

差分能量攻击所需样本数量研究

李志强, 严迎建, 段二朋

(解放军信息工程大学电子技术学院, 郑州 450004)

摘 要: 对分组密码算法差分能量攻击的样本数量选取问题进行研究。通过建立差分能量信号的信噪比模型, 推导出样本数量的数学表达式为 $N > (8\sigma^2 + \varepsilon^2(\alpha n + n - d)) / d^2 \varepsilon^2$, 根据 σ 和 ε 计算得到攻击所需样本数量为 8 000。分别用 5 000 组和 8 000 组随机明文对高级加密标准算法进行差分能量攻击, 结果证明, 当样本数量为 8 000 时可以得到正确密钥, 效果结果优于 5 000 组明文的情况。

关键词: 分组密码算法; 高级加密标准; 差分能量攻击; 样本数量

Research on Sample Amounts Needed by Differential Power Attack

LI Zhi-qiang, YAN Ying-jian, DUAN Er-peng

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

【Abstract】 Aiming at the problem of sample amount to differential power attack of block cipher, by establishing the SNR model of differential power signal, this paper proposes the expression of the sample amount: $N > (8\sigma^2 + \varepsilon^2(\alpha n + n - d)) / d^2 \varepsilon^2$. After measuring the parameters σ and ε , the numerical value is got, which is about 8 000. Using the 5 000 samples and 8 000 samples separately to finish the Differential Power Attack(DPA) to Advanced Encryption Standard(AES), and gets the right key when the samples' amount is 8 000. The result is better than when it is 5 000, so the expression proposed is reasonable.

【Key words】 block cipher algorithm; Advanced Encryption Standard(AES); Differential Power Attack(DPA); sample amount

DOI: 10.3969/j.issn.1000-3428.2012.24.031

1 概述

能量攻击技术的概念最早由文献[1-2]提出, 主要分为简单能量攻击(Simple Power Analysis, SPA)^[3]和差分能量攻击(Differential Power Analysis, DPA)^[4]两大类, 其中, 差分能量攻击因其较强的抗干扰能力和较高的准确率而应用得更为广泛。

国内外关于电路中的降噪问题已进行了大量的研究, 比如文献[5]中提到, 为了减小噪声干扰, 进行如下操作: (1)在差分能量攻击中, N 次随机的密码运算, 每一次均以相同的明文重复进行 M 次; (2)对 M 个重复明文样本的功耗曲线求均值, 总共得到 N 个功耗曲线。由于目标信号的值非常小, 因此降噪技术在测量旁道泄露信息时显得尤为重要。文献[6]证明, 通过随机计算增大测量噪声来掩盖旁道信息, 可以抵抗能量分析攻击。

在实际的攻击中, 需要大量的样本进行加解密运算, 进而采集功耗信息作统计分析, 以消除电路中噪声带来的影响。然而对于样本数量, 现有的文献都没有进行说明, 而是直接用一定量的随机数据进行密码运算。显然, 这给应用带来了不便。本文根据实际差分能量攻击结果对信噪比的要求, 对所需样本数量进行定量分析。

2 差分能量攻击原理

差分能量攻击重复采集大量的功耗数据, 并对其进行分析以得出密钥。差分能量攻击的原理^[6]如下: 利用某个状态字节的值作为区分函数, 借鉴基于汉明重量的功耗模型^[4]中功耗与状态字节中 1 的个数呈正比, 本文假设状态字节为 1 时功耗为 $P+a$, 状态字节为 0 时功耗为 P 。当攻击者猜测到正确密钥时的差分能量攻击如图 1 所示, 其中, 每一行表示一组明文加密得到的一组功耗数据, 猜测的值即攻击者利用猜测密钥得到的算法的中间值。

