一种对嵌入式加密芯片的增强 DPA 攻击方法*

尹文龙, 丁国良, 刘昌杰, 郭 华
(军械工程学院 计算机工程系, 石家庄 050003)

摘 要: 针对传统 DPA 攻击方法需要波形数据精确对齐的缺点,提出了一种基于离散傅里叶变换的增强 DPA 攻击方法,并对目前常用的嵌入式芯片以 DES 加密算法为例进行了 DPA 攻击实验。实验结果表明采用这种增强的 DPA 攻击方法能够克服传统 DPA 攻击方法的缺点。

关键词: 差分功耗分析; 数据加密标准; 离散傅里叶变换; 旁路攻击
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0712-02
doi:10.3969/j.issn.1001-3695.2010.02.085

Enhanced DPA technique for embed encrypted CMOS chip

YIN Wen-long, DING Guo-liang, LIU Chang-jie, GUO Hua
(*Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang* 050003, *China*)

Abstract: This paper presented an enhanced DPA technique to defeat the popular DPA shortcoming, which was that the waveform data must be precise alignment. And made waveform matching based on discrete Fourier transforms. After that performed the standard analysis. The experiment demonstrates the enhanced DPA technique can overcome the shortcoming of popular DPA.

Key words: differential power analysis(DPA); DES; discrete Fourier transforms; side channel attacks(SCA)

0 引言

对嵌入式加密芯片进行 DPA(差分功耗分析)[1]攻击是获取这些加密系统密钥的有效途径。DPA 是 SCA(旁路攻击)技术的一种,DPA 攻击的思想为:以电路的功耗特性为基础,利用功耗与内部密钥的关系,将大量采样到的包含该内部密钥运算的功耗波形数据根据所猜测的密钥进行划分,使得所划分的两部分具有不同的功耗特性。最后,对两部分的功耗数据相减得到功耗差分曲线,如果猜测正确,差分曲线将出现明显的尖锋,如图 1 所示。

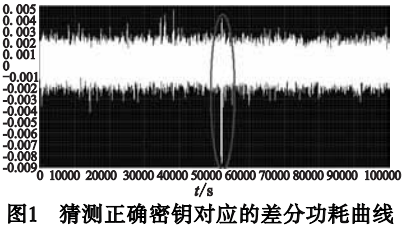

图1 猜测正确密钥对应的差分功耗曲线

DPA 攻击能够成功的前提是所有功耗波形相对于某一加密运算过程必须精确对齐,如果往功耗波形中加入随机延时,或功耗数据采集时有偏差,由于各条功耗曲线相同操作时间点不对齐,加密系统处理不同数据(0 和 1)的功耗差异不能在大量采集样本中得到累积,DPA 攻击将会失败[2]。为此,本文提出了一种增强的 DPA 攻击方法对常用的嵌入式加密芯片(单片机、智能卡、FPGA 芯片)进行攻击,并以 DSE(data encryption standard,数据加密标准)算法为例对攻击过程作了详细说明,其他加密算法(3DES、AES、RSA)与此类似。

1 攻击的总体方案

1.1 功耗波形数据采集

功耗波形数据采集就是采集包含所要分析功耗分量的功耗数据。对于不同的加密算法,要分析的功耗分量不同,因此功耗数据的采集时机也不尽相同,如对 DES 算法常采集第一轮或最后一轮的功耗数据。而波形采集次数一般会比较多,并且在采集同一批数据的时候芯片内部的密钥是不变化的。只有这样,所有被采集的功耗波形中才会拥有相同的密钥信息。

针对同一密钥,本文对嵌入式加密芯片输入 M 组明文 PT_i $(0 \leqslant i \leqslant M-1)$。利用数字示波器进行功耗数据采样,记为 $S_i[j]$,设采样点为 N 个$(0 \leqslant j \leqslant N-1)$,$S_i[j]$为输入明文 PT_i 后加密过程功耗采样的第 j 个采样点。对应于明文 PT_i 的密文输出记为 CT_i。

