文章编号：0253-374X(2014)02-0315-05 DOI:10.3969/j.issn.0253-374x.2014.02.024

差分侧信道密码分析中泄露模型的线性回归分析

尹慧琳[1]，杨筱菡[2]
(1. 同济大学 中德学院，上海 200092；2. 同济大学 数学系，上海 200092)

摘要：从统计学线性回归模型的角度研究密码设备差分侧信道分析攻击中泄露模型的建模及估计，在不需对设备信息泄露有提前了解的情况下，得出线性回归泄露模型，克服了传统泄露模型的局限性. 首先，分析能耗泄露的随机模型从而构建线性回归模型，然后用最小二乘估计和最小一乘估计两种方法求解线性回归模型的系数，最后基于八位控制器 PayTV-AES 智能卡平台实现能耗泄露的建模及系数估计. 通过对两种求解方法结果的比较，提出最小二乘估计比最小一乘估计更适合用于泄露模型的线性回归分析；通过对被估模型系数曲线的分析，提出线性回归分析可以用于测量数据的预处理，以提高泄露模型建模效率.

关键词：智能卡安全；差分侧信道密码分析；差分能量攻击；泄露模型；线性回归分析
中图分类号：TP309 **文献标志码**：A

Linear Regression Analysis for Leakage Model of Differential Side Channel Cryptanalysis

YIN Huilin[1], *YANG Xiaohan*[2]
(1. Chinese-German School for Postgraduate Studies, Tongji University, Shanghai 200092, China; 2. Department of Mathematics, Tongji University, Shanghai 200092, China)

Abstract: An advanced statistical method, linear regression model, is proposed to construct the power leakage model for the differential side-channel-analysis (DSCA) attacks on cryptographic devices. Even with only a limited knowledge on how the device leaks information, the linear regression leakage model can be constructed, which overcomes the limitations of the traditional leakage models. First, the stochastic approach for analysis of power leakage is investigated and the linear regression model is built. Then the coefficients of the linear regression model are estimated with two methods: least square estimator(LSE) and least absolute estimator(LAE). Finally the mathematical model and methods are realized by an experimental analysis of an advanced encryption standard (AES) implementation on an 8-bit microcontroller based PayTV smartcard platform. A comparative analysis of both estimators shows that LSE is more suitable than LAE concerning the linear regression analysis of leakage model. In addition, investigation on the curves of the estimated model coefficients shows that linear regression analysis can be applied to preprocessing the measurement traces and the preprocessing helps to increase the efficiency of leakage modeling.

Key words: smartcard security; differential side channel cryptanalysis; differential power analysis; leakage model; linear regression analysis

密码芯片实现中，密码算法基于某个物理设备并采用软件或硬件方式实现，物理设备会与其环境发生物理交互作用. 攻击者有可能主动策划并检测这种交互作用，进而产生有助于密码分析的信息，比如运行时间、能耗、电磁信息等侧信道信息，对密码芯片实施侧信道攻击[1-2]. 相对于传统密码分析攻击及侵入式物理攻击手段，侧信道分析攻击由于其较高的分析效率及较低的攻击成本，成为密码芯片安全的最主要威胁. 统计学是侧信道分析尤其是差分分析攻击研究的基础，统计分析方法的应用能够使攻击者辨析出淹没在噪声中的细微相关性，有效破解密钥. 差分能量分析攻击是最典型的一种侧信道差分分析攻击，本文以差分能量分析(DPA, differential power analysis)攻击[3]为具体对象，对泄露模型的建模及求解进行研究.

差分能量分析过程中除了能耗测量，尤为关键的两步是：第一步，根据能耗泄露模型，由加密运算的中间值得到预测能耗值；第二步，根据辨别环节，对预测能耗值与实测能耗值进行统计分析，从大量猜测密钥中辨别出正确密钥. 泄露模型和辨别环节是侧信道分析中至关重要的两个要素. 已有的典型

收稿日期：2013-04-15
基金项目：国家自然科学基金(60903033)；中央高校基本科研业务费专项资金(0905915)
第一作者：尹慧琳(1977—)，女，讲师，工学博士，主要研究方向为信息安全. E-mail:yinhuilin@tongji.edu.cn
通讯作者：杨筱菡(1977—)，女，讲师，理学博士，主要研究方向为应用统计. E-mail:xiaohyang@tongji.edu.cn

