

针对智能卡的断电式功耗分析攻击

赵崇征¹, 张 鹏², 赵 强²

(1 北京橙时代信息技术有限公司, 北京 100080; 2 军械工程学院 计算机工程系, 河北 石家庄 050003)

摘 要: 针对智能卡采用个人身份码和密码算法双重保护机制, 提出一种截断电源式的功耗分析方法, 突破个人身份码的输入次数限制, 通过穷举搜索获取个人身份码. 并利用差分功耗分析技术, 在 40000 个明文样本的情况下, 攻击得到原型智能卡中 DES 密码的密钥.

关键词: 智能卡; 功耗分析; 个人身份码; 数据加密标准

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2011)04-0171-05

A Power Analysis Attack with Cut off Power Technique Against Smart Cards

ZHAO Chong-zheng¹, ZHANG Peng², ZHAO Qiang²

(1 Beijing Orange Time Information Technology Co. Ltd. 100080, China;

2 Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: The personal identification number (PIN) and encryption technologies are commonly used to form dual protection mechanism for smart cards. In this paper, a novel power analysis attack with a cut off power technique against smart cards is proposed. This attack can bypass the restriction on the times of PIN inputs to obtain it through the exhaustive search. And the differential power analysis experiment on DES implemented in an exemplary smart card showed that the secret key of DES was recovered successfully with 40000 plaintext samples.

Key words: smart cards; power analysis; personal identification number; data encryption standard

1 引言

近年来, 智能卡(Smart Cards)的应用正在不断增长. 从传统的信用卡和借记卡, 到移动电话 GSM 卡、电子护照、新一代身份证、健康保险卡和驾驶执照等身份卡, 到处可见智能卡的身影. 与上一代只具有数据存储能力的磁条卡相比, 新型的智能卡拥有更为完善的防篡改设计和身份认证与数据加密机制, 能有效地对付伪造和数据偷窃行为. 由于普遍采用防篡改设计, 因此智能卡可以抵御电子显微扫描等侵入式攻击方式, 但是, 在面对新型的非侵入式旁路攻击(Side Channel Attack, SCA)^[1]技术时, 智能卡的安全性受到很大威胁. 已经有许多利用功耗分析旁路攻击技术对智能卡进行成功攻击的案例^[2-6].

这些案例几乎无一例外地都回避了如何突破当前智能卡所采用的个人身份码(Personal Identification Number, PIN)认证技术这一问题, 它们都将 PIN 码作为已知前提. 但是, 当 PIN 码未知时(这是更为常见的情况), 特别是采用有限尝试次数的 PIN 码认证机制时, 传统的功耗分析技术将难于进行. 文中利用主动断电式的功耗分析技术突破 PIN 码认证保护机制, 并进一步获取智能卡的内部加密密钥.

2 智能卡的安全机制

智能卡的安全大致可分为两个部分: 硬件安全与功能实现安全. 硬件安全是指智能卡如何应对外界恶意攻击者对智能卡的非法使用与敏感数据窃取; 功能实现安全是指智能卡采用什么手段保障数

收稿日期: 2010-06-08; 修回日期: 2010-08-15

基金项目: 国家自然科学基金项目(60940019); 国家“八六三”计划项目(2007AA01Z454)

据存储、签名认证等承载功能的安全实现. 二者相辅相成, 缺一不可. 对于前者, 最常见的是采用包含 PIN 认证的三方认证机制与防篡改设计; 对于后者, 一般采用 DES、AES、RSA、SHA 等数据加密或签名算法实现.

2.1 三方认证机制

智能卡的使用必须与读卡器(如 POS 终端机)接合进行. 为了保障智能卡是合法卡, 其使用者是合法用户, 并且智能卡插入的读卡器是合法终端, 必须对三方进行认证. 一般可采用三层认证方式(见图 1). 其认证流程为: 读卡器发送一个随机数给智能卡, 智能卡使用对称密码算法进行加密(密钥与终端共享)后送回, 读卡器解密后与自己发送的随机数进行比对. 随后, 由智能卡生成一个随机数发送给读卡器, 读卡器加密后返回由智能卡进行解密比对, 从而完成硬件双方身份认证, 并且在双方之间建立起一个秘密信道. 当然, 由于任何时候智能卡都不能发起通信, 上述第二步也必须先由读卡器发出请求, 智能卡响应请求才发送随机数. 第三步即采用 PIN 认证对使用者身份进行确认. PIN 通常为 4 至 8 位十进制数, 为了防止穷举攻击, 使用者只有有限次(如 3 次)输入尝试机会. 一旦输入全部错误, 智能卡将被锁死.

