Journal of Computer Applications
计算机应用,2014,34(5):1283 - 1287,1330
ISSN 1001-9081
CODEN JYIIDU
2014-05-10
http://www.joca.cn

文章编号:1001 - 9081(2014)05-1283-05
doi:10.11772/j.issn.1001-9081.2014.05.1283

内置确定性子密钥相关系数功耗分析

李金良[1],郁　昱[1,2*],付　荣[2],李祥学[1]
(1.华东师范大学 计算机科学与技术系,上海 200241; 2.清华大学 交叉信息研究院,北京 100084)
(*通信作者电子邮箱 yuyu@yuyu.hk)

摘　要:针对 Komano 等(KOMANO Y, SHIMIZU H, KAWAMURA S. BS-CPA: built-in determined sub-key correlation power analysis. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010,E93-A(9):1632 - 1638.)对 dpacontest.org 平台提供的数据进行研究后提出的内置确定性子密钥相关系数功耗分析(BS-CPA)方法进行分析,并从破解所需功耗数据和成功率方面将 BS-CPA 与差分功耗分析(DPA)、相关系数功耗分析(CPA)进行比较分析,发现 BS-CPA 虽然理论上方法可行,但远未达到其声称的效果,进而从密码设备加密过程中寄存器状态的变化与功耗值的关系来选取中间变量,通过去除噪声和错误峰值,找到与密钥最相关数据点来缩小攻击范围。对于相同数量功耗数据,部分点攻击与全部点攻击相比,完全破解 64 位密钥的成功率最大可以提高 60%。实验结果表明改进后的模型攻击效率得到提升,达到同样成功率需要功耗数据少,攻击结果稳定。

关键词:差分功耗分析竞赛; 内置确定性子密钥相关系数功耗分析;攻击模型;智能卡安全
中图分类号: TP309.1　　**文献标志码**:A

Built-in determined sub-key correlation power analysis

LI Jinliang[1], YU Yu[1,2*], FU Rong[2], LI Xiangxue[1]
(1. *Department of Computer Science and Technology, East China Normal University, Shanghai* 200241, *China*;
2. *Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing* 100084, *China*)

Abstract: To study the Built-in determined Sub-key Correlation Power Analysis (BS-CPA) proposed by Yuichi Komano *et al.* (KOMANO Y, SHIMIZU H, KAWAMURA S. BS-CPA: built-in determined sub-key correlation power analysis. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A(9): 1632 - 1638.) based on the data set of dpacontest.org, this paper compared the efficiency of Differential Power Analysis (DPA), Correlation Power Analysis (CPA) and BS-CPA from the number of power consumption trace and success rate, the result shows that although BS-CPA works out nicely in theory, it is far from the reaching of the efficiency claimed by the authors, and then the intermediate was chosen by the relationship between the statement of executed cryptographic device' s register and power consumption. Attack surface was narrowed by the reduction of noise and ghost peak, the most relative point was filtered out. Compared with the whole point attack, the biggest success rate of partial point attack can be increased by 60% to crack the 64 bit keys for the same number traces. The experiment results prove that the improved model is able to increase the efficiency and decrease the needed power consumption trace for the same success rate, and the result is stable.

Key words: Differential Power Analysis (DPA) contest; Built-in determined Sub-key Correlation Power Analysis (BS-CPA); attack model; smart card security

0　引言

差分功耗分析(Differential Power Analysis, DPA)最初是由 Kocher 等[1]在 1999 年提出,其主要原理是利用密码设备在执行过程中产生的旁路信息,如文献[1]中提到的能量消耗,文献[2]中的电磁辐射以及文献[3]中的执行时间等物理特性与密钥之间的关系来获取密钥。以功耗分析为典型代表的侧信道攻击(Side-Channel Attack, SCA)方法的出现,极大地增强和扩展了传统的密码分析方法,对密码设计和芯片实现工艺构成了严峻挑战。目前,我国人民银行的标准 PBOC3.0 里面主要采用三重数据加密标准(Triple Data Encryption Standard, 3DES)分组加密算法,因此对于数据加密标准(Data Encryption Standard, DES)加密算法及其在密码设备上具体实现过程的安全性研究很有意义。DPA 竞赛[4]是由 Telecom PairsTech COMELEC 部门组织,目的主要是为来自不同院校和公司的研究人员提供一个相对客观公正地评估不同攻击方法的平台,以促进 DPA 攻击改进和发展,该竞赛得到了国际密码协会(International Association For Cryptologic Research, IACR)[5]举办的主流会议 CHES(Cryptographic Hardware And Embedded Systems)[6]的倡导和响应。文献[7]提到的相关系数功耗分析(Correlation Power Analysis, CPA)攻击是对一阶 DPA 攻击的改进,通过分析能量消耗和中间变量之间的关系来获取密钥,选取的中间变量与密钥以及已知信息(如明文

收稿日期:2013-11-18;**修回日期**:2013-12-31。　**基金项目**:国家自然科学基金资助项目(61103221)。
作者简介:李金良(1986 -),女,湖北荆门人,硕士研究生,主要研究方向:信息安全; 郁昱(1981 -),男,江苏张家港人,助教,博士,主要研究方向:信息安全、密码学; 付荣(1989 -),男,贵州六盘水,硕士研究生,主要研究方向:信息安全; 李祥学(1974 -),男,上海人,副教授,博士,主要研究方向:信息安全、密码学、编码学。

《计算机应用》Journal of Computer Applications

或者密文)相关,例如,数据加密标准或者高级加密标准(Advanced Encryption Standard, AES)加密可以选取替换盒(Substitution BOX, SBOX)输出。差分功耗攻击、简单功耗攻击(Simple Power Analysis, SPA)以及相关系数功耗分析攻击等基本分析方法,都是运用数学模型建立芯片功耗与密钥之间的关系。

