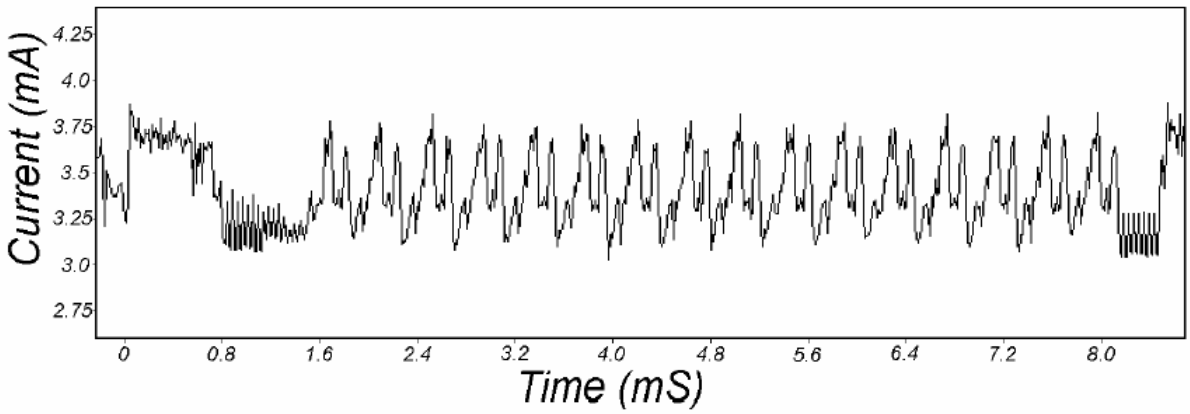


Figure 1: SPA trace showing an entire DES operation.

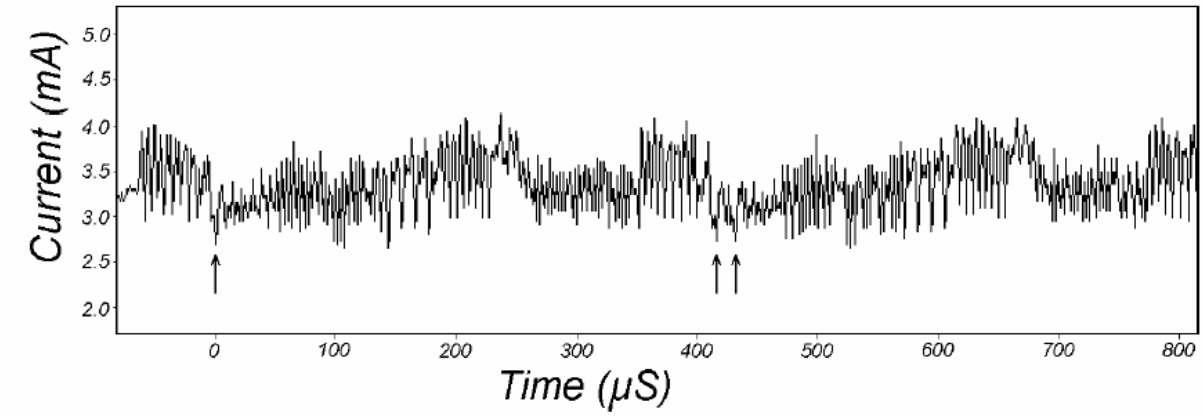


Figure 2: SPA trace showing DES rounds 2 and 3.

Дифференциальный Анализ Питания.*(Differential Power Analysis)*

Дифференциальный анализ питания является более мощной атакой, нежели SPA, и более сложен для предотвращения. В то время, как SPA атаки главным образом строятся на визуальном анализе с целью выделения значимых флуктуаций питания, DPA атака использует статистический анализ и технику коррекции ошибок для выделения информации, имеющей корреляции с секретными ключами. Для использования статической техники анализируются результаты 1000 транзакций.

Реализация DPA атак состоит из двух этапов: Накопление и анализирование данных. Накопление информации для DPA может быть выполнено, как описывалось ранее отбором проб потребляемого устройством напряжения во время криптографических операций как функцию от времени. Для DPA, множество криптографических операций, используют искомый ключ.

