智能卡芯片中 TDES 密码电路的差分功耗攻击

欧海文[1,2], 李起瑞[1,2,3], 胡晓波[3], 赵　静[1,3]
(1. 西安电子科技大学 通信工程学院, 西安 710071; 2. 北京电子科技学院, 北京 100070; 3. 北京中电华大电子设计有限责任公司, 北京 100102)

摘　要: 使用相关性分析方法进行差分功耗攻击 (DPA) 实验,成功攻击了 TDES 密码算法。结果表明,相关性分析方法对简单的功耗模型具有很好的攻击效果且实施简单,对于 HD 功耗模型,获得 TDES 每一轮的圈密钥所需最少曲线条数仅为 3 500 条;同时,由于 TDES 和 DES 电路的实现结构相同,对两者进行 DPA 攻击的方法相同。

关键词: 智能卡芯片; 相关性分析; 功耗模型; 三重加密标准; 差分功耗攻击
中图分类号: TN918　　**文献标志码**: A　　**文章编号**: 1001-3695(2012)03-0927-03
doi:10.3969/j.issn.1001-3695.2012.03.035

Experimental implementation of DPA attacks on TDES design on smartcard

OU Hai-wen[1,2], LI Qi-rui[1,2,3], HU Xiao-bo[3], ZHAO Jing[1,3]
(1. *School of Telecommunications Engineering*, *Xidian University*, *Xi'an* 710071, *China*; 2. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 3. *CEC Huada Electronic Design Co.*, *Ltd*, *Beijing* 100102, *China*)

Abstract: This paper used the correlation analysis method, and firstly conducted a successful DPA attacks on TDES hardware implementation. Experimental results show that for the simple power consumption models, correlation attacks provide good results and are extremely easy to manipulate. With the Hamming distance model, the lowest number of traces needed to successfully reveal the each round key is approximately 3 500 power traces. Meanwhile, the DPA attacks on TDES and DES are same because of their same implementation structure.

Key words: smartcard chip; correlation analysis technique; power consumption model; triple data encryption standard (TDES); differential power analysis (DPA)

差分功耗攻击(DPA)是一种快速、低成本、可实施的密码芯片攻击技术,可以有效获取密码芯片中的关键数据和密钥,已严重威胁到了智能卡芯片的安全性。自 1998 年由 Kocher 等人[1]提出后,DPA 得到了国内外学者和厂商的广泛关注。

1　功耗攻击的物理基础

DPA 研究的是加密电路的功率信号与密码系统的密钥等敏感数据的相关性。目前,绝大多数的芯片都是采用 CMOS 技术,CMOS 门电路是由上拉 P-MOS 晶体管和下拉 N-MOS 晶体管电路构成的。PN 结是互补的,当输入电流稳定时,只有一个结导通。图 1 是一个典型的 CMOS 反相器的结构,以其为例来说明 CMOS 门电路的功耗。

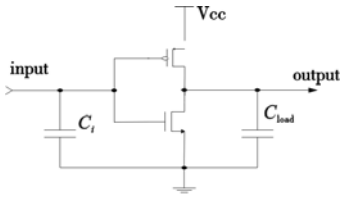

图1　CMOS反相器结构

a)反向泄露电流产生的静态功耗 $p_{leakage}$,很小,约占整体功耗的 5%。

b)反相器发生 0 到 1 或 1 到 0 变化时,从源到地的短路电流功耗 $p_{short_circuit}$,约占整体功耗的 15%。严格地讲,0 到 1 和 1 到 0 变化时的两种功耗大小是有差别的,但是这种差别显然远小于发生翻转与保持之间的功耗差异,可以忽略。

c)逻辑门翻转引起负载电容充放电导致的动态功耗的 p_{switch},相对前两项,这部分功耗是电路功耗的主要部分,约占 80%。反相器的动态功耗 p_{switch} 表达式为

$$p_{switch} = C_L V_{DD}^2 P_{0\to1} f \tag{1}$$

其中:C_L 是负载电容;V_{DD} 是电源电压;$P_{0\to1}$ 是 0 到 1 翻转的概率;f 是输入更新的频率。因此,CMOS 电路的功耗模型可以表示为

$$P_{total} = p_{leakage} + p_{short_circuit} + p_{switch} \tag{2}$$

如果芯片中一个 CMOS 门改变了状态,这种改变势必影响电路功耗的变化,可以在电源 V_{DD} 端串联电阻予以监测,这是进行 DPA 分析的物理基础。

2　功耗模型

DPA 研究的是加密电路的功率信号与密码系统的密钥等敏感数据的相关性。功耗大小与处理数据的大小和类型直接相关,这种关系在门电路一级表现为 CMOS 门电路充放电的次数;在寄存器一级表现为寄存器单元 0、1 之间翻转的次数;在

