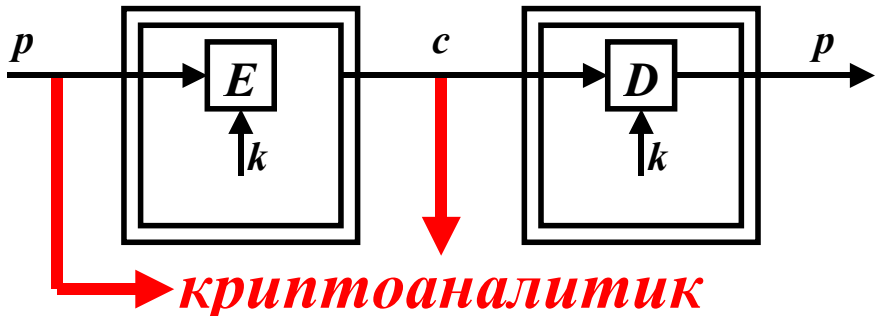
Жуков А.Е.

Криптоанализ по побочным каналам (Side Channel Attacks)[*)]

Атаки по сторонним или побочным каналам (side channel attacks, SCA) – это вид криптографических атак, использующих информацию, полученную по ***сторонним или побочным каналам*** [1]. Под информацией из побочных каналов понимается информация, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом.

Обычно предполагается, что криптографические вычисления реализуются в виде идеальных “чёрных ящиков” в том смысле, что текущее состояние вычислительного процесса закрыто от враждебного наблюдателя. Единственной информацией, доступной криптоаналитику, является общая структура алгоритма шифрования, шифртекст и, зачастую, соответствующий ему открытый текст. С учётом этих допущений, уровень безопасности определяется исходя из математических свойств криптоалгоритма и вычислительных возможностей криптоаналитика. Заметим, что и в классическом криптоанализе наличие какой-либо дополнительной информации (например знание промежуточной гаммы) существенно снижает стойкость системы.



- **Криптоанализ только по шифртексту (*Ciphertext only attack*)**
- **Криптоанализ по известному открытому тексту (*Known plaintext attack*)**
- **Криптоанализ по выбранному открытому тексту (*Chosen plaintext attack*)**
- **Криптоанализ по выбранному шифртексту (*Chosen ciphertext attack*)**

[*)] Доклад на конференции *РусКрипто 2006*

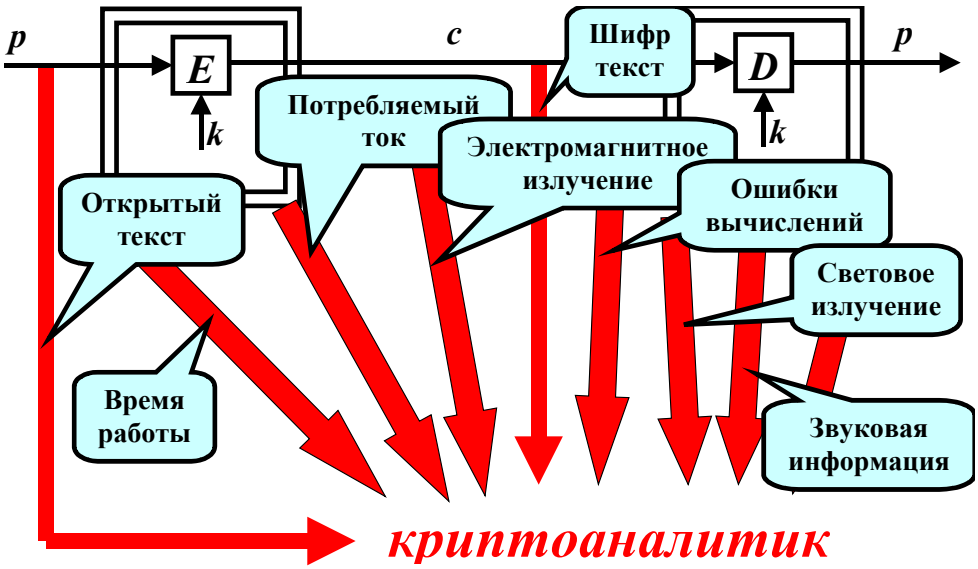
В то же время криптографический примитив можно рассматривать как минимум с двух точек зрения: с одной стороны, как абстрактный математический объект, а именно преобразование некоторых входных данных в некоторые выходные, возможно, параметризованное ключом; с другой стороны, этот примитив должен быть внедрён в программу, которая будет запускаться на некоем процессоре, в некой среде, и, следовательно, будет иметь специфические характеристики. В реальности криптоалгоритмы всегда встроены в программное обеспечение или аппаратные средства на физических устройствах, взаимодействующих с окружающей средой и подверженных её влиянию.

