能量分析攻击及其防御策略研究

李 欣 范明钰
（电子科技大学 信息安全研究中心）

摘 要：针对密码系统的旁路攻击已从时间攻击发展到更为有效的能量分析攻击阶段。本文即从两类能量分析攻击方式的原理入手，对其产生背景、技术原理、实施手段等进行了详细介绍，并在其中引入具体攻击DES算法的实例。最后，给出了针对此类攻击的防御策略。

关键词：能量分析 SPA DPA 防御策略

引 言

当前，针对密码算法的研究已经进入一个白热化时代，各种曾经看似“牢不可破”的强密码算法接连被推翻。其中，我国学者王小云教授成功破解MD5算法便是一例。而对于以密码算法为核心的安全芯片而言，继续采用仅仅针对其密码算法的攻击方式就显得片面。事实上，密码系统的安全性在与其所采用的算法息息相关的同时，其硬件体系设计、工作原理以及工作进程中的安全性同样重要。这一点在现实中往往被忽视，从而成为密码系统安全性链条中的薄弱环节。

本文所阐述的能量分析攻击(Power Analysis Attacks)[1]，就是针对密码系统运行时的能量泄漏所进行的攻击。通过对泄漏信息的分析，获得安全芯片内部的运算执行情况，从而获取密钥，破译系统。作为旁路攻（Side-channel Attacks）[2]的一种，能量分析攻击已经成为极其有效的攻击手段，因此防御此类攻击的研究也显得尤为重要和紧迫。

能量分析攻击

就密码系统的攻击方式而言（图1），传统观点认为：仅有输入信息和输出信息对于攻击者是可用的，事实上并非如此：在系统进行加解密及处理密钥的工作进程中泄漏出的信息同样可用，甚至更有价值。（见图1）

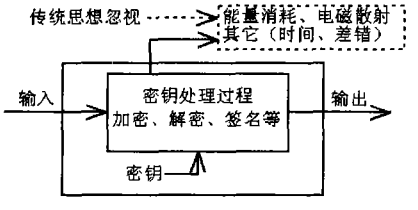

图1 传统观点与现实不符

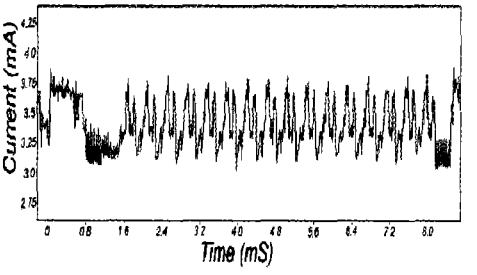

图2 DES算法的SPA轨迹图

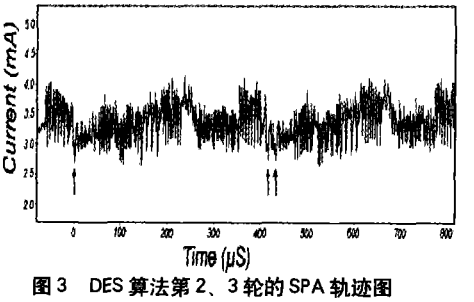

图3 DES算法第2、3轮的SPA轨迹图

密码系统的运作由半导体逻辑门执行，逻辑门由受电压控制的晶体管构成。电流流经晶体管底层，电荷在晶体管逻辑门上加载或卸载。电流再将电荷释放给其它晶体管逻辑门、线路以及电路负载。充放电的过程消耗了能量，产生了电磁辐射，这些都可为外界检测和获取。同时，微处理器逻辑单元的晶体管遵循一定的“开－关”规则，因而通过监听能量消耗就有可能识别其宏观特性。能量分析攻击正是基于以上原理进行的，其基础建立在Paul Kocher于1995年提出的时间攻击(Timing Attacks)[3]之上。

一般地，可将能量分析攻击分为两类[1]：简单能量分析（Simple Power Analysis，SPA）攻击和差分能量分析(Differential Power Analysis，DPA)攻击。

1．简单能量分析(SPA)攻击

简单能量分析(Simple Power Analysis，SPA)[1, 4, 8]直接观察和检测系统能量消耗。能耗大小直接取决于微处理器输入指令、处理数据和运行算法的不同。对于不同操作对象，微处理器的能量消耗具有显著变化。通过绘制能量消耗轨迹图，再辅之以数据加密算法理论来分析，即可确定密码设备及其采用加密算法的主要特

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

征细节。比如，RSA[3]中乘法和开方运算的区分，DES[5]中置换和移位操作的区分。

能耗轨迹图由密码设备工作时的一组能量消耗测量结果组成，比如以1ms为单位以5MHz的频率采样可产生一个包含5000个样本点的轨迹图。以一张采用DES算法[6, 7]的智能卡芯片的能耗轨迹图（图2）为例，就可以清晰地看到DES16轮运算的电流变化状况。

图3则是同一轨迹更高精度的us级描绘，图形展示了DES加密操作在进行第二轮和第三轮运算时的电流变化。从中可以看到：56-bit密钥分为两个28-bit之后，在第二轮进行了一个比特的循环左移，而在第三轮则是两个比特左移。于是，建立在密钥比特移位和中间运算基础之上的特定条件触发的可见的能量变化就成为SPA攻击成功的根本原因。