1.2 波形数据预处理

由于嵌入式加密芯片加入了随机延时或在采样时存在偏差,在 1.1 节中采集到的波形数据间存在偏移,如果直接进行分析处理,结果会很不理想。因此采用基于离散傅里叶变换的方法对波形数据进行匹配处理,具体方法如下:

设两个波形信号 $f(n)$ 和 $g(n)$,假设 n 的范围是$(-M,\cdots,M)$,因此波形长度 $M=2M+1$。让 $F(k)$ 和 $G(k)$ 表示两个波形

收稿日期: 2009-06-03; **修回日期**: 2009-08-13 **基金项目**: 国家"863"计划资助项目(2007AA01Z454);国家自然科学基金资助项目(60571037)

作者简介:尹文龙(1980-),男,河北人,讲师,硕士,主要研究方向为计算机应用技术(yinwenlong1949@sina.com);丁国良(1968-),男,江苏人,副教授,博士,主要研究方向为嵌入式系统、信息安全;刘昌杰(1970-),男,山东人,讲师,硕士,主要研究方向为计算机体系机构;郭华(1978-),男,河南人,讲师,硕士,主要研究方向为信息安全.

的离散傅里叶变换(discrete Fourier transform,DFT),则

$$F(k)=\sum_{n=-M}^{M}f(n)W_N^{kn}=A_F(k)e^{j\theta_F(k)} \tag{1}$$

$$G(k)=\sum_{n=-M}^{M}g(n)W_N^{kn}=A_G(k)e^{j\theta_G(k)} \tag{2}$$

其中:$W_N^{kn}=e^{-j\frac{2\pi}{N}}$。$A_F(k)$和$A_G(k)$为振幅,$e^{j\theta_F(k)}$和$e^{j\theta_G(k)}$为相位。交叉相位频谱(或规格化交叉频谱)$R(k)$定义为

$$R(k)=\frac{F(k)\overline{G(k)}}{|F(k)\overline{G(k)}|}=e^{j\theta(k)} \tag{3}$$

其中:$\overline{G(k)}$表示 $G(k)$的共轭,而且 $\theta(k)=\theta_F(k)-\theta_G(k)$。POC(phase-only correlation)函数 $r(n)$是 $R(k)$的逆离散傅里叶变换(inverse discrete Fourier transform,IDFT),表示为

$$r(n)=\frac{1}{N}\sum_{k=-M}^{M}R(k)W_N^{-kn} \tag{4}$$

如果两个波形间有相似,POC 函数给出了明显的急剧峰值(当$f(n)=g(n)$,POC 函数变成 Kronecker delta 函数);如果两个波形间没有相似,峰值不明显。波峰的高度表示波形的匹配程度,而波峰的位置表示波形间的偏移。因此,如果将原始波形中加入噪声,那么 POC 函数中波峰的高度将会下降。现在考虑连续区间中的波形,设$f_c(t)$是实数变量 t 在连续区间中的波形,本文用 δ 表示波形的偏移,因此偏移后的波形可以表示为$f_c(t-\delta)$,假定$f(n)$和$g(n)$是$f_c(t)$和$f_c(t-\delta)$的采样波形,则

$$f(n)=f_c(t)|_{t=nT} \tag{5}$$

$$g(n)=f_c(t-\delta)|_{t=nT} \tag{6}$$

其中:T 是采样间隔,变量 $n=-M,\cdots,M$。为简单起见,设定 $T=1$,则$f(n)$与$g(n)$之间的交叉相位频谱和 POC 函数为

$$R(k)=\frac{F(k)\overline{G(k)}}{|F(k)\overline{G(k)}|}\approx e^{j\frac{2\pi}{N}k\delta} \tag{7}$$

$$r(n)=\frac{1}{N}\sum_{k=-M}^{M}R(k)W_N^{-kn}\approx\frac{\alpha}{N}\frac{\sin\{\pi(n+\delta)\}}{\sin\{\frac{\pi}{N}(n+\delta)\}} \tag{8}$$

