物理可观测下 DES 的安全性研究

陈开颜,张 鹏,邓高明,赵 强
(中国人民解放军军械工程学院计算机工程系,河北石家庄 050003)

摘 要: 利用物理观测效应进行的旁路攻击,是通过对密码设备工作时泄漏的时间、功耗等信息的分析,获取密码系统的密钥或相关秘密信息.已有大量防护对策但并没有从根本上阻止攻击.本文在 AT89C52 上加载了 DES 算法,并在该平台上对差分功耗旁路攻击与防护方法进行了实验和验证.根据 Micali 和 Reyzin 建立的物理观测密码术理论模型,将该模型具体化,对可以抵抗黑盒攻击的密码要素进行修正以抵抗基于物理泄漏的旁路攻击,将 RO(random oracle)模型用于物理观测现实世界的安全性证明,给出了对称加密方案物理可观测下安全性定义,并对 DES 定义了在 DPA 攻击下的安全性.

关键词: 数据加密标准; 差分功耗分析; 随机预言模型; 可证安全; 旁路分析 (侧信道分析); 物理观测密码术

中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2009) 11-2389-07

Research on the DES Physical Observable Security

CHEN Kai-yan, ZHANG Peng, DENG Gao-ming, ZHAO Qiang
(*Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang, Hebei* 050003, *China*)

Abstract: The security of cryptographic implementations with respect to "physical observation attacks" named side-channel attacks, in which adversaries are enhanced with the possibility to exploit physical leakages such as power consumption or electromagnetic radiation. A lot of countermeasures have been experimented, but do not fundamentally prevent them. In this paper, DES is implemented on AT89C52. DPA and countermeasure experiments have been done on this platform. Physically Observable cryptography is built by Micali and Reyzin who initiated a theoretical analysis of side-channels. Our work is to apply the "Physical-Observation" attacks to practice for Symmetric Encryption schemes and find out how it is applied to DES-DPA attack practice for Symmetric Encryption schemes with random oracle model.

Key words: data encryption standard (DES); differential power analysis (DPA); random oracle model; provable security; side-channel analysis; physical observable cryptography

1 引言

近年来出现的计时攻击、功耗分析攻击、电磁分析攻击等物理可观测旁路攻击(Side Channel Attacks,简记为 SCA)方法,从算法在具体工程实现时伴随产生的物理特性入手,通过对算法运行在密码设备上泄漏的时间、功耗等信息的分析,获取密码系统的密钥或相关秘密信息.这类技术绕过了对算法直接、烦琐的数学分析,在针对具体密码芯片实现的破解研究中显示出了良好的实用性.因此该方法一经提出,就伴随着大量针对旁路攻击的防护对策[1~4],但并没有从根本上阻止攻击.此攻击方式使密码系统的设计陷入了困境,既没有系统的攻击方式,也没有系统的解决方案.每几个月就会有新类型的旁路攻击方法出现,现实中旁路攻击要比经典攻击影响大得多,但是在设计和实现密码应用时并没有系统考虑物理观测效应对密码体制安全性的影响.在黑盒模型下可以抵抗攻击的密码要素,面对具有物理观测能力的敌手时显得无能为力.

本文针对 AT89C52 芯片实现的数据加密标准(Data Encryption Standard,简记为 DES)进行运行时的物理观测效应——主要是功耗泄漏的分析.首先介绍了芯片功耗泄漏的机理、差分功耗分析的方法及防护对策的原理以及实验验证结果.在讨论 Micali 和 Reyzin 物理观测密码术的基础上,对可以抵抗黑盒攻击密码要素进行修改以抵抗基于物理泄漏的旁路攻击,将 RO(random orcale)模型用于物理观测现实世界的安全性证明,建立对称加密方案物理可观测模型,给出对称加密方案 DES 旁路攻击下的安全性定义.

收稿日期:2007-07-31;修回日期:2009-06-10
基金项目:国家自然科学基金(No. 60571037);国家 863 高技术研究发展计划(No. 2007AA01Z454)

2 芯片功耗与数据泄漏的机理

密码系统的实现,不管是保护私密信息的智能卡的处理器单元,还是 FPGA 中保障安全和保护知识产权的 IP 核,都在大规模数字集成电路芯片上实现. CMOS 技术是目前数字集成电路的核心技术.

2.1 CMOS 集成电路的功耗

在 CMOS 集成电路中,功耗由三部分组成,即

$$P_{tot} = P_{dyn} + P_{short} + P_{leak}$$

其中 P_{tot}表示总体功耗, P_{dyn}表示动态切换功耗, P_{short}表示短路电流功耗, P_{leak}表示漏电流功耗. 另外在一些特殊的逻辑电路中,如伪 NMOS 逻辑,还存在静态电流功耗.