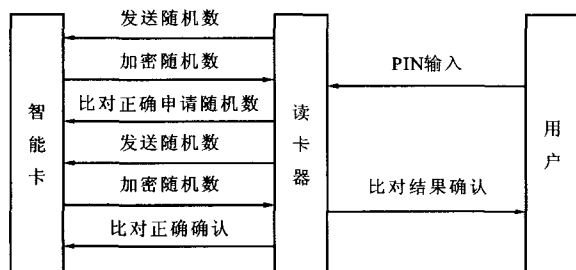


图 1 智能卡系统认证示意图

2.2 PIN 认证算法

最常见的 PIN 认证方式见算法 1.

算法 1 PIN 认证 VerifyPIN()

```
Function VerifyPIN(pin, length)
{ RemainingCounter=TriesLimit;
if RemainingCounter>0
{ Input(pin, length);
if length==CardPinLength &
CompareArrays(pin, CardPin, length)==true
{ RemainingCounter= TriesLimit;
return true;
}
RemainingCounter--; }
return false;
```

}

上述算法中, RemainingCounter 为尝试计数器, 该值一般存在 EEPROM 中, 断电内容不失. CompareArrays 对输入的 pin 与真实 CardPin 进行比对. 为了加快速度, 该函数通常以按位方式进行比对, 一旦某位对比不相同, 则函数返回错误. 其算法伪码见算法 2.

算法 2 数组比对算法 CompareArrays()

```
Function CompareArrays(value1, value2, length)
{ for (i = 0; i < length; i++)
{ if (value1[i] != value2[i])
return false;
}
return true;
}
```

显然, 算法 2 的运行同输入 pin 值密切相关, 若与 CardPin 不相同的位出现越早, 则算法 2 结束越快. 这将使得算法执行时间或功耗表现有所不同.

当然, 为了增强安全性, CardPin 可能并不是以明文方式进行储存, 而是通过对称密码算法(如 DES^[7])进行加密后进行存储. 此时需要对输入的 pin 以相同密钥进行加密后再输入算法 1 进行认证, 同时算法 2 对应于按字节(对于 DES 加密来说共 8 字节)方式进行比对, 一旦某字节对比不相同, 则函数返回错误.

2.3 功能实现安全

为了实现数字签名, 智能卡一般采用以 RSA、SHA 等密码算法为核心的密码机制; 为了实现数据加密, 一般使用对称密码算法. 以后者为例, 可以用 DES 算法实现, 此时需要对 DES 的密钥进行保护. 该密钥可以由授权用户写入, 但非授权用户无法读取.

可见, 智能卡安全包括 pin 安全与秘密密钥安全, 一旦 pin 被获取, 则智能卡可被非法用户所使用, 而一旦秘密密钥被窃取, 则智能卡被完全破解.

3 针对 pin 的断电式功耗分析攻击

由于智能卡 pin 的位数不长, 以典型的 4 位为例, 此时 pin 的可能值空间为 10000, 完全可以通过穷举搜索的方式打到正确的值. 但是, 由于尝试次数的限制, 无法实现穷举搜索. 算法 1 中, 当输入 pin 值不正确时, RemainingCounter 值将减 1. 如果能够在 CompareArrays() 函数运行之后, 并且在该计数器值变化之前的时刻对智能卡实现断电, 冻结 RemainingCounter 计数器, 则既可通过 CompareAr-

rays()的运行情况分析输入 pin 的正确性,又可保留尝试次数.通过重新上电并测试另一个 pin 值,可以实现穷举攻击.