其中:δ 为两个波形间的偏移值;α 为峰值,表示两个波形的相似度,$\alpha=1$ 表示两个波形是一样的,当给波形中加入噪声时,α 的值会减小,在实际应用中 $\alpha\leqslant 1$。在匹配中,首先任意选择一个波形作为参考,根据式(8)计算 POC 函数 $r(n)$,从而确定其他波形和参考波形间的偏移误差 δ;然后根据偏移误差 δ 调整其他的波形,实现了所有波形的精确对齐(波形匹配)。

1.3　波形数据分析

DES 将 64 位的明文输入经过 16 轮加密等一系列变换输出 64 位密文,64 位密钥中的 56 位用于加密,其余 8 位用于奇偶校验。详细的 DES 算法描述可参见文献[3]。对 DES 进行 DPA 攻击时可以采用第一轮或对后一轮的功耗数据进行分析攻击,在此本文选用最后一轮的功耗数据。

最后一轮 DES 加密的流程如图 2 所示。第 15 轮操作输出的密文为 64 位,等分成左(L_{15})、右(R_{15})两部分。R_{15}经过一个 E 变化扩展成 48 位,然后与第 16 轮子密钥 K_{16}进行异或操作,结果再经过 8 个 6 变 4 的 S 变化为 32 位。再经过一个 P 换位操作,与 L_{15}进行异或操作得到第 16 轮输出的左 32 位 L_{16},而 R_{16}直接由 R_{15}得到。第 16 轮的输出再经过一个置换操作即可得到密文 CT。

攻击的第一步是获取第 16 轮的子密钥 K_{16}(48 位),再通过 K_{16}获取最终的 64 位密钥。把 K_{16}等分成 8 个子密钥块($K_{16}^1,\cdots,K_{16}^8$),每个子密钥块为 6 个二进制位,其取值范围为 0 ~ 63。具体的攻击方法为:对每个子密钥块从 0 ~ 63 进行遍历,在每次遍历时选取一个 D 函数对波形数据进行分类;然后对两组波形数据取平均值,最后做差。如果最终的曲线出现尖峰说明子密钥块猜测正确。D 函数为 L_{15}中的某一位。

2　攻击实验

2.1　对单片机或智能卡的攻击

对单片机攻击的实验的原理如图 3 所示。示波器(Tektronix DPO4104,1 GHz BW, 5G sample/s)的 2 通道接收单片机(89C52)加密模块的触发信号,1 通道用电压探针(Tektronix P6139A,500 MHz 8.0 pF)采集来采集电阻 R 两端电压数据。攻击过程如下:在 PC 机上生成 64 位随机明文,通过串口发送至单片机。单片机收到明文后利用存储在其中的密钥对明文进行 DES 加密,在加密过程中加入随机延时,并在第 16 轮加密操作时对示波器产生数据采集的触发信号。示波器在收到触发信号之后,采集电阻 R 两端电压数据(可反映单片机的功耗),并将数据通过 USB 总线送至 PC 机,最后在 PC 机上运行分析程序攻击出 64 位的密钥。

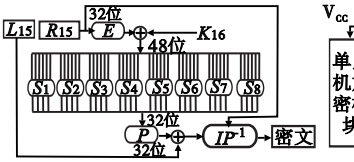

图2　DES第16轮至密文输出结构示意图

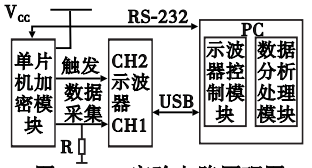

图3　DPA实验电路原理图

设定明文输入和电压数据采样为 500 组,采样深度100 000 点,采样频率 500 MS/s。如图 3 所示,为第一个子密钥块 K_{16}^1猜测正确功率差分曲线(出现明显的尖峰),采用相同的方法可以攻击出其他 7 个子密钥块,由此可以得到 K_{16}。对于智能卡由于其内部为一个 C51 的单片机核,可以用单片机来模拟对智能卡的攻击,攻击的实验平台和攻击过程与单片机类似。