图4展现了两种不同运算的能耗轨迹图，均在以3.5714MHz为频率的七个时钟周期内。不同微处理器指令产生不同的能量消耗从而导致不同时钟周期内的图形差异。图中上面的轨迹是SPA中跳转指令的执行规律，而下面的轨迹则是未使用跳转指令的情况。可以明显地看到，差异出现在第六个时钟周期内。

正是由于SPA能够揭示指令的操作执行次序，因此可以用来有效地攻击运作过程依从于被处理数据的执行顺序和执行路径的密码系统。例如：

——DES密钥表：计算密钥表时，包含一个28位密钥的循环移位运算。该运算根据最末一位的不同而采取相反的规则。此时，“0”“1”的能耗轨迹必然有所差别，通过SPA分析即可很快获取有用信息。

——DES置换：DES算法执行过程中，需要进行大量的置换运算。如果运算存在条件分支，必然会有随着“0”“1”的不同引发能耗的差异。

——比较：比较运算一定伴随“0”“1”判断，从而产生SPA易于识别的大量特征。

——乘法：乘法运算与操作数和汉明重量密切相关，大量密码芯片的内部信息可由此获得。

——幂运算：幂运算就是在其指数为“1”时反复执行乘法操作。如果平方和相乘具有不同的能量消耗特征、使用不同的时间、或者由不同的指令区分，那么指数同样可以被获取。

2. 差分能量分析（DPA）攻击

建立在SPA基础之上的DPA[1, 4]更具有攻击性。在SPA中，一系列的指令操作会导致容易检测的、易于视觉观察的大规模能耗变化，若被操作数据间的相互关系由于能量变化小、检测出错、或噪声干扰等原因被掩盖，SPA就很难获取有效信息；而DPA则会使用统计分析方法和纠错技术来提取密钥的相关信息。其分析过程可分两个阶段：数据采集和数据分析。数据采集就是对正在工作的密码系统进行能耗采样，并作出时间 能耗轨迹图；数据分析则是采用统计学方法，精心设计针对目标算法的统计函数来鉴别能耗的细微差别，从而获取密钥信息。

下面以DPA方式同样攻击DES算法[1, 7]为例做具体说明。

图5为DES中S盒的生成过程，32bit的输入R扩展为48bit后与48bit密钥K进行每6bit相异或的运算，之后进入S盒过程。将8个S盒的4bit合并后实施置换的操作，是DES算法安全性的焦点，上一轮S盒的输出对下一轮多个S盒产生影响。因为S盒的输入与密钥K非线性相关，这便为DPA攻击提供了切入点。DPA分析过程如下：

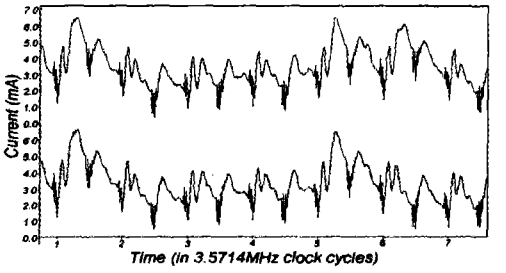

图4 不同时钟周期内的SPA轨迹图

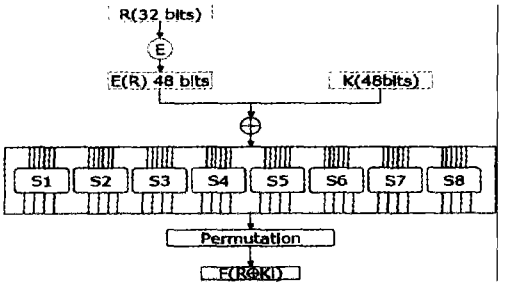

图5 DES中S盒的输入与输出

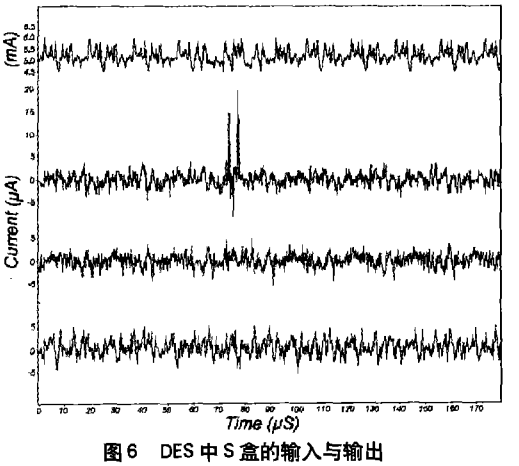

图6 DES中S盒的输入与输出

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

选择区分函数（Partition Function）$F(\ )$作用于S盒的输出函数，通过猜想密钥K_i来产生S盒输出，并假定此输出发生在固定时间且该时间点不随输入变化而变化。对每一个输入，在S盒的计算过程中检测并收集离散时间能量信号样本点$S_i(j)$，这里i为输入I的参数，j为时间采样点。使用区分函数$F(\ )$用以下公式将$S_i(j)$分为两部分：

$$S_0=\{S_i(j)|F(PTI_i)=0\} \qquad S_1=\{S_i(j)|F(PTI_i)=1\}$$

对于每一个输入I，如果区分函数$F(\ )$的输出为0，则对应的$S_i(j)$信号划分为一类，记作S_0；输出为1的划分为另一类，记作S_1。此时，能量消耗的差异变得非常明显。

