

针对密码芯片的电磁模板分析攻击

邓高明, 张 鹏, 赵 强, 陈开颜
(军械工程学院 计算机工程系, 河北 石家庄 050003)

摘 要: 给出一种简单的电磁信号的获取办法, 说明密码芯片的电磁信号能够用一个手工绕制的金属线圈获取, 并且其信号幅度和操作数的汉明重量相关. 在描述模板攻击原理和步骤的基础上, 介绍了针对密码芯片的电磁模板分析攻击, 并且针对一个单片机(AT89C52)上实现的 DES 密码系统进行了电磁模板分析攻击实验, 实验成功恢复了 DES 第 16 轮使用的 48 位子密钥.

关键词: 电磁; 模板分析; 密码芯片; DES

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2010)01-0001-04

EM Template Analysis for Cipher Chips

DENG Gao-ming, ZHANG Peng, ZHAO Qiang, CHEN Kai-yan

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: In this paper, it is shown that the electromagnetic (EM) emanation of cryptographic chips could be captured easily with a handmade loop probe, and its amplitude is related to the hamming weight of the related operands. Based on the description of the principle and steps of template analysis, EM template analysis attack against cryptographic chips was introduced. Additionally, an experiment of EM template analysis attack against a singlechip (AT89C52) implemented DES was given, and the 48-bit subkey used in the 16th round of DES was recovered.

Key words: EM; template analysis; cryptographic chips; DES

1 引言

自从 Kocher^[1]1996 年提出旁路攻击以来, 密码学界对旁路攻击已经有了比较深入的研究. 旁路攻击通过观测密码系统实现过程中的物理泄漏信息(比如功耗^[2], 电磁泄漏^[3], 时间消耗^[4]等等)来萃取其中存储的秘密信息. 由于这种方法简单而有效, 传统的针对数学基础的密码分析研究也开始转向这种针对密码系统实现的密码分析方法.

最近, 一种称为模板攻击(Template Attack, TA)^[5]的概率攻击方法被提出. 模板攻击根据泄漏信息的数据相关性和操作相关性进行攻击, 首先为每一个可能的密钥构建一个泄漏信息特征的模板, 之后根据获取的一份和多份泄漏的信息寻找最匹配

的模板, 进而推断最可能的正确密钥. 自提出以来, 模板攻击几乎都被用于功耗分析^[6-7], 而很少用于电磁分析, 主要是由于功耗信号比电磁信号更容易获取. 但是, 文中的研究发现, 密码芯片工作过程中辐射的电磁信号可以用一个放在芯片表面上的手制金属线圈采集到, 而且信号的幅度和芯片中运算的数据汉明重量具有一定的相关性. 文中在介绍电磁模板分析攻击原理和方法的基础上, 给出了一个针对单片机实现的 DES 密码系统的攻击实例.

2 密码芯片的电磁辐射

密码芯片的电磁辐射是旁路信号的一种, 它和流过芯片的电流有关. 在 IC 电磁兼容标准 IEC61967^[8]中, 传导电磁辐射和发射电磁辐射被认

收稿日期: 2008-12-12; 修回日期: 2009-02-12

基金项目: 国家自然科学基金项目(60571037); 国家“八六三”计划项目(2007AA01Z454)

为是噪声并要求低于一定的阈值. 把 IC 的电磁辐射在一定的阈值以下能防止它与其他电子设备之间发生干扰. 但是, 芯片辐射的电磁信号与芯片中处理的数据是相关的, 因此, 执行密码算法的设备辐射的电磁信号中蕴含着和密钥信息相关的有用信息.

2.1 电磁辐射的产生

图 1 给出的是 CMOS 数字电路的基本组成单元——反相器. 反相器可以看作是一个推拉开关: 输入接地时切断下面的晶体管, 产生高电平输出. 高电平输入时刚好相反, 将输出接地拉到低电平. 当一个比特位从 0 翻转到 1, 或者从 1 翻转到 0 同样成立, 反相器的 NMOS 管和 PMOS 管会导通一小段时间. 这就导致一个从 V_{DD} 到 V_{SS} 的短暂的电流脉冲. 而这个在 CMOS 门的输出变化时产生的电流会在芯片周围产生一个变化的电磁场, 这个变化的电磁场可以用感应探头检测到.