在上述功耗中, P_{dyn}所占比例最大,通常达到 90 % 以上[5]. 在图 1 所示的节点充放电等效电路图中,当开关向上闭合时,电容开始充电,向下闭合时电容开始放电. V 表示理想的恒压源, R_c 和 R_d 表示等效充电电阻和放电电阻, C_L 表示等效负载电容,根据电路理论可知 t 时刻电容上的电流 $i_c(t)$ 为:

$$i_c(t) = C_L \frac{\mathrm{d}v_c(t)}{\mathrm{d}t}$$

从 t_0 到 t_1 时刻对电容进行充电,设初始时电容上无电荷,其压降 $v_c(t_0) = 0$,经过充电后电容达到最大电压 $v_c(t_1) = V$,从电压源中消耗的能量为:

$$E_s = \int_0^t V i_c(t)\,\mathrm{d}t = C_L V \int_0^t \frac{\mathrm{d}v_c(t)}{\mathrm{d}t}\mathrm{d}t = C_L V \int_0^V \mathrm{d}v_c = C_L V^2$$

假设电容充放电的频率即系统的时钟频率为 f,电路中节点 i 的切换概率为 α_i,那么单个节点的动态功耗为:

$$P_i = \alpha_i C_{Li} V^2 f_i$$

对于 M 个节点的系统,其总体动态功耗为:

$$P_{dyn} = \sum_{i=1}^{M} P_i = \sum_{i=1}^{M} \alpha_i C_{Li} V^2 f = V^2 f \sum_{i=1}^{M} \alpha_i C_{Li}$$

可见,系统总体动态功耗与电源电压、时钟频率、电路等效电容以及节点切换概率有关. CMOS 系统设备工作过程中节点的状态切换活动直接与执行的具体操作相关,这些操作对系统工作过程中的功耗起决定作用.

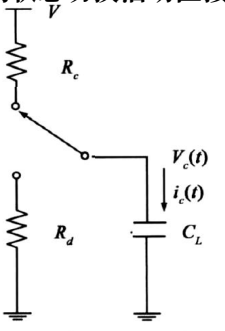

图1 CMOS电路动态切换等效电路图

2.2 加密设备功耗与操作数据之间的关系

由 2.1 分析可知加密设备(芯片)的功耗,主要体现在对数据的处理上. 当进行数据处理时,功耗的大小与所处理的数据量的大小和数据的类型直接相关. 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 到 1 或者 1 到 0 翻转的次数,因而在操作数一级,表现为原始操作数和结果之间的汉明距离(Hamming Distance)[6]. 所以,可以用原始操作数和结果之间的汉明距离模拟芯片中数据处理过程中的功耗情况.

根据上面的分析,可以用寄存器变化前后的两个状态,也就是寄存器单元 0 和 1 翻转的个数对功耗进行模拟,上升到操作数一级就是用原始操作数和结果之间的汉明距离模拟功耗,用函数表示为:

$$P_R = \lambda \cdot H(D \oplus R) + \mu$$

其中,λ是一个由电路系统决定的功耗常量; H 表示数据的汉明重量,也就是一个二进制数据中 1 的个数; D 和 R 分别表示寄存器单元中存储的原始操作数和操作结果; $H(D \oplus R)$ 就表示 D 和 R 之间的汉明距离,也就是 D 和 R 之间对应的不同的比特位的个数; μ 表示随机噪声.

3 差分功耗分析原理及其对 DES 攻击的实验结果

3.1 差分功耗分析原理

差分功耗分析(Differential Power Analysis,简记为 DPA)根据测量到的 N 个明文加密时的功耗曲线,通过统计分析中的均值差方法获取旁路信号中携带的密钥信息[8].

进行 DPA 攻击,首先需要(1) N 个随机的明文输入 $PT_i(1 \le i \le N)$; (2) $S_i[j]$:对第 i 次功耗进行离散采样形成的功耗数组,其中 $1 \le i \le N$, j 表示采样的时间点; (3) 对应于 PT_i 的相应密文输出 $CT_i(1 \le i \le N)$; (4) 人为定义的一个与密钥密切相关的函数 $D(.)$,其作用是将基于采样时间点 j 的信号数组集合$\{S_i[j] \mid 1 \le i \le N\}$分成两个子集合:

$$S_0 = \{S_i[j] \mid D(.) = 0, 1 \le i \le N\},$$

$$S_1 = \{S_i[j] \mid D(.) = 1, 1 \le i \le N\}$$

第二步计算集合 S_0 与 S_1 平均功耗值($|S_0| + |S_1| = N$):

$$A_0[j] = \frac{1}{|S_0|} \sum_{S_i[j] \in S_0} S_i[j]$$

$$A_1[j] = \frac{1}{|S_1|} \sum_{S_i[j] \in S_1} S_i[j]$$

将这两个均值按照对应的离散时间点进行相减,可以

得到 DPA 偏差信号数组 $T[j]$, $T[j] = A_0[j] - A_1[j]$.

