

针对密码芯片的电磁频域模板分析攻击

邓高明 赵 强 张 鹏 陈开颜 刘晓芹

(军械工程学院计算机工程系 石家庄 050003)

摘 要 在密码运行过程中随机地插入时延是常用的防御时域旁路攻击的方法,该方法可导致密码算法的关键运算步骤在多次运行过程中出现在不同的时刻,以此抵抗时域分析攻击.在深入研究密码芯片电磁辐射产生机理及其数据相关性的基础上,根据能量守恒定律分析并通过实验验证了电磁信号的数据相关性从时域经 Fourier 变换到频域时依然存在,且不受时域信号中随机时间延迟的影响.根据这一特性,提出一种在密码芯片电磁辐射频域信号上进行模板分析的方法.对运行 RC4 密码算法的微控制器的攻击实验表明,在密码程序中插入随机时延使得时域模板分析失效的情况下,对频域信号的分析依然可以恢复 RC4 的原始密钥,且不增加攻击的时间复杂度.

关键词 旁路攻击;电磁;频域模板分析;密码芯片;RC4

中图法分类号 TN309 **DOI号:** 10.3724/SP.J.1016.2009.00602

EM Frequency Domain Template Analysis on Cipher Chips

DENG Gao-Ming ZHAO Qiang ZHANG Peng CHEN Kai-Yan LIU Xiao-Qin

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

Abstract A general countermeasures against time domain side channel attacks is to insert random delays into the executing sequence of cipher algorithm, in which the interesting operations will occur at different time in multi runs of the cipher. To break this countermeasures, this paper analyzes the generation of the electromagnetic(EM) emissions of cipher chips and its dependence with the data operated in chips, with the law of energy conservation, this paper finds out the fact that the data dependence of the EM signals emitted from the cipher chips can remain when it is transformed from time domain to frequency domain, and that the data dependence in frequency domain signals will not be affected by inserting random delays into time domain signals. With this property of the frequency domain signals, this paper presents a new EM frequency domain template analysis. Experiments of EM frequency domain template analysis on a micro-controller (AT89C52) implemented RC4 show that the genuine key of RC4 can still be recovered after inserting random delays in source code, while template analysis in time domain is invalidation. Furthermore, the time complexity of this new template analysis is no more than the analysis in time domain.

Keywords side channel attacks; EM; frequency domain template analysis; cryptographic chips; RC4

收稿日期:2008-12-06;最终修改稿收到日期:2009-03-05. 本课题得到国家自然科学基金项目(60571037)、国家“八六三”高技术研究发展计划项目基金(2007AA01Z454)资助. 邓高明,男,1983年生,博士研究生,研究方向为电磁信息检测与主动防护技术. E-mail: denggaoming26@163.com. 赵 强,男,1945年生,教授,博士生导师,研究领域包括集成电路信息安全、集成电路主动防护技术. 张 鹏,男,1976年生,博士研究生,研究方向为电磁信息检测与主动防护技术. 陈开颜,女,1970年生,副教授,研究方向包括电磁信息检测与主动防护技术、计算机应用安全. 刘晓芹,女,1983年生,博士研究生,研究方向为集成电路安全.

1 引言

密码算法的安全性主要包括两方面内容: 一方面是数学上的安全性; 另一方面是与实现相关的安全性. 当前主流密码算法在数学上都具有较高的安全性, 经受了大量数学分析的考验, 几乎无法破解. 但是密码算法在一定的物理设备上实现时可能泄露各种各样的旁路信息(side channel information)(如运行时间、功率消耗、电磁辐射等), 这些旁路信息中和密钥相关的部分可以为破解密码系统提供帮助. 旁路攻击(Side Channel Attacks, SCAs)就是利用密码算法实现时泄露的旁路信息来实施破解的攻击方法, 比如计时攻击(timing analysis)、电磁分析攻击(electromagnetic analysis)以及功耗分析攻击(power analysis)等. 电磁分析攻击作为最有效的旁路攻击技术之一, 是通过在密码芯片周围放置线圈, 测量芯片在运算期间辐射的电磁信号, 研究电磁场与内部处理数据之间的相关性而获取内部秘密参量. Quisquater 等人^[1]和 Gandolfi 等人^[2]给出了在密码设备(如智能卡)上的电磁分析攻击的实验结果, 并与功耗分析攻击进行了比较. Agrawal 等人^[3]发现电磁辐射由多重信号组成, 每一种泄漏都是有关底层计算的不同信息.