泄露模型[4]有比特模型、汉明重量模型、模板,相应的辨别环节分别为均值差、Pearson 相关系数、Bayes 判别. 这些泄露模型都有其局限性,比特模型和汉明重量模型需要首先已知设备信息泄露特征,只适用于特定的密码芯片及设备,并以强假设条件为前提;模板使用多元正态分布描述刻画能耗迹的特征,但构建模板需要大量能耗迹,在实际攻击应用中也受到限制. 本文从统计学的角度对泄露模型进行分析,提出了线性回归模型,通过线性回归分析,估计得到中间值与泄露值之间的关系. 首先在分析智能卡等密码设备的能耗泄漏的随机模型的基础上构建线性回归模型,然后用最小二乘估计和最小一乘估计两种方法求解线性回归模型的系数,最后通过 PayTV-AES 智能卡平台实验实现上述理论方法并对建模及求解结果进行比较分析,发现并证实以下两点结论:最小二乘估计比最小一乘估计更适合用于泄露模型的线性回归分析;可以基于线性回归分析对测量数据进行预处理,以提高泄露模型建模及攻击效率.

1 能耗泄露线性回归模型

1.1 能耗测量随机模型

智能卡等密码设备的 CMOS 电路能耗为构成该 CMOS 电路的各个逻辑元件的能耗之和,当逻辑元件的内部信号或输出信号发生转换时产生动态能耗,动态能耗是总能耗的主导因素,依赖于被处理的数据[3]. 能耗测量中不可避免地包含噪声. 所以将能耗测量值视为两部分,一是与被处理数据有关的实际能耗值,为确定量;二是与被处理数据无关的噪声,为随机量. 用随机变量 M 表示能耗测量值,由确定量 l 和随机噪声 R 构成,设 x 为(部分)输入明文,k 为(部分)真实密钥,将 t 时刻的测量值 M_t 表示为

$$M_t(x,k) = l_t(x,k) + R_t \tag{1}$$

确定量 l_t 与明文 x 及密钥 k 有关,随机量 R_t 与明文及密钥无关,一般情况下认为均值 $E(R_t)=0$.

设加密运算的中间值为 $y=\varphi(x,k)$,测量值 M_t 又可表示为

$$M_t(y) = \delta_t(y) + R_t \tag{2}$$

通常密码设备基于数字电路实现,数据以比特位的形式被处理,所以能耗分析也基于数据的二进制位[5]. 考虑式(2)中确定量部分 $\delta(\cdot)$ 的二进制域代数特征,当自变量 y 表示为二进制形式 $y=(y_{n-1}\cdot y_{n-2}\cdots y_0)_2$ 时,$\delta(y)$ 表达式为

$$\delta(y) = \beta_{-1} + \sum_{i=0}^{n-1}\beta_i y_i + \sum_{i_1,i_2=0}^{n-1}\beta_{i_1,i_2}y_{i_1}y_{i_2} + \cdots + \sum_{i_1,\cdots,i_d=0}^{n-1}\beta_{i_1,\cdots,i_d}y_{i_1}y_{i_2}\cdots y_{i_d} \tag{3}$$

其中 β 为实系数,绝大多数的智能卡等密码设备具备 IBL(independent bit leakage,独立位泄露)特性[6],即不同位导致的泄露是独立的,即 $\beta_{-1},\beta_0,\cdots,\beta_{n-1}$ 远大于其他参数,于是式(3)可以简化为线性方程

$$\delta(y) = \beta_{-1} + \sum_{i=0}^{n-1}\beta_i y_i \tag{4}$$

由此可知测量值的确定量部分可以表示为加密运算中间值各二进制位的线性函数.