合适的 D 函数的选择是 DPA 攻击的关键. 正确的 D 函数能产生所期望的 DPA 偏差信号,有助于验证所猜测的密钥子集的正确性. D 函数是一个只与密文和子密钥相关的函数,以 DES[7] 为例,为获取最后 1 轮 1 号 S-盒对应的 6 位子密钥,可选择如下的 D 函数:

$$D(C_1, C_6, K_{16}) = C_1 \oplus SBOX1(C_6 \oplus K_{16})$$

其中 C_1、C_6 分别对应 DES 最后 1 轮左 32 位输出结果中的 1 比特和 6 比特; K_{16} 是第 16 轮子密钥进入 1 号 S-盒的部分; $SBOX1()$ 是一个选择函数,选择 1 号 S-盒 4 位输出中的第 1 位.

第三步求功耗均值差. 在加密算法实现的过程中,需要密钥位参与运算,其为 0 或 1 不同值时会产生不同的功耗. 假设 D 函数所取的位参与操作的时刻发生在 j^*,期望功耗平均值之差 ε 为:

$$E[s_{ij} | D(.,.,.) = 0] - E[s_{ij} | D(.,.,.) = 1] = \varepsilon, \text{ for } j = j^*$$

当 $j \neq j^*$ 时,加密执行的位与 D 无关,差分功耗曲线亦与 D 无关,即:

$$E[s_{ij} | D(.,.,.) = 0] - E[s_{ij} | D(.,.,.) = 1] = 0, \text{ for } j \neq j^*$$

随着随机输入明文的数目 N 的增加,DPA 偏差信号数组 $T[j]$ 趋向于:

$$\lim_{N \to \infty} T[j] = E[s_{ij} | D(.,.,.) = 0] - E[s_{ij} | D(.,.,.) = 1]$$

上式表明只要随机输入明文的数目 N 足够大, $T[j]$ 在 j^* 时刻有偏差尖峰信号 ε,而在其它时刻趋于 0. 由于 S-盒输出的统计误差,不能保证在非 j^* 时刻差分功耗曲线与 D 完全无关, $T[j]$ 不总是趋于 0,但偏差的尖峰仍在 j^* 时刻出现.

可以通过穷举猜测的办法经 2^6 次猜测得到第 16 轮子密钥中的其中 6 位 K_{16},即 D 函数的一个输入. 对于每次猜测获得的功耗曲线进行划分,获得差分功耗曲线 $T[j]$. 如果适当选择 D 函数,只要 D 位参与运算及密钥猜测正确,差分功耗曲线会有尖峰出现. 用这种方法可以确定第 16 轮进入第一个 S-盒运算的 6 位子密钥,同理可以确定第 16 轮分别进入其他 7 个 S-盒的 6 位子密钥.

3.2　针对 DES 的 DPA 攻击实验

获取 DES 芯片工作过程中的功耗是进行 DPA 攻击的前提. 功耗的测量可以通过在芯片的 V_{dd} (或 V_{ss}) 和电源 + 5V (或 GND) 之间串联一个小阻值电阻,并对其电压进行测量的方法来实现.

根据图 2 的实验电路原理图搭建实验平台. 在目标电路板上由 AT89C52 单片机运行 DES 加密程序 (DES 程序和密钥预先用烧写器存储在单片机中);在目标电路板和稳压电源之间串连一个电阻 R,并由数字存储示波器通过测量电阻 R 上的压降的变化来观测单片机电路板的功耗变化;由 PC 机通过 RS232 串口向加密模块发送随机明文并接收加密模块发回来的密文;同时通过 USB 接口接收由数字存储示波器发来的对应这次加密的功耗波形数据. 具体实验参数见表 1.

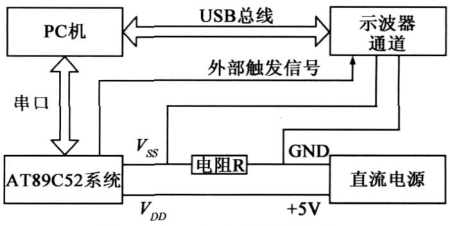

图2　DPA实验电路原理图

表 1　实验参数表

采样次数(总明文样本量 N)	40000
采样率	25Mp/ s
时间单位	40. 0μs
采样深度	每条波形曲线 10000 个点
预触发时间	170. 000μs
DES 密钥(64 位)	{0xa1 ,0x68 ,0x7e ,0xfb ,0x90 ,0x63 , 0x45 ,0x6e}
DES 有效密钥(56 位)	{0x0a ,0xd1 ,0xff ,0xd9 ,0x0c ,0x51 , 0x37}
对应的第 16 轮 48 位子密钥	{0xf5 ,0xbd ,0x82 ,0x28 ,0xe4 ,0xda}
上述 48 位子密钥对应的 2 进制	111101 , 011011 , 110101 , 000010 , 001010 ,001110 ,010011 ,011010

经实验得到差分功耗曲线. 正确的密钥对应的差分曲线出现明显的尖峰(见图 3) ,而错误的密钥对应的差分曲线没有明显的尖峰(见图 4) .