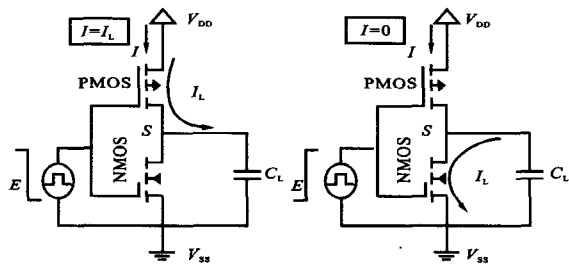


图 1 CMOS 倒相器在输入信号 E 出现上升沿和下降沿时的动态功耗

根据楞次定律, 穿过探头的电感力取决于磁通量的变化率, 其表示如下^[9]:

$$v = -\frac{d\phi}{dt}, \quad \phi = \iint \vec{B} \cdot d\vec{A} \quad (1)$$

式中, v 表示探头的输出电压, ϕ 表示探头感应的磁通量, t 表示时间, $\vec{B}$ 表示磁场, 而 $\vec{A}$ 表示磁力线穿透的区域.

基于安培定理的麦克斯韦方程将磁场的产生表示如下:

$$\vec{\nabla} \times \vec{B} = \mu \vec{J} + \epsilon \mu \frac{\partial \vec{E}}{\partial t} \quad (2)$$

式中, $\vec{J}$ 表示电流密度, $\vec{E}$ 表示电场, ϵ 表示电导率, 而 μ 表示磁导率.

式(1)和式(2)说明探头的输出电压 v 为电流密度 $\vec{J}$ 和 $\vec{E}$ 电场成正比, 也就是和翻转的晶体管数量成正比.

2.2 电磁辐射的数据相关性

在一定时间内通过物理旁路泄漏的数据取决于

该时间内从一个状态到另一个状态的翻转数^[2]. 一个微处理器可以被建模成一个依靠时钟信号触发在不同状态之间转换的状态机. 而这些状态又和 CMOS 电路的逻辑门翻转有关. 假设用到的状态是一个定长的机器字 R . 另外还要给出两条更严格的假设条件:

(1) 假设从 0 翻转到 1 和从 1 翻转到 0 需要相同的能量.

(2) 假设所有的机器位都非常平衡, 翻转时都需要相同的能量.

这些假设在普通 IC 上都是基本可以满足的, 使得我们模型的表达非常简便.

汉明重量是一个机器字中为 1 的比特数. 如果一个 m 位的数据编码为 $D = \sum_{j=0}^{m-1} d_j 2^j$, 其中 $d_j = 0$ 或 1, 那么它的汉明重量为 $H(D) = \sum_{j=0}^{m-1} d_j$. 那么从 R 转换到 D 的翻转位数就是 $H(D \oplus R)$, 这就是 D 和 R 之间的汉明距离. 在操作数一级, 密码设备的功耗可以用源操作数和目的操作数之间的汉明距离来表示, 即

$$P_R = \lambda \cdot H(D \oplus R) + \mu \quad (3)$$

式中, λ 是一个和系统相关的常数, μ 是随机噪声.

电路中执行的每个指令都可以看作是按一定的路径激活了一定数目的晶体管. 活动晶体管的总数目是操作相关的, 因此在决定每个操作的电流和功耗是有很重要的作用. 流过集成电路的电流是密码系统信息泄漏的主要途径. 和密码系统中执行的操作相关的信息可以通过电流、功耗, 或者是电磁测量来获取.

3 模板分析攻击

3.1 模板攻击介绍

模板分析攻击利用密码芯片中泄漏的与被操作的数据相关的电磁辐射信号进行密码分析.

在模板分析攻击中需要有一个重要的假设前提, 那就是攻击者要能够完全控制一个和被攻击设备类似的设备. 也就是说攻击者要能够不受限制地多次调用一个和被攻击设备类似的设备, 并且参数可以是自己设定的. 这个假设前提可以很容易实现, 因为被攻击的设备通常都是标准设备, 其类似的设备都是可以很容易通过合法途径获得的.

在这个假设的基础上, 攻击者就可以通过被完全控制的设备对所有可能的密钥构建模板, 然后用同样的方法在被攻击的设备运行时获取一组旁路信

号并将之与已构建好的模板相匹配. 匹配效果最好的模板对应的密钥就是最可能的正确密钥.

3.2 模板攻击的步骤

电磁模板分析攻击由两个步骤组成:

(1) 模板构建阶段

为了将电磁曲线按不同的密钥值分类, 需要预先为每个可能的密钥都构建一个模板. 该模板反映了和密钥对应的电磁曲线的统计特性, 也就是说模板反映了曲线上所有点的概率分布的特性. 为了对电磁曲线中的噪声信号建模, 需要用到高斯模型.