本文主要研究了 Komano 等[8]提出的内置确定性子密钥相关系数功耗分析攻击(Built-in determined Subkey Correlation Power Analysis, BS-CPA),该攻击是对原有 CPA 的扩展,基本思想是利用已经攻击得到的子密钥来计算当前未知的子密钥,更加有效地利用密钥信息,从而减少破解密钥所需的功耗数据数量,但是相比传统的攻击手段,其攻击结果过于理想,并不符合其提出的攻击模型的优化。

针对上述问题,本文主要分析对比 DPA、CPA 和 BS-CPA 的效率和成功率,深入解析 BS-CPA 存在的问题,并进行了改进。通过对不同攻击方法进行大量攻击测试,分析几种主要攻击方法的真实差距,发现 BS-CPA 仅仅在 CPA 的基础上有一点提高,对其中声称的"改进明显"的攻击结果,也进行了比较研究,根据实验结果分析推测其应该是在功耗数据中进行了一定的数据预处理,提高攻击的准确性,减小了攻击的难度。

1 相关背景

1.1 汉明重量模型和汉明距离模型

常用的攻击模型有汉明重量模型和汉明距离模型。文献[9]提到的汉明重量模型中,攻击者假设能量消耗与所处理的数据中被置位的比特数成正比,不考虑前后的变化状态,可以表示成 $\boldsymbol{W} = aHW(\boldsymbol{D}) \oplus b$, $\boldsymbol{W}$ 表示假设能量消耗值,HW 是汉明重量函数,$\boldsymbol{D}$ 是与处理数据相关的中间变量,a 是一个标量系数,b 是与噪声、时间、位移等相关的变量。文献[9]中提到的汉明距离模型基本思想是计算数字电路在某时刻内 1→0 和 0→1 转化的总数,之后利用转化的总数来刻画电路的能量消耗,这里假设所有的 1→0 和 0→1 转化所产生的能量消耗都相同,不考虑各个元件和不同导线寄生电容的区别,并且忽略元件的静态能量消耗,总能量消耗可以简单地表示为 $\boldsymbol{W} = aHD(\boldsymbol{D},\boldsymbol{R}) \oplus b$,其中:$\boldsymbol{W}$ 是假设能量消耗,HD 是汉明距离函数,$\boldsymbol{D}$ 是与所处理数据相关的中间变量,$\boldsymbol{R}$ 是参考状态,a 和 b 意义与上文相同,通常汉明距离 $HD(\boldsymbol{D},\boldsymbol{R})$ 可以通过 $HW(\boldsymbol{D} \oplus \boldsymbol{R})$ 计算得到。

以 DES 加密算法为例,其加密流程如图 1 所示,解密过程相同,只是密钥逆序,这保证了加密和解密能够使用一个电路结构,不同加密的细节可能略有变化,但是它们的基本结构相同。实验初始阶段,直接对 SBOX 的输出用汉明重量模型建模,将功耗迹按照汉明重量值进行分类解析,由于每个 SBOX 盒的输出为 4 个比特位,共有 16 种取值(0000,0001,0010,…,1110,1111),其汉明重量值是比特位为 1 的个数,分别对应(0,1,1,2,…,3,4)因此其汉明重量值范围为[0,4],例如 SBOX 输出为 1011,那么对应的汉明重量 HW(SBOX)为 3。由于 SBOX 盒输出与明文和密钥相关,理论上通过大量的统计分析可以找出每个 SBOX 对应的子密钥 sub-key,最终获取整个密钥。为了简化实现过程,根据 Thanh-Ha Le 等提到的 Multi-bit DPA 方法[10]将功耗迹按照 SBOX 盒输出的汉明重量分为两类(汉明重量值属于[0,2)为一类,汉明重量值属于[2,4]为另外一类)进行分析,但实验结果表明其效果并不理想,由此推断汉明重量模型不符合所用加密设备产生的功耗。进一步分析 DES 加密在芯片中具体实现,由于每轮加解密过程在同一寄存器中实现,可以选取相邻轮数在寄存器中的汉明距离进行建模。由于密钥和明文(或密文)之间的相关性在第一轮和最后一轮最强,在加密过程中,相关性在其他轮中被逐渐分散,因此选择首尾两轮作为攻击目标。为了描述密钥对功耗数据的影响,考虑将第 1 轮和第 2 轮输出的右 32 位的汉明距离(或者第 15 轮和第 16 轮输出的左 32 位的汉明距离)作为攻击目标值。$\boldsymbol{R}_0$ 和 $\boldsymbol{R}_1$ 的汉明距离与密钥密切相关,因此这是一个合理的攻击模型,可以表示为:

$$HD(\boldsymbol{R}_0,\boldsymbol{R}_1) = HW(\boldsymbol{R}_0 \oplus \boldsymbol{R}_1)$$