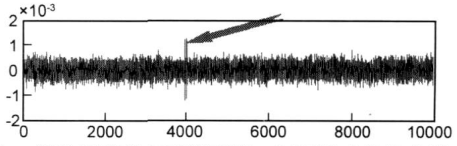

图3　箭头所指是正确猜测的6位密钥对应的尖峰

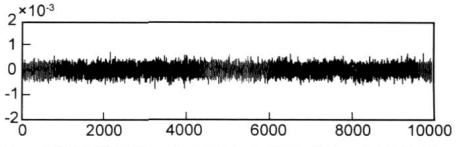

图4　猜测错误的6位密钥对应的差分功耗曲线

在 40000 个明文样本的条件下,成功获取了 DES 第 16 轮加密的 48 位子密钥,根据 DES 产生密钥的标准算法,我们用回溯的办法并穷举剩余的 8 位密钥可以得到 DES 完整的 56 位密钥.

利用 DPA 方法,把针对密钥的搜索空间从 2^{56} 减少到 $2^6 \times 8 + 2^8 = 768$,大约减少到穷举法搜索密钥空间的 $768/2^{56} \approx 1/9.4 \times 10^{13}$,明显地暴露了 DES 密码在 DPA 攻击下的脆弱性.

4 DES 算法的 DPA 防护实验

常用的防护方法有硬件级、系统级、器件级、软件级以及算法级的防护等. 本文从算法角度讨论防护措施. 第 2 节中分析了对密码芯片产生威胁的泄漏主要是由于内部对数据进行的操作引起的,只要在运算中不使用秘密信息,那么物理泄漏就不会危及该秘密信息的安全;同时信息泄漏依赖于被选择的测量,可以将泄漏的信息在时间这一维度上随机化,使得测量结果所蕴含的秘密信息难以萃取.

从对 DES 的 DPA 攻击的角度来看,根据攻击者选取 D 函数的位置,只有 DES 第一轮或是最后一轮操作中的异或运算(⊕XOR)对 DPA 攻击是敏感的,可以对这个异或操作加以防护以隐蔽秘密信息. 这里给出两种方法并加以实验验证:(1)因为异或运算满足交换律 $\delta = \Phi \oplus \Gamma = \Gamma \oplus \Phi$,可以将每轮加密时异或操作数的位置互换同样不影响最终结果,而根据 $\delta = \Phi \oplus \Gamma$ 选取的 D 函数对于 $\delta = \Gamma \oplus \Phi$ 运算却是不起作用的,使得 DPA 攻击时 D 函数的选择出现随机错误;(2)在异或运算操作做随机次的空操作循环,从而引入时间轴的随机移动,以达到功耗曲线的随机化效果. 图 5～图 7 分别是没有防护措施以及加入两种防护措施的实验结果.

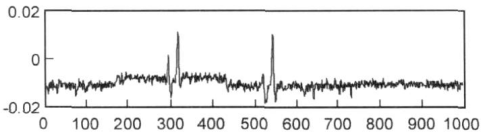

图5 没有防护手段的异或操作差分功耗曲线

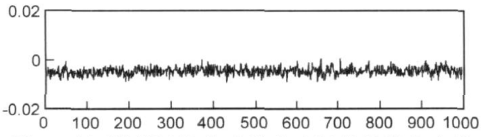

图6 时间轴的随机移动差分功耗曲线没有尖峰

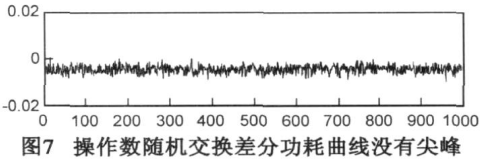

图7 操作数随机交换差分功耗曲线没有尖峰

由此得出如下两个结论:

结论 1 当具有 DPA 能力的敌手不能确定每轮加密时执行的异或运算是 $\delta = \Phi \oplus \Gamma$ 还是 $\delta = \Gamma \oplus \Phi$ 时,DES 算法面对具有 DPA 攻击能力的敌手是安全的.

结论 2 为了使得 DES 算法面对具有 DPA 攻击能力的敌手是安全的,使异或运算 $\delta = \Phi \oplus \Gamma$ 在整个 DES 运算中执行的时刻发生随机移动(在异或操作之前加入随机个空操作,而这些空操作并不影响运算的最终结果).