模板由均值向量和协方差矩阵构成. 假设子密钥长度是 l 位, 因此为所有可能的子密钥构建 2^l 个模板. 用每个子密钥对同一个明文 p 加密 m 次, 并获取对应的 m 条电磁曲线, 每条曲线有 n 个采样点, 即 $t_{i1}, t_{i2}, \dots, t_{in} (1 \leq i \leq m)$. 接下来, 电磁曲线样本组成了一个矩阵 $T_{m \times n}$, 且对应的均值向量可以计算如下:

$$\begin{aligned} \bar{t} &= \langle \bar{t}_1, \bar{t}_2, \dots, \bar{t}_n \rangle \\ &= \langle \frac{1}{m} \sum_{i=1}^m t_{i1}, \frac{1}{m} \sum_{i=1}^m t_{i2}, \dots, \frac{1}{m} \sum_{i=1}^m t_{in} \rangle \end{aligned} \quad (4)$$

因为所有的曲线都是从同一个操作获取的, 存在的随机噪声可以用样本与样本均值作差的方法求得. 对一个可能的子密钥的所有样本曲线, 对应的噪声矩阵 $N_{m \times n}$ 为

$$N_{m \times n} = \begin{bmatrix} t_{11} - \bar{t}_1 & t_{12} - \bar{t}_2 & \dots & t_{1n} - \bar{t}_n \\ t_{21} - \bar{t}_1 & t_{22} - \bar{t}_2 & \dots & t_{2n} - \bar{t}_n \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} - \bar{t}_1 & t_{m2} - \bar{t}_2 & \dots & t_{mn} - \bar{t}_n \end{bmatrix} \quad (5)$$

矩阵中的每一行组成了一条电磁样本曲线的噪声向量, 而矩阵的每一列是一个反映该时间点的噪声的随机变量.

一般用协方差来描述两个随机变量之间的线性相关性, 两个随机变量 N_i 和 N_j 之间的协方差可以通过下式计算:

$$\text{cov}(N_u, N_v) = \frac{1}{m-1} \sum_{k=1}^m (t_{ku} - \bar{t}_u)(t_{kv} - \bar{t}_v) \quad (6)$$

为了描述两个以上随机变量之间的协方差, 需要一个协方差矩阵. 噪声信号的协方差矩阵定义如下:

$$C_{m \times n} = \begin{bmatrix} \text{cov}(N_1, N_1) & \text{cov}(N_1, N_2) & \dots & \text{cov}(N_1, N_n) \\ \text{cov}(N_2, N_1) & \text{cov}(N_2, N_2) & \dots & \text{cov}(N_2, N_n) \\ \vdots & \vdots & \ddots & \vdots \\ \text{cov}(N_n, N_1) & \text{cov}(N_n, N_2) & \dots & \text{cov}(N_n, N_n) \end{bmatrix} \quad (7)$$

因此, 一个可能的子密钥的模板可以定义为一个 2 元组: $T = \langle \bar{t}, C \rangle$.

为了创建这样一个模板, 需要采集大量的电磁曲线样本. 显然, 曲线样本量越大模板就越精确.

(2) 模板匹配阶段

一旦通过一个被完全控制的芯片完成了所有模板的构建, 就可以用被攻击的芯片对模板构建阶段中用到明文 p 进行加密, 并采集对应的芯片运行时的电磁曲线 t' , 并将其与先前构建好的模板进行比较. t' 即与模板 $\langle \bar{t}, C \rangle$ 匹配的概率为

$$p(t'; \langle \bar{t}, C \rangle) = \frac{1}{\sqrt{(2\pi)^m |C|}} \exp\left(-\frac{1}{2}(t' - \bar{t})^T C^{-1}(t' - \bar{t})\right) \quad (8)$$

直观上来说, 概率最大的就是匹配得最好的模板, 其对应的也就应该是最可能的正确密钥. 这就是所谓的最大似然估计方法.

4 针对 DES 的电磁模板分析攻击

4.1 DES

DES(Data Encryption Standard) 是 1970 年由 IBM 提出的密码算法, 自从 1977 年被美国国家标准局采用作为数据加密标准以来, 因其加密速度快和安全性高的特点被广泛应用在各种密码芯片中.

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. DES 加密算法的密钥空间为 2^{56} . 如图 2 所示, DES 第 1 轮迭代公式为

$$L_1 = R_0, R_1 = L_0 \oplus f(R_0, K_1),$$

式中, $f(R_0, K_1) = P(S(E(R_0) \oplus K_1))$, K_1 表示第 1 轮子密钥, P 表示置换运算, S 表示 S 盒选择运算, E 表示扩展置换运算. DES 轮函数 f 如图 3 所示.