收稿日期: 2011-07-10; **修回日期**: 2011-08-18

作者简介:欧海文(1963-),男,教授,硕导,博士,主要研究方向为密码编码、密码应用技术等;李起瑞(1985-),男,硕士研究生,主要研究方向为信息安全、侧信道攻击与防御技术(liqiruihenan@163.com);胡晓波(1980-),女,高级工程师;赵静(1987-),女,硕士研究生,主要研究方向为信息安全、随机数发生器等.

操作数一级表现为原始操作数与结果之间的汉明距离 HD (Hamming distance)[2] 的大小,原始操作数与结果之间的汉明距离模拟芯片中数据处理时的功耗情况。汉明距离模型为

$$W = HD(r, r') = HW(r \oplus r') \tag{3}$$

其中:W 表示模拟功耗值;HW 表示数据的汉明重量(Hamming weight);r 和 r' 分别表示寄存器变化前后的状态;$HW(r \oplus r')$ 表示 r 和 r' 的汉明距离。在程序中用不同类型的变量可以模拟不同的寄存器,如可用 4 位的变量模拟一般芯片中的 4 位寄存器,用上述汉明距离模型就可以对加密过程中寄存器的翻转进行模拟。

3　差分功耗分析

差分功耗分析根据采集到的 N 条功耗曲线,通过使用各种统计分析方法获得密码芯片功耗信号中携带的密钥信息。

3.1　相关性分析[3]

在进行 DPA 分析时,输入 N 个不同的随机明文进行加密运算,并采集对应的 N 条功耗曲线 $S_d[j]$, $d = 1, \cdots, N$, d 表示不同的明文输入,j 表示信号采样的时间点。将这些曲线作对齐处理,这是 DPA 进行的前提条件。下面使用皮尔森相关公式来计算实际的功耗曲线与中间数据的相关性。

$$r_{i,j} = \frac{\sum_{d=1}^{N}(h_{d,i} - \overline{h_i}) \cdot (t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{N}(h_{d,i} - \overline{h_i})^2 \cdot \sum_{d=1}^{N}(t_{d,j} - \overline{t_j})^2}} \tag{4}$$

其中:i 表示假想的子密钥 K_b;$t_{d,j}$ 表示第 d 条功耗曲线上采样点 j 处的功耗值;$\overline{t_j}$ 表示所有功耗曲线上采样点 j 处的平均功耗值;$h_{d,i}$ 表示对应于子密钥 i 的第 d 条功耗曲线上根据功耗模型计算出的功耗值,结合第 2 章中功耗模型,可以假定 $h_{d,i}$ 表示中间数据如(S-Box 输出值)的汉明距离或汉明重量;$\overline{h_i}$ 表示对应于子密钥 i 的所有功耗曲线的平均功耗,结合第 2 章中功耗模型,可以假定 $\overline{h_i}$ 表示中间数据(如 S-Box 输出值)的平均汉明距离或平均汉明重量。式(4)也可用于计算功耗曲线与输入明文或输出密文之间的相关性,这时不再需要假想的子密钥 i,变为

$$r_j = \frac{\sum_{d=1}^{N}(h_d - \overline{h}) \cdot (t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{N}(h_d - \overline{h})^2 \cdot \sum_{d=1}^{N}(t_{d,j} - \overline{t_j})^2}} \tag{5}$$

此时,假想的功耗 h_d 表示输入密文或输出密文的 1 bit 或 1 Byte 的汉明重量或汉明距离。

当计算完所有采样点处 $r_{i,j}$ 的值后,会得到对应于不同假想子密钥 i 的所有相关曲线,其中出现最高尖峰的曲线所对应的子密钥 i 为正确的猜想子密钥。同样,对于 r_j 而言,曲线上尖峰越高,输入密文或输出密文与功耗曲线的相关性就越大。

