

功耗分析攻击中滤噪方法的研究

陈艾东^{1,2}, 孙敦灿², 杨航江², 王飞雁²

(1 电子科技大学 计算机科学与工程学院, 四川 成都 610054; 2 成都信息工程学院 信息安全研究所, 四川 成都 610225)

摘 要: 在真实环境的功耗分析攻击中发现, 功耗曲线经常受到大量噪声的影响. 为了提高攻击效率, 分析了几种常用滤波方法的特点, 针对具体的功耗分析问题在真实环境下进行了实验. 对几种滤波效果进行了对比, 得出滑动平均滤波最适合解决此类问题的结论.

关键词: 密码分析; 边信道攻击; 功耗分析攻击; 滤噪算法

中图分类号: TN918.91

文献标识码: A

文章编号: 1000-7180(2012)08-0107-04

Research on Filtering Noise Method of the Power Analysis Attack

CHEN Ai-dong^{1,2}, SUN Dun-can², YANG Hang-jiang², WANG Fei-yan²

(1 College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China; 2 Institute of Information Security, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: The power consumption curves were often affected by plenty of noise in real environment attack. In order to improve the efficiency of the attack, this paper analyses characteristics of several common filtering noise methods and completes experiments to the specific questions. At last, it compares the filtering effects and draws a conclusion that moving average filter is the most suitable method to solve this kind of problem.

Key words: cryptanalysis; side channel attack; power consumption analysis attack; filtering noise algorithm

1 引言

边信道攻击是一种从密码设备中获取秘密信息的密码攻击方法. 常见的边信道攻击有时间攻击^[1] (Timing Attack)、功耗分析攻击^[2] (Power Analysis Attack)、电磁攻击^[3] (Electric Magnetic attack) 和故障攻击^[4] (Fault attack) 等, 在文献[1-4]中有经典的论述. 以功耗分析攻击中的模板攻击作为 RSA 密码算法的攻击手段.

由于密码芯片的真实功耗轨迹湮没在大量的噪声中, 因此在对密码算法做功耗分析攻击之前, 对采集到的含有大量噪声的功耗曲线进行滤波是十分必要的.

2 功耗分析攻击

在真实环境下, 进行功耗曲线的采集要受到设

备、环境等多方面的影响, 具体功耗的组成如下式:

$$P_{\text{total}} = P_{\text{op}} + P_{\text{data}} + P_{\text{el. noise}} + P_{\text{const}} \quad (1)$$

P_{total} : 总功耗

P_{op} : 操作依赖分量

P_{data} : 数据依赖分量

$P_{\text{el. noise}}$: 电子噪声

P_{const} : 恒定分量

$$P_{\text{op}} + P_{\text{data}} = P_{\text{exp}} + P_{\text{sw. noise}} \quad (2)$$

P_{exp} : 能量消耗分量

$P_{\text{sw. noise}}$: 转换噪声

在式(2)中的 P_{exp} 是带给攻击者最多信息的分量, 在操作大致相同的各个模乘中 P_{op} 稳定, 而在有不同的操作数进行运算时, P_{data} 不同.

功耗攻击是边信道攻击的一种, 它是根据密码系统的能耗与被处理数据或操作之间的依赖性进行攻击的^[5]. 选择明文攻击是一种传统的密码分析方

收稿日期: 2012-03-08; 修回日期: 2012-05-10

基金项目: 国家自然科学基金资助项目(60873216); 四川省科技攻关重点项目(2012GZ0017); 四川省应用基础研究基金资助项目(2011JY0100)

法,将其与功耗攻击相结合,在被控设备上输入特定的明文或消息,使用被攻击密码系统加密,得到相应密文.在此过程中捕获功耗曲线,寻找其功耗特征与秘密信息的相关性,以便恢复密钥.

3 滤波方法简介

湮没在大量噪声中的密码算法的真实功耗信息是时变的、非平稳的,不容易区分出来,给攻击增加了难度.因此在攻击之前对所采集到的功耗信号进行滤波,对研究分析密码算法是很有帮助的.

常用的滤波方法有低通滤波法、防脉冲干扰平均滤波法、巴特沃斯滤波法、滑动平均滤波法等.