5 物理观测密码术

3.2 的实验结果表明,旁路攻击方法可以显著降低密码攻击的复杂度,威胁密码系统的安全性. 密码学标准模型假定密码系统是数学函数,它的安全源于数学理论的严密性. 密码方案具体实现过程中呈现出的物理观测效应说明黑盒模型假定的局限性. 现有的旁路攻击防护对策,多属被动防护,并没有从根本上阻止攻击. 其根本原因在于并没有真正建立抗旁路攻击的理论模型,所有的防护研究仍基于启发式的安全和经验主义的攻击.

迄今为止在旁路攻击建模方面最重要的研究成果之一是 Micali 和 Reyzin 提出的物理可观测(Physical Observable,简记为 PO)密码术模型[9]. 该模型尝试对芯片物理运算、信息泄漏和攻击者的能力进行建模,并力求在电磁辐射等物理泄漏环境下对密码算法的实现进行安全性证明. 在该模型中,每个密码操作都是物理上可观测的,密码运算由抽象计算机器执行,并定义抽象计算机器为一组虚拟存储图灵机(virtual-memory turing machine 简记为 VTM)的集合,记为 $A = \{A_1, A_2, \cdots, A_n\}$. 这些 VTM 作为子程序彼此调用,并且共享一个特定的公用存储器. 所有 VTM 的输入和输出都是二进制串,并且总是位于一些虚拟存储器中. 抽象计算机和 VTM 虽然并不是物理设备,但是它们能表示逻辑运算和不同的物理实现. 密码运算的物理实现被定义为虚拟存储物理图灵机(简记为物理 VTM). 一个物理 VTM 是一个二元组 (L_i, A_i),其中 A_i 是一个抽象 VTM,L_i 是一个泄漏函数,如果 $A = \{A_1, A_2, \cdots, A_n\}$ 是一个抽象的计算机,那么称 $P_i = (L_i, A_i)$ 是 A_i 的一个物理实现,$P = (P_1, P_2, \cdots P_n)$ 是抽象计算机 A 的一个物理实现.

显然,维系一个抽象计算机与一个物理实现(密码芯片)之间的唯一纽带是上述所谓的泄漏函数. 该函数定义为有三个输入的函数 $L(C_A, M, R)$:

- C_A 是抽象计算机 A 的当前内部配置,它是所有可被观测的物理量的集合.
- M 是测量物理观测泄漏仪器的设置.
- R 是一个随机串,对测量过程的随机性进行建模. 例如,R 对泄漏信息的噪声进行建模.

如果一个敌手能访问物理 VTM 的泄漏函数的输出并且能够决定泄漏函数的第二个输入 M,就说该敌手观测到一个物理 VTM. 对于一个输入为 x_A 的攻击 A,观测到一个物理 VTM P_i(输入为 x_P,产生输出为 y_P)之后,输出为 y_A 这样的一个过程,记为:

$$y_P \leftarrow P(x_P) \hat{\mathrm{I}} A(x_A) \rightarrow y_A$$

物理观测密码术的目的就是要使攻击者观测到的

泄漏函数 L 的输出 y_A,对于攻击是不可利用或利用价值不高的.

Micali 和 Reyzin 是在一个"小"尺度上关注物理观测密码术:它检验的是物理观测对于单向函数和置换之类的基本要素具有安全性的证据,问题是模型如何应用于一个较"大"的尺度上. Dent[10]在该模型下对于数字签名方案提出一种物理安全性定义. Standaert 等人[11]将该模型应用于更为具体的硬件环境(比如电路、信号和密码操作组成的密码实现系统)中,尝试对泄漏函数具体化,对块密码的抗差分功耗分析能力进行了讨论. 本文针对对称加密方案在物理观测下的安全性进行分析,探讨对称加密方案在物理观测下的可证安全性.

6　物理观测下对称加密方案的可证安全性定义

加密方案(encryption schemes)是将传输的原始信息转换成除合法接收者之外不可理解的信息形式. 常用加密方案主要有对称(或私钥)加密方案(symmetric or private-key schemes)和非对称(或公钥)加密方案(asymmetric or public-key schemes)[12]. 本文主要讨论对称加密方案在具有物理观测能力的敌手攻击下的可证明安全性定义.

Goldwasser 等人阐述了可证明安全性,并给出了具有可证明安全性的加密和签名方案[13,14]. 然而,以上方案的可证明安全性是以严重牺牲效率为代价的,因此以上方案虽然在理论上具有重要意义,但不实用. 20 世纪 90 年代中期出现了"面向实际的可证明安全性"的概念,特别是 Bellare 等提出的 RO(random oracle,随机预言)模型方法论[15],使纯理论的可证明安全性,在实际应用领域取得进展. 本文将 RO 模型方法论用于物理可观测密码术,通过 ORACLE 问答器安全测试给出可以抵抗物理可观测攻击对称密钥系统的充要条件.