Первая точка зрения соответствует “классическому” криптоанализу, вторая – побочному.

Почти все осуществленные на практике удачные атаки на криптосистемы используют слабости в реализации и размещении механизмов криптоалгоритма. Эти слабости часто позволяют взломщикам полностью обойти защиту или существенно ослабить её теоретическую стойкость. Такие атаки основаны на корреляции между значениями физических параметров, измеряемых в разные моменты во время вычислений (потребление энергии, время вычислений, ЭМИ и т.п.), и внутренним состоянием вычислительного устройства, имеющим отношение к секретному ключу. Именно эту корреляцию между побочной информацией и операциями с секретным ключом пытается обнаружить SCA.

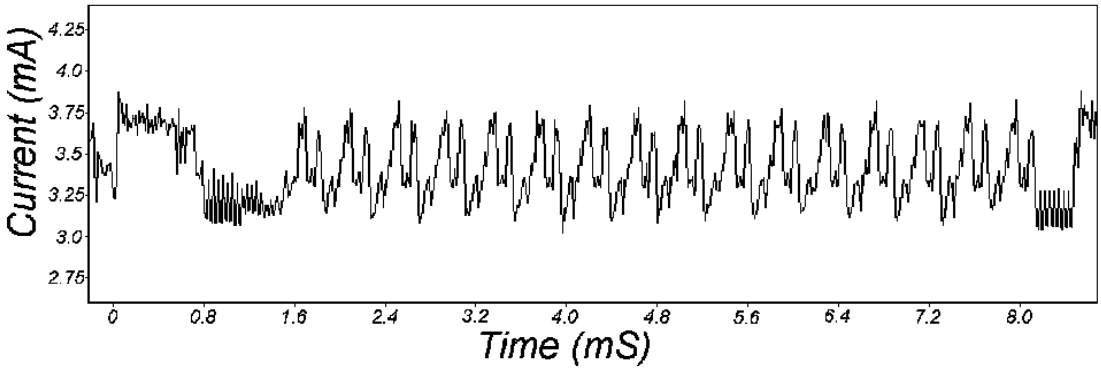
На практике SCA на много порядков более эффективны, чем традиционные атаки, основанные только на математическом анализе шифрующего алгоритма. Атаки по побочным каналам используют особенности реализации для извлечения секретных параметров, задействованных в вычислениях. Такой подход менее обобщённый,

поскольку привязан к конкретной реализации, но как правило более мощный, чем классический криптоанализ.



Итак, как уже говорилось, обычный криптоанализ рассматривает криптоалгоритмы как чисто математические объекты, в то время как криптоанализ по побочным каналам также принимает во внимание их реализацию. Поэтому атаки SCA также называют атаками на реализацию (implementation attacks).

В последние годы резко возросло количество криптографических атак, использующих особенности реализации и рабочей среды. Такие атаки SCA собирают физическую информацию о работе криптографического устройства и не рассматриваются в традиционных криптографических моделях безопасности. Например, противник может отслеживать энергию, потребляемую смарт-картой, когда она выполняет операции с закрытым ключом, такие, как расшифрование или генерация подписи.



SPA trace showing an entire DES operation.

Противник может также замерять время, затрачиваемое на выполнение криптографической операции, или анализировать поведение криптографического устройства при возникновении определённых ошибок. На практике побочную информацию собрать порой несложно, поэтому нужно обязательно учитывать угрозу SCA при оценке защищённости системы

Следует отметить, что конкретная атака на побочный канал в некоторых средах может не представлять угрозы. Например, атаки, измеряющие потребление энергии криптографического устройства, весьма вероятны, если устройство представляет собой смарт-карту, питающуюся от внешнего, недоверенного источника. Но если устройство – компьютер, расположенный на охраняемой территории, то подобная атака не представляет угрозы.

Классификация атак по побочным каналам

Атаки по побочным каналам классифицируются по следующим трём типам [2]:

- По контролю над вычислительным процессом: ***пассивные*** и ***активные***.
- По способу доступа к модулю: ***агрессивные*** (invasive), ***полуагрессивные*** (semi-invasive) и ***неагрессивные*** (non-invasive).
- По методу, применяемому в процессе анализа: ***простые*** – simple side channel attack (***SSCA***) и ***разностные*** – differential side channel attack (***DSCA***).