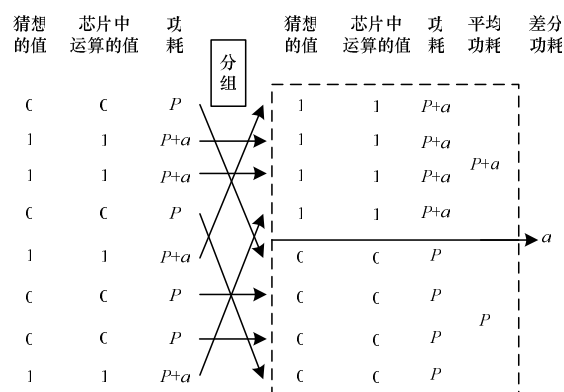


图1 猜测到正确密钥时的差分能量攻击

作者简介: 李志强(1989—), 男, 硕士研究生, 主研方向: 密码学, 集成电路设计; 严迎建, 副教授、博士; 段二朋, 硕士研究生

收稿日期: 2011-09-14 **修回日期:** 2011-11-04 **E-mail:** johnlee126@126.com

然后攻击者利用自己猜想的值将功耗数据分为2组。在之后的数据分析阶段,攻击者先求出各组的功耗均值,再将2个功耗均值求差。图1中所示为密钥猜测正确时攻击者恰好将有差异的功耗数据分为2组。

当攻击者猜测到错误密钥时的差分能量攻击如图2所示。从中可以看出,攻击者利用错误密钥得到的中间值不符合芯片中运算的值,在用猜想的值对功耗数据进行分组时,相应地将2组有差异的功耗数据打乱在一起,因此,攻击者最后得到的差分功耗不为 a 。由于功耗数据是基于猜测密钥运算的中间值进行分组的,每一个猜测密钥对应一个分组,而只有正确的密钥可以将2组具有差异的功耗数据区分开,因此正确密钥的差分功耗值是最大的。

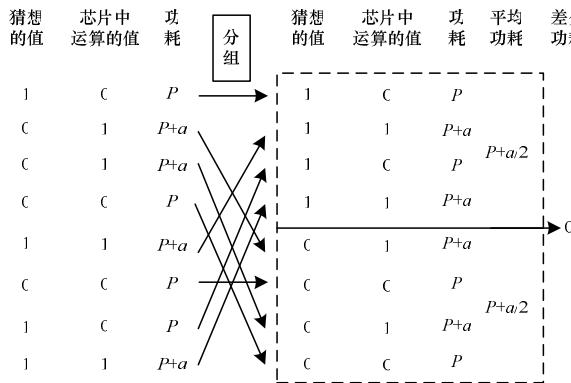


图2 猜测到错误密钥时的差分能量攻击

3 差分功耗信号的信噪比

功耗测量与分析平台中不可避免地有噪声出现,对差分功耗信号的信噪比进行建模有利于进一步确定差分功耗分析中的样本数。差分功耗信号的数学建模要在实际测量的基础上经过理论推导得到,差分功耗信号建模过程如图3所示。