3.1 攻击方法

不失一般性,攻击针对一个接触型智能卡系统原型,其中智能卡由等效芯片实现,读卡器由 51 单片机设计等效电路实现.读卡器与智能卡之间接口符合 ISO 7816 标准^[8].攻击原理见图 2.攻击系统主要由智能卡芯片、读卡器电路、断电控制电路、功耗测量与分析部分等组成.

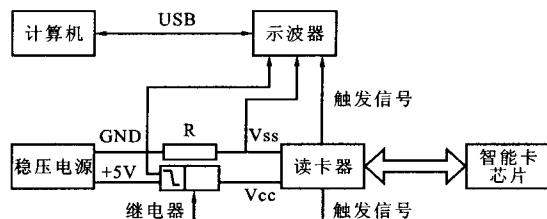


图2 针对智能卡 pin 的功耗分析攻击示意图

图2中,在外部稳压电源与读卡器的地端之间串联电阻R,通过对R上的压降进行测量实现功耗测量,这也是功耗分析攻击普遍采用的功耗测量模式.断电式攻击过程为:

(1) 系统上电工作,计算机初始化示波器,输入猜测 pin 值;

(2) 当读卡器进行 CompareArrays 操作时,触发示波器记录功耗信号;

(3) CompareArrays 操作完成时,触发继电器断开电源,示波器将功耗轨迹传给计算机;

(4) 分析得到的功耗信号,验证猜测 pin 值是否正确;

(5) 若 pin 值不正确,则更改猜测值,并重新执行步骤(1)~(4),直至找到正确的 pin.

上述步骤中,最关键的在于两种触发信号的产生与功耗信号分析技术.对于示波器的触发,为简化,实验是通过在 VerifyPIN 算法中相关位置插入信号发生指令实现.当然,如果为了保证 VerifyPIN 算法的完整性,也可以在算法调度时触发,这样记录的功耗轨迹稍长,但分析方法不变.下面分别给出继电器的触发与功耗信号分析技术.

3.2 断电策略

对读卡器进行断电的关键在于时机.必须在 RemainingCounter 计数器值变化之前的瞬时完成.为简化,实验是在该计数器变化之前插入信号发生指令实现继电器触发.尽管在实际情况中这种指令插入方式无法实现,但是仍然有方法可以精确地控

制继电器动作.其假设前提是攻击者拥有已知 pin 的同类型智能卡,并且相同类型智能卡的运行功耗特性类似.这种假设条件是很容易满足的,事实上,这也正是被广泛使用的模板分析^[9]所必须的条件之一.以使用 DES 加密 pin 的智能卡为例,采用触发断电并加强 3.1 节的攻击策略如下:

(1) 对已知 pin 的智能卡进行操作,记录 CompareArrays()函数(算法2)的运行计时与功耗特征;

(2) 定位算法2中循环体中第一次、第二次循环结束的時刻,分别记为 t_1 、 t_2 ;

(3) 通过计时电路将继电器的断开時刻定位在 t_1 時刻;

(4) 对被攻击智能卡输入猜测 pin,可以获得算法2中第一次循环的功耗轨迹,并与第一步中的轨迹进行对比,如不同则说明猜测错误,更换猜测 pin 后重复执行第(4)步,如相同则执行第(5)步;

(5) 通过计时电路将继电器的断开時刻定位在 t_2 時刻;

(6) 对被攻击智能卡输入与第(4)步相同的猜测 pin,可以获得算法2中前两次循环的功耗轨迹,并与第一步中的轨迹进行对比,如不同则说明猜测错误,更换猜测 pin 后重复执行第(4)步,如相同则判断得到正确 pin.

事实上,由于 DES 对 pin 进行加密后得到 8 字节密文,若猜测 pin 正确,则算法2的循环需要执行 8 次比对.但是由于 DES 的混乱作用,两个不同的 pin 值进行加密后第 1 字节相同的概率为 $1/2^8$,对于 10000 的 pin 值空间来说肯定会产生碰撞(即不同的 pin 值产生的密文第 1 字节相同),前 2 字节都相同的概率为 $1/2^{16}$,此时产生碰撞的概率已经很小(约为 0.15),因此可以通过密文前 2 字节的对比确定 pin 值.而上述第 4 步是为了更快地预先排除非正确 pin.