针对密码芯片的模板攻击(template attack)^[4]是密码旁路攻击的一种. 模板攻击根据密码设备泄漏旁路信息的数据相关性和操作相关性进行攻击, 首先为密钥空间中所有的密钥分别构建一个泄漏信息特征的模板, 之后根据获取的一份或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或有效缩小密钥搜索空间. Rohatgi 等人 2002 年在密码硬件与嵌入式系统(Cryptographic Hardware and Embedded Systems, CHES'02)国际会议上首先撰文提出, 可以将密码芯片整个工作时间内多个时刻泄露旁路信息的量值看作多维随机变量, 将已知密钥情况下对应各个密钥的旁路信息的概率分布作为对应各个密钥的模板, 通过判断在未知密钥情况下获取的相同类型旁路信息样本最可能属于哪个已知密钥的分布来进行模板的匹配, 进而推断未知密钥或缩小其搜索空间^[4]. 自那以来, 模板攻击一直是旁路攻击研究领域的热点, Agrawal 等人在 CHES'05 上发表文章将模板分析和差分功耗分析(Differential Power Analysis, DPA)相结合, 提出了一种模板加强的 DPA 攻击(template-enhanced

DPA attack)^[5]; Archambeau 等人在 CHES'06 上发表文章提出从旁路样本中选取有效点构成样本的主子空间(principal subspaces), 以减小模板攻击的运算量^[6]; 同一次会议上, Gierlichs 等人将模板攻击和随机方法进行比较, 利用基于 T 检验的算法评价了模板攻击的效率^[7]; 在 CHES'08 上 Standaert 等人结合了功耗和电磁两种旁路信号, 采用主成分分析(Principal Component Analysis, PCA)和 Fisher 判别进行模板分析^[8].

以上的这些模板攻击几乎都将时域的旁路信号看作多维随机变量进行分析, 要求多个信号样本在同一个时刻的量值属于同一维随机变量, 即时域信号在时间点上精确对齐, 否则属于不同随机变量的样本会交错混淆, 导致模板不准确, 这就成为时域信号模板分析的一个致命弱点. 在密码运行过程中随机地插入时延是常用的防御时域旁路攻击的方法, 该方法可导致密码算法的关键运算步骤在多次运行过程中出现在不同的时刻, 从而使时域分析攻击失效. 2000 年 Messerges 将 RSA 模幂算法的操作随机化, 提出一种伪随机扫描(RAD)模幂算法, 能够显著地抑制所有他列举的功耗分析方法的攻击^[9]. 2006 年, 韩军提出了一种将 RSA 算法中的伪操作随机化的新方法^[10], 此后还发表文献总结出将系统运行时间随机化是一种直接有效的防御方法, 并建立了随机时间延迟防御 DPA 攻击的理论模型^[11], 本文的实验也验证了这一点.

从信息理论中可知, 信号经傅立叶变换, 其总能量保持不变, 符合能量守恒定律. 因此密码芯片的功耗和电磁辐射信号的数据相关性在信号从时域经 Fourier 变换到频域时依然存在, 且不受时域中随机时间延迟的影响, 如 Aigner 等人在文献[12]中就曾指出在密码旁路分析中的时域信号差异, 在频域中同样会体现出来, Chin 也曾证明频域中旁路攻击的有效性^[13], 还有实验^[14]表明频域内的差分功耗分析攻击是可行的. 根据频域信号这一特性, 本文提出一种针对密码芯片电磁辐射频域信号进行模板分析的方法——频域模板分析攻击(Frequency-Domain Template Attack, FDTA). 在获取密码芯片电磁辐射之后, 利用快速傅立叶变换(FFT)将时域的电磁信号变换到频域, 然后在频域信号中找到和密钥相关的成分, 并以此构建模板. 本文的实验验证: 该攻击方法有效克服了时域信号分析中要求时间点精确对齐的缺点, 可用于破解插入随机延时的密码芯片.

2 RC4 密码算法

本文以运行 RC4 密码算法原型的微控制器为攻击对象来介绍模板攻击. RC4 密码算法^[15]是 Rivest 在 1987 年为 RSA 数据安全公司开发的可变密钥长度的序列密码. 在开始的 7 年时间里它是受专利保护的, 但在 1994 年有人把它匿名张贴到 Cypherpunks 的邮件列表中, 该算法的源代码开始为互联网的用户所熟知. 但这并不影响 RC4 密码算法的安全, 因为其安全性仅依靠所使用的密钥. 由于其加密速度很快 (大约是 DES 的 10 倍), RC4 加密算法被广泛应用于各种嵌入式密码系统中, 如 IEEE802.11b 中定义的 WEP 和 IEEE802.11i 中定义的 TKIP, 其核心密码算法就是 RC4.

RC4 以输出反馈 (OFB) 方式工作: 密钥序列与明文相互独立. 其密钥长度从 1~2048 位可变, 常用的为 40~256 位. 加密算法包含两个部分: 一个称为 KSA (Key Scheduling Algorithm) 的密钥扩展算法和一个称为 PRGA (Pseudo Random Generation Algorithm) 的伪随机数产生算法, 这两个算法需要用到一个 256 单元的密钥存储块 *Key* 和一个 256 单元的 S 盒 *State*, 所用的原始密钥 *K* 被重复填入 *Key* 中直到 *Key* 被填满. 这两个算法描述如下.