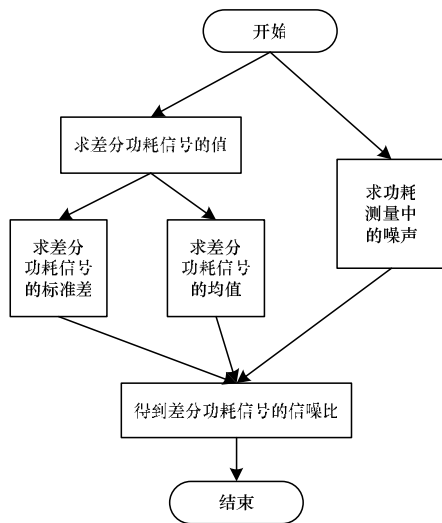


图3 差分功耗信号建模过程

3.1 功耗测量与分析平台中的噪声

在测量密码芯片运算的功耗时,至少有5种噪声:外部噪声,固有噪声,量化噪声,采样噪声以及算法噪声。

外部噪声由外部的环境产生,由于电阻的电压非常

小,差分探头很容易受到实验室中外界环境的影响。

固有噪声来源于密码芯片内部的电容随机地充放电,例如各个逻辑单元的寄生电容会根据输入的不同进行充放电,进而影响到密码芯片的功耗。

由于密码芯片串联电阻的电压为模拟信号,差分探头在采集时会利用其内部的A/D转换器将模拟电压信号转换为数字电压信号,这种量化过程中会生成量化噪声。

采样噪声在量化功耗信号的时间点和密码芯片运算的时间点不对应时产生。

在实际测量中,如果密码芯片的连续2组输入不同,那么后一组的功耗会受到前一组数据的影响,这就是算法噪声。

功耗测量中的噪声可以基于统计学计算出来,用 N_i 表示功耗测量中的噪声, S_i 表示一次测量得到的功耗曲线, $E(S_i)$ 表示多次测量得到的均值, i 为各次测量的序号,则噪声 N_i 可以由下式表示:

$$N_i = S_i - E(S_i)$$

如果采集到的功耗曲线为同一个输入,上式将不包括算法噪声,如果采集到的功耗曲线的输入各不相同,则上式可以将功耗分析平台运转时所有的噪声都表示出来。但此时 N_i 只表现出一次测量中的噪声,因此,可以进一步求 N_i 的最大值或对 N_i 求均值得到 $E(N_i)$,从而更好地表示功耗测量中的噪声。噪声测量过程如图4所示。

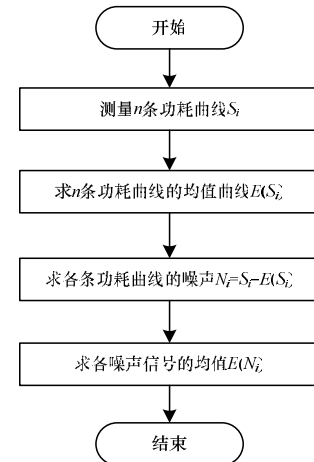


图4 噪声测量过程

3.2 差分功耗信号值的计算

为了定量地评估功耗分析平台的精确度,以及定量地分析能量攻击需要的样本数,需要基于概率统计学的知识计算数据处理后差分功耗信号 $T[j]$ 的信噪比SNR。首先确定信号 $T[j]$ 的分布:

$$T[j] = A_0[j] - A_1[j] \quad (1)$$

其中:

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

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

由于DPA中通常是基于汉明重量相差为1确立区分

函数的, 因此先介绍基于汉明重量的功耗模型。它是指采样功耗 P 和算法相关的寄存器状态字节的汉明重量存在线性关系, 功耗模型如式(2)所示:

$$P_j = aH(R) + l + w \quad (2)$$

其中, P_j 表示采样功耗, 它包括以下 3 个部分:

(1) 正在处理的寄存器数据的功耗, R 表示寄存器的状态字节, $H(R)$ 表示 R 的汉明重量, 即 R 中 1 的个数, a 是汉明重量与功耗之间的线性增益;

(2) 与处理数据无关的其他部分的功耗;

(3) 与算法无关的热噪声。

在通常情况下, l 和 w 都是常量, 所以:

$$\langle H \rangle_{s_i=1} - \langle H \rangle_{s_i=0} = (1 + \frac{3}{2}) - (0 + \frac{3}{2}) = 1$$