为了更好地说明 DES 加密过程,作以下定义:$\boldsymbol{L}_i$ 和 $\boldsymbol{R}_i$ 表示第 i 轮加密时,加密值的左 32 位和右 32 位值;l_i 和 r_i 表示第 i 轮解密时,解密值的左 32 位和右 32 位值;F 表示加解密中的轮函数,其中包括 S 盒变换、扩展和异或等操作;$\boldsymbol{A}$ 表示随机明文,每一条功耗数据都是对这一随机明文的加密记录;$\boldsymbol{B}$ 表示加密之后的密文。从 DES 加密过程中,可以得到下面的加密关系:

$$\boldsymbol{L}_1 = \boldsymbol{R}_0, \boldsymbol{R}_1 = F(\boldsymbol{key}_1, \boldsymbol{R}_0) \oplus \boldsymbol{L}_0;$$
$$\boldsymbol{L}_2 = \boldsymbol{R}_1, \boldsymbol{R}_2 = F(\boldsymbol{key}_2, \boldsymbol{R}_1) \oplus \boldsymbol{L}_1;$$
$$\cdots$$
$$\boldsymbol{L}_{15} = \boldsymbol{R}_{14}, \boldsymbol{R}_{15} = F(\boldsymbol{key}_{15}, \boldsymbol{R}_{14}) \oplus \boldsymbol{L}_{14};$$
$$\boldsymbol{L}_{16} = \boldsymbol{R}_{15}, \boldsymbol{R}_{16} = F(\boldsymbol{key}_{16}, \boldsymbol{R}_{15}) \oplus \boldsymbol{L}_{15};$$

最后将得到输出的密文:

$$\boldsymbol{B} = IP^{-1}(\boldsymbol{L}_{16} \| \boldsymbol{R}_{16})$$

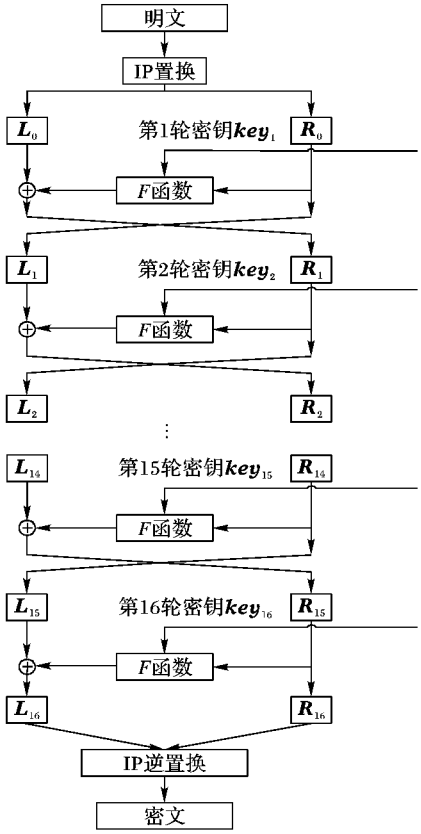

图 1 DES 加密流程

同理,对于解密过程来说,基本流程相同,密钥逆序,最后加密的子密钥第一个进行解密,最先加密的子密钥在最后进

Journal of Computer Applications 《计算机应用》

行解密：

$$IP(\boldsymbol{B}) = \boldsymbol{l}_0 \| \boldsymbol{r}_0$$

注意到，这里有：

$$\boldsymbol{l}_0 = \boldsymbol{L}_{16}$$
$$\boldsymbol{r}_0 = \boldsymbol{R}_{16}$$
$$\boldsymbol{l}_1 = \boldsymbol{r}_0 = \boldsymbol{R}_{16} = \boldsymbol{R}_{15}$$
$$\boldsymbol{r}_1 = F(\boldsymbol{key}_{16}, \boldsymbol{r}_0) \oplus \boldsymbol{l}_0 = F(\boldsymbol{key}_{16}, \boldsymbol{R}_{15}) \oplus \boldsymbol{L}_{16} = \boldsymbol{L}_{15}$$
$$\boldsymbol{l}_2 = \boldsymbol{r}_1 = \boldsymbol{L}_{15} = \boldsymbol{R}_{14}$$
$$\boldsymbol{r}_2 = F(\boldsymbol{key}_{15}, \boldsymbol{r}_1) \oplus \boldsymbol{l}_1 = F(\boldsymbol{key}_{15}, \boldsymbol{R}_{14}) \oplus \boldsymbol{R}_{15} = \boldsymbol{L}_{14}$$
$$\cdots$$
$$\boldsymbol{l}_{15} = \boldsymbol{r}_{14} = \boldsymbol{L}_2 = \boldsymbol{R}_1$$
$$\boldsymbol{r}_{15} = F(\boldsymbol{key}_2, \boldsymbol{r}_{14}) \oplus \boldsymbol{l}_{14} = F(\boldsymbol{key}_2, \boldsymbol{R}_1) \oplus \boldsymbol{R}_2 = \boldsymbol{L}_1$$
$$\boldsymbol{l}_{16} = \boldsymbol{r}_{15} = \boldsymbol{L}_1 = \boldsymbol{R}_0$$
$$\boldsymbol{r}_{16} = F(\boldsymbol{key}_1, \boldsymbol{r}_{15}) \oplus \boldsymbol{l}_{15} = F(\boldsymbol{key}_1, \boldsymbol{R}_0) \oplus \boldsymbol{R}_1 = \boldsymbol{L}_0$$

最终，将得到解密输出，即原始明文：

$$IP^{-1}(\boldsymbol{l}_{16} \| \boldsymbol{r}_{16}) = IP^{-1}(\boldsymbol{L}_0 \| \boldsymbol{R}_0) = \boldsymbol{A}$$