算法 1. KSA.

输入: 密钥 *Key*[256]

输出: S 盒 *State*[256]

for (*i*=0; *i*<256; *i*++)

State[*i*]=*i*;

j=0;

for (*i*=0; *i*<256; *i*++){

j=*j*+*Key*[*i*]+*State*[*i*];

swap(*State*[*i*], *State*[*j*]);

}

算法 2. PRGA.

输入: S 盒 *State*[256]

输出: 伪随机数序列 *R*

i=*j*=0;

loop{

i=*i*+1;

j=*j*+*State*[*i*];

swap(*State*[*i*], *State*[*j*]);

R=*State*[*State*[*i*]+*State*[*j*]];

}

PRGA 算法产生的伪随机数序列 *R* 用于与明文异或产生密文 (加密), 或者与密文异或产生明文

(解密). 其中 KSA 算法中密钥扩展的一次循环称为 1 轮.

RC4 中的 KSA 是攻击的目标所在, 从上述算法可以看到, 密钥 *Key* 在扩展的每一轮中都被用到, 因而在密钥扩展的过程中泄露的旁路信息将包含和密钥相关的成分. 为便于分析, 本文的实验中在 AT89C52 单片机上实现了一个密钥长度为 8 位的 RC4 加密算法原型, 对密钥扩展第一轮进行分析就可以获取这 8 位密钥. 这并不影响本文所描述攻击的能力, 更长的密钥只需要对更多的密钥扩展轮进行分析.

3 电磁模板分析攻击

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 电磁兼容的标准 IEC61967^① 中, 传导电磁辐射和发射电磁辐射被认为是噪声并要求低于一定的阈值. IC 的电磁辐射限制在一定的阈值以下, 能防止与其他电子设备发生的无意干扰. 但是, 对于执行密码算法的设备而言, 对电磁辐射还需要有额外的考虑. 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, 电磁模板分析正是利用这一特性进行密码分析的. 与功耗分析相比, 电磁分析不需要在电路中串联电阻, 因而极大地提高了攻击的适应能力.

3.1 电磁辐射产生及其时域特性

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 1 翻转到 0 或者从 0 翻转到 1 时, 反相器的 PMOS 管或 NMOS 管会导通一小段时间. 这就导致一个从 VDD 到 VSS 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.

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^[16]:

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

① International Electrotechnical Commission. IEC 61967: Integrated Circuits — Measurement of Electromagnetic Emissions, 150 kHz to 1 GHz, 2003. <http://www.iec.ch/>

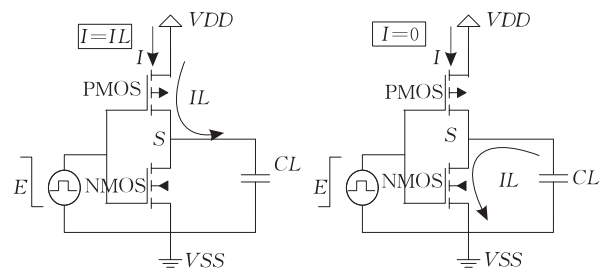


图1 CMOS倒相器在输入信号 E 出现上升沿和下降沿时的动态电流

其中 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, B 表示磁场, 而 S 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:

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

其中 \mathbf{J} 表示电流密度, \mathbf{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 和电流密度 \mathbf{J} 以及电场 \mathbf{E} 成正比, 也就是和芯片内部翻转的晶体管数量成正比。

一个微控制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, 这样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。假设用到的状态是一个定长的机器字 R 。那么可以用汉明重量或汉明距离对旁路信号进行建模。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, 则它的汉明重量为 $H(D) = \sum_{j=0}^{m-1} d_j$ 。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, 微控制器的内部电流可以用源操作数和目的操作数之间的汉明距离来表示, 即

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

其中, λ 是一个和系统相关的常数, μ 是随机噪声。

从式(3)可以看出, 微控制器内部电流大小是和操作数的汉明重量(汉明距离)相关的, 结合式(1)和式(2), 微控制器工作时辐射的电磁信号也与其内部处理的数据是相关的。

为了说明电磁信号的数据相关性, 在 AT89C52 单片机中执行一条 MOV(赋值)指令, 但其源操作数的汉明重量分别为从 0~8 9 个不同的值, 并且

用一个 20 匝的铜螺线圈放在单片机表面感应其运行时产生的变化的电磁场信号, 线圈产生的感应电压用数字存储示波器采集并存储。对每个汉明重量的操作数执行 MOV 指令 10^3 遍并将采集到的电磁曲线^①求平均, 最后得到对应 9 个汉明重量的电磁曲线如图 2 所示。从图中可以看出, 这 9 条曲线的模式是相同的, 但其幅度随汉明重量不同而有明显区别。