选择最后一轮的 S-box 的输入作为攻击点. 由于一个 S-box 的输入是 6 位的, 就需要构建 2^6 个模板.

4.2 实验配置

实验中在 AT89C52 单片机中实现 DES 密码程序, 用一个放在单片机表面上的手制的铜线圈感应单片机运行时泄漏的电磁信号 (见图 4、图 5), 用数字存储示波器进行采集 (Tektronix DPO4032, 被动探头 P6139A, 差分探头 TDP0500) 并通过 USB 传输到 PC 机存储, 示波器的采集过程由 PC 机上用 Lab-Window 编写的虚拟仪器控制平台实现自动控制, 并且该虚拟仪器还通过 RS232 将明文发往单片机.

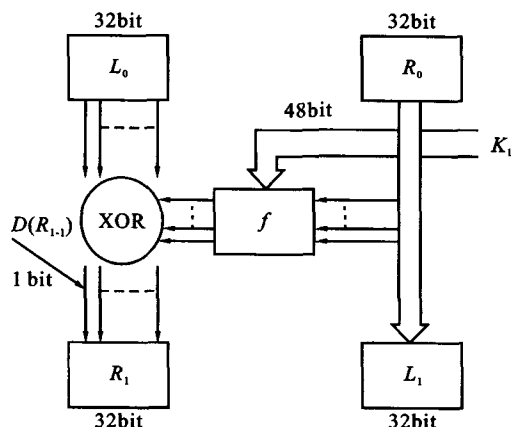


图2 DES轮加密过程

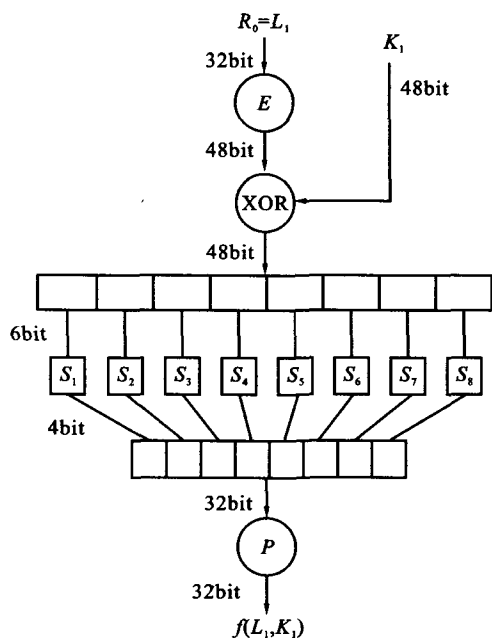


图3 DES轮函数 \$f\$

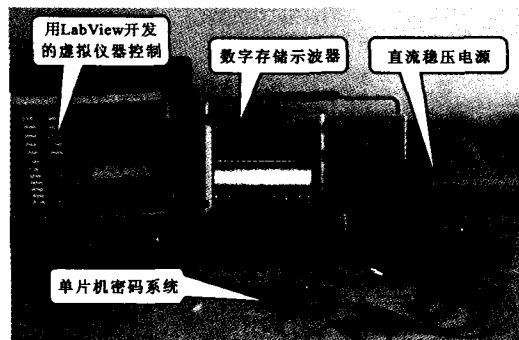


图4 实验设置

4.3 实验结果

首先,在一个AT89C52单片机上用所有26个可能的子密钥分别对同一个明文加密104次,并按

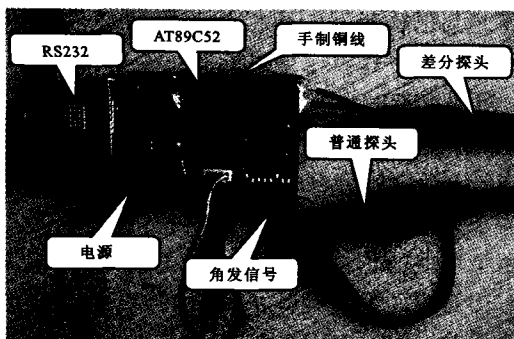


图5 被攻击的单片机密码系统

3.2节中描述的方法构建26个模板,然后在一个同样的单片机上用同一个未知的密钥加密同一个明文,并用同样的实验设置采集并记录其电磁曲线,接下来,按式(8)计算该电磁曲线与所有模板的匹配概率,最后根据最大概率值推断最可能的6位正确子密钥。