2.2　对 FPGA 的攻击

目前 FPGA 的种类很多,但其中有大于 50% 的份额被 Xilinx 公司抢占,在本文选用 Xilinx 公司的 Spartan3(PQ208),对其他种类的 FPGA 的攻击与此类似。Spartan3 在工作时需要三个工作电压,即内核电压(1.2 V)、辅助电压(2.5 V)、I/O 电压(3.3 V)。而 Spartan3 芯片的所有地线是并结在一起的。在进行数据采集时实质是要采集内核电压所引起的功耗变化。在对 Spartan3 进行功耗数据采集有两种方案:a)芯片的地线和电源地线之间串联一个电阻,通过电压探针采集电阻两端的电压的变化,但此时电压变化反映的是总功耗变化,只能近似地表示内核的功耗变化;b)在内核电压和芯片之间置一个电流探针(Tektronix CT-2,1.2 kHz ~ 200 MHz),通过电流的变化反映内核的功耗变化。在实际的应用中本文采用第二种方案。对 FPGA 攻击的其他步骤与单片机类似。

3　结束语

实验证明,对采取插入随机延时防护措施的加密芯片,或无法获取精确的采集触发信号的加密芯片,传统的 DPA 攻击方法失效,但本文的增强 DPA 攻击方法仍然能够快速、准确地找到正确密钥,这对嵌入式加密系统又提出了新的挑战。

(下转第 717 页)

算法 7　白名单机制中的 TPM_LoadKey 算法

输入:parentHandle,wrkHandle,keyInfo
输出:returnCode,wrappedKey,whitelistBlob
inKeyPlain: = Decrypt(inKey,parentHandle)
if inKeyPlain. Keyflags. revocable = TRUE then
　hashval: = Hash(REVOC_LABEL||inKey. pubKey||WRK||TPM. revCounter)
　if hashval! = whitelistblob then Return RET_FAIL
Continue as in the specification
return TPM_SUCCESS,keyHandle

3　黑白名单相结合的撤销机制

为简化对黑白名单机制中各操作的效率比较,假设一个 TPM 的所有可撤销密钥数量为 M,已撤销密钥数量为 N,哈希运算 hash(REVOC_LABEL||keyHandle. pubKey||SRK|| TPM. lastHash)和 hash(REVOC_LABEL||keyInfo. pubKey|| WRK||TPM. revCounter)的运算时间相同(设为 T_H),并忽略数据传输的通信开销。这样,黑名单机制中密钥撤销的开销为 T_H,加载一个可撤销密钥的开销为 NT_H;白名单机制中加载一个可撤销密钥的开销为 T_H,撤销密钥的开销为 $(M-1)T_H$。可见,黑名单机制中密钥撤销是常量时间,但加载密钥的开销与已撤销密钥的数量呈线性。虽然可以通过清理协议清除黑名单,但协议的实现十分复杂。而白名单机制中密钥的加载十分高效,但密钥撤销的开销较大,它与系统中可撤销密钥的数量呈线性。黑白名单机制中各操作效率对比如图 2 所示。

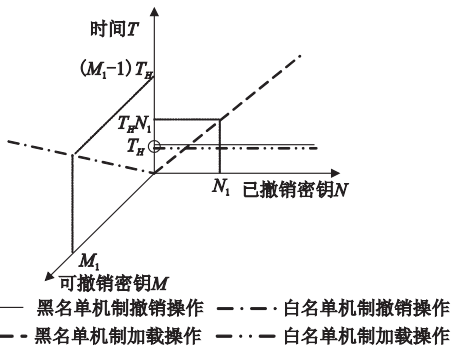

图2　黑白名单机制中各操作效率对比

将黑白名单结合可以提高密钥撤销和加载的效率。利用黑名单完成通常的密钥撤销操作,另外再维护一个白名单来有效地清理黑名单。如果一个密钥被撤销,它首先被添加到黑名单中,TPM 将拒绝加载黑名单中的任何密钥;当生成一个新的可撤销密钥时,同时为它生成一个白名单块,TPM 也将拒绝加载任何不在白名单中的可撤销密钥。当黑名单太大时,TPM 所有者可以通过为所有不在黑名单中的密钥生成一个新的白名单来清除黑名单。