3.2　均差分析

与相关性分析方法相比较,均差分析方法只是在功耗数据的计算方法上不同。同样,在分析过程中,首先输入 N 个不同的随机明文进行加密运算,并采集对应的 N 条功耗曲线 $S_d[j]$, $d = 1, \cdots, N$, d 表示不同的明文输入,j 表示信号采样的时间点;然后建立一个分堆函数 $D(\mathrm{CTO}, K_b) \rightarrow \{0, 1\}$, CTO 是密文,$K_b$ 是密钥的一部分。根据假定的 K_b 值计算 D 函数的值,将功耗曲线分为两堆:

$$S_0 = \{S_d[j] \mid D = 0\} \quad S_1 = \{S_d[j] \mid D = 1\} \tag{6}$$

令

$$T[j] = \frac{1}{S_1}\sum_{S_d[j] \in S_1} S_d[j] - \frac{1}{S_0}\sum_{S_d[j] \in S_0} S_d[j] \tag{7}$$

其中:$|S_0| + |S_1| = N$。如果功耗曲线的样本空间足够大,采样噪声的影响足够小,模型 D 选择适当,$T[j]$ 就会出现明显的尖峰值,说明所猜测的 K_b 是正确的;否则,猜测错误。对于 DES 算法的一个 S-Box 最多,需要猜测 2^6 次,如此循环,可以确定一轮中所有 S-Box 对应的子密钥。主密钥中剩余的 8 位可通过穷举攻击或再分析一轮运算获得整个主密钥。

相关性分析方法对于简单的功耗模型来说具有较好的攻击效果且实施简单,尤其是它不需要先对平台设备进行噪声评估[4]。文献[5]中比较了上面两种方法,指出相关性分析所需测量样本数量比均差分析方法少一半。所以,本文使用相关性分析方法对智能卡芯片中 TDES 算法进行 DPA 攻击。

4　DPA 攻击过程

4.1　TDES 的 DPA 攻击

DES 算法采用 64 位明文输入和 64 位密钥输入,经过一系列变换得到 64 位密文输出。其结构如图 2 所示。

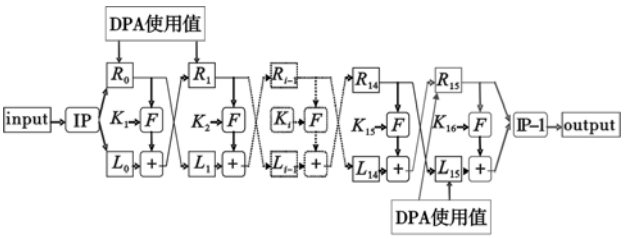

图2　DES结构及功率泄露点

目标芯片中实现了两密钥的 TDES 算法,实现时利用单一 DES 电路进行三次加/解密运算,实现方式为 $\mathrm{CTO} = E_{K1}[D_{K2}[E_{K1}[PTI]]]$。其中:$E$ 是加密运算,D 是解密运算。其基本原理结构如图 3 所示。电路使用了左右各 32 位的寄存器,用于保存每轮运算开始和结束时的值,因此实验中选择 HD 功耗模型,分别对 TDES 的第一次 DES 的第一轮运算和第三次 DES 的最后一轮运算进行 DPA 分析。在对第一次 DES 的第一轮运算攻击时使用图 2 中左边位置处标记的 R_0 和 R_1;对第三次 DES 的最后一轮运算进行 DPA 分析时使用图中 R_{15} 和 L_{15}。针对 S-Box$_1$ 的 4 bit 输出,在时钟上升沿传递到右边寄存器的某 4 位,这 4 位寄存器的结果与前一个时钟周期计算 HD,即为功耗 $h_{d,i}$ 的值,使用式(4)计算各猜测的子密钥对应的相关曲线。