3.3 pin 输入判断策略

对功耗轨迹进行比对实际上有点类似于逆向工程.已经有一些应用的实例.如前所述,判断的前提是当算法2循环体中 if 语句判断比对相同操作对应的功耗特征相同,并且与比对不同的功耗特征不同.对功耗轨迹进行对比的具体技术可以采用神经网络、模板、差分等多种方法.

4 针对秘密密钥的功耗分析攻击

当 pin 值被破解以后,就可以进一步获取智能卡密码算法的秘密密钥,仍以 DES 密码算法为例,

可以采用差分功耗分析(Differential Power Analysis, DPA)方法^[2]进行攻击。

4.1 差分功耗分析原理

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,它采用分而治之策略,将密钥分成若干个子密钥块分别进行猜测。

第 1 步:进行 DPA 攻击,首先需要 ① N 个随机的明文输入 $PT_i (1 \leq i \leq N)$; ② $S_i[j]$: 对第 i 次功耗进行离散采样形成的功耗数组, j 表示采样的时间点; ③ 对应于 PT_i 的相应密文输出 CT_i ; 事实上 PT_i 和 CT_i 只需要知道其中之一就可以了。下面以获取 CT_i 为例。

第 2 步:定义一个与 b 位子密钥块 K_b 密切相关的函数 $D(CT_i, K_b)$, 并猜测令 $K_b = 0$, 将基于采样时间点 j 的信号数组集合 $\{S_i[j] | 1 \leq i \leq N\}$ 分成两个子集合:

$$S_0 = \{S_i[j] | D(\cdot) = 0, 1 \leq i \leq N\}$$

$$S_1 = \{S_i[j] | D(\cdot) = 1, 1 \leq i \leq N\}$$

第 3 步:计算集合 S_0 与 S_1 平均功耗值

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

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

$$|S_0| + |S_1| = N$$

并得到 DPA 差分信号数组

$$T[j] = A_0[j] - A_1[j]$$

第 4 步:如果 $T[j]$ 代表的差分功耗曲线上在某个位置出现明显的尖峰,那么代表 K_b 猜测正确,继续执行第 5 步。否则,转第 2 步,并修改猜测令 $K_b = K_b + 1 (K_b \leq 2^b)$ 。循环运行直到 K_b 猜测正确。

第 5 步:按上述方法获取所有的子密钥块以后,计算得到整个密钥。

合适的 D 函数的选择是 DPA 攻击的关键。正确的 D 函数能产生期望的 DPA 差分信号,这个信号能够验证所猜测的密钥子集的正确性。实验采用的 D 函数见文献^[4]。

4.2 针对智能卡 DES 的 DPA 攻击

实验原理图如图 3 所示。由计算机产生随机明文,通过读卡器传送给智能卡执行 DES 加密,密钥预先存储在智能卡芯片中。在读卡器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读卡器的功耗变化。在执行 DES 加密时,由读卡器触发示波器记录功耗

波形,并通过 USB 接口回传给计算机。

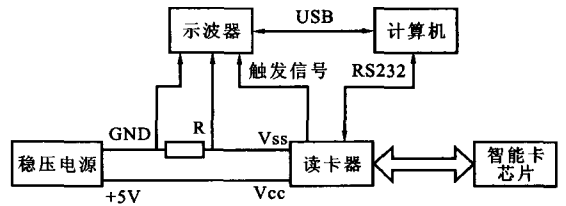


图 3 针对智能卡 DES 的功耗分析攻击示意图

针对 DES 第 16 轮加密的第 1 字节子密钥,采用 Tektronix DPO4032 示波器,每条轨迹 25M/s 采样率, $40\mu s$ 采样时间,共 40000 个明文样本情况下,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 4),而错误的密钥对应的差分曲线没有明显的尖峰(见图 5)。利用同样的方法可以获取 48 位子密钥。根据 DES 产生密钥的标准算法,可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。