Следующие шаги представляют собой пример PDA атак обрабатываемых для технических считывателей. (Более детальная информация последует далее.) Следующие пояснения предполагают детальные знания DES алгоритма.

1. Делаются измерения потребления питания последних нескольких раундов 1000 DES операций. Каждый простой набор состоит из 100000 начальных установок. Собранная информация может быть представлена в двумерном массиве S[0…999][0…99999], где первый индекс - это номер операции, а второй индекс- это «проба». Для этого примера предполагается, что атакующий имеет ещё шифрованные тексты, C[0…999].
2. Атакующий далее выбирает ключе зависимую отобранную функцию D. В этом случае, отобранная функция будет иметь вид D(Ki,C), где Ki – некоторая ключевая информация, а C – это шифротекст. Например, целью атакующего является найти 6 битов ключа DES, который предоставляется как входной в DES S box 4, значит Ki – 6 битовый вход. Результат D(Ki,C) будет получен начальной перестановкой (Initial Permutation) на C для получения R и L, выполняя расширение E на R, извлекая 6-ти битовый входные данные в S4, делая операцию XOR с нужным битом (например, более значимым битом) из S результат отобран. Перестановка P применяется к биту. Результат D(Ki,C) функции устанавливается в 0, если однобитовая P перестановка результата и соответствующий бит в L равны, и иначе D(Ki,C) даёт 1.
3. Дифференциальная средняя запись T[0…63][0…99999] состоит из набора данных, используя результат функции D, В частности:
$$T[i][j] = \sum_{k=0}^{999}\left(D(i,C[k]) - \frac{1}{2}\right)(S[k][j])$$
4. Атакующим известно, что здесь есть одно корректное значение для Ki; другие значения некорректны. Цель атаки определить корректные значения. В записи T[i][0…99999] где i=Ki, D(i,C[k]) для каждого k будет соответствующее значение в нужном бите в L из DES операций перед тем как DES F функция была XORена. Когда устройство выполняет DES операции, значение этого бита было сохранено в регистрах, регулируемых в логических областях, и.т.д. … давая определяемые перепады питания. Таким образом, часть значений T[i=Ki], где те биты были представлены и/или манипулированны, набор «проб» T[i] покажет наклон потребления питания. Однако, для «проб» , таких что T[i!=Ki], значение D(i,C[k]) не будет соответствовать какой-либо операции на самом деле выполняющейся устройством. Как результат, запись T[i] не будет коррелировать с чем-нибудь действительно выполняющемся, и будет усреднена к нулю. (В действительности, T[i!=Ki] будет показывать малые флуктуации от статических свойств S таблиц. Однако, большие наклоны будут соответствовать большим значениям Ki.)
5. Шаги, описанные выше, затем повторяются для оставшихся S-блоков для нахождения 48 битного ключа для последнего раунда. Атака может быть повторена для нахождения предшествующих раундовых подключей (или оставшиеся 8 бит могут быть найдены используя 8-бит быстрый поиск.)

На картине, расположенной ниже показаны 4 кривые, полученные при использовании ввода открытого текста в DES функцию шифрования в смарт-карте. Вверху изображено среднее потребление питания во время DES операций. Внизу изображены три дифференциальных кривых, где первая представляет использование правильного варианта значения для K_s. Нижние две кривые представляют использование некорректного значения для K_s. Эти зависимости были подготовлены с использованием 1000 замеров. Хотя сигналы отчетливо видны, в них присутствует умеренное количество шума.