1.2　差分功耗分析攻击

差分功耗分析攻击（DPA）是利用大量的功耗数据进行统计分析的方法。通常，按照处理的比特位数可以分为单比特差分功耗分析（Mono-bit Differential Power Analysis，Mono-bit DPA）攻击[10]34 和多比特差分功耗分析（Multi-bit Differential Power Analysis，Multi-bit DPA）攻击[10]35。Mono-bit DPA 攻击是将采集到的功耗数据按照所处理的一位比特（b）分为两部分，例如 DES 加密算法第一个 SBOX 输出的第一个比特位，之后，计算两类的差值 $\Delta_D(b)$，其表达式如式（1）所示：

$$\Delta_D(\boldsymbol{b}) = \frac{\sum_{i=1}^{N} D(\boldsymbol{C}_i, \boldsymbol{b}, \boldsymbol{K}_S) W(\boldsymbol{C}_i)}{\sum_{i=1}^{N} D(\boldsymbol{C}_i, b, \boldsymbol{K}_S)} - \frac{\sum_{i=1}^{N} (1 - D(\boldsymbol{C}_i, \boldsymbol{b}, \boldsymbol{K}_S)) W(\boldsymbol{C}_i)}{\sum_{i=1}^{N} (1 - D(\boldsymbol{C}_i, \boldsymbol{b}, \boldsymbol{K}_S))} \tag{1}$$

D 是区分函数，$\boldsymbol{C}_i$ 对应明文或者密文，$\boldsymbol{b}$ 是与已知明文或者密文相关的中间变量，$\boldsymbol{K}_S$ 是假设密钥，$W(\boldsymbol{C}_i)$ 对应真实能量消耗。理论上，如果采集的功耗数据数量充分，并且加密数据分布均匀，那么正确的密钥对应的差分值在某个时刻最大，由此可以判断出正确的子密钥。Multi-bit DPA 是对 Mono-bit DPA 的改进，它同时利用多个比特位进行计算分析，目前主要有两种方法。一种是 Messerges 等[11] 提出，这种方法同时计算 d 个比特位然后将功耗数据分为两大类，可以表示为式（2）：

$$\begin{cases} \boldsymbol{G}_0 = \{W(\boldsymbol{C}_i), i = 1,2,\cdots,N \mid HW(\boldsymbol{C}_i, \boldsymbol{B}, \boldsymbol{K}_S) < d/2\} \\ \boldsymbol{G}_1 = \{W(\boldsymbol{C}_i), i = 1,2,\cdots,N \mid HW(\boldsymbol{C}_i, \boldsymbol{B}, \boldsymbol{K}_S) \geqslant d/2\} \end{cases} \tag{2}$$

其中：$HW(\boldsymbol{C}_i, \boldsymbol{B}, \boldsymbol{K}_S)$ 表示汉明重量，$\boldsymbol{C}_i$，$\boldsymbol{K}_S$ 与上文相同，$\boldsymbol{B}$ 是选取的中间变量，这里对应 SBOX 输出的多个比特位，差分值通过 $\Delta_H(\boldsymbol{B}) = \sum(\boldsymbol{G}_1 W(\boldsymbol{C}_i))/N_1 - \sum(\boldsymbol{G}_0 W(\boldsymbol{C}_i))/N_0$ 计算，N_0 和 N_1 是属于 $\boldsymbol{G}_0$，$\boldsymbol{G}_1$ 集合的数量。另一种方法是单独计算 $\boldsymbol{B}$ 中的每一个比特 $\boldsymbol{b}_i$，然后得到所有比特位的总和，$\sum_D(\boldsymbol{B}) = \Delta_D(\boldsymbol{b}_i) + \cdots + \Delta_D(\boldsymbol{b}_n)$，Bevan 等[12] 计算了 4 比特的情况，这种方法只有在所有比特位能够同时以同样方式影响能量消耗的情况下有效。Le 等[13] 提出的 PPA（Partioning Power Analysis）方法对多比特差分功耗分析攻击进行了一般化推理，将功耗数据分为 $d+1$ 组进行分析。

1.3　相关系数功耗分析攻击

相关系数是确定数据间线性关系常用的方法，CPA 通过分析能量消耗和假设能量模型（HD 或者 HW）之间的关系来获取密钥，根据文献[7]，能量消耗 W 和能量模型线性相关，正确密钥所对应相关系数最大，相关系数 ρ_{WH} 可以通过式（3）计算得到：

$$\hat{\rho}_{\mathrm{WH}}(\boldsymbol{R}) = \frac{N\sum W(\boldsymbol{C}_i) HD_{i,R} - \sum W(\boldsymbol{C}_i) \sum HD_{i,R}}{\sqrt{N\sum W(\boldsymbol{C}_i)^2 - \left(\sum W(\boldsymbol{C}_i)\right)^2} \sqrt{N\sum (HD_{i,R})^2 - \left(\sum HD_{i,R}\right)^2}} \tag{3}$$

其中：N 表示功耗数据数量，$W(\boldsymbol{C}_i)$ 对应已知明文 $\boldsymbol{C}_i$ 的能量消耗，$HD_{i,R} = HD(\boldsymbol{R} \oplus \boldsymbol{C}_i)$ 是 $\boldsymbol{C}_i$ 和参考状态 $\boldsymbol{R}$ 之间的汉明距离。

1.4　内置确定性相关系数分析

BS-CPA 由 Komano 等[8] 提出，它是对 CPA 的改进，其主要思想是利用已经确定的子密钥来计算未确定的子密钥。在计算某个 SBOX 盒对应子密钥的过程中，例如 SBOX_1，其他 SBOX_i 对应操作产生的能量消耗就是噪声，那么信噪比（Signal-to-Noise Ratio，SNR）就比较低。如果攻击者能够利用之前已经确定的子密钥来计算当前子密钥，那么之前确定的子密钥所对应的 SBOX 盒产生的信息泄露就从噪声转化为信号，从而增加信噪比，因此破解密钥所需要的功耗数据数量就相应减少。BS-CPA 相关系数计算如式（4）所示：

$$\hat{\rho}_{\mathrm{WH}}(\boldsymbol{R}) = \left[N\sum W(\boldsymbol{C}_i) HD_{i,sb,SB} - \sum W(\boldsymbol{C}_i) \sum HD_{i,sb,SB}\right] \cdot \left\{\left[N\sum W(\boldsymbol{C}_i)^2 - \left(\sum W(\boldsymbol{C}_i)\right)^2\right]^{-1/2} \cdot \left[N\sum (HD_{i,sb,SB})^2 - \left(\sum HD_{i,sb,SB}\right)^2\right]^{-1/2}\right\} \tag{4}$$