3.1 低通滤波法

低通滤波的特性可以用如下方程来表示:

$$y_n = ax_n + (1-a)y_{n-1} \quad (3)$$

式中, x_n 表示当前的数据, y_{n-1} 表示上一次的滤波输出值, a 表示滤波系数, y_n 表示本次滤波输出值.

由式(3)可知,本次滤波的输出值 y_n 主要取决于上次滤波的输出值 y_{n-1} ,本次的采样值 x_n 只起到一些辅助性的修正作用,滤波的系数 a 是可以自行设定的.低通滤波算法对周期性干扰具有良好的抑制作用,适用于波动频繁的参数滤波^[6].滤波算法的截止频率可由下式计算:

$$f_L = a/2\Omega t \quad (4)$$

式中, a 为滤波系数, t 为采样间隔时间.

低通滤波的不足之处是带来了相位滞后,滞后的程度取决于 a 值的大小.

3.2 防脉冲干扰平均滤波法

防脉冲干扰平均滤波法以算术平均作为算法基础,对连续 N 个采样数据值,去掉这 N 个数据中的一个最大值 max 和一个最小值 min ,然后计算 $N-2$ 个采样数据的算术平均值.算法流程如图1所示.

在实际使用时, N 的选择会影响滤波的效果.一般来说, N 选择 3 到 14 之间的数值.

3.3 巴特沃斯滤波法

巴特沃斯(Butterworth)滤波器是一种具有最大平坦幅度响应的低通滤波器,起伏最小,在阻频带则逐渐下降为零.在振幅对数对角频率的波特图上,从某一边界角频率开始,振幅会随着角频率的增加而逐步减少,并且趋向负无穷大.

巴特沃斯低通滤波器的平方幅度响应为

$$|H(j\omega)|^2 = \frac{1}{1 + \left(\frac{\omega}{\omega_c}\right)^{2n}} \quad (5)$$

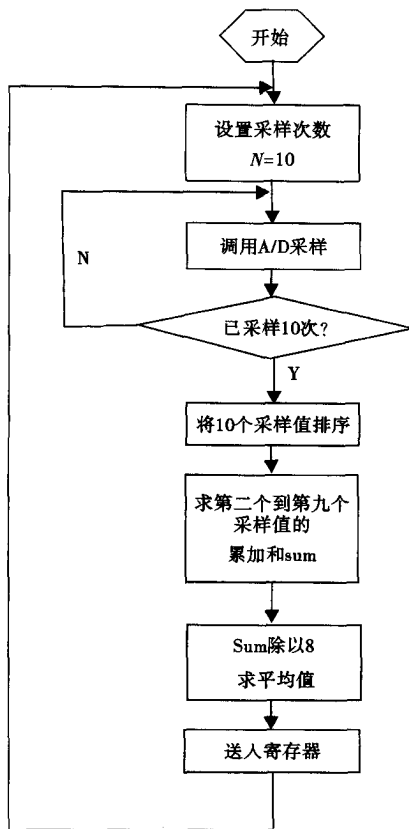


图1 防脉冲干扰平均滤波法流程图

式中, n 为滤波器的阶数, ω_c 为低通滤波器的截止频率.阶数 n 越高,其幅频特性越好,但由于具有有较长的过渡带^[7],巴特沃斯滤波在过渡带上很容易造成失真.

3.4 滑动平均滤波法

滑动平均滤波法的原理是:连续取 L 个采样值看成一个滑动窗口,该滑动窗口的长度固定为 L ,每次采样到一个新数据放入窗口尾,并将窗口首部的数据去掉,这样就始终保持滑动窗口中有 L 个数据.把滑动窗口中的这 L 个“最新”数据进行算术平均运算,就可获得新的滤波结果.表达式为

$$y[n] = \frac{1}{L} \sum_{K=0}^{L-1} x[n-K] \quad (6)$$

式中, L 为滑动窗口的宽度. L 点滑动平均滤波器的频率响应^[8]是

$$H(e^{j\omega}) = \frac{1}{L} \sum_{K=0}^{L-1} e^{-j\omega K} = \left[\frac{\sin(\omega L/2)}{L \sin(\omega/2)} \right] e^{-j\omega(L-1)/2} \quad (7)$$

滑动平均滤波相当于一个低通滤波器,衰减了较高频率的信号,对数据起到平滑的作用^[9].滑动平均滤波法对周期性的干扰有良好的抑制作用,平滑度高,并且适用于高频振荡的系统.