Известные атаки через побочные каналы и способы противодействия.

Еще раз отметим, что SCA использует информацию, полученную из реализации криптографических алгоритмов и протоколов. Эти данные могут представлять собой замеры времени, расхода мощности или электромагнитного излучения. Другими формами информации из побочного канала могут быть результаты вычислений при программных или аппаратных ошибках.

Отсюда вывод, что конкретная реализация очень важна для безопасности, и малейшее различие в реализации может привести к большой разнице в безопасности.

На сегодняшний день выделено более десяти побочных каналов. Рассмотрим наиболее важные из них.

Атака по времени (Timing attacks).

Это – самая первая из атак по побочным каналам, появившаяся в гражданской криптографии [3]. Вычисления в реализациях криптографических алгоритмов часто выполняются за различные интервалы времени. Если при этом из этого разброса времени можно получить некоторую информацию о скрытых параметрах и если иметь достаточно знаний о конкретной реализации, то точный статистический анализ мог бы полностью восстановить эти скрытые параметры. Атака по времени основана на измерении времени, необходимого модулю шифрования для выполнения операции шифрования. Это информация может вести к раскрытию информации о секретном ключе. Например, тщательно измеряя время, требуемое для выполнения операции экспоненцирования $\boldsymbol{a}^{\boldsymbol{x}}$ в алгоритме Diffie-Hellman, атакующий может найти вес секретной экспоненты $\boldsymbol{x} = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0)$ (если бит $x_i = 1$ то выполняется дополнительная инструкция) и даже ее точное значение.

Вычисление $y = a^x$ по схеме Горнера:
Вход: $\boldsymbol{x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0)}$

$\boldsymbol{R \leftarrow 1}$
for $\boldsymbol{i = n-1}$ **to 0**
  $\boldsymbol{R \leftarrow R^2}$
  if $\boldsymbol{x_i = 1}$ **then** $\boldsymbol{R \leftarrow R * a}$
next $\boldsymbol{i}$
$\boldsymbol{y = R}$

Для определения точного значения $\boldsymbol{x}$ используется следующая математическая модель [3]: Пусть t_i – независимые одинаково распределенные случайные величины, равные времени вычисления i-й

итерации в схеме Горнера. Задавая значения $x_{b-1}, \ldots, x_1, x_0$, можно вычислить параметры случайной величины $r_{b-1}+\ldots+r_1+r_0$, где r_i распределены так же, как t. Рассмотрим дисперсию случайной величины

$$(t_{n-1}+\ldots+t_1+t_0) - (r_{b-1}+\ldots+r_1+r_0) =$$
$$= (t_{n-1}+\ldots+t_{b+1}+t_b) +(t_{b-1}- r_{b-1}) +\ldots+ (t_1- r_1) + (t_0- r_0)$$

Она равна $(n-b+2(b-c))D_t = (n+b-2c)D_t$, где c – число угаданных битов в $x_{b-1}, \ldots, x_1, x_0$, а D_t – дисперсия случайной величины t.

Зачастую время обработки данных в криптосистемах немного изменяется в зависимости от входных значений. Это является следствием оптимизации производительности и широкого круга иных причин. Характеристики выполнения зависят как от ключа шифрования, так и от входных данных (например, открытого текста или шифртекста).

По существу, атака по времени – способ получения какой-либо скрытой информации путем точного измерения времени, которое требуется пользователю для выполнения криптографических операций. Один простой подход по защите – добиться независимости параметров вычисления от входных данных. Выполнимость такого подхода зависит от вычисления. Например, в RSA можно накладывать случайные данные (зашумление) на параметры перед выполнением операции для того, чтобы сбить с толку, а затем произвести обратные действия.

На самом деле с момента написания статьи Кочера [3] (1996) пользователям RSA решительно рекомендовалось использовать зашумление. Другое средство противостояния атакам такого рода – устранить условные переходы в реализации алгоритма, чтобы время шифрования было одинаковым.

Эффективность предложенных средств такова: накладывание шума ослабляет силу временной атаки, добавляя около 2-10% вычислительных

расходов, но не устраняет ее, тогда как удаление ветвлений часто устраняет атаку, но за весьма значительную цену [2].