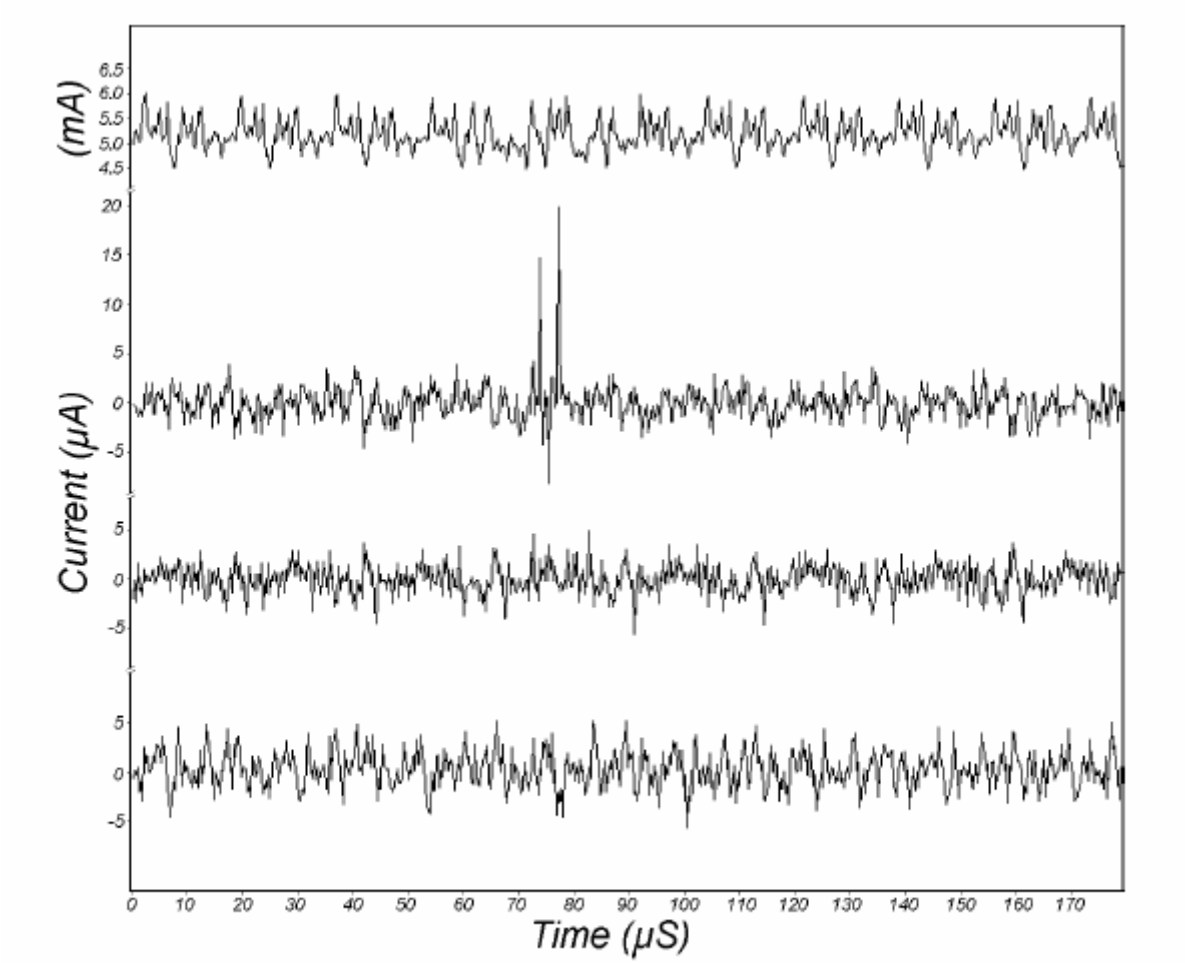


Figure 4: DPA traces, one correct and two incorrect, with power reference.

На изображении ниже, показан средний результат единичных бит при подробном замере потребления питания. Наверху показана кривая потребления питания. В середине показано квадратичное отклонение в замерах потребления питания. Наконец, последняя кривая представляет собой дифференциальную зависимость, полученную с $m=10^4$. Заметьте, что регионы, которые не коррелируют с битом ближе к нулю, чем другие значения, показывая тем самым, что небольшой шум или ошибка сохраняется.