1.2 线性回归模型

由对 $\delta(y)$ 的分析可知式(1)中的确定量 $l_t(x,k)$ 可用相应的线性方程表示. 下面具体分析线性方程的形式及参数. 设 l_t,l' 分别表示相应于真实密钥的、任意密钥的泄露值确定量,l_t^* 表示与 l_t 足够接近的泄露值确定量,$F:=\{l':\{0,1\}^p\times\{0,1\}^s\to\mathbf{R}\}$ 表示 l' 的集合,其中 p 为明文二进制位数,s 为密钥二进制位数,$\mathbf{R}$ 为实数域. 结合实际应用需求,将集合 F 缩小范围,先将 F 缩小为子集 F_t,F_t 包含 l_t 或至少包含了 l_t^*,然后将 F_t 具体化为 $F_t=\boldsymbol{F}_{u;t}$,$\boldsymbol{F}_{u;t}$ 为 t 时刻的 u 个已知函数

$$g_{jt}:\{0,1\}^p\times\{0,1\}^s\to\mathbf{R} \tag{5}$$

张成的实数向量空间,其中 j 取值为 0 到 $u-1$,即

$$\boldsymbol{F}_{u;t}:=\{l':\{0,1\}^p\times\{0,1\}^s\to \mathbf{R}\mid\sum_{j=0}^{u-1}\gamma'_j g_{jt},\text{其中}\ \gamma'_j\in\mathbf{R}\}, \tag{6}$$

式中:γ'_j 为系数.

于是可得线性回归模型

$$l_t(x,k) = \sum_{j=0}^{u-1}\gamma_{jt}g_{jt}(x,k) \tag{7}$$

式中:γ_{jt} 为系数.

关于 u 及向量空间 $\boldsymbol{F}_{u;t}$ 的选取有多种方式[7],可以根据实际情况选择. 比如对加密中间值 $\varphi(x,k)$ 的 8 个比特位进行加权建模时,u 选为 9,即

$$l_t(\varphi(x,k)) = \gamma_{0t} + \sum_{j=1}^{8}\gamma_{jt}g_j(\varphi(x,k))$$

其中 $g_j(\varphi(x,k))\in\{0,1\}$ 为中间值的第 j 位;如果只是重点对中间值的某 4 个特定比特位进行建模,则 u 选为 5;如果不仅对比特位系数,还要对二阶系数进行分析,则 u 选为 10 或 16 等. 通常 u 越大,用来估计系数所需要的能耗迹越多.

2 线性回归系数估计

回归分析的目的是估计模型的参数以便达到数

据的最佳拟合，即对式(7)中系数进行估计，通常用最小二乘估计. 基于最小二乘估计定理[5]对系数进行估计. 设 k 为真正密钥，对于任意泄露值确定量

$$l' := \sum_{j=0}^{u-1} \gamma'_j g_{jt} \in \boldsymbol{F}_{u,t} \tag{8}$$

有

$$\sum_{n=1}^{N} (m_t(x_n,k) - l'(x_n,k))^2 = \|\boldsymbol{m}_t - \boldsymbol{A\Gamma}\|^2 \tag{9}$$

式中：

$$\boldsymbol{A} := \begin{bmatrix} g_0(x_1,k) & g_1(x_1,k) & \cdots & g_{u-1}(x_1,k) \\ g_0(x_2,k) & g_1(x_2,k) & \cdots & g_{u-1}(x_2,k) \\ \vdots & \vdots & & \vdots \\ g_0(x_i,k) & g_1(x_i,k) & \cdots & g_{u-1}(x_i,k) \\ \vdots & \vdots & & \vdots \\ g_0(x_N,k) & g_1(x_N,k) & \cdots & g_{u-1}(x_N,k) \end{bmatrix}$$

$$\boldsymbol{\Gamma} := (\gamma'_0,\cdots,\gamma'_{u-1})^{\mathrm{T}}$$

$$\boldsymbol{m}_t := (m_t(x_1,k),\cdots,m_t(x_N,k))^{\mathrm{T}}$$

如果 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ 正则，满足式(9)取最小值的解为

$$\boldsymbol{\Gamma}^* = (\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{m}_t \tag{10}$$

即线性回归模型系数的估计值由式(10)求出，常用的运算软件比如 matlab 等直接提供求解函数.

根据大数定理 $\frac{1}{N}\sum_{n=1}^{N}(m_t(x_n,k) - l'(x_n,k))^2 \xrightarrow{N\to\infty} E((M_t(X,k) - l'(X,k))^2)$，由式(10)求得的模型系数得到泄露值确定量的表达式为

$$l_t^*(x,k) = \sum_{j=0}^{u-1} \gamma_{jt}^* g_{jt}(x,k) \tag{11}$$

由此得到能耗泄露模型.