与 CPA，HD 相比计算方式不同，BS-CPA 中 $HD_{i,sb,SB}$ 与中间变量，已确定的 SBOX 和当前需要计算的 SBOX 相关。

2　BS-CPA 攻击模型分析

一个准确合理的攻击模型对于功耗分析攻击至关重要，攻击者需要选择一个合适的中间变量进行建模，来刻画智能卡加密过程中的功耗特性。该中间变量应该能够体现功耗数据和真实密钥之间的相关性，通常可以选择中间变量为 SBOX 盒输出。

2.1　原 BS-CPA 模型及其问题

由于每个 SBOX 盒的输出是相互独立的，可以单独对每个 SBOX 盒进行计算分析，并行处理这些数据。原 *CPA* 攻击方法仅仅使用的敏感数据来破解第 i 个子密钥，但是实际操作中，所有的子密钥都是来源于同一个原始的真实密钥，如果攻击者能够利用其他的 SBOX 盒来得到更多关于真实密钥的有用信息，攻击效率会显著提高，这就是 BS-CPA 的基本思想。根据 Komano 等[8] 所说，破解出各个 SBOX 所需功耗数据数量最多为 65 条，通过实验，采用同样方法对数据包

Journal of Computer Applications 《计算机应用》

secmatv3_20070924 进行测试，图 2 的(a)、(b)、(c)分别显示了 DPA、CPA、BS-CPA 攻击的成功率结果，横轴表示攻击所需功耗数据数量，纵轴表示成功率。

整体上看，随着功耗数据的增加，DPA、CPA 和 BS-CPA 攻击成功率逐渐上升，但是 BS-CPA 并不能得到 Yuichi Komano 等所描述的结果。如果数据不进行任何处理，直接利用数据包中所有的点，要达到成功率 90% 以上，BS-CPA 攻击需要的功耗数据数量为 6 000 条左右。为了找出产生这种差异值的原因，本文对攻击模型进行研究，分析可能存在的问题。

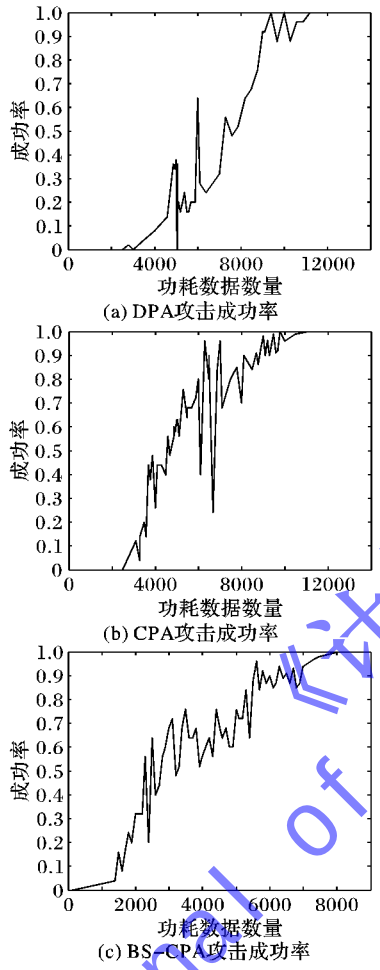

图 2 DPA、CPA 和 BS-CPA 攻击成功率比较

在 BS-CPA 中，原作者选取中间变量 $b_i = L_{15,i} \oplus L_{16,i} = R_{16,i} \oplus F(key_i, L_{16,i}) \oplus L_{16,i}$，并且认为使用 $L_0 \oplus L_1$（或者 $R_0 \oplus R_1$）也可以作为一种有效的攻击模型，但是从图 1 的流程图中可以发现，$L_1 = R_0$，因此可以得到 $HW(L_0 \oplus L_1) = HW(L_0 \oplus R_0)$，这意味着不能建立攻击模型和密钥之间的关系，同理对于 $R_{15} \oplus R_{16}$ 也不可行。

2.2 改进的模型

在差分功耗分析中，一种常用的策略是分治思想，就是将密钥分为 8 段子密钥，由于各个子密钥相互独立，可以实现单独破解。密码设备运行过程中产生的功耗数据依赖于寄存器的跳变次数，DES 加密设备运行时，每轮加解密过程在同一寄存器中实现，例如第一轮加密过程中，当寄存器的内容从 R_0 变化为 R_1 时，所产生的功耗值与汉明距离 $HD(R_0, R_1)$ 相关，又有 $R_1 = F(key_1, R_0) \oplus L_0$，因此可以选取中间变量为 $R_0 \oplus R_1$，该中间变量与明文密钥相关。具体实现分析：针对第 1 轮的攻击模型：$R_0 \oplus R_1 = R_0 \oplus F(key_1, R_0) \oplus L_0$，这里存在一个实现问题：如果直接采用分治法，需要将 R_0、L_0、key_1 全部分为对应的 8 段，在 F 函数变换前得到相对应的 R_0 拆分比较复杂，直接进行分治不太可行。观察 F 函数的细节：$F(key_1, R_0) = P(sbox(key_1 \oplus E(R_0)))$，如果进行一次 P 矩阵的逆变换，攻击模型就能依据 8 个 S 盒的输出直接划分为 8 部分，本文最终选取中间变量 $P^{-1}(R_0 \oplus R_1)$，并按汉明距离模型进行攻击。改进的攻击模型表示为：

$$\begin{aligned} &P^{-1}(R_0 \oplus R_1) = \\ &P^{-1}(R_0 \oplus F(key_1, R_0) \oplus L_0 = \\ &P^{-1}(R_0 \oplus P(sbox(key_1 \oplus E(R_0))) \oplus L_0 = \\ &P^{-1}(R_0 \oplus L_0) \oplus sbox(key_1 \oplus E(R_0)) \end{aligned}$$