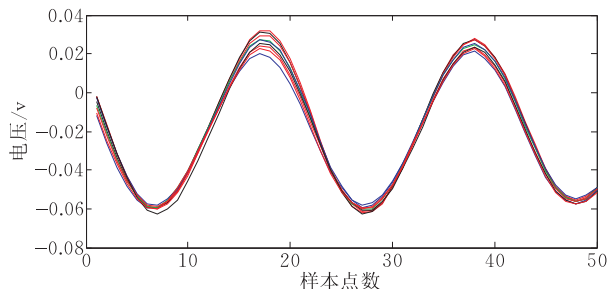


图2 9 个不同操作数 MOV 指令进行操作时的电磁曲线

以 RC4 密钥扩展为例, 图 3 显示的是 RC4 密钥扩展时对应的一条电磁曲线, 可以清楚地看到对应密钥扩展循环的重复特征(图中椭圆圈起的部分)。仅以密钥扩展第一轮为分析对象, 图 4(a) 是 100 条密钥相同的样本曲线两两作差取绝对值后的累加和, (b) 是 100 条密钥不同的样本曲线两两作差取绝对值后的累加和, 可以看到(a)曲线幅值较为一致, 都较小, 而(b)曲线中出现多处尖峰, 这正是由于不同密钥在这几处产生的电磁辐射有较大差异造成的, 即说明尖峰处是电磁曲线和密钥相关的部分。

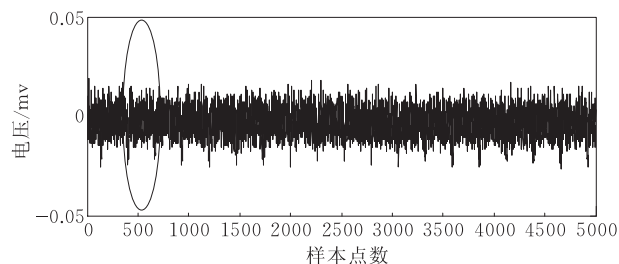
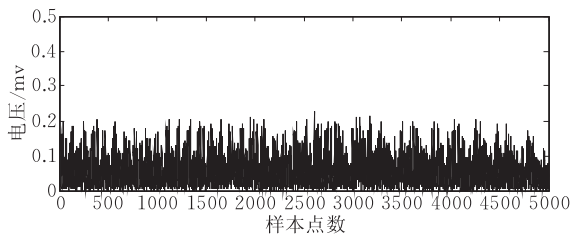


图3 RC4 密钥扩展操作时的电磁曲线

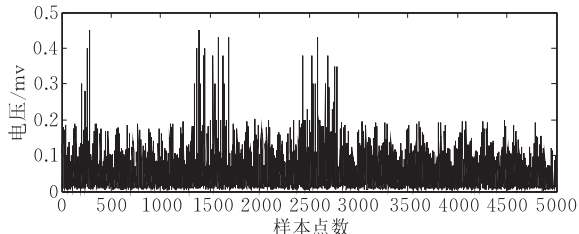
3.2 模板分析攻击

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, 并且参数可以自己设定。这个假设前提很容易实现, 因为被攻击的设备通常都是标准设备, 其类似的设备很容易

① 本文中定义对芯片运行过程中监测到一段时间内的电磁信号轨迹为一条电磁曲线。



(a) 100条密钥相同的样本曲线两两作差后的累加



(b) 100条密钥不同的样本曲线两两作差后的累加

图 4 RC4 密钥扩展第一轮电磁辐射曲线对比

通过合法途径获得. 在这个假设的基础上, 攻击者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.

模板分析攻击由两个步骤组成.

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.

假设子密钥长度是 l 位, 因此需要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 $t_{i1}, t_{i2}, \dots, t_{in} (1 \leq i \leq m)$. 在实际分析过程中, 由于一条电磁曲线中样本点可能较多 (n 可达到 10^3 到 10^6), 可以从中选取少部分和密钥相关的有效点 (interesting points) 组成电磁信号样本, 具体的选取方法可参考文献[18], 本文实验部分 4.1 节中采用的就是这种有效点选取方法.

这样, 电磁曲线样本组成了一个矩阵 $t_{m \times n}$, 对应的均值向量计算如下:

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

因为所有的曲线都是从同一个操作获取的, 存在的随机噪声用样本与样本均值作差的方法求得. 对某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

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

矩阵中的每一行组成了一条电磁样本曲线的噪声向量, 而矩阵的每一列是反映该时间点的噪声的一个随机变量.

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:

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

因此, 一个模板定义为一个 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.