Другой – инженерный – подход к защите – разработать аппаратные средства так, чтобы выполнение для выполнения каждой операции требовалось постоянное время, вне зависимости от данных.

Атаки по энергопотреблению. Атаки по мощности (Power Analysis Attacks).

Конечно, атака по анализу мощности пригодна в основном для аппаратной реализации криптосистем. Атака по анализу мощности особенно эффективна и успешно выполняется при атаке на смарт-карты и другие системы, в которых хранится секретный ключ.

Существует огромное множество литературы, посвященной атакам по мощности и средствам противостояния этим атакам [2]. За последние годы было опубликовано больше 200 статей по данному вопросу. В настоящее время исследования побочных каналов большей частью сосредоточены на атаках по анализу энергопотребления.

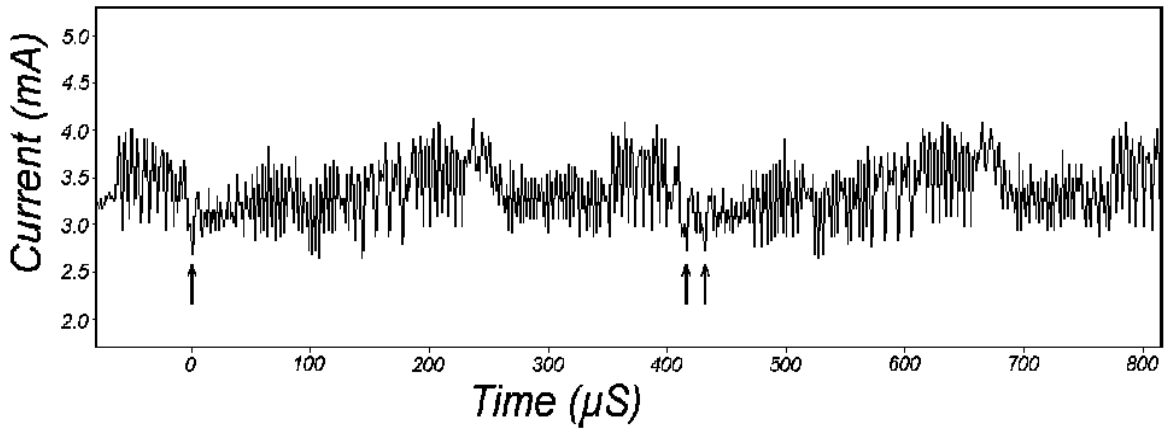
Чтобы измерить потребляемую схемой мощность необходимо последовательно с цепью питания или заземления подключить резистор малого сопротивления (например, 50 ом). Падение напряжения, деленное на сопротивление, даст силу тока. Современные лаборатории располагают оборудованием, способным производить цифровые измерения напряжения на исключительно высоких частотах (более 1 ГГц) и с превосходной точностью (ошибка менее 1%). Устройства, способные измерять с частотой от 200 МГц, и подключаемые к компьютеру стоят менее $400 [4].

По существу атака по мощности может быть разделена на простую (SPA) и разностную (DPA). Целью SPA является информация о конкретных выполняемых инструкциях в системе и о конкретных обрабатываемых данных. Эта информация получается по параметрам мощности. Согласно [5], простая атака по мощности (Simple Power Analysis) для смарт-карт обычно

занимает несколько секунд, в то время как проведение разностной атаки по мощности (Differential Power Analysis) может занять несколько часов.

Простая атака по мощности (Simple Power Analysis).

Простая атака по мощности обычно основывается на визуальном анализе потребляемой мощности во время работы алгоритма шифрования. Кроме того криптоаналитику нужны точные данные о реализации алгоритма. Этот метод использует непосредственные данные измерений, собранные во время выполнения криптографических операций и может дать как сведения о работе устройства, так и информацию о ключе. Так стрелками на рисунке отмечены моменты записи единичных битов ключа.



SPA trace showing DES rounds 2 and 3.

Разностная атака по мощности (Differential Power Analysis).