定义 $R_0(i)$ 和 $L_0(i)$ 分别表示 R_0 和 L_0 的 $(i-1)*4+1 \sim i*4$ 位 $(i = 1,2,\cdots,8)$，在分治策略下，第一轮加密中第 i 个子密钥的攻击模型为：$P^{-1}(R_0(i) \oplus L_0(i)) \oplus sbox_i(key_1(i) \oplus E(R_0(i)))$。

原 BS-CPA 基本思想是利用已破解的子密钥来分析未破解的子密钥，实际实现中是利用第 $1 \sim i-1$ 个子密钥的汉明距离来计算第 i 个子密钥的汉明距离。那么改进的 BS-CPA 中，第 i 个子密钥的攻击距离就是：

$$\sum_{t=1}^{i-1} HD(P^{-1}(R_0(t) \oplus L_0(t)) \oplus sbox_t(key_1(t) \oplus E(R_0(t)))), \ i \in (1,8]$$

这里定义 $HD(i)$ 为第 i 个子密钥的汉明距离，$AM(i)$ 为第 i 个子密钥的攻击模型，可以得到：$AM(i) = \sum_{t=1}^{i-1} HD(t)$。

如果将汉明距离都看作正值，$AM(i)$ 将随着加密过程递增，$AM(1)$ 最小，$AM(8)$ 最大。为了保持攻击模型的一致性，考虑使用全部的汉明重量，以保持各个 $AM(i)$ 的平衡。对于未知的汉明重量，使用默认子密钥进行计算 $(key1_{缺省})$，最终，得到修改后的第 i 个子密钥的攻击模型为：

$$\begin{aligned} AM(i) = &\sum_{t=1}^{i-1} HD(P^{-1}(R_0(t) \oplus L_0(t)) \oplus \\ &sbox_t(key_t(t) \oplus E(R_0(t)))) + \\ &\sum_{t=i}^{8} HD(P^{-1}(R_0(t) \oplus \\ &L_0(t)) \oplus sbox_t(key1_{(缺省)} \oplus E(R_0(t)))) \end{aligned}$$

3 各种攻击方法的成功率与分析

本实验数据来自 dpacontest.org 平台，其中包括了不同智能卡的实测功耗数据，原作者选择 secmatv1_2006_04_0809 数据包，其使用的智能卡通过专用供电实现。本研究选择数据包 secmatv3_20070924，该功耗数据所采集的智能卡具有“时钟树”结构，通过常见的模块电源共享机制供电，更具一般性，但这意味着泄露信息会减少 1.5% 到 3%，产生的功耗数据所含电子噪声更大，密钥破解更加困难。

本文对 DPA、CPA、BS-CPA 攻击进行大量测试，使用功耗数据初始值设置为 1 000 条，反复进行功耗攻击，统计成功攻击（破解密钥和真实密钥相同）的次数，随后逐步增加所用功耗数据，统计攻击成功率与功耗数据的关系，比较不同攻击方法在使用同一数据来源时，攻击成功率的变化。

图 3 和图 4 分别显示了 DPA 和 CPA 在使用 3000 条功耗

Journal of Computer Applications 《计算机应用》

数据时，获取正确密钥的结果。理论上说，正确密钥假设值可以在差分时间轴某个时刻观察到一个明显的峰值，而错误的预测密钥以及不相关的时间点不会出现峰值的变化；否则可能导致攻击失败。从图3中可以看出，DPA的峰值较窄，并且结果明显。而CPA的结果中，峰值范围较宽，相关性在峰值附近呈现逐渐变化的趋势，这会使得密钥预测复杂，甚至导致攻击成功率的下降。

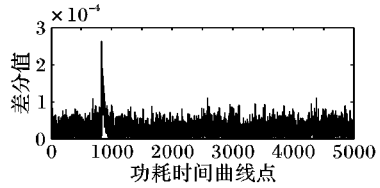

图3　DPA正确攻击结果

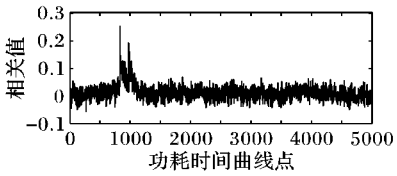

图4　CPA正确攻击结果

一方面，实际芯片的加密过程是连续而非离散的，与密钥相关的操作将在一定时间内执行，在CPA的攻击结果中，可以观察到峰值范围较宽，随着加密过程的不断进行，密钥值的相关性将会逐渐分散在其他数据中。从图4中可以看出，峰值的模式呈现为在最高点右侧逐渐减弱的趋势。从门电路级别分析，当加密的某一轮刚开始时，只有几个门电路在计算密钥值。之后，随着数据的扩散，越来越多的门电路开始计算和密钥相关的数据，此时电路中的功耗值与密钥的相关性变得越来越大。随着新的数据进入门电路，密钥相关性在门电路中又将慢慢减弱，这个过程使得CPA攻击中峰值范围较大。