模板匹配阶段.

通过一个被完全控制的芯片完成了所有模板的构建后, 用被攻击的芯片对模板构建阶段中用到的明文 p 进行加密, 并采集对应的芯片运行时的电磁曲线 t' , 与先前构建好的模板进行比较. t' 与模板 $\langle \bar{t}, C \rangle$ 匹配的概率可通过式(8)求得. 根据极大似然法则, 概率最大的就是匹配得最好的模板, 对应的就是最可能的正确密钥.

$$p(t'; \langle \bar{t}, C \rangle) =$$

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

3.3 电磁辐射频域模板分析

当加密系统在加密过程中插入了随机时延后, 采集的时域信号对于相同操作时间点不对齐, 电磁模板构建和匹配时会出现大的错误率, 时域模板分析失效. 示波器采集的数据可看作能量有限信号, 时域内信号的能量等于频域内信号的能量, 即信号经傅立叶变换, 其总能量保持不变, 符合能量守恒定律^[17], 依据前述的时域电磁信号的数据相关性可将

时域数据转换为频域数据进行模板分析攻击. 由于示波器采集的数据为有限长、离散数据, 故使用离散傅立叶变换(DFT).

长度为 N 的有限长序列 $x(n)$ ($0 \leq n \leq N-1$) 的离散傅立叶变换 $X(k)$ 仍然是一个长度为 N ($0 \leq k \leq N-1$) 的频域有限长序列^[17], 变换关系式为

$$X(k) = \text{DFT}[x(n)] = \sum_{n=0}^{N-1} x(n)W^{nk}, \quad 0 \leq k \leq N-1 \quad (9)$$

式中符号 $\text{DFT}[\cdot]$ 表示取离散傅立叶变换, $W = e^{-j(\frac{2\pi}{N})}$.

快速傅立叶变换(Fast Fourier Transform, FFT)是一种快速、通用地进行 DFT 的计算方法, 故 FFT 也可用上式描述. 时域信号 $s_i[j]$ 的 FFT 为

$$S_i[k] = \text{FFT}[s_i[j]] = \sum_{j=0}^{N-1} s_i[j]W^{jk}, \quad 0 \leq k \leq N-1, 0 \leq j \leq N-1, 0 \leq i \leq M-1 \quad (10)$$

根据离散傅立叶变换时移特性^[17]: 若 $\text{DFT}[x(n)] = X(k)$, $y(n) = x(n-m)_N R_N(n)$ (时移 m 位), 则 $\text{DFT}[y(n)] = W^{mk} X(k)$.

这表明信号 $x(n)$ 在时域中沿时间轴时移(延时) $-m$ 位, 等效于在频域中其 DFT 乘以相移因子 W^{mk} , 即信号时移后, 其幅度谱不变, 只是相位谱产生附加变化. 插入随机延时的 $s_i[j]$ 就是一组有不同时移的时域信号, 进行 DFT, 其频谱 $\text{DFT}[s_i[j]]$ 含

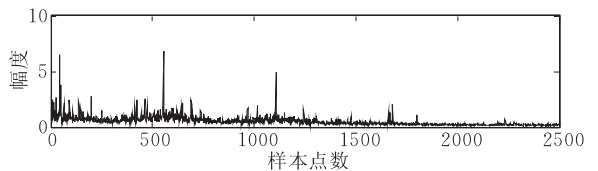
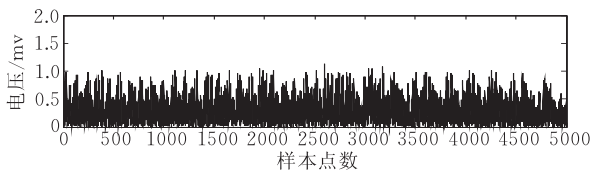
有不同的相位因子 W^{mk} , 下面利用功率谱密度概念解决时域中时移对旁路攻击影响的问题.

若 $f(t)$ 是功率有限信号, 从 $f(t)$ 中截取 $|t| \leq T/2$ 的一段, 得到一个截尾函数 $f_T(t)$ 如下,

$$f_T(t) = \begin{cases} f(t), & |t| \leq T/2 \\ 0, & |t| > T/2 \end{cases} \quad (11)$$

令 $\text{fourier}[f_T(t)] = F_T(\omega)$, 若极限 $P(\omega) = \lim_{T \rightarrow \infty} \frac{|F_T(\omega)|^2}{T}$ 存在, 则定义它为 $f(t)$ 的功率谱密度函数, 或简称功率谱, 记作 $P(\omega)$. 功率谱表示单位频带内信号功率随频率的变化情况, 它反映了信号功率在频域的分布. 功率谱是频率 ω 的偶函数, 它保留了频谱 $F_T(\omega)$ 的幅度信息而丢掉了相位信息, 故凡是具有相同幅度谱(不论相位谱是否相同)的信号都有相同的功率谱.