4 实验分析及对比

将以上四种滤波方法在相同的实验条件下进行对比,以找出对 RSA 密码算法具有良好滤波效果的滤波器,帮助研究密码算法的功耗.

4.1 实验环境

对 8051 芯片进行测试,平台组成^[10]如图 2 所示.

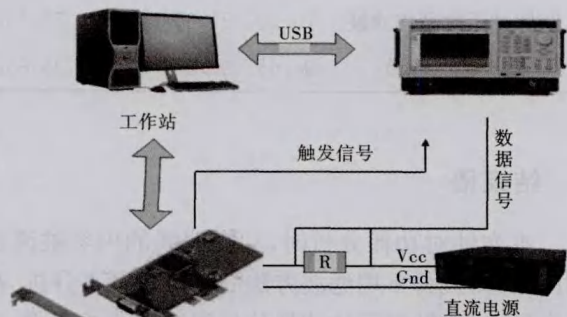


图2 功耗分析平台框架

功耗分析平台中,工作站与示波器 USB 相连,对示波器与接口板进行设置.发送指令或者数据到接口板,接收返回数据.示波器采用的 Tektronix PPO4032,接收指令采集功耗曲线和触发信号.采样频率为 1 MHz,采样点 1 MHz,示波器 1 通道信号触发,2 通道数据采集,触发模式为 auto,下降沿触发.

4.2 噪声的影响

由于电子噪声、转换噪声等影响,RSA 密码算法功耗轨迹中的字节分界尖峰就不容易区分出来.而这个字节分界尖峰恰恰是对 SPA 攻击来说是相当重要的信息^[11].本文研究的目的是经过滤波之后,能够把 RSA 密码算法的字节分界尖峰凸现出来.

4.3 滤噪效果对比

图 3 是 RSA 密码算法的原始功耗曲线完整截图,由于噪声的缘故,密码算法的各个轮次的模幂运算和字节分界尖峰等均无法看到.

图 4 是对图 3 中矩形框部分的放大展示,下面的几种滤波结果都是针对这个细节部分的放大显示.在图 4 中,看到的依然是很多的噪声,无法区分出各轮次的模幂运算和字节分界尖峰.

图 5 是低通滤波后的效果截图.从图中可以看到,各轮次的模幂运算和字节分界尖峰(矩形框标注部分)可以看得出来,但依然不是很明显.

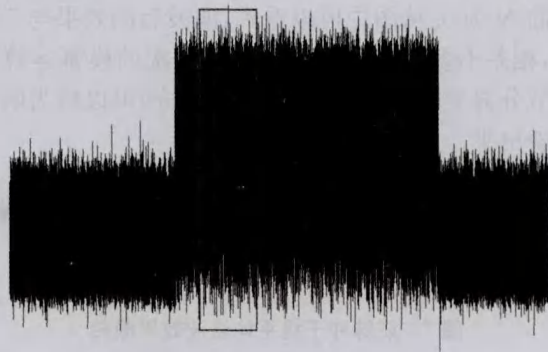


图3 RSA 密码算法原始功耗曲线



图4 RSA 密码算法原始功耗曲线细节

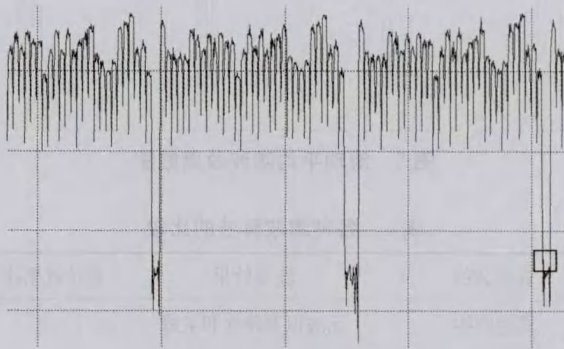


图5 低通滤波效果截图

图 6 是巴特沃斯滤波后的效果截图.选取的通带频率为 0.32,阻带频率为 0.4.从图中可以看到,滤波后的效果与图 5 相比相差很多,可见巴特沃斯滤波法并不适合于 RSA 密码算法功耗曲线.