另一方面，随着功耗分析所使用的数据不断增加，功耗数据和预测密钥之间的相关性将变得更加复杂、难以预测。当所使用的功耗数据未经任何预处理，没有进行对齐、滤波和重采样时，这一现象更为明显。过多的功耗数据将会引入大量噪声，反而会影响功耗分析的准确性。

图5是DPA，CPA，BS-CPA以及改进BS-CPA攻击成功率的对比图，横轴表示攻击所用的功耗数据数量，纵轴表示成功率。首先，随着功耗数据数量的增加，DPA，CPA，BS-CPA的成功率逐渐上升；其次，整体看来，CPA攻击效率比DPA高，BS-CPA比CPA高，改进后BS-CPA相比原BS-CPA方法效率有所提高，利用破解出的密钥信息来帮助攻击未破解的密钥有一定的效果，但改进并不明显，随着功耗数据增加，各种攻击方法差异值逐渐缩小，但中间存在波动；第三，CPA是计算功耗数据和预测密钥的相关性，与DPA相比，它只需较少的数据量就能达到同样的攻击效果。但是在测试中发现，随着功耗数据的不断增加，CPA的成功率反而波动很大，甚至减小了60%。这一现象可能是由于噪声，或者攻击模型不够准确。

通过某些“技巧”能够“提高”攻击的效果，一种非常有效的方法是将功耗数据中与密钥值最相关的部分提取出来进行攻击，即有针对性地使用部分功耗数据点而非所有功耗数据进行攻击。这种技巧甚至能超过DPA、CPA、BS-CPA等攻击方法本身的差距。在具体实验过程中，首先对功耗数据进行分析，在对所有点(0～5 000)进行DPA和CPA攻击后，结果如图3和图4所示，根据攻击结果可以确定第一轮加密在整体加密过程中的相对位置(800～1 000)，通过峰值找到第一轮子密钥的相关位置点，缩小攻击范围，只对部分功耗数据点进行分析。图5可以看出，针对部分点进行攻击(dpaPartion，cpaPartion)比用全部点(dpaAllPoint，cpaAllPoint)效果好。如果对加密设备和运行指令足够了解，可以直接通过少量的功耗数据确定出每一轮加密的精确时间段，直接提取出最相关部分数据点进行分析，从而减少攻击所需要的功耗数据。这一方法能去除大量噪声和错误峰值，大大提高攻击成功率。通常选取的攻击点越精确，所需功耗数据越少，且测试效果更好。

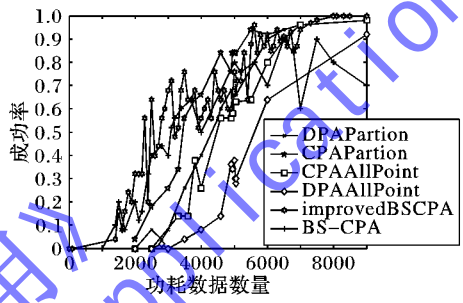

图5　DPA、CPA、BS-CPA以及改进BS-CPA成功率对比

4　结语

在本文中，对基于专用集成电路(Application Specific Integrated Circuit，ASIC)的secmatv3系统智能卡进行了DPA、CPA、BS-CPA的大量攻击测试，比较了不同攻击方法在不同功耗数据下，恢复出正确密钥的成功率，并对BS-CPA进行深入研究，与DPA相比，CPA具有更好的攻击效果，理论上BS-CPA可以提高攻击效率，但从实际攻击成功率的对比可以看出，BS-CPA效果并不太理想，密码设备在实现加解密过程中产生的功耗值受到多方面影响，改进的BS-CPA相比原方法有进一步提高，这与具体模型和实现方法有很大关系，但找到一种通用的方法提高所有设备攻击效率比较困难。进一步可以针对AES分组算法进行分析，并将第一轮和最后一轮进行结合，利用已经破解出的密钥来计算当前密钥，这样能够提高信噪比，攻击效率将会有进一步的提高。此外，可以考虑使用自己的功耗数据，对设备和数据测试各个阶段实现细节进行分析，进行更加一般的攻击测试，研究不同攻击方式的适用情况。

参考文献：

[1] KOCHER P C, JAFFE J, JUN B. Differential power analysis [C]// CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1999: 388－397.

[2] QUISQUATER J J, SAMYDE D. ElectroMagnetic Analysis (EMA): measures and counter-measures for smart cards [C]// E-SMART '01: Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security. Berlin: Springer-Verlag, 2001: 200－210.

[3] BONNEAU J, MIRONOV I. Cache-collision timing attacks against AES [C]// CHES 2006: Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2006: 201－215.

(下转第 1330 页)

Journal of Computer Applications 《计算机应用》

[3] CHEN K, ZHENG W. Cloud computing: system instances and current research [J]. Journal of Software, 2009, 20(5): 1337 – 1348. (陈康, 郑纬民. 云计算: 系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337 – 1348.)

[4] ZENG L, ENATALLAH B, NGU A, *et al*. QoS-aware middleware for Web services composition [J]. IEEE Transactions on Software Engineering, 2004, 30(5): 311 – 327.

[5] SHAO L, ZHANG J, WEI Y, *et al*. Personalized QoS prediction for Web services via collaborative filtering [C]// ICWS 2007: Proceedings of the 2007 IEEE International Conference on Web Services. Piscataway: IEEE, 2007: 439 – 446.

[6] SHAO L, ZHOU L, ZHAO J, *et al*. Web service QoS prediction [J]. Journal of Software, 2009, 20(8): 2062 – 2073. (邵凌霜, 周立, 赵俊峰, 等. 一种 Web Service 的服务质量预测方法[J]. 软件学报, 2009, 20(8): 2062 – 2073.)