仍以 RC4 密钥扩展的第一轮为例, 但是在每轮密钥扩展过程中插入随机多个空操作以达到随机时间延迟的效果, 图 5(a) 是 100 条密钥不同的时域样本曲线两两作差后的累加和, (b) 是这 100 条时域样本曲线作 FFT 并求功率谱之后两两作差的累加和, 由于功率谱是频率的偶函数, 故只需取一半的样本点(2500 个)即可. 可以看出时域中由于时间偏移导致样本数据相关性无法显现, 但在频域中依然可以清晰地找出信号与密钥相关的位置.



(a) 100 条密钥不同的时域样本曲线两两作差后的累加和

(b) 100 条密钥不同的样本频域曲线两两作差后的累加和

图 5 RC4 密钥扩展第一轮加入随机时延后电磁辐射的时域曲线与频域曲线对比

4 攻击实验

4.1 实验方案

在 AT89C52 单片机中实现 RC4 加密程序, 原始密钥长度为 8 位, 虽然这与实际中使用的 RC4 加密芯片的密钥长度有所差别, 但从旁路攻击的角度来看, 二者是非常类似的, 而 8 位密钥长度也是 RC4 的经典密钥长度, 实验中仅以此来说明攻击的有效性.

实验平台原理图如图 6, 单片机系统使用 11.0592MHz 的晶振频率, 用一个放在单片机表面

上的 20 匝铜线圈感应单片机运行时泄漏的电磁信号, 线圈感应得到的电压信号用数字存储示波器 (Tektronix DPO4032, 被动探头 P6139A, 差分探头 TDP0500) 进行采集并通过 USB 传输到 PC 机存储, 示波器的采集过程由 PC 机 (Pentium IV4 2.8GHz, 160G HDD, 1G DDR RAM, USB 及 RS232 接口) 上用 LabWindow 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.

为得到 RC4 密钥扩展算法插入随机时延前后的对比攻击结果, 在插入随机时延前后分别进行两个攻击实验. 针对未插入随机时延的 RC4 算法的攻

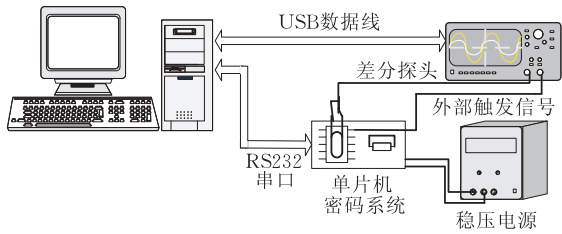


图 6 实验平台示意图

击实验步骤如下：

1. 在 AT89C52 单片机上实现算法 1, 用所有可能的 8 位原始密钥(共 256 个)分别进行 10^3 次密钥扩展, 与此同时用数字存储示波器采集线圈上的感应电压信号(采样长度为 5000 点)并送 PC 机存储成 256 个样本矩阵 $t_{1000 \times 5000}^i$, 用 Matlab 编写的程序将电磁曲线转换成频域信号并求功率谱曲线(由于是偶函数, 只需取 2500 个样本点), 同样存储成 256 个样本矩阵 $f_{1000 \times 2500}^i (i=1, 2, \dots, 256)$;
2. 采用 Rechberger 等人提出的从旁路样本中提取和密钥相关的有效点的方法^[18]. 分别将对应不同密钥的时域信号样本求均值 $\bar{t}_{1 \times 5000}^i = \frac{1}{1000} \sum_{l=1}^{1000} t_{l \times 5000}^i$, 将这 256 个均值曲线两两作差求绝对值后累加, 得到差值曲线 $\Delta \bar{t}_{1 \times 5000} = \sum_{k=1}^{256} \sum_{l=1}^{k-1} \cdot |\bar{t}_{1 \times 5000}^k - \bar{t}_{1 \times 5000}^l|$, 从该差值曲线中选取幅值最大的 20 个点^①, 以其列坐标为索引从矩阵 $t_{1000 \times 5000}^i$ 中抽取 20 列得到新的样本矩阵 $t_{1000 \times 20}^i$, 用同样的方法得到样本矩阵 $f_{1000 \times 20}^i$, 这两个矩阵包含了与密钥相关的信息.
3. 根据 3.2 节描述的原理, 分别利用得到的样本矩阵 $t_{1000 \times 20}^i$ 和 $f_{1000 \times 20}^i$ 构建对应各个已知密钥的时域电磁模板 $T = \langle \bar{t}, C \rangle$ 和频域电磁模板 $F = \langle \bar{f}, C \rangle$.
4. 用同样的方法获取对应任意密钥 k' 的一条电磁曲

线, 根据步 2 得到的列坐标抽取出样本 $t'_{1 \times 20}$ 和 $f'_{1 \times 20}$, 根据式(8)分别计算该时域样本和频域样本与模板的匹配概率.