将上述步骤反复进行8次,就可以获得DES最后一轮使用的48位子密钥,根据DES密钥扩展算法可以反推到原始密钥的48位,最后对剩余的8位密钥进行穷举搜索,可以恢复出DES的56位原始密钥。

5 结束语

旁路攻击研究中,大多研究文献都关注于功耗的模板分析攻击.文中的实验结果表明,密码芯片的电磁泄漏可以用手制的线圈采集到,并且比在芯片地和电源地之间串连一个电阻获取密码芯片的功耗泄漏还简单.而且从密码芯片获取的电磁信号的幅值与芯片中处理的数据的汉明重量相关.在介绍模板分析攻击的原理和步骤的基础上,通过对单片机上实现的DES密码系统的电磁模板分析攻击,验证了该方法的可行性和有效性。

参考文献:

- [1] Paul Kocher. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems[C]// Advances in Cryptography; Proceedings of Crypto '96. New York, Springer-Verlag, 1996.
- [2] 陈志敏. 安全芯片旁路功耗分析及抗攻击措施[D]. 上海:上海交通大学, 2007.
- [3] 张鹏,陈开颜,赵强. PDA上ECC电磁分析神经网络分类方法[J]. 微电子学与计算机, 2006, 23(11): 139-141.

(下转第8页)

5 结束语

元胞自动机是一种很适合算法作曲的方法,通过寻找能够演化出复杂现象的规则和初始化方案,再通过相应的映射机制,配以节奏和音色,就可以生成美妙的音乐.目前的问题在于复杂且适合构建音乐的规则需要大量的实验进行寻找,其次评价生成音乐是否悦耳的量化指标体系还不完善,有待于更深入的研究.

参考文献:

- [1] Bilotta E, Pantano P, Talarico V. Synthetic harmonies: an approach to musical semiosis by means of cellular automata[J]. Artificial Life VII, 2000, 35(2): 153-159.
- [2] 雷霆, 余镇危. 网络流量行为分析的一维元胞自动机模型[J]. 微电子学与计算机, 2007, 24(10): 99-102.
- [3] Bilotta E, Pantano P, Talarico V. Music, mathematics and artificial life [C]// 11th ECMI Symposium. Italy

Palermo, 2000.

- [4] Eduardo Reck Miranda. Introduction to cellular automata music research[J]. DIGITAL music online tutorials on computer music, 2003(8): 1-5.
- [5] Dave Burraston, Ernest Edmonds. Cellular automata in generative electronic music and sonic art [C]// Historical and Technical Review, Faculty of Information Technology. Sydney, Australia, 2005, 16(3): 165-185.
- [6] Wolfram S. Cellular automation [EB/OL]. [2009-01-19] (2005-09-12). http://mathworld.wolfram.com/new/2005-09-12/wolfram_tones/.

作者简介:

王存睿 男, (1980-), 讲师. 研究方向为系统仿真.

段晓东 男, (1963-), 博士, 教授. 研究方向为复杂网络与非线性信息处理技术.

刘向东 男, (1967-), 博士, 教授. 研究方向为非线性信息处理和算法复杂性.

李志洁 女, (1980-), 博士, 讲师. 研究方向为算法设计.

(上接第4页)

- [4] 邓高明, 张鹏, 陈开颜, 等. Cache 在旁路攻击中的理论应用及其仿真实现[J]. 微电子学与计算机, 2007, 24(5): 82-85.
- [5] Suresh Chari, Josyula R Rao, Pankaj Rohatgi. Template attacks [C]// Cryptographic Hardware and Embedded Systems (CHES 2002). Berlin: Springer-Verlag, 2002: 13-28.
- [6] Agrawal D, Rao J R, Rohatgi P, et al. Templates as master keys [C]// Cryptographic Hardware and Embedded Systems (CHES 2005). Edinburgh: Springer, 2005: 15-29.
- [7] Francois-Xavier Standaert, Cedric Archambeau. Using subspace-based template attacks to compare and combine

power and electromagnetic information leakages [C]// Cryptographic Hardware and Embedded Systems (CHES 2008). Berlin: Springer, 2008: 411-425.

- [8] International Electrotechnical Commission. IEC 61967: integrated circuits - measurement of electromagnetic emanations, 150 kHz to 1 GHz [S]. New York: IEC, 2003.
- [9] Raymond A Serway, John W Jewett. Physics for scientists and engineers [M]. 6th ed. Saunders: Saunders college publishing, 2003.

作者简介:

邓高明 男, (1983-), 博士研究生. 研究方向为电磁信息检测与主动防护技术.