其中, H 表示某一时刻的状态字节的汉明重量, 由于以 S 盒输出的 1 位作为区分函数, 因此 S 盒输出中的一位已固定为 1 或 0, 剩下 3 位的平均汉明重量为 $\frac{3}{2}$, 即:

$$\langle H \rangle_{s_i=1} = 1 + \frac{3}{2}$$

若功耗和汉明重量之间的正比系数为 ε , 则 2 组功耗之间的差分功耗均值为 ε 。

对于基于汉明重量的功耗模型, $T[j]$ 可以由测量汉明重量之差为 1 的功耗曲线得到; 而对于基于汉明距离的功耗模型, $T[j]$ 可以由测量汉明距离为 1 的功耗曲线得到。例如, 在宽度为 3 的 ROM 中存有 0~7 共 8 个数, 如图 5 所示, 每个时钟周期都由 ROM 读出一个数到寄存器中, 将此电路下载到现场可编程门阵列(Field Programmable Gate Array, FPGA)中, 利用功耗采集平台测量其功耗信息。由于相邻周期 ROM 输出值的汉明距离为 1, 因此每个周期的功耗即为汉明距离下的 $T[j]$ 。

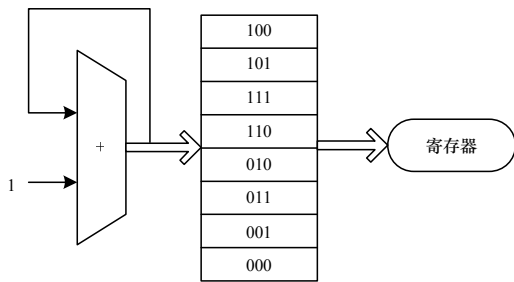


图 5 计算 $T[j]$ 的电路示意图

对于汉明重量功耗模型的 $T[j]$, 可以采集连续由同一地址读出的 2 条功耗曲线求其差值, 例如连续由地址 1 读出数据和由地址 2 读出数据的功耗曲线, 求它们的差值即可获得汉明重量差为 1 的 $T[j]$ 值。

3.3 差分功耗信号的信噪比模型

所选区分函数不同, 其信噪比模型也会不同。本文以 S 盒输出汉明重量作为区分函数, 对单比特差分能量攻击和多比特差分能量攻击的信噪比模型进行分析。

3.3.1 单比特差分能量攻击信噪比模型

由于噪声信号表示信号波动的幅度, 因此由前面测量

得到的噪声信号可以计算出一组功耗信号 $S_i[j]$ 的方差为:

$$\sigma^2 = \text{var}\{S_i[j]\} = \frac{1}{N} \sum_{j=0}^{N-1} (S_i[j] - E\{S_i[j]\})^2 \quad (3)$$

其中, N 表示样本数。但式(3)只表示了除算法噪声以外的各种噪声信号的方差。由于只在数据运算时才产生算法噪声, 因此数据运算时的噪声可以用上一次的数据和目前这一时刻数据的汉明差表示, 即和 ε 有关。对于数据运算以外时间段内的算法噪声, 可以将其出现的概率设为 α , $\alpha \in [0, 1]$ 且 $\alpha \approx 0$, 因为大部分时钟周期用在了非数据依赖函数的运算上。算法噪声由 ε 和 α 共同决定。

首先考虑 DPA 差分功耗的噪声部分^[7], 其概率分布为 D_{noise} , $S_i[j]$ 平均非算法噪声方差为 σ^2 。假定当 $i \neq k$ 时 $S_i[j]$ 独立于 $S_k[j]$, 如果 N 个信号分为集合 S_0 和 S_1 , 则:

$$\begin{aligned} \text{var}\{A_0[j]\} &= \text{var}\left\{\frac{1}{|S_0|} \sum_{S_i[j] \in S_0} S_i[j]\right\} = \\ &= \left(\frac{2}{n}\right)^2 \text{var}\left\{\sum_{S_i[j] \in S_0} S_i[j]\right\} = \frac{2\sigma^2}{N} \end{aligned} \quad (4)$$

$$\begin{aligned} \text{var}\{A_1[j]\} &= \text{var}\left\{\frac{1}{|S_1|} \sum_{S_i[j] \in S_1} S_i[j]\right\} = \\ &= \left(\frac{2}{n}\right)^2 \text{var}\left\{\sum_{S_i[j] \in S_1} S_i[j]\right\} = \frac{2\sigma^2}{N} \end{aligned} \quad (5)$$