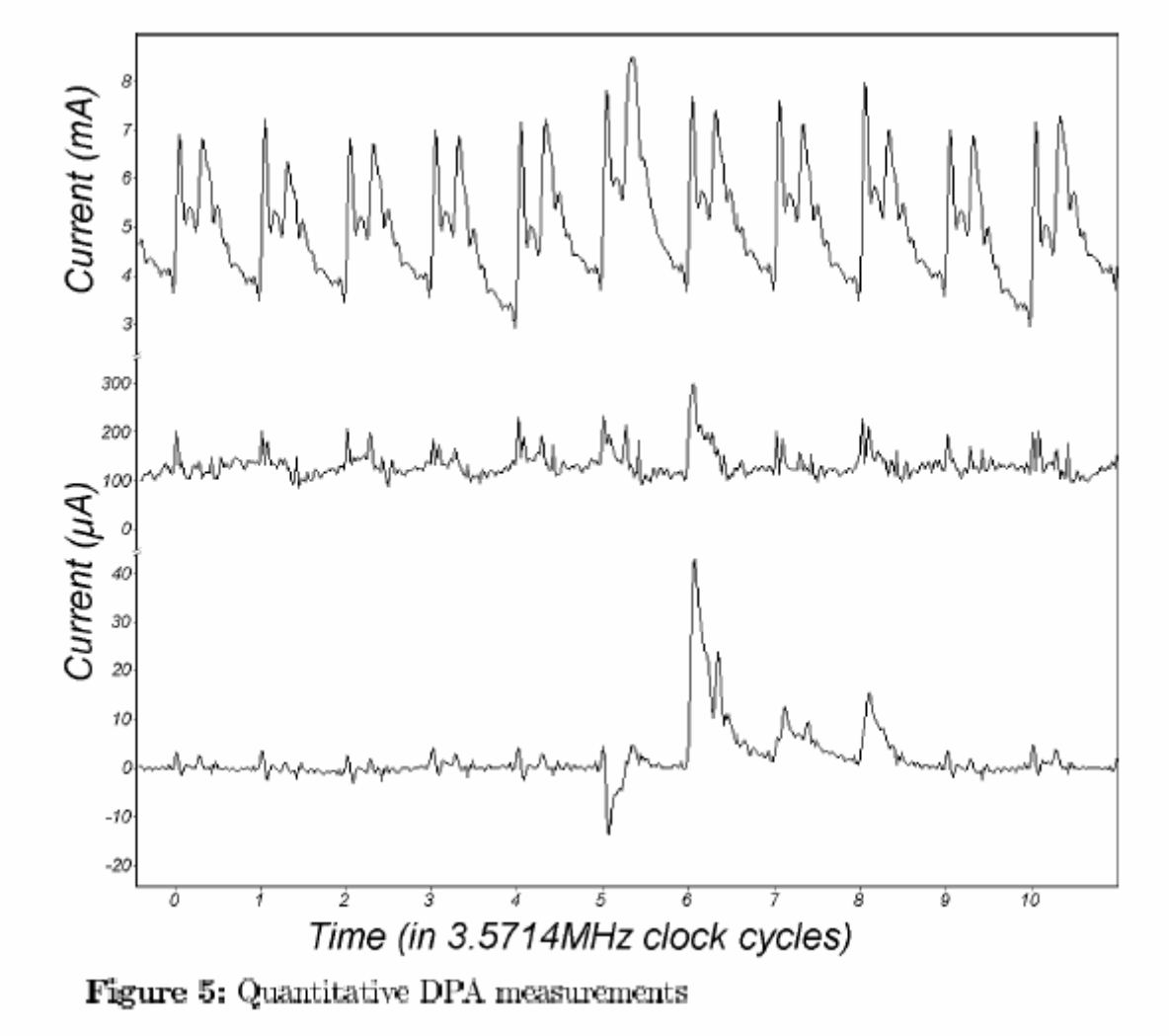
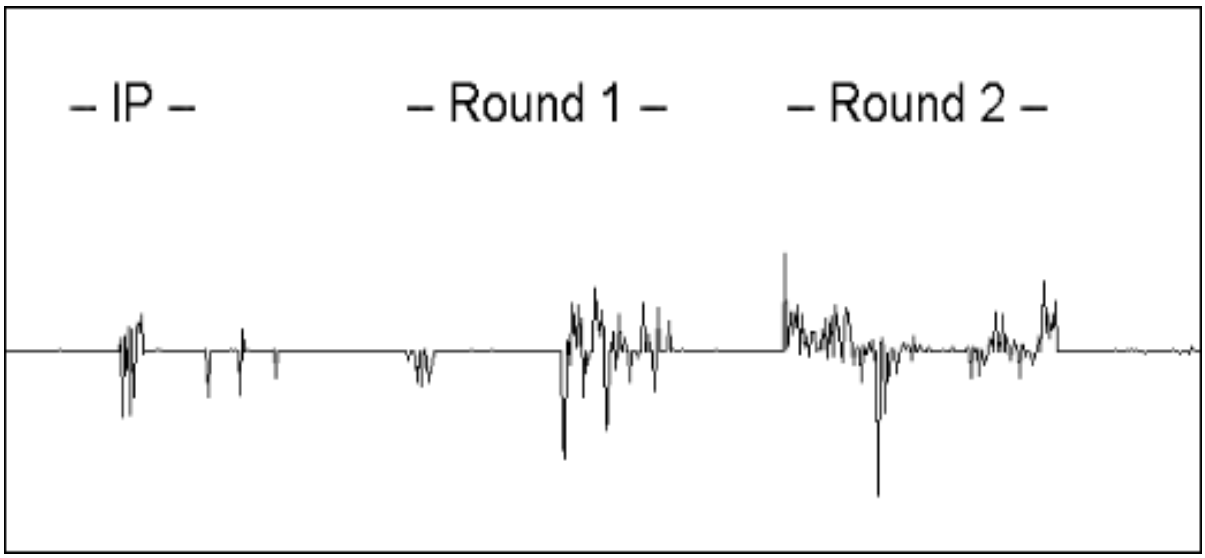