目前最常见的密文安全性要求有两种:单向性(One-Wayness,简记为 OW)和不可分辨性(Indistinguishability,简记为 IND). 如果密文是不可分辨的,那么一定是单向的. 文献[16]立足面向实际的可证明安全性理论,考虑更为准确地进行安全度量的具体安全性,给出了在选择明文攻击(chosen-plaintext attack,简记为 CPA)等敌手模型下对称加密方案的四种安全性定义,即左右不可分辨 LOR(Left-or-Right indistinguishability)、真实或随机不可分辨 ROR(real-or-random indistinguishability)、寻找并猜测安全性 FTG(find-then-guess Security)、语义安全性 SEM(semantic security). 并且指出,在可归约的意义下,LOR 与 ROR 安全性等价,FTG 与 SEM 安全性等价.

本文以 FTG 安全性为例,在 CPA 敌手模型下,回顾对称加密方案不可分辨性之 FTG 的定义,进而给出在有物理观测能力的 CPA 敌手模型下,对称加密方案不可分辨性之 PO-FTG 的定义.

6.1　对称加密方案的安全性定义

定义 1(对称加密方案定义)　一个对称加密方案 S(是概率多项式时间算法(probabilistic polynomial - time algorithms,简记 PPTAs),用三元组(K, ε, D)描述:

(1) K 为密钥生成算法,对于输入 1^r, $r \in N$,算法 K 产生一个来自$\{0,1\}^*$中的密钥.

(2) 加密算法 ε 和解密算法 D 是从输入$\{0,1\}^* \times \{0,1\}^*$到输出$\{0,1\}^*$上的映射.

(3) 对于任意由算法 K 产生的密钥 $k \in \{0,1\}^*$、明文 $m \in (\{0,1\}^*$,均有 $D(k, \varepsilon(k, m)) = m$.

其中 r 为加密方案的安全参数.

FTG 安全也是多项式时间下的安全概念. 这种安全假定敌手的攻击分两个阶段,在寻找(find)阶段,敌手要找到两个等长消息 x_0 和 x_1,同时在该阶段敌手还找到一些相关的状态信息,以留后用. 在猜测(guess)阶段,从明文 x_0 和 x_1 的密文中任选一个 y,如果敌手能够根据 find 阶段获得的状态信息 s,识别出由哪个明文生成的 y 就为"获胜". 如果对于定义合理的敌手模型获胜的次数没有明显超过一半,那么该方案就是安全的加密方案.

$S\varepsilon = (K, \varepsilon, D)$ 是一个对称加密方案, $b \in (0,1)$, $k \in N$. A_{cpa} 是一个可以访问加密 oracle $\varepsilon_k(\cdot)$ 的多项式时间选择明文攻击敌手,攻击实验包括 find、guess 两个阶段:

实验 $Exp^{FTG\text{-}cpa\text{-}b}_{S\varepsilon, A_{cpa}}(k)$:

$K \xleftarrow{R} \kappa(k)$;

$(x_0, x_1, s) \leftarrow A^{\varepsilon_k(\cdot)}_{cpa}(k, \text{find})$;

$y \leftarrow \varepsilon_k(x_b)$;

$d \leftarrow A^{\varepsilon_k(\cdot)}_{cpa}(k, \text{guess}, y, s)$;

Return d.

其中 x_0, x_1 等长, s 是可能有用的状态信息.

定义敌手的优势为:

$$Adv^{FTG\text{-}cpa}_{S\varepsilon, A_{cpa}}(k) = \Pr[Exp^{FTG\text{-}cpa\text{-}1}_{S\varepsilon, A_{cpa}}(k) = 1] - \Pr[Exp^{FTG\text{-}cpa\text{-}0}_{S\varepsilon, A_{cpa}}(k) = 1]$$

加密方案的优势函数定义为:

$$Adv^{FTG\text{-}cpa}_{S\varepsilon}(k, t, q_e, \mu_e) = \max_{A_{cpa}}\{Adv^{FTG\text{-}cpa}_{S\varepsilon, A_{cpa}}(k)\}$$

其中最大值是针对所有时间复杂度为 t、对加密 Oracle $\varepsilon_k(\cdot)$ 的询问次数不超过 q_e、询问的总比特数不超过 μ_e 的 A_{cpa} 敌手而言. 也就是对给定的资源,最聪明的攻击者的优势. 安全的密码方案是指在合理的资源参数下,敌手的优势函数的值很"低".

定义 2 (不可分辨性之 FTG):如果对于任意多项式时间敌手的优势,$Adv^{FTG\text{-}cpa}_{S\varepsilon,A}(\cdot)$是可忽略的,则称该对称加密方案是 FTG-CPA 安全的.