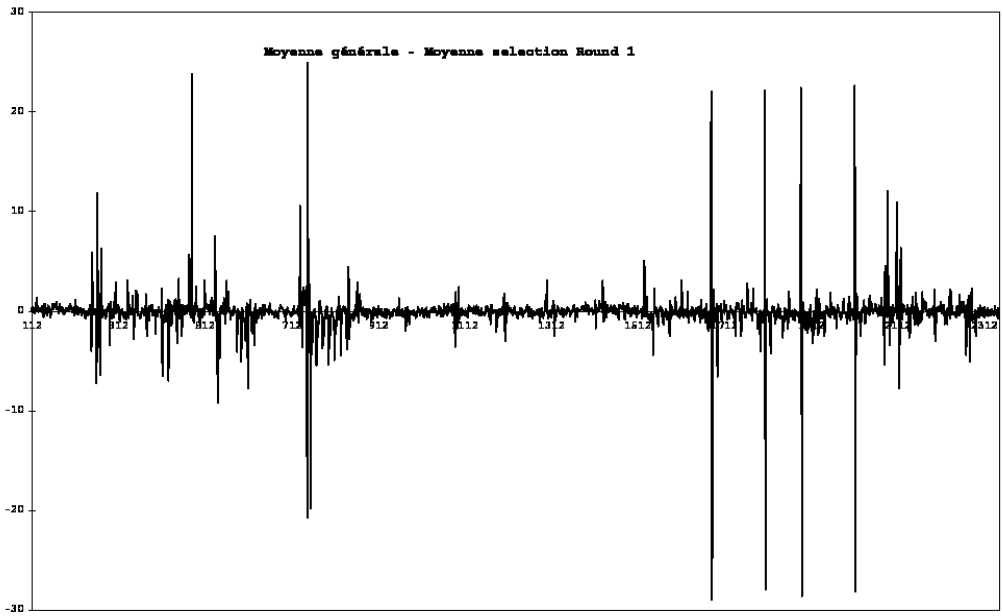
DPA – одно из самых мощных средств для проведения атак, использующих побочные каналы, причем эта атака требует очень маленьких затрат. Один из вариантов данного подхода, может обнаружить ключи DES, используя менее, чем 15 испытаний для большинства смарт-карт.

В отличии от простых атак, разностные атаки, основанные на анализе потребляемой мощности, включают в себя не только визуальное наблюдение,

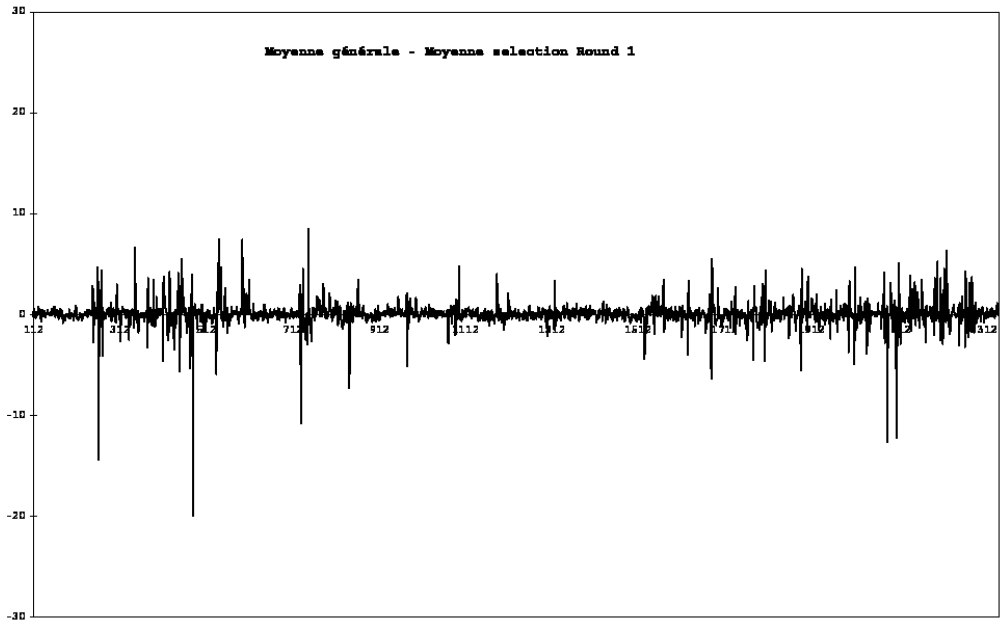
но так же статистический анализ и статистические методы исправления ошибок для получения информации о ключах.

Помимо огромного количества причин изменения энергопотребления, связанных с последовательностью выполнения инструкций, существуют так же причины, тесно связанные с информацией, которая обрабатывается. Эти изменения достаточно малы и иногда «затемняются» ошибками измерения и другим шумом. В таких случаях возможно взломать систему, используя статистические функции, привязанные к алгоритму шифрования. При этом DPA зачастую не нуждается в данных о конкретной реализации и в качестве альтернативы использует статистические методы анализа.