当测量数据较少，且数据中夹杂有异常点时，异常点会有较大的偏差，其平方值相对更大，导致最小二乘法的回归线失真较大. 为了减少奇异数据的影响，采用最小一乘估计. 最小一乘估计直接求绝对值的最小值，可以消除平方运算带来的影响，得到更精确的估计结果.

设 k 为真正密钥，对于任意 $l' := \sum_{j=0}^{u-1} \gamma'_j g_{jt} \in \boldsymbol{F}_{u,t}$，有

$$\sum_{n=1}^{N} |m_t(x_n,k) - l'(x_n,k)| = |\boldsymbol{m}_t - \boldsymbol{A\Gamma}| \tag{12}$$

其中各参数 $\boldsymbol{A},\boldsymbol{\Gamma},\boldsymbol{m}_t$ 都与(9)式中相同. 最小一乘估计通过迭代、拟合或线性规划等方法求解，运算软件一般不直接提供求解函数，计算过程比最小二乘估计复杂.

3　基于 PayTV-AES 智能卡的泄露模型线性回归建模实例分析

3.1　PayTV-AES 智能卡及测量配置

PayTV-AES 智能卡基于 ATMega744 八位单片机实现，密码算法采用对称密码算法 AES[8]. 该智能卡的供电端串联一电阻，示波器采用 Picoscope5000(带宽 250 MHz，实时采样频率 1 Gs^{-1}，记录长度 128 M)，电阻两端的电压正比于智能卡的工作电流，卡供电电压恒定，则电阻电压与卡的能耗成正比. 电压测量曲线作为能耗迹用于泄露模型建模分析，能耗迹数 $N=200$，测量时间 $t=1600$.

3.2　最小二乘估计和最小一乘估计

将加密过程的中间值选为 AES 中 S 盒的输出，即 $\varphi(x,k)=S(x\oplus k)$. 对中间值的各比特位进行加权建模，$u=9$，$l_t(S(x\oplus k))$ 近似为

$$l_t^*(S(x\oplus k)) = \gamma_{0t} + \sum_{j=1}^{8} \gamma_{jt} g_j(S(x\oplus k)) \tag{13}$$

其中 $g_j(S(x\oplus k))\in\{0,1\}$ 表示中间值的第 j 位. 分别用最小二乘估计、最小一乘估计求解系数 $\boldsymbol{\Gamma}=[\gamma_{0t},\gamma_{1t},\cdots,\gamma_{8t}]$，运算环境为 matlab，最小二乘估计直接运用 matlab 提供的函数，最小一乘估计采用迭代方法实现. 线性回归泄露模型系数中的 γ_{0t} 为常数项，不包含与运算数(明文及密钥)有关的信息；$\gamma_{1t},\cdots,\gamma_{8t}$ 分别为加密运算中间值的各比特位的权重系数，体现了密钥对能耗泄露的影响，所以本文重点分析系数 $\gamma_{1t},\cdots,\gamma_{8t}$. 图 1 和图 2 分别给出了最小二乘估计和最小一乘估计的系数 $\gamma_{1t},\cdots,\gamma_{8t}$ 曲线. 在同样的软硬件运算环境下运算时间分别为 0.160 s 和 6.776 s，最小一乘估计所消耗的时间远远大于最小二乘估计.

由两组曲线观察到，最小一乘估计结果的毛刺明显多于最小二乘估计，对噪声过于敏感. 具体的标准偏差值 $b_{1t},\cdots,b_{8t}$ 如表 1 所示. 比较两行中所列系数，最小一乘估计结果的标准偏差大于最小二乘估

表 1　线性回归模型系数的标准偏差

Tab.1　Standard deviation of the coefficients linear regression models

方法	b_{1t}	b_{2t}	b_{3t}	b_{4t}	b_{5t}	b_{6t}	b_{7t}	b_{8t}
最小二乘估计	1.013 1	1.649 1	1.230 4	1.273 1	1.222 7	1.304 0	1.306 1	1.116 0
最小一乘估计	1.240 0	1.885 9	1.458 0	1.983 6	1.593 1	1.453 5	1.760 9	1.574 3