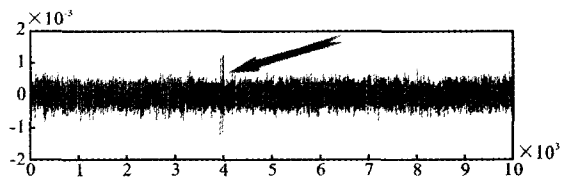


图 4 正确猜测的 DES 6 位密钥对应的差分功耗曲线尖峰

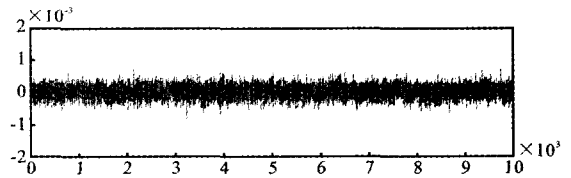


图 5 猜测错误的 DES 6 位密钥对应的差分功耗曲线

5 结束语

尽管现代智能卡普遍采用防篡改设计,可以有效抵御芯片拆解等侵入式攻击方式,并且通过 pin 认证机制,可以抵御需要大量攻击样本的非侵入式功耗分析攻击。文中提出的精确控制断电方式的功耗分析技术,可以破解带尝试次数限制的 pin 认证机制,并且获得差分功耗分析所需要的样本,从而突破智能卡的安全机制。需要对智能卡的安全机制进行改进或更新,以抵御此类攻击。

参考文献:

- [1] Quisquater Jean Jacques, Samyde D. Side channel cryptanalysis[C]// Southeast European Cooperative Initiative

- SECI 2002. [S. L.]; SEC, 2002:179—184.
- [2] Kocher P, Jaffe J, Jun B. Differential power analysis [C]// Proceedings of Advances in Cryptology. San Francisco, CA, USA; LNCS, 1999:388—397.
- [3] Messerges T S, Dabbish E A, Sloan R H. Investigations of power analysis attacks on smartcards[C]// Proceedings of USENIX Workshop on Smartcard Technology. Chicago, Illinois, USA; USE/X, 1999:151—162.
- [4] Messerges Thomas S, Dabbish Ezzy A, Sloan Robert H. Examining smartcard security under the threat of power analysis attacks[J]. IEEE Transactions on Computers, 2002, 51(5):541—552.
- [5] Peeters E, Standaert FX, Quisquater J J. Power and electromagnetic analysis: improved model, consequences and comparisons[J]. Special Issue of Integration, The VLSI Journal: Embedded Cryptographic Hardware, 2007, 40(1):52—60.
- [6] Mangard S, Oswald E, Popp T. Power analysis attacks—revealing the secrets of smart cards[M]. New York:Springer, 2007.
- [7] National institute of standards and technology. FIPS 46—3 data encryption standard(DES) [EB/OL]. (1999) [2010—06—08]. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>, 1999.
- [8] ISO. International Standard ISO 7816—3. Identification Cards: Integrated Circuits Cards with Contacts [S]. USA:ISO, 1997.
- [9] Chari S, Rao J R, Rohatgi P, et al. Cryptographic hardware and embedded systems—CHES 2002 [C]// Proceedings of 4th International workshop. Redwood Shores, CA, USA; LNCS, 2003:13—28.

作者简介:

赵崇征 男, (1977—), 博士. 研究方向为银行卡防欺诈研究、基于旁路攻击理论的攻击与防御.

张 鹏 男, (1976—), 博士. 研究方向为电磁信息检测与主动防护技术等.

赵 强 男, (1945—), 教授, 博士生导师. 研究方向为信息安全等.

(上接第 170 页)

- [4] 周国昌, 沈绪榜. 基于 LS CSIMD 的可变阶 FIR 并行算法研究[J]. 计算机工程, 2007, 33(1):7—9.
- [5] Chengzhi Pan. Streaming computing platform Design: DVB—T implementation on a reconfigurable architecture [D]. California: University of California, Irvine. 2005.
- [6] Amir Hosein Kamalizad. Several DVB—T cores mapping into morphosys architecture[D]. California: University

of California, Irvine. 2003.

作者简介:

周国昌 男, (1978—), 博士研究生. 研究方向为计算机结构、嵌入式片上设计.

张立新 男, (1968—), 研究员. 研究方向为卫星导航技术研究.