图6 巴特沃斯滤波效果截图

图 7 是防脉冲干扰平均滤波法的效果截图.此

处的 N 为 5. 从图中可以看到, 滤波后的效果与 5 相比, 相差不多, 但是比 6 要好. 各轮次的模幂运算和字节分界尖峰(图中矩形框标注部分)可以较为明显地看出来.



图 7 防脉冲干扰平均滤波效果截图

图 8 是滑动平均滤波后的效果截图, 滑动平均的 N 选择为 5. 从图中可以看到, 各轮次的模幂运算和字节分界尖峰都可以很明显地看出来, 效果比低通滤波、巴特沃斯滤波、防脉冲干扰平均滤波法都要好. 可见, 滑动平均滤波很适合于对 RSA 密码算法的功耗曲线进行处理. 对比如表 1 所示.

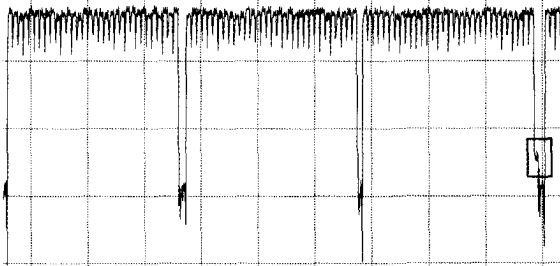


图 8 滑动平均滤波效果截图

表 1 各种滤波算法的比较

算法名称	滤波效果	算法效果排序
原始曲线	无法识别轮次和尖峰	
单纯放大	无法识别轮次和尖峰	
低通滤波	可以识别轮次和尖峰但不明显	②
巴特沃斯滤波	效果差于低通滤波	④
防脉冲干扰平均滤波	可以较为明显分辨出轮次和尖峰	③
滑动平均滤波	可以很明显分辨出轮次和尖峰	①

4.4 滤波后攻击效果对比

在图 2 所示的攻击环境中, 对 8051 安全芯片的 RSA 密钥进行攻击. 这种芯片处理数据的位数是 8 位(即安全性芯片在处理数据时是按照字节为单位读取密钥进行模幂运算的). 每次执行完一个字节密钥的模幂运算后, 都要读取下一个字节的密钥和中间数据的处理. 而这种操作就会造成功耗信息在时间上的泄露, 形成图 8 中带有台阶的分界下尖峰. 攻击中应用这种特殊的下尖峰, 分界每个字节密钥, 形成汉明重量模板进行攻击.

在各种滤波方法应用后, 对功耗分析准确率统计如表 2 所示.

表 2 滤波后功耗分析准确率对比

曲线名称	500	1 000	2 000	5 000
原始曲线	51.2%	52.3%	54.1%	55.8%
低通滤波	83.2%	84.3%	86.4%	87.6%
巴特沃斯滤波	62.9%	64.1%	65.9%	67.6%
防脉冲干扰平均滤波	70.5%	71.6%	73.5%	75.2%
滑动平均滤波	94.6%	95.5%	97.2%	98.8%

5 结束语

本文针对功耗分析时, 功耗曲线的内容被湮没的问题, 对几种常用滤波方法的特点进行了分析. 在真实环境下, 针对具体功耗分析问题进行了实验, 对几种滤波效果进行了对比, 得出滑动平均滤波最适合解决此类问题的结论

参考文献:

- [1] Kocher P, Jaffe J, Jun B. Differential power analysis [J]. CRYPTO 1999, Lecture Notes in Computer Science, 1999(1666): 388-397.
- [2] Messetges T S, Dabbish E A, Sloan R H. Investigations of power analysis attacks on smartcards [C] // Proc USENIX Workshop Smartcard Technology Chicago, Illinois, USA: IEEE, 1999: 151-161.
- [3] Rao J R, Rohatgi P. EMpowering side-channel attacks [R]. preliminary technical report, IBM T. J. Watson Research Center, 2001.
- [4] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems [C] // Proc of Crypto'97. Santa Barbara, California, USA: [s. n.], 1997.
- [5] Stefan Mangard, Elisabeth Oswald, Thomas Popp. Power analysis attacks revealing the secrets of smart cards advances in information security [M]. New York: Springer, 2007.
- [6] 胡建建, 曾培峰, 唐莉萍, 等. 基于高斯低通滤波的音乐节拍提取 [J]. 东华大学学报, 2011(1): 72-75.
- [7] 何岭松, 王峻峰. 巴特沃斯小波变换算法在故障诊断中的应用 [J]. 华东理工大学学报, 2000, 28(10): 31-33.
- [8] James H McClellan, Ronald W Schafer, Mark A Yoder. 信号处理引论 [M]. 北京: 电子工业出版社, 2005.

(下转第 114 页)

提出的优化算法和传统 CORDIC 算法的资源消耗情况如表 2 所示.

表 2 不同算法下, FPGA 资源的消耗情况

	Logic elements	Registers	Memory bits
传统算法	2 588	1 476	34
本文算法	2 147	1 218	34

可以看出, 使用本文提出的算法实现的 DDS 比传统算法在不仅在 register 方面比减少了约 17% 的资源, 而且在 logic elements 方面也减少了约 17% 的资源, 这是因为在减少角度和幅度量化的同时, 也就相应的减少了加/减法器的位宽, 也就会减少 logic elements 资源.

5 结束语

本文通过对传统 CORDIC 算法中流水结构的存储单元进行优化, 在不影响精度的情况下节约了 FPGA 的资源. 而且当迭代次数和量化位宽越宽时, 节约的 FPGA 资源将会更多. 应用本文算法在 altera 公司的 FPGA 中实现的 DDS 已经成功应用在频标实验中.

参考文献:

- [1] 王勇, 吕善伟, 冯克明, 等. 基于 CORDIC 算法的 DDS 在铷原子频标中的应用[J]. 宇航计测技术, 2005, 25(3): 15-18.
- [2] Volder J E, The CORDIC trigonometric computing technique[J]. IRE Trans Electron Computers, 1959 (EC-8): 330-334.
- [3] 沈志, 王宏远, 王振. 无相位截断误差的 DDS 设计[J]. 微电子学与计算机, 2011, 28(3): 70-72.
- [4] Pramod K Meher, Javier Valls, Sridharan K. 50 Yearsof CORDIC: algorithms, architectur-es and applications [J]. IEEE Trans On Circui-ts and systems-I: Regular papers, 2009(56): 1893-1906.
- [5] Walther J S. A unified algorithm for elementary functions[C]//Proc 38 th Spring Joint Computer Conf Atlantic City, NJ: IEEE, 1971: 379-385.
- [6] 张天瑜. 基于旋转模式的改进型 CORDIC 算法研究 [J]. 微电子学与计算机, 2010, 27(3) 93-97.

作者简介:

陈义和 男, (1983-), 硕士, 工程师. 研究方向为电路和信号处理.

余 磊 男, (1979-), 博士, 副研究员. 研究方向为原子频标技术与实验.

李交美 男, (1956-), 研究员, 博士生导师. 研究方向为原子频标.

(上接第 110 页)

- [9] 戴永寿, 牛慧, 彭星, 等. 基于自回归滑动平均模型和粒子群算法的地震子波提取 [J]. 中国石油大学学报, 2011, 35(3): 47-50.
- [10] 孙敦灿, 陈运. 功耗分析平台中混合编程的应用研究 [J]. 成都信息工程学院学报, 2011, 26(2): 127-131
- [11] 陈俊, 陈运. 抗功耗分析攻击的椭圆曲线梳状优化算法

[J]. 成都信息工程学院学报, 2010, 25(4): 341-344

作者简介:

陈艾东 女, (1978-), 博士生, 讲师. 研究方向为边信道攻防与物联网安全.