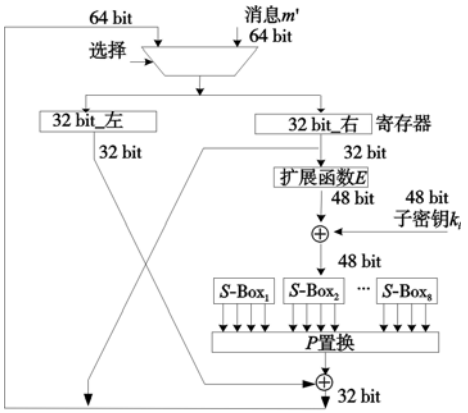

图3　TDES实现原理

4.2　攻击平台

图 4 为对某智能卡芯片进行功耗攻击的实验平台结构。

所选智能卡芯片为内置 8051CPU 内核的双界面 IC 卡,支持接触和非接触两种工作模式,工作电压范围为 2.1 ~ 5.5 V。实验中芯片采用接触式工作模式,工作电压为 2.1V(因为,根据经验智能卡在正确工作的前提下,供电电压越低时进行 DPA 攻击越容易),接口类型为 ISO/IEC 7816 接口,芯片中硬

件实现了 TDES 算法。将卡片插入具有与其匹配的带有特定探头的 DPA 攻击平台上,并在平台电源 GND 端与电源 GND 间串联一个 50 ohm 的电阻,利用数字存储示波器(DSO)对电阻两端电压采样。实验中使用了一台 Lecroy/WP960 数字存储示波器,通过 GPIB 总线向 PC 机传输数据并受控于 PC,其具有 2 GHz 模拟带宽和 4 GHz 的最大采样率,本实验中使用 1GHz 采样率。PC 机中生成随机明文,通过 RS232 串口发送至 DPA 攻击平台,芯片收到明文后运行 TDES 加密算法,同时触发 DSO 对电阻上的电压进行采样并存储,通过 GPIB 总线传输给 PC 机。外部时钟源提供 3.571 MHz 的方波时钟信号,并与平台 50 ohm 阻抗匹配以防止时钟信号反弹,实验中方波信号电压范围为 600 mV ~ 1.6 V。

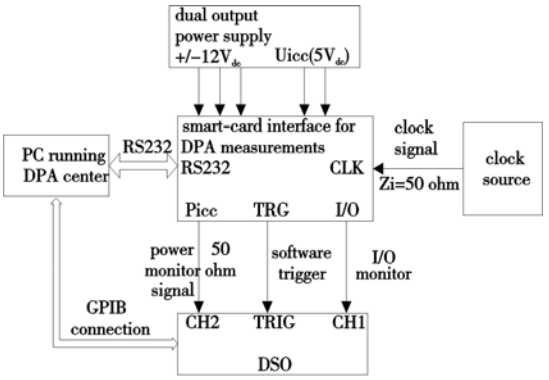

图4　DPA攻击平台

4.3　攻击结果

首先验证智能卡芯片中 TDES 算法的正确性。使用一组明文 M = "95BD6A9B5C91C25A" 和两密钥 K_1 = "CC118E987-194F5E3"、K_2 = "DB1314B677461FEE" 进行验证,得到正确结果 C = "3B55ED767A0EF3F4"。接下来随机更换明文输入,采集相对应的功耗曲线并计算中间结果。

实验中共采集了 10 万条功耗曲线,将曲线对齐。对齐方法很多,如时域信号变换为频域信号分析方法[6] 和基于模式匹配的方法。实验中对于没有任何防护措施的芯片,只需在曲线上找到幅度满足一定阈值(最大)的某个特征点作为标志位,进而对齐曲线。图 5 显示了利用某幅值最大的特征对齐的两条功耗曲线。

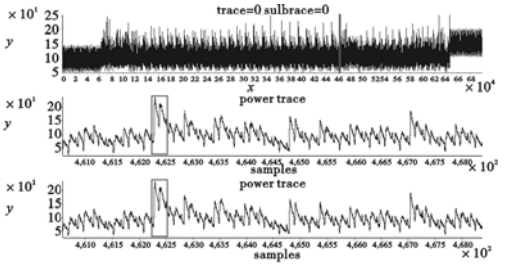

图5　使用特征对齐的曲线

在已对齐的曲线上,需要找到 TDES 执行的确定区域,才能进行 DPA 分析。使用式(5)对输入数据和输出数据分别与功耗曲线进行相关性分析,确定两者的区域。如果功耗曲线与输入数据或输出数据相关,那么进行相关性分析后会在相关曲线上出现明显的尖峰。每一 Byte 输入或输出对应一条相关性曲线,所以 8 Byte 的输入或输出对应 8 条相关性曲线。