6.2 物理观测下对称加密方案的安全定义

$S\varepsilon=(K,\varepsilon,D)$是对称加密方案,$P(S\varepsilon)$是与其对应的物理实现.$A_{PO,cpa}$是具有物理观测能力的多项式时间选择明文攻击敌手.$state$是加密方案运行时敌手观测到的中间物理状态.攻击实验包括 find、guess 两个阶段:

实验 $Exp^{PO\text{-}FTG\text{-}cpa\text{-}b}_{P(S\varepsilon),A_{PO,cpa}}(k)$:

$K\xleftarrow{R}\kappa(k)$;

$(x_0,x_1,s)\leftarrow A^{\varepsilon_K(\cdot)}_{PO,cpa}(k,\text{find})$;

$y\leftarrow P_\varepsilon(x_b)\hat{I}A^{\varepsilon_K(\cdot)}_{PO,cpa}(k)\rightarrow state$;

$d\leftarrow A^{\varepsilon_K(\cdot)}_{PO,cpa}(k,\text{guess},y,s,state)$;

Return d.

定义敌手的优势为:

$$Adv^{PO\text{-}FTG\text{-}cpa}_{P(S\varepsilon),A_{PO,cpa}}(k)=\Pr[Exp^{PO\text{-}FTG\text{-}cpa\text{-}1}_{P(S\varepsilon),A_{PO,cpa}}(k)=1]-\Pr[Exp^{PO\text{-}FTG\text{-}cpa\text{-}0}_{P(S\varepsilon),A_{PO,cpa}}(k)=1]$$

加密方案的优势函数定义为:

$$Adv^{PO\text{-}FTG\text{-}cpa}_{P(S\varepsilon)}(k,t,q_e,\mu_e)=\max_{A_{PO,cpa}}\{Adv^{PO\text{-}FTG\text{-}cpa}_{S\varepsilon,A_{PO,cpa}}(k)\}$$

定义 3 物理观测下的不可分辨性之 PO-FTG:如果对于任意多项式时间敌手的优势,$Adv^{PO\text{-}FTG\text{-}cpa}_{P(S\varepsilon),A}(\cdot)$是可忽略的,则称该对称加密方案是 PO-FTG 安全的.

6.3 功耗泄漏下 DES 的安全性定义实例

基于以上论述,本节进一步将物理观测下对称加密方案的安全性定义实例化,给出功耗泄漏下 DES 加密方案的安全性定义.

对于具有 DPA 攻击能力的敌手模型,如果攻击者从对获取密码算法执行的功耗轨迹分析中,不能获取密钥信息,那么该 DES 是安全的.

实例:$S\varepsilon=(K,\varepsilon,D)$是 DES 加密方案,$P_{DES}$是与其对应的物理实现.$A_{DPA,cpa}$是具有 DPA 攻击能力的多项式时间选择密文攻击敌手.$state()$为敌手观测到的中间物理状态,这里为异或运算产生的功耗轨迹.攻击实验包括 find、guess 两个阶段:

实验 $Exp^{DPA\text{-}FTG\text{-}cpa\text{-}b}_{P_{DES},A_{DPA,cpa}}(k)$:

$K\xleftarrow{R}\kappa(k)$;

$(x_0,x_1,s)\leftarrow A^{\varepsilon_K(\cdot)}_{DPA,cpa}(k,\text{find})$;

$y\leftarrow P_{DES}(x_b)\hat{I}A_{DPA,cpa}(k)\rightarrow state()$;

$d\leftarrow A_{DPA,cpa}(k,\text{guess},y,s,state())$;

Return d.

定义敌手的优势为:

$$Adv^{DPA\text{-}FTG\text{-}cpa}_{P_{DES},A_{DPA,cpa}}(k)=\Pr[Exp^{DPA\text{-}FTG\text{-}cpa\text{-}1}_{P_{DES},A_{DPA,cpa}}(k)=1]-\Pr[Exp^{DPA\text{-}FTG\text{-}cpa\text{-}0}_{P_{DES},A_{DPA,cpa}}(k)=1]$$

加密方案的优势函数定义为:

$$Adv^{DPA\text{-}FTG\text{-}cpa}_{P_{DES}}(k,t,q_e,\mu_e)=\max_{A_{DPA,cpa}}\{Adv^{DPA\text{-}FTG\text{-}cpa}_{P_{DES},A_{DPA,cpa}}(k)\}$$

结论 DPA 攻击下的不可分辨性之 DPA-FTG:如果对于任意多项式时间敌手的优势,$Adv^{DPA\text{-}FTG\text{-}cpa}_{P_{DES},A}(\cdot)$是可忽略的,则称该对称加密方案是 DPA-FTG 安全的.