Figure 5: Quantitative DPA measurements

В то время, как эффекты одного переключающего транзистора будут нормальными будет возможно идентифицировать наблюдения потребления питания устройством, статические операции используемые в DPA способны достоверно определить очень малые различия между изменением питания.

Рисунок, приведённый ниже - это DPA кривая обычной смарт-карты, показывающая изменение потребления питания от выбранного одного входного бита к DES функции шифрования, используемой как генератор случайных чисел.(Функция D была выбрана равной значению 5-го бита нешифрованного текста). Входное начальное перемешивание помещает этот бит как часть R регистра, действующей в первом раунде F функции вычисления и результатах. Раунд 2 действует (из-за использования режима счётчика) ещё сильнее. Измерение было представлено 1000 замерами.



Дифференциальный анализ высокого порядка.
(High-Order Differential Power Analysis)

Еще более сложный метод анализа – HO-DPA. В то время как DPA-техника анализирует информацию между образцами данных на протяжении отдельного события, метод анализа дифференциалов высокого порядка можно использовать для коррелирования информации между многими криптографическими субоперациями. В DPA-атаках высокого порядка сигналы собираются от многих источников, для их сбора применяются различные техники измерения, а сигналы с различными сдвигами по времени комбинируются в процессе применения методов ДАП.

В высоко-порядковой DPA атаке, сигналы собираются из многих источников, сигналы собираются, используя технику различных измерений, также собираются сигналы с различными временными сдвигами во время применения техники DPA. В добавок, могут быть применены большинство дифференциальных функций (D), а также много «продвинутых» сигналообрабатывающих функций. Основные HO-DPA вычислительные функции являются более общей формой стандартных DPA функций, например:

$$T[i][j] = \mathbf{F}_0\left(\sum_{k=0}^{n}\mathbf{F}_1\left(D(i, C[k],...)\mathbf{F}_2\left(S_0[i][j], S_1[i][j], S_2[i][j],...\right)\right)\right)$$

На сегодняшний день HO-DPA представляет большой интерес для разработчиков систем и исследователей, так как не известно реально существующих систем, которые уязвимы к HO-DPA, но не уязвимы к DPA. Однако HO-DPA считается более эффективный, чем DPA.