结合后的机制要求修改 TPM_WhitelistTransformKey 命令,并添加一个测试密钥是否在黑名单中的操作,如算法 8 所示。如果密钥在黑名单中,则不为它生成白名单块,迁移命令返回一个错误。此外,还需要修改 TPM_WhitelistCommit 命令,使它将 TPM 内部的哈希值置为 0^k。将黑白名单结合,可以得到两方面的最高效率:撤销密钥可以在常量时间内完成,并且可以维护很短的黑名单以实现高效的密钥使用。虽然更新白名单的开销很大,但它并不需要频繁更新。

算法 8　结合机制中的 TPM_WhitelistTransformKey 算法

输入:srkHandle,parentHandle,wrkHandle,revokedHandle,
　revElement,inKey,Nonce
输出:returnCode,whitelistBlob
Switch (TPM_ShowRevListElement (srkHandle, revElement, parentHandle,inKey,Nonce))
　Case: RET_FAIL
　　return RET_FAIL
　Case: RET_OK
　　whitelistBlob: = Hash(REVOC_LABEL||inKey. pubKey||WRK||TPM. revCounter + 1)
　　return TPM_SUCCESS,whitelistBlob
　Case: RET_ REVOC
　　Continue to compare with next blacklist item

4　结束语

受 TPM 存储能力的限制,密钥并不直接存储在 TPM 中,而是加密后保存在外部设备上。这种方式导致密钥存储事实上并不受 TPM 的控制,它只作为对密钥的访问控制设备,因而 TPM 不能销毁被攻破的外部存储密钥。针对这个问题,本文提出了利用黑白名单撤销 TPM 密钥的机制,它们都只需要对 TPM 的命令集作少量修改,并能保证与现有规范的向后兼容。为最大化密钥撤销和加载操作的效率,增强撤销机制的可实施性,最后提出将黑白名单相结合的撤销机制。

参考文献:

[1] Trusted Computing Group. Trusted platform module (TPM) specifications [R/OL]. (2008-06-15). https://www. trustedcomputinggroup. org/specs/TPM.
[2] Trusted Computing Group. TCG specification architecture overview revision 1.2[R/OL]. (2004-04-28). https://www. tru-stedcomputinggroup. org.
[3] BRICKELL E, CAMENISCH J, CHEN Li-qun. Direct anonymous attestation[C]//Proc of the 11th ACM Conference on Computer and Communications Security. New York: ACM Press, 2004:132-145.
[4] KÜHN U, KURSAWE K, LUCKS S, *et al*. Secure data management in trusted computing[C]//Proc of Workshop on Crypographic Hardware and Embedded Systems. Heidelberg: Springer,2005:324-338.
[5] Trusted Computing Group. TCG TPM specification version 1.2 revision 103,TPM main part 2 TPM structures[R/OL]. (2006-10-26). https://www. trustedcomputinggroup. org.
[6] Trusted Computing Group. TCG TPM specification version 1.2 revision 103,TPM main part 3 command[R/OL]. (2006-10-26). https://www. trustedcomputinggroup. org.

(上接第 713 页)

参考文献:

[1] KOCHER P, JAFFE J, JUN B. Introduction to differential power analysis and related attacks [J]. IEEE Trans on Electron Devices, 1998,50(2): 462-470.
[2] CLAVIER C, CORON J, DABBOUS N. Differential power analysis in the presence of hardware countermeasures [C]//Proc of CHES, Lect Notes Comput Sci. London: Springer-Verlag,2000:252-263.
[3] 刘尊全. 刘氏高强度公开加密算法设计原理与装置[M]. 北京:清华大学出版社,1996 : 101-199.
[4] 蒋惠萍,毛志刚. 一种差分功耗攻击的改进 DES 算法及其硬件实现[J]. 计算机学报, 2004,27(3):334-339.
[5] 韩军,曾晓洋,汤庭鳌. DES 密码电路的抗差分功耗分析设计[J]. 半导体学报,2005,26(8):1646-1653.
[6] 褚杰,赵强,丁国良,等. 数据加密标准密码系统差分功耗分析攻击[J]. 兵工学报, 2008,29(9):1039-1044.