考虑第 4 部分的结论 1 和结论 2,该方法使实验中的中间状态 $state()$,即异或运算呈现的功耗轨迹不能反应出与密钥相关的运行信息,即敌手的观测信息并没有破坏异或运算的单向性.用可证安全的归约方法可推知敌手获取的观测信息不能破坏不可分辨性.敌手的攻击优势 $Adv^{DPA\text{-}FTG\text{-}cpa}_{P_{DES},A}(\cdot)$是可忽略的,则称改进后的 DES 算法在该类型的功耗观测下是可证安全的.

7 总结与展望

本文通过实验验证了对密码设备执行时的物理观测效应的分析,敌手可以利用有限的资源在多项式时间内获取密钥信息,然而传统的加密方案并没有考虑物理观测效应对密码体制安全性的影响,使得加密方案的安全性定义在具有物理观测能力的敌手模型下显得束手无策.文章在 Micali 和 Reyzin 模型基础上,结合对称加密方案的可证安全定义,给出物理可观测下对称加密方案的可证安全定义,构建了物理观测环境下的 DES 系统安全性方案模型并形式化表述了 DES-DPA 物理观测可证安全性.如果敌手从获取的物理泄漏信息不能推导出秘密信息,那么该观测是无效的;当密码设备的物理泄漏不可避免时,可转而期望于对算法的改进,使秘密信息不直接参与运算,这就涉及到如何设计和实现新的密码应用的问题,使之能适应当前大量存在的旁路攻击环境.

参考文献:

[1] M L Akkar, C Giraud. An implementation of DES and AES secure against some attacks[A]. Cryptographic Hardware Embedded System-CHES 2001[C]. Paris: Springer-Verlag, 2001. 309 - 318.

[2] J A Fournier, S Moore, H Li, R D Mullins, G. S Taylor. Security evaluation of asynchronous circuits[A]. Cryptographic Hardware Embedded System-CHES 2003[C]. Cologne: Springer-Verlag, 2003. 137 - 151.

[3] S Mangard. Hardware countermeasures against DPA-a statistical analysis of their effectiveness[A]. CT-RSA 2004[C]. San Francisco: Springer-Verlag, 2004. 222 - 235.

[4] 李翔宇,孙义和. 采用数据流模式提高乱序执行密码芯片的安全性[J]. 电子学报, 2007, 35(2): 202 - 206.
Li Xiang-yu, Sun Yi-he. Improve the security of random executing encryption ICs by the data flow mode[J]. Acta Electron-

ica Sinica,2007,35(2):202 - 206. (in Chinese)

[5] G Yeap. Practical Low Power Digital VLSI Design[M]. USA: Kluwer Academic Publishers,1998.

[6] E Brier, C Clavier, F Olivier. Correlation power analysis with a leakage model[A]. Cryptographic Hardware Embedded System-CHES 2004[C]. Boston: Springer-Verlag,2004. 16 - 29.

[7] Federal Information Processing Standards Publication 46 - 3 (FIPS PUB 46 - 3): Data Encryption Standard[S].

[8] T S Messerges, E A Dabbish, R H Sloan. Examining smartcard security under the threat of power analysis attacks[J]. IEEE Transactions on Computers,2002,51(5):541 - 552.

[9] S Micali, L Reyzin. Physically observable cryptography (extended abstract)[A]. 1st Theory of Cryptography Conference[C]. Cambridge, MA: Springer-Verlag,2004. 278 - 296.

[10] A W Dent, J MaloneLee. The physically observable security of signature schemes[A]. Cryptography and Coding: 10th IMA International Conference[C]. Cirencester, UK: Springer-Verlag,2005. 220 - 232.

[11] F X Standaert, T G Malkin, M Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks[OL]. http://eprint.iacr.org/2006/139.

[12] O Goldreich, Foundations of Cryptography-Basic Applications[M]. Cambridge University Press,2004.

[13] S Goldwasser, S Micali. Probabilistic encryption[J]. Journal of Computer and System Science,1984,28:270 - 299.

[14] S Goldwasser, S Micali, R Rivest. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal of Computing,1988,17(2):281 - 308.

[15] M Bellare, P Rogaway. Random oracles are practical: a paradigm for designing efficient protocols[A]. The 1st ACM Conf. on Computer and Communications Security[C]. New York: ACM Press,1993. 62 - 67.

[16] M Bellare, A Desai, E Jokipii, P Rogaway. A concrete security treatment of symmetric encryption[A]. In 38th Annual Symposium on Foundations of Computer Science[C]. Miami Beach: IEEE Computer Society Press,1997. 394 - 403.

作者简介:

陈开颜　女,1970 年生于黑龙江齐齐哈尔. 中国人民解放军军械工程学院计算机工程系软件工程教研室副教授,博士研究生. 研究方向为信息安全.

E-mail: chen.wu2007@yahoo.com.cn

张　鹏　男,1976 年生于湖北罗田. 中国人民解放军军械工程学院计算机工程系博士研究生. 研究方向为电磁信息检测与主动防护技术、信息安全.