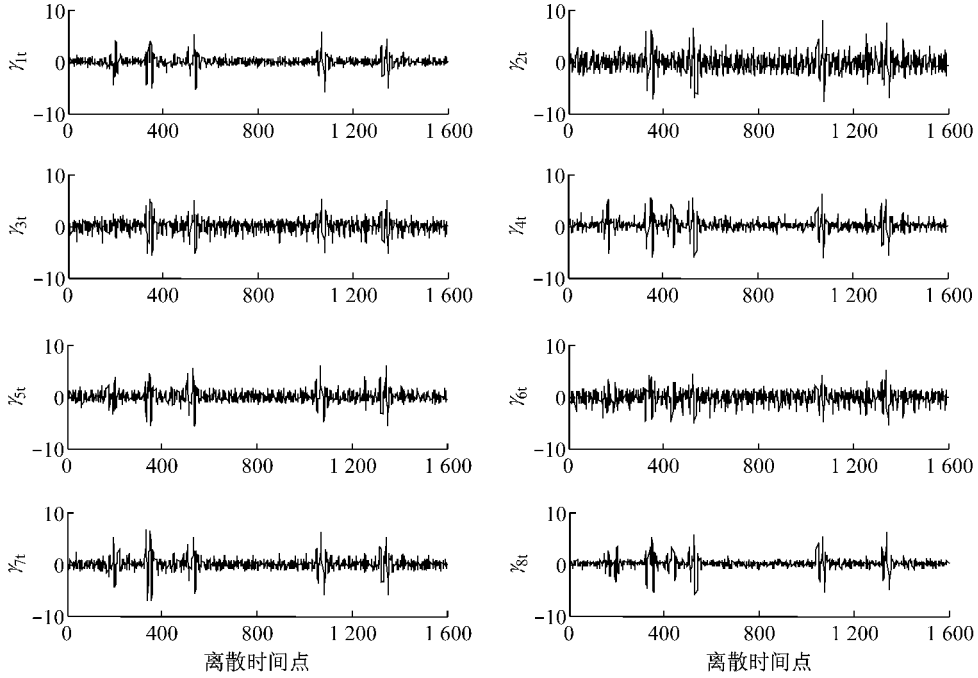

图1 最小二乘估计的系数 $\gamma_{1t},\cdots,\gamma_{8t}$

Fig.1 Coefficients of the least square estimator $\gamma_{1t},\cdots,\gamma_{8t}$

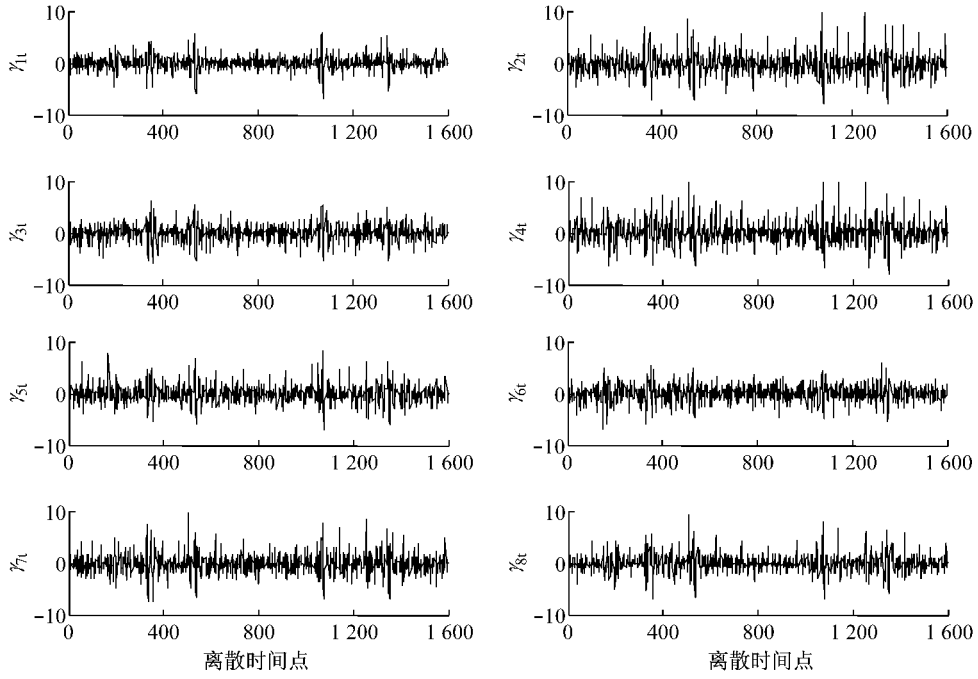

图2 最小一乘估计的系数 $\gamma_{1t},\cdots,\gamma_{8t}$

Fig.2 Coefficients of the least absolute estimator $\gamma_{1t},\cdots,\gamma_{8t}$

计结果的标准偏差. 基于运行时间及系数的标准偏差两方面的比较,证明最小二乘估计比最小一乘估计更适合用于泄露模型的线性回归分析.