Cryptography Research проводит реальные разработки для выявления проблем безопасности аппаратуры и их противостояния.

DPA и схожие атаки охватывают традиционные инженерные уровни абстракции. Пока большинство прежде известных криптоаналитических атак основаны на изучении криптографических алгоритмов, к DPA уязвимы транзисторы и режимы электрических цепей, операции микропроцессора, и.т.д.

Программное обеспечение и алгоритмы:

Наиболее эффективным решением для разработки реализации криптосистем является предположение, что существует утечка информации. Cryptography Research разработала подходы для существующих криптографических систем безопасности (включая RSA, DES, DSA, Diffie-Hellman, El Gamal, и Elliptic Curve systems), которые остаются ещё безопасными даже при предположении, что возможна утечка информации. В случаях, где физические аппаратные утечки чрезмерны, применяется техника уменьшения утечек и их маскировка.

Специалисты Cryptography Research разработали ряд методов противодействия DAP и связанным с ним атакам. В частности, создана конструкция полупроводниковой вентильной логики, обеспечивающая значительно меньший уровень просачивания информации. Для систем с физическими или стоимостными ограничениями в Cryptography Research разработаны аппаратные и программные методы, которые включают в себя сокращение просачиваемой информации, внесение шума в измерения, декоррелирование внутренних переменных и секретных параметров, а также декоррелирование по времени криптографических операций (П. Кочер, Д. Джаффе, В. Джун "Введение в дифференциальный анализ питания").

Заключение:

Техника анализа питания это крутая фишка, так как очень большое количество устройств, уязвимых этой технике используется. Атаки легки для выполнения, имеют низкую стоимость на устройство, и проводятся без непосредственного контакта, что делает их выявление сложным. Так как DPA автоматически размещает коррелированные регионы в потреблении питания устройства, атака может быть автоматической и малой. В конечном счёте, эти атаки не теоретические, и не ограничиваются применением к смарт-картам. Только надёжные по отношению к DPA решения могут иметь реальные перспективы. DPA выставляет на первый план необходимость людям, которые разрабатывают алгоритмы, протоколы, программное обеспечение, и аппаратную часть работать вместе для производства защищённых изделий.

Ссылки:

1. R. Anderson, M. Kuhn, \Low Cost Attacks on Tamper Resistant Devices," Security Protocol Workshop, April 1997, http://www.cl.cam.ac.uk/ftp/users/rja14/tamper2.ps.gz.
2. R. Anderson and M. Kuhn, \Tamper Resistance { a Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, November 1996, pp. 1-11.
3. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
4. E. Biham and A. Shamir, “Diffrential Fault Analysis of Secret Key Cryptosystems," Advances in Cryptology: Proceedings of CRYPTO '97, Springer-Verlag, August 1997, pp. 513-525.
5. D. Boneh, R. DeMillo, and R. Lipton, \On the Importance of Checking Cryptographic Protocols for Faults," Advances in Cryptology: Proceedings of EUROCRYPT '97, Springer-Verlag, May 1997, pp. 37-51.
6. Jameco Electronics, “PC-MultiScope (part #142834)," February 1999 Catalog, p. 103.
7. P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology: Proceedings of CRYPTO '96, Springer-Verlag, August 1996, pp. 104-113.
8. M. Matsui, \The First Experimental Cryptanalysis of the Data Encryption Standard," Advances in Cryptology: Proceedings of CRYPTO '94, Springer-Verlag, August 1994, pp. 1-11.
9. National Bureau of Standards, \Data Encryption Standard," Federal Information Processing Standards Publication 46, January 1977.
10. National Institute of Standards and Technology, \Secure Hash Standard," Federal Information Processing Standards Publication 180-1, April 1995.
11. J. Dhem, F. Koeune, P. Leroux, P. Mestr_e, J. Quisquater, and J. Willems, \A practical implementation of the timing attack," UCL Crypto Group Technical Report Series: CG-1998/1, 1998.
12. R.L. Rivest, A. Shamir, and L.M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21, 1978, pp. 120-126.
13. Проблемы защиты смарт-карт.