继续使用公式：$Avg(S_0)=\frac{1}{|S_0|}\sum_{S_i(j)\in S_0}S_i(j)$

$$Avg(S_1)=\frac{1}{|S_1|}\sum_{S_i(j)\in S_1}S_i(j)$$

两式相减就得到信号的差分量：$T(j)=|Avg(S_0)-Avg(S_1)|$

差分量$T(j)$较大时，由区分函数划分的两个信号在j时刻就具有较大的能量消耗。由此，芯片处理数据中的"0""1"值在较好的区分函数的选择下一一明确。

图6为已知明文的DES加密芯片的能耗轨迹图。第一条为DES运作过程中平均能耗的参考能量曲线，下面三条为不同猜想下的K_i最终产生的差分量曲线，显然可见第一条的K_i猜想正确。

在DPA的基础上，还提出了一种改进型的高阶差分能量分析(High Order-Differential Power Analysis,HO-DPA)。HO DPA综合分析多源采集到的信号、不同测量技术采集到的信号、以及具有不同时间偏移量的信号。其处理函数更具一般性和通用性。

能量分析攻击的防御策略

1. SPA的防御

防御SPA攻击的技术思想并不复杂：避免在进行条件分支操作时使用密钥或其它有价值的中间变量就可以掩盖大量的SPA信息特征；用创造性的编码使得算法固化在各个分支内部可以避免条件选择时信息的泄漏；对于采用对称密码算法的系统进行金属外壳屏蔽可将可探测的能量消耗减小；另外，人为在能量消耗中加入噪声或添加额外的计算程序也是防御SPA攻击的有效办法。

2. DPA的防御

防御DPA攻击的技术大致可分为以下几类[4]：

(1) 减小信号强度。其主要实现途径包括：进行连续执行路径编码、选取能耗中泄漏更少信息的算法、平衡汉明重量和状态变换、对设备实施物理屏蔽等。

(2) 在能耗测量时加入随机噪声。噪声将扰乱或湮没安全芯片运作中泄漏出的有效信息，大大降低DPA分析成功的概率。

(3) 在算法中使用非线性密钥。这会使密码系统的运作过程与其能耗轨迹难以相互对应，达到扰乱DPA分析的目的。

(4) 引入随机过程中断(Random Process Interrupt，RPI)指令。在CPU指令的正常执行序列中插入虚拟指令，打乱有效指令的执行次序，使得能耗轨迹与真实有效指令不匹配；或采用时间转移策略令算法与该算法运行时间点不匹配。从而抵御DPA攻击的成功实施。

结 论

能量分析攻击不同于常规针对加密算法或安全系统的"强攻"策略，其原理设计巧妙、实施设备简易；为非入侵性攻击，不易察觉，不留痕迹；可自动进行，不需相关目标信息。因而对此类攻击及其防御手段的研究已经且必将继续成为安全领域的热点。

参考文献

[1] P. Kocher, J. Jaffe and B. Jun. Differential Power Analysis. In Advances in Cryptology, CRYPTO'99. 1999. Springer LNCS 1666. 386-397.

[2] N.P.Smart. Physical Side-Channel Attacks on Cryptographic Systems. Software Focus. 2000. 1(2): 6-13.

[3] P.Kocher. Timing attacks on implementations of Diffie-Hellman, RSA,DSS and other systems. In Advances in Cryptology, CRYPTO' 96. 1996. Springer LNCS 1109. 104-113.

[4] T.Messerges, E.Dabbish, R.Sloan. Investigations of Power Analysis Attacks on Smartcards. Proceedings of USENIX Workship Smartcard Technology. 1999. 151-161.

[5] National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46. 1999.

[6] E.Biham and A.Shamir. Differential Cryptanalysis of the Data Encryption Standard. 1999. Springer-Verlag.

[7] L.Goubin, J.Patarin. DES and Differential Power Analysis. Proceedings of CHES' 99, Lecture Notes in Computer Science. 1999. vol.1717, Springer-Verlag. 158-172.

[8] E.Hess, N.Janssen, B.Meyer, T.Schutze. Information Leakage Attacks Against Smart Card Implementations of Cryptographic Algorithms and Countermeasures. Proceedings of EUROSMART Security Conference, 2000. 55-64.

[9] C.Clavier, J.Coron, N.Dabbous. Diferential Power Analysis in the Presence of Hardware Countermeasures. Proceedings of Cryptographic Hardware and Embedded Systerms(CHES2000). Lecture Notes in Computer Science. 2000. 252-263.

[10] L.Benini, A.Macii, E.Macii. etc. Energy-Aware Design Techniques for Differential Power Analysis Protection. DAC-40: ACM/IEEE Design Automation Conference. 2003. 36-41.

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net