针对插入随机时延的 RC4 算法的攻击实验需要先 在单片机中实现算法 3, 该算法在密钥扩展过程中插入了随机多个空操作, 以达到密钥相关操作的时间点随机化的目的. 之后重复步 1~4 的过程, 得到插入随机时延后的时域和频域模板匹配结果.

算法 3. M-KSA.

输入: 密钥 $Key[256]$

输出: S 盒 $State[256]$

```
for( i=0; i<256; i++)
    State[i]=i;
j=0;
for(i=0; i<256; i++){
    for(i=0; i<rand(); i++)
        nop(); //插入随机多个空操作
    j=j+Key[i]+State[i];
    swap(State[i], State[j]);
}
```

4.2 实验结果及分析

这里选取 4 个有代表性的密钥匹配情况进行对比得到结果如表 1 和表 2 所示. 表中每一行是将最左列的原始密钥与 4 个密钥进行匹配的结果, 从表 1 可以看出在未插入随机时延之前, 时域和频域模板匹配都能得到较好的结果; 从表 2 可以看出在插入随机时延之后, 时域模板匹配得到的结果无法分辨正确密钥, 而频域模板匹配结果几乎不受随机时延的影响.

表 1 针对未插入随机时延的 RC4 密码芯片电磁模板分析结果

原始密钥	匹配密钥							
	时域模板匹配结果				频域模板匹配结果			
	00000000	10010001	10111101	11111111	00000000	10010001	10111101	11111111
00000000	0.85	0.64	0.23	0.08	0.79	0.46	0.33	0.01
10010001	0.15	0.79	0.18	0.11	0.25	0.65	0.18	0.15
10111101	0.18	0.24	0.85	0.15	0.20	0.33	0.70	0.26
11111111	0.03	0.12	0.34	0.89	0.02	0.21	0.45	0.77

表 2 针对插入随机时延的 RC4 密码芯片电磁模板分析结果

原始密钥	匹配密钥							
	时域模板匹配结果				频域模板匹配结果			
	00000000	10010001	10111101	11111111	00000000	10010001	10111101	11111111
00000000	0.24	0.25	0.32	0.03	0.72	0.31	0.18	0.09
10010001	0.23	0.43	0.43	0.12	0.33	0.77	0.24	0.07
10111101	0.08	0.16	0.33	0.20	0.17	0.25	0.80	0.34
11111111	0.02	0.12	0.27	0.69	0.12	0.15	0.33	0.79

4.3 攻击性能分析

设子密钥块长度为 k 比特, 每个密钥采集 s 个

① Rechberger 等人证明了 20 个有效点足以包含和密钥相关的信息.

样本以构建模板。从实验步骤可以看到,传统的时域模板分析攻击包括有效样本点的选取和模板构建与匹配两部分,这两部分的时间开销都是和模板数量成正比的,即整个攻击时间复杂度为 $O(2^k)$ 。频域模板分析比传统的时域模板分析多了一个将时域信号转换到频域信号的过程,而该过程需要进行 $2^k \times s$ 次 FFT 运算,因此频域模板分析的时间复杂度依然为 $O(2^k)$,说明时域和频域模板分析的时间复杂度是随着子密钥块的长度增长而成指数增长的,但是旁路攻击方法对密码算法进行分析,是将整个密钥化整为零分成小的密钥块进行攻击的,只要子密钥块的长度在一定范围内模板分析的时间复杂度依然是可以接受的。

5 结束语

本文通过深入研究密码芯片电磁辐射的产生机理,分析了电磁信号的数据相关性并构建汉明重量模型和汉明距离模型以表达这种相关性,指出该相关性从时域信号经 Fourier 变换到频域信号时依然存在,且不受时域信号中随机时间延迟的影响,根据这一特性提出的电磁频域模板分析是一种有效的旁路攻击方法。随机时间延迟被认为是抵御时域分析攻击的重要方法,但是本文研究表明其并不能抵抗频域模板分析攻击。与已有的时域信号模板分析攻击相比,本文提出的攻击方法并不增加攻击的时间复杂度。