Для этого криптоаналитик делает предположение о ключе и использует это предположение и функцию выбора D, например выход какого-то S-блока, чтобы разделить замеры на две части: одна, для которой значение параметра равняется 0 и другая, для которой оно равно 1. Замеры усредняются в каждой группе и затем рассматривается разница между этими усредненными замерами. Если предположение о ключе было неверным, эти две группы некоррелированны, и разность усредненных замеров уменьшается с ростом размера выборки (см. рис., приведенные ниже) [4].



Difference of the curves MC and MC' when the 6 bits are correct



An example of difference of the curves MC and MC' when the 6 bits are false

Атаки по ошибкам вычислений (Fault Attacks).

Ошибки аппаратного обеспечения, появляющиеся во время работы соответствующего криптографического модуля, фактически серьезно затрагивают его безопасность. Это ошибочное поведение или ошибочные выходные данные могут стать важными побочными каналами и даже иногда существенно увеличивают уязвимость шифра к криптоанализу. Разностный анализ по ошибкам (DFA) состоит в изучении результата работы алгоритма шифрования в нормальных и ненормальных условиях при одном и том же входе (открытом тексте) [7]. Ненормальные условия обычно получаются созданием ошибки в процессе (кратковременная ошибка) или перед процессом (постоянная ошибка) работы.

Атаки по ошибкам на криптографические алгоритмы изучаются с 1996 года [6] и с того времени почти все криптографические алгоритмы были подвергнуты таким видам атаки .

Осуществимость атаки по ошибкам (или по крайней мере ее эффективность) зависит от возможностей злоумышленника вызывать ошибки в системе специально или пользоваться сбоями естественного

происхождения. Ошибки наиболее часто происходят из-за скачков напряжения, сбоев тактовой частоты или из-за излучений различных типов. В основном ошибки классифицируются по следующим аспектам:

- Точность, которую нарушитель может достичь при выборе времени и места, где появляется ошибка во время работы криптографического модуля.
- Длина данных, на которые влияет ошибка: например, только один бит.
- Постоянство ошибки: является ли ошибка кратковременной или постоянной.
- Тип ошибки: например инверсия одного бита, изменение одного бита, но только в одном направлении (например, с 1 на 0), изменение бита на случайное значение и др.

В общем, успешная атака по ошибкам на криптографические модули или устройства требует двух шагов: шаг создания ошибки и шаг использования ошибки. Ошибки могут быть вызваны в смарт-картах путем внешнего влияния на нее и помещения ее в неправильные условия. Некоторые из них – аномальное и внезапное понижение или повышение напряжения, температуры, излучения, освещения и др.

DFA широко изучены с теоретической точки зрения и кажутся применимыми почти ко всем симметричным криптосистемам.

Атаки по электромагнитному излучению (ElectroMagnetic Analysis).

Будучи электрическими устройствами, компоненты компьютера излучают электромагнитное излучение во время выполнения операций. Нарушитель, который может наблюдать эти излучения и понять их связь с выполняющимися вычислениями и используемыми данными, возможно, сможет получить значительную информацию об этих вычислениях и самих данных. Мерам борьбы с электромагнитным излучением посвящена большая

литература и большое количество нормативных документов. Как и атаки по анализу мощности, атаки по электромагнитному анализу могут быть также разделены на две большие категории: простые (SEMA) и дифференциальные (DEMA) [8], [9], [10].

Возможность использования электромагнитных излучений уже известна в военных кругах в течение длительного времени. Например недавно рассекреченный документ TEMPEST, изданный Национальным Агентством Безопасности (NSA), исследует различные компрометирующие излучения, включая электромагнитное, излечения проводов и распространение акустического сигнала. Имеется обширная несекретная литература по средствам таких атак и методам борьбы с ними. Например, Кун (Kuhn) [10] описывает способ осуществления и предотвращения атак, основанных на обработке информации с экрана монитора, полученной из его электромагнитного излучения. Quisquater [9] и Gandolfi [8] впервые представили результаты экспериментов для атак по анализу ЭМ излучения криптографических устройств, таких как смарт-карты, и сравненили такие атаки с атаками по анализу мощности.

Атака по видимому излучению (Visible Light Attacks).