如图 6 所示,输入数据区域出现叠加的 8 条带有尖峰的相关曲线,它的位置肯定在 TDES 执行之前;输出数据区域出现叠加的 8 条带有尖峰的相关曲线,它的位置肯定紧跟在 TDES 执行之后。直接观察也可看到,输入与输出区域的曲线特征十分相似,而且在输入数据位置后面紧跟着 16 个与之相似的特征,可知这里是读取 16 Byte 密钥区域。因此,可以确定位于密钥区域与输出区域之间的部分就是 TDES 执行的区域。

使用 HD 功耗模型,分别对 TDES 的第一次 DES 的第一轮运算和第三次 DES 的最后一轮运算进行 DPA 攻击。如图 7 所示,上图是 TDES 区域放大后的曲线;中间曲线表示 64 条相关曲线的叠加,目的是将它们进行对比找出具有最高尖峰的一条曲线,其对应的子密钥即是正确的子密钥。可以看到,在第一次 DES 的第一轮运算的 S-Box$_1$ 对应位置曲线上出现明显的尖峰,DPA 攻击成功,得到 S-Box$_1$ 对应的 6 bit 正确子密钥;如下面曲线所示,对于第三次 DES 的最后一轮运算的 S-Box$_1$ 攻击同样成功,对其他 S 盒的攻击与之类似。实际上,实验中尝试了使用最少的曲线条数进行 DPA 攻击,发现对 DES 运算每一轮的圈密钥攻击成功所需的最少曲线条数仅为 3 500 条。可见,对 TDES 的攻击方法和对 DES 的完全相同。

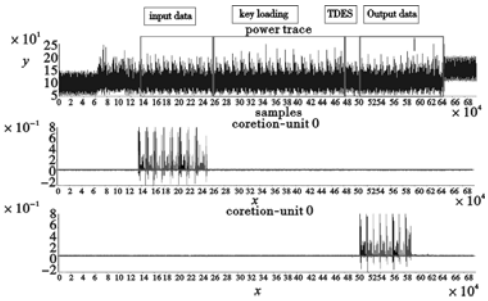

图6　TDES区域分析

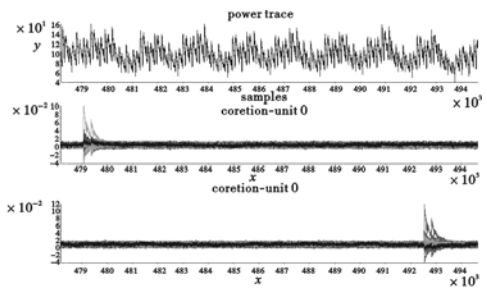

图7　DPA攻击结果

5　结束语

本文基于实际的智能卡芯片进行了 DPA 攻击实验,成功攻击了 TDES 算法。实验表明,由于 TDES 和 DES 密码电路的实现结构相同,对两者进行 DPA 攻击的方法相同。为避免密钥受到 DPA 攻击,在智能卡芯片中设计有效的防护措施是十分必要的。

参考文献:

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Proc of Advances in Cryptology-CRYPTO. [S. l.]: Springer-Verlag, 1999: 388-397.

[2] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model [C]//Proc of CHES. Berlin: Springer, 2004: 16-29.

[3] AGRAWAL D, Jr RAO, ROHATGI P. Multi-channel attacks[C]// Proc of the 5th International Workshop on CHES. Berlin: Springer-Verlag, 2003: 2-16.

[4] KAMOUN N, BOSSUET L, GHAZEL A. Experimental implementation of DPA attacks on AES design with flash-based FPGA technology [C]//Proc of International Multi-Conference on Systems, Signals and Devices. 2009: 1-4.

[5] De MULDER E, ORS S B, PRENEEL B, *et al*. Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems[J]. Elsevier An International Journal Computers and Electrical Engineering, 2007, 33(5): 367-382.

[6] GEBOTYS C, HO S, TIU A. EM analysis of Rijindael and ECC on a PDA[C]//Proc of CHES. 2005.