[7] ZHENG Z, MA H, LYU M, *et al*. WSRec: a collaborative filtering based Web service recommender system [C]// ICWS 2009: Proceedings of the 2009 IEEE International Conference on Web Services. Piscataway: IEEE, 2009: 437 – 444.

[8] ZHANG L, ZHANG B, NA J, *et al*. An approach for Web service QoS prediction based on service using information [C]// ICSS 2010: Proceedings of the 2010 IEEE International Conference on Service Sciences. Piscataway: IEEE, 2010: 324 – 328.

[9] HANG J, HU Z. Multiple-signal prediction model for QoS of Web services inspired by immune system [J]. Journal of Guangxi University: Natural Science Edition, 2009, 34(4): 535 – 539. (黄景文, 胡志华. Web 服务 QoS 的免疫多信号预测模型研究[J]. 广西大学学报: 自然科学版, 2009, 34(4): 535 – 539.)

[10] LIU K, WANG H, XU Z. A Web service selection mechanism based on QoS prediction [J]. Computer Technology and Development, 2007, 17(8): 103 – 105. (刘克非, 王红, 许作洋. 一种基于服务质量预测的 Web 服务选择方法[J]. 计算机技术与发展, 2007, 17(8): 103 – 105.)

[11] ZHANG J, SONG J, A short-term prediction for QoS of Web service based on RBF neural networks [J]. Journal of Liaoning Technical University: Natural Science Edition, 2010, 29(5): 918 – 921. (张金宏, 宋杰. 基于 RBF 神经网络的 Web 服务 QoS 短期预测[J]. 辽宁工程技术大学学报: 自然科学版, 2010, 29(5): 918 – 921.)

[12] LIU Z, WANG Z, ZHOU X, *et al*. Dynamic prediction method for Web service QoS based on case based reasoning [J]. Computer Science, 2011, 38(2): 119 – 122. (刘志中, 王志坚, 周晓峰, 等. 基于事例推理的 Web 服务 QoS 动态预测研究[J]. 计算机科学, 2011, 38(2): 119 – 122.)

[13] LI M, HUAI J, GUO H. An adaptive Web services selection method based on the QoS prediction mechanism [C]// WI-IAT '09: Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology. Washington, DC: IEEE Computer Society, 2009: 395 – 402.

[14] MALAK J S, MOHSENZADEH M, SEYYEDI M A. Web service QoS prediction based on multi Agents [C]// ICCTD '09: Proceedings of the 2009 IEEE International Conference on Computer Technology and Development. Piscataway: IEEE, 2009: 265 – 269.

[15] LEYMANN F, ROLLER D, SEHMID M-T. Web services and business process management [J]. IBM System Journal, 2002, 41(2): 198 – 211.

[16] HWANG S-Y, WANG H, TANG J, *et al*. A probabilistic approach to modeling and estimating the QoS of Web service-based workflows [J]. Information Sciences, 2007, 177(23): 5484 – 5503.

[17] TAO C, FENG Z. QoS-aware Web service composition based on probability approach [J]. Journal of Tianjin University, 2010, 43(10): 860 – 865. (陶春华, 冯志勇. 基于概率方法的 QoS 感知 Web 服务组合[J]. 天津大学学报, 2010, 43(10): 860 – 865.)

[18] KIEPUSZEWSKI B, ter HOFSTEDE A H M, BUSSLER C. On structured workflow modeling [C]// Proceedings of the 12th International Conference on Advanced Information Systems Engineering. London: Springer-Verlag, 2000: 431 – 445.

[19] GEEBELEN D, GEEBELEN K, TRUYEN E, *et al*. QoS prediction for Web service compositions using kernel-based quantile estimation with online adaptation of the constant offset [J]. Information Sciences, 2014, 268: 397 – 424.

(上接第 1287 页)

[4] Telecom ParisTech. DPA contest 2008/2009 [EB/OL]. [2013-08-09]. http://www.dpacontest.org/.

[5] International Association for Cryptologic Research. Cryptographic Hardware and Embedded Systems (CHES) [EB/OL]. [2013-08-09]. http://www.iacr.org/meetings/ches.

[6] EISENBARTH T. Workshop on cryptographic hardware and embedded systems 2008(CHES 2008) [EB/OL]. [2013-08-09]. http://www.chesworkshop.org/.

[7] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model [C]// CHES 2004: Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2004: 16 – 29.

[8] KOMANO Y, SHIMIZU H, KAWAMURA S. BS-CPA: built-in determined sub-key correlation power analysis [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A(9): 1632 – 1638.

[9] MANGARD S, OSWALD E, POPP T. Power analysis attacks: revealing the secrets of smart cards [M]. New York: Springer Publishing Company, 2010.

[10] LE T H, CANOVAS C, CLÉDIÈRE J. An overview of side channel analysis attacks [C]// ASIACCS '08: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2008: 33 – 43.

[11] MESSERGES T S, DABBISH E A, SLOAN R H. Examining smart-card security under the threat of power analysis attacks [J]. IEEE Transactions on Computers, 2002, 51(5): 541 – 552.

[12] BEVAN R, KNUDSEN E. Ways to enhance differential power analysis [C]// Proceedings of the 5th International Conference. Berlin: Springer-Verlag, 2002: 327 – 342.

[13] LE T H, CLÉDIÈRE J, CANOVAS C, *et al*. A proposition for correlation power analysis enhancement [C]// CHES 2006: Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2006: 174 – 186.

Journal of Computer Applications 《计算机应用》