综合考虑 A_0 和 A_1 , 两者相互独立, 因此, 分布为 D_{noise} 的点的平均非噪声方差为 $4\sigma^2/N$ 。

为了找出算法噪声的分布, 考虑一个 n 比特宽的数据。假定这些被操作的数据是随机的, 则它们的汉明重量服从二项分布, 其均值为 $n/2$, 方差为 $n/4$ 。连续 2 次运算数据的汉明差为 1 时的信号值为 ε , 易知连续运算数据的汉明距离同样服从二项分布, 因此, 信号均值为 $n\varepsilon/2$, 方差为 $n\varepsilon^2/4$ 。 N 个样本的平均运算对非算法噪声方差的影响与噪声方差一样。假定算法噪声百分比为 α , 则由算法噪声产生的噪声方差为 $\alpha\varepsilon^2 n/N$ 。由于算法和非算法噪声相互独立, 因此总噪声为 $(4\sigma^2 + \alpha\varepsilon^2 n)/N$ 。

SNR 的信号部分对应的差分功耗分布为 D_{signal} 。与前面相似, 差分功耗的噪声部分或者方差可以分为算法和非算法噪声。非算法噪声方差与前面相同, 为 $4\sigma^2/N$, 且算法噪声可以确定。以 S 盒输出汉明重量作为区分函数有着固定正在处理数据的某一位的作用。如果一个数据是 n 比特宽, 则余下的未被固定的平均汉明重量为 $(n-1)/2$, 方差为 $(n-1)/4$ 。所以, 信号的算法噪声等于 $(n-1)\varepsilon^2/N$ 。再者, 假定算法和非算法噪声相互独立, 总的噪声方差为 $(4\sigma^2 + (n-1)\varepsilon^2)/N$ 。

综上, D_{noise} 的统计参数为:

$$\begin{aligned} E\{T[j] | j \neq j^*\} &= 0 \\ \text{var}\{T[j] | j \neq j^*\} &= \frac{4\sigma^2 + \alpha n \varepsilon^2}{N} \end{aligned} \quad (6)$$

D_{signal} 的统计性质为:

$$\begin{aligned} E\{T[j^*] | j = j^*\} &= \varepsilon \\ \text{var}\{T[j^*] | j = j^*\} &= \frac{4\sigma^2 + (n-1)\varepsilon^2}{N} \end{aligned} \quad (7)$$

经过S盒输出全1,用来测量噪声。

功耗平台工作稳定后,开始进行功耗数据采集,测得结果如下:

$$\varepsilon'_{0-1} = 3.462 \text{ mV}$$

$$\sigma_{0-1}^2 = 3.57 \times 10^{-6} \text{ mV}^2$$

$$\varepsilon'_{1-0} = 1.155 \text{ mV}$$

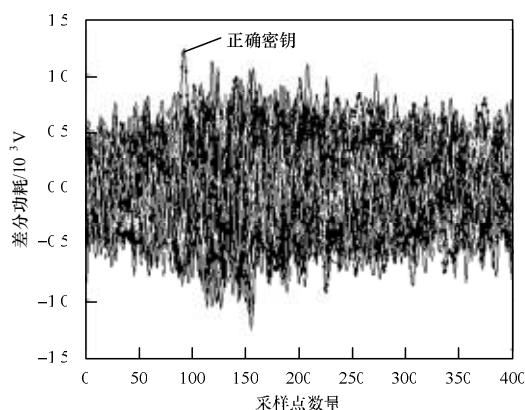
$$\sigma_{1-0}^2 = 3.85 \times 10^{-5} \text{ mV}^2$$

测量寄存器翻转功耗时,采用的明文样本经轮运算至寄存器输出,结果为16个1或者0,因此:

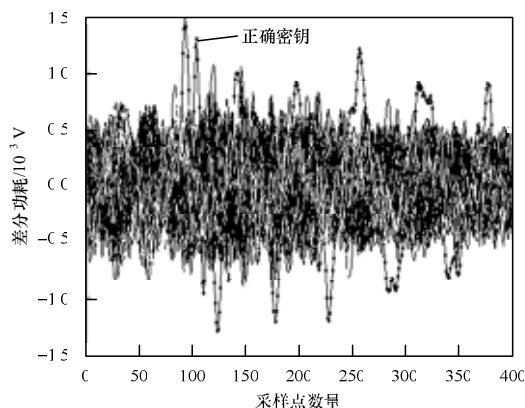
$$\varepsilon_{0-1} = \frac{1}{16} \varepsilon'_{0-1}$$

$$\varepsilon_{1-0} = \frac{1}{16} \varepsilon'_{1-0}$$

参考式(16),得样本数量 $N \approx 8\,000$ 。基于上述平台对AES算法进行实际攻击^[8-9],取样本数量为5 000和8 000分别进行实际攻击,结果如图7所示。



(a)样本数量为5 000时的攻击结果



(b)样本数量为8 000时的攻击结果

图7 不同样本数量时的攻击结果

由图7的攻击结果可以发现,样本量为5 000时正确密钥的功耗尖峰不明显,存在“ghost peak”,而样本量为8 000时正确密钥的差分功耗曲线尖峰十分明显。由此可

见,式(16)是正确的。

通过对样本数量的分析,发现对同一分组密码算法来说,针对不同的实现方式进行攻击所需要的样本量存在很大差别。文献[2]仅用1 000条功耗曲线就对智能卡实现的DES算法进行了成功的攻击,而在本文所提出的实验平台上,对基于FPGA实现的DES算法^[10]进行攻击则需要大约4 000条功耗曲线。

5 结束语

本文从实际的差分能量攻击出发,建立了单比特能量攻击和多比特能量攻击信噪比模型,在此基础上推导出了这2种情况下样本数量的表达式,并对其进行了实验验证。研究结果对能量攻击和抗能量攻击能力的量化评估都有重要的意义。

参考文献

- [1] Kocher P, Jaffe J, Jun B. Introduction to Differential Power Analysis and Related Attacks[EB/OL]. [2011-01-22]. <http://www.cryptography.com/dpa/technical.1998>.
- [2] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// Proc. of CRYPTO'99. [S. l.]: Springer-Verlag, 1999: 388-397.
- [3] Mangard S. A Simple Power Analysis(SPA) Attack on Implementations of the AES Key Expansion[C]//Proc. of the 5th International Conference on Information Security and Cryptology. [S. l.]: Springer, 2003.
- [4] Messerges T. Using Second-order Power Analysis to Attack DPA Resistant Software[C]//Proc. of Workshop on Cryptographic Hardware and Embedded Systems. [S. l.]: Springer-Verlag, 2000.
- [5] 张鹏, 邓高明, 邹程, 等. 差分功率分析攻击中的信号处理与分析[J]. 微电子学与计算机, 2009, 26(11): 1-4.
- [6] Sasaki A, Abe K. Algorithm-level Evaluation of DPA Resistance to Cryptosystems[J]. Electrical Engineering in Japan, 2008, 165(3): 1221-1228.
- [7] 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.
- [8] 刘政林, 韩煜, 邹雪城, 等. AES能量攻击的建模与分析[J]. 计算机工程与科学, 2008, 30(3): 17-20.
- [9] 韩煜, 邹雪城, 刘政林, 等. AES硬件实现的能量分析攻击仿真[J]. 微电子学与计算机, 2007, 24(12): 47-50.
- [10] Data Encryption Standard[EB/OL]. [2011-01-10]. http://en.wikipedia.org/wiki/Data_Encryption_Standard.

编辑 张帆