参 考 文 献

- [1] Quisquater J J, Samyde D. Electromagnetic analysis (EMA): Measures and countermeasures for smart cards//Proceedings of the Smart Cards Programming and Security (e-Smart 2001). Cannes, France, 2001: 200-210
- [2] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'01). Paris, France, 2001: 251-261
- [3] Agrawal D, Archambeault B, Rao J R, Rohatgi P. The EM side-channel(s): Attacks and assessment methodologies//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'02). Redwood Shores, CA, USA, 2002: 29-45
- [4] Chari S, Rao J R, Rohatgi P. Template attacks//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'03). Cologne, Germany, 2003: 13-28
- [5] Agrawal D, Rao J R, Rohatgi P, Schramm K. Templates as master keys//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'05). Edinburgh, UK, 2005: 15-29
- [6] Archambeau C, Peeters E, Standaert F X, Quisquater J J. Template attacks in principal subspaces//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'06). Yokohama, Japan, 2006: 1-14
- [7] Gierlichs B, Lemke-Rust K, Paar C. Templates vs. Stochastic Methods//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'06). Yokohama, Japan, 2006: 15-29
- [8] Standaert François-Xavier, Archambeau Cedric. Using sub-space-based template attacks to compare and combine power and electromagnetic information leakages//Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'08). Washington, D. C., USA, 2008: 411-425
- [9] Messerges T S. Power analysis attacks and countermeasures for cryptographic algorithms[Ph. D. dissertation]. Graduate College of the University of Illinois, Chicago, 2000
- [10] Han Jun, Zeng Xiao-Yang, Tang Ting-Ao. Power trace analysis attack and countermeasures for RSA cryptographic circuits. Chinese Journal of Computers, 2006, 29(4): 590-596(in Chinese)
(韩军, 曾晓洋, 汤庭鳌. RSA 密码算法的功耗轨迹分析及其防御措施. 计算机学报, 2006, 29(4): 590-596)
- [11] Han Jun, Zeng Xiao-Yang, Tang Ting-Ao. Modeling timing randomization in cryptographic chip against power analysis attack. Computer Engineering, 2007, 33(2): 6-8(in Chinese)
(韩军, 曾晓洋, 汤庭鳌. 基于时间随机化的密码芯片防攻击方法. 计算机工程, 2007, 33(2): 6-8)
- [12] Aigner M, Oswald E. Power analysis tutorial. Institute for Applied Information Processing and Communication, University of Technology Graz, Technical Report, Austria, 2000
- [13] Chin Chi Tiu. A new frequency-based side channel attack for embedded systems [Ph. D. dissertation]. Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada, 2005
- [14] Chu Jie, Zhao Qiang, Ding Guo-Liang, Zhang Peng, Deng Gao-Ming. Differential power spectral density analysis attacks for symmetric encrypted systems. Computer Engineering, 2008, 34(10): 10-13(in Chinese)
(褚杰, 赵强, 丁国良, 张鹏, 邓高明. 对称加密系统差分功率谱分析攻击. 计算机工程, 2008, 34(10): 10-13)
- [15] Bruce Schneier. Applied Cryptography, Protocols, Algorithms, and Source Code in C. 2nd Edition. Beijing: China Machine Press, 2000(in Chinese)
(Bruce Schneier 著, 吴世忠, 祝世雄, 张文政等译. 应用密码学, 协议、算法与 C 源程序. 第 2 版. 北京: 机械工业出版社, 2000)

[16] Serway R A. Physics for Scientists and Engineers. Saunders Golden sunburst series. Saunders College Publishing, 1996

[17] Zhen Jun-Li, Ying Qi-Hang, Yang Wei-Li. Signal and System. 2nd Edition. Beijing: Higher Education Press, 2000(in Chinese)

(郑君里, 应启珩, 杨为理. 信号与系统. 第2版. 北京:高等

教育出版社, 2000)

[18] Christian Rechberger, Elisabeth Oswald. Practical template attacks//Proceedings of the Information Security Applications, 5th International Workshop (WISA 2004). Jeju Island, Korea, 2004: 443-457



DENG Gao-Ming, born in 1983, Ph. D. candidate. His current research interests include electromagnetic emission measurement and protection.

ZHAO Qiang, born in 1945, professor, Ph. D. supervisor. His current research interests include ICs’ security and protection, electromagnetic emission measurement and protection.

Background

This work is supported by the National Natural Science Foundation of China under grant No. 60571037, and the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z454. They aim to evaluate the security of cipher chips under side channel attacks, especially under power analysis and EM analysis.

In these two programs, the power model of CMOS de-

ZHANG Peng, born in 1976, Ph. D. candidate. His current research interests include electromagnetic emission measurement and protection.

CHEN Kai-Yan, born in 1970, Ph. D. candidate, associate professor. Her current research interests include electromagnetic emission measurement and protection, computer security.

LIU Xiao-Qin, born in 1983, Ph. D. candidate. Her current research interests include ICs’ security and protection.

vice was built with Hamming Weight or Hamming Distance model, and popular ciphers such as DES, AES, RSA and RC4 implemented in a micro-controller were analyzed with side channel attacks, especially power analysis and EM analysis, and the experiments showed a good result. Besides, a formal security model for cipher under side channel attack is analyzed, and it is hopeful to evaluate the security of cipher chips under side channel attack.