Кун (Kuhn) [11] продемонстрировал (как с помощью сложного анализа, так и экспериментально), что средняя яркость света, излучаемого монитором и отраженного от стены, может помочь при восстановлении сигнала, изображенного на CRT (поэтому защита CRT только от утечки информации через ЭМ излучение недостаточно). Особенностью такой атаки является то, что она не требует физического доступа к устройству.

Акустическая атака (Acoustic Attacks).

Хотя большинство исследований атак через побочные каналы сосредоточены на электромагнитных излучениях, потреблении мощности и с недавнего времени рассеянию видимого света с CRT дисплеев, Шамир в [12] продемонстрировал предварительное доказательство того, что существует связь между звуком процессора и проводимыми им вычислениями.

Атаки на кэш (Cache-based Attacks).

Если процессор осуществляет доступ к данным, которые не хранились в КЭШе, т.е. если появляется недостаток кэш-памяти, то в вычислениях произойдет некотороя задержка, пока необходимые данные не будут загружены из основной памяти в КЭШ. Измерение такой задержки может дать возможность нарушителю определить частоту переполнения КЭШа. Именно здесь и возникает побочный канал утечки, близко связанный с атаками по времени [13].

Предотвращение атак по внешнему каналу

Маскирование (Blinding)

Методы, используемые для подписи «вслепую», могут быть приспособлены для защиты обрабатываемых данных. Это должно защитить практически от всех видов атак по внешнему каналу.

Вычисления, не зависящие от данных

В идеале время выполнения операций, выполняемых модулем, не должно зависеть от обрабатываемых данных. Другими словами, время, которое требуется на выполнение операции, должно быть полностью независимым от входных данных и значения ключа. Если в зависимости от

значения битов входа или ключа выполняются различные подоперации, то эти подоперации должны выполняться за одинаковое количество тактов.

Возможность сделать время выполнения операции постоянным для любых данных предотвращает все временные атаки.

Условные переходы

Отказ от процедур, которые используют для условных переходов секретные промежуточные значения или ключи, замаскирует многие характеристики атак по внешнему каналу.

В идеале программная реализация кода не должна содержать операторов ветвления. Аналогично, они не должны содержать операторы условного выполнения, такие как IF. Вычисления должны выполняться через функции, использующие элементарные операции (такие как AND, OR и XOR) и не использующих ветвление и условное выполнение участков кода.

Добавление задержек

Наиболее очевидный путь предотвратить временные атаки – сделать так, чтобы все операции занимали одинаковое время. К сожалению, это не всегда возможно. Кроме того реализации с фиксированным временем, вероятно, будут медленными; многое из оптимизации не может применяться, т.к. все операции должны занимать столько времени, сколько требуется для самой медленной из них.

Уравнивание времени умножения и возведения в квадрат

Время, затрачиваемое устройством на умножение и на возведение в степень должно быть одинаковым. Благодаря этому свойству злоумышленник не сможет узнать когда и сколько было выполнено умножений, и сколько возведений в степень.

Уравнивание времени может быть достигнуто путем выполнения обеих операций независимо от того, какая из них необходима в данный

момент. На любом этапе, если потребовалась одна операция, то должны быть выполнены обе, а результат одной из них проигнорирован.

Балансировка потребляемой мощности

По возможности должны применяться методы балансировки потребляемой мощности. Следует добавить неиспользуемые (с точки зрения алгоритма) регистры и вентили, на которых выполняются бесполезные операции для того, чтобы сделать уровень потребляемой энергии постоянным значением.

Такие методы, с помощью которых энергопотребление (если смотреть извне) остается постоянным и не зависит от битов входа и ключа, предотвращают все виды атак по каналу энергопотребления.

Добавление шума

Средства защиты от ЭМ атак по специфичности реализации разделяются на две широкие категории: уменьшение мощности сигнала и уменьшение информативности сигнала.

Второй подход против DPA включает внесение шумов в измерения потребляемой мощности. Одно из предложенных решений в [15] против DPA с использованием шума заключается в добавлении случайных вычислений, которые увеличивают уровень шума настолько, что становится невозможным определить смещения всплесков DPA.

Экранирование

На практике сильное физическое экранирование, как замечено в [4], может сделать атаки невыполнимыми, но при этом существенно влияет на размеры и стоимость устройства.

Выполнение шифрования дважды

Возможное решение (представленное в [7]) против атак по ошибкам вычислений заключается в прогоне шифрования дважды и выдаче результата, только если они совпадают.

Исследования в области криптоанализа по побочным каналам

Два новых проекта, имеющих отношение к исследованиям SCA в Европе, привлекли внимание криптографической общественности, особенно тех, кто интересуется атаками SCA. Это проекты SCARD (Side Channel Analysis Resistant Design Flow) [16] and ECRYPT (European Network of Excellence for Cryptology) [17]. Оба этих проекта – международные совместные проекты Европейских исследователей из криптографических научно-исследовательских институтов и соответствующих отраслей промышленности.

В проекте SCARD предлагается улучшить стандартный ход разработки микрочипа – от высокоуровневого описания системы и описания транспортного уровня до сетевого списка вентильного уровня, а также размещение и направление микрочипа – для обеспечения возможности разработки цепей и систем, устойчивых к анализу побочных каналов. Более того, планируется изучить целиком, шаг за шагом, явление побочного анализа и предоставить подходящие инструменты для анализа, а также инструменты для разработчиков систем безопасности. Эти дополнения к традиционному ходу разработки считаются необходимыми для обеспечения возможности разработки следующего поколения защищённых устройств.

ECRYPT – созданная 4 года назад сеть, финансируемая Information Societies Technology Programme of the European Commission. Она стремится к глобальной надёжности и структуре безопасности, и её цель – усилить сотрудничество Европейских исследователей, занимающихся информационной безопасностью, в частности, криптологией и цифровыми водяными знаками. Для достижения этой цели, 32 ведущих участника объединяют усилия в пяти виртуальных лабораториях, специализирующихся в различных областях исследования, одна из которых – безопасные и

эффективные реализации (VAMPIRE). Одна из четырёх рабочих групп VAMPIRE – группа исследователей, занимающихся анализом SCA.

Уже из этих двух проектов можно сделать вывод, что в Европе ведутся интенсивные совместные международные исследования атак SCA.

Литература

1. http://en.wikipedia.org/wiki/Side_channel_attack
2. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. http://eprint.iacr.org/200?/388.pdf
3. P. Kocher. *Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems*. CRYPTO'96, LNCS 1109, pp.104-113, 1996.
4. P. Kocher, J. Jaffe, B. Jun. *Differential power analysis*. CRYPTO'99,LNCS 1666,pp.388-397,1999.
5. J. Black, H. Urtubia. *Side-channel attacks on symmetric encryption schemes: the case for authenticated encryption*. Proc of 11th USENIX Security Symposium, pp.327-338, 2002.
6. D. Boneh, R.A. DeMillo, R.J. Lipton. *On the importance of checking cryptographic protocols for faults*. EUROCRYPT '97,LNCS 1233, pp.37-51,1997.
7. E. Biham, A. Shamir. *Differential fault analysis of secret key cryptosystems*. CRYPTO '97,LNCS 1294,pp.513-525,1997.
8. K. Gandolfi,C.Mourte,F. Olivier. *Electromagnetic Analysis: Concrete Results*. CHES 2001,LNCS 2162,pp.251-261, 2001.
9. J.J. Quisquater, D. Samyde. *Electromagnetic analysis (EMA): measures and counte- rmeasures for smart cards*. E-smart 2001,LNCS 2140,pp.200–210,2001.
10. M.G. Kuhn, R.J. Anderson. *Soft tempest: hidden data transmission using electromagnetic emanations*. Information Hiding 1998,LNCS 1525,pp.124-142,1998.
11. M. Kuhn. *Optical Time-Domain Eavesdropping Risks of CRT Displays*. Proc of the 2002 Symposium on Security and Privacy, pp.3-18,2002.

12. A. Shamir, E.Tramer. *Acoustic cryptanalysis: on nosy people and noisy machines*. Eurocrypt 2004 rump session, 2004.

13. Y. Tsunoo, T. Saito, T. Suzaki, M. Shigeri, H. Miyauchi.*Cryptanalysis of DES Implemented on Computers with Cache*. CHES 2003, LNCS 2779, pp.62–76, 2003.

14. S. Chari, C. Jutla, J. Rao, P. Rohatgi. *Towards sound approaches to counteract power-analysis attacks*. CRYPTO'99, LNCS 1666,pp398-412,1999.

15. T.S. Messerges, E.A. Dabbish, R.H. Sloan, *Examining smart-card security under the threat of power analysis attacks.* IEEE Trans. Computers, 51(5), pp.541-552, 2002.

16. http://www.scard-project.org/

17. http://www.ecrypt.eu.org/