3.3 基于线性回归分析对测量数据进行预处理

由图1可以看出,$\gamma_{1t},\cdots,\gamma_{8t}$的明显振荡部分在时间上几乎是同步的. 为便于研究该现象,首先对基于HW(Hamming Weight)泄露模型的差分能量分析(DPA)攻击相关系数曲线及能耗测量迹进行分析. 图3所示为基于HW的DPA攻击的对应于真实密钥的相关系数曲线,相关系数在 T_1 至 T_5 的5个时间区间内有明显振荡并存在尖峰值,基于对DPA攻击原理的理解,在这些时间区间(更准确地说是在

其中的某几个时刻），密钥参与运算，并且对能耗产生影响. 在其他时刻，相关系数基本为零，曲线毛刺由噪声引起，密钥对能耗不产生影响.

图 4 所示为 γ_{0t} 与测量迹的偏差，表示了常数项系数对测量迹的跟随程度. 可以发现，曲线明显振荡对应的时间区间与 $T_1,\cdots,T_5$ 基本是一致的，原因在于，在这些时间区间内，密钥参与运算，常数项不受密钥影响，无法跟随能耗迹，所以产生明显偏差. 观察图 1，$\gamma_{1t},\cdots,\gamma_{8t}$ 的明显振荡部分的时间区间也恰好与 $T_1,\cdots,T_5$ 一致，密钥对能耗产生影响，通过调整中间值各比特位的权重系数的大小来跟随能耗迹的变化，从而得到能耗模型. 基于以上分析可知，正是 $T_1,\cdots,T_5$ 的 5 个时间区间内的能耗测量点才含有密钥信息，其余时间的测量点在建模过程中可以剔除. 由此，可以通过线性回归分析的方法对测量数据进行预处理、剔除所包含信息与模型无关的测量点，从建模所需的数据处理量的角度讲，建模效率得到了提高.

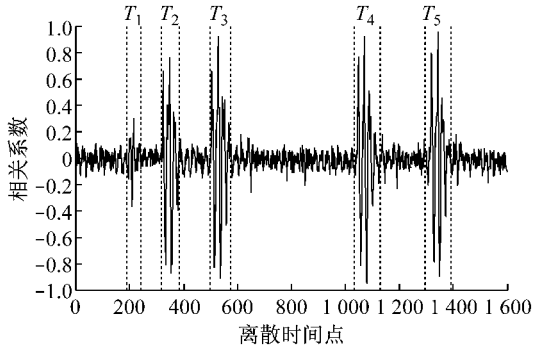

图 3　基于 HW 泄露模型的 DPA 攻击相应真实密钥的相关系数曲线

Fig. 3　Correlation coefficient curves of the true key during DPA attack based on HW leakage model

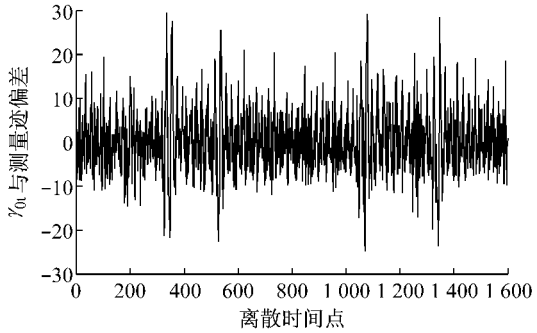

图 4　系数 γ_{0t} 与测量迹的偏差

Fig. 4　Deviation of the coefficient γ_{0t} and the measurement trace

4　结语

在智能卡等密码设备的差分侧信道分析攻击中，泄露模型直接影响攻击的效果及密码设备的安全性. 传统的泄露模型在实际应用中都有其局限性，本文从统计学的角度分析密码设备的能耗泄漏模型，首先基于对随机模型的分析构建线性回归模型，然后用最小二乘估计和最小一乘估计两种方法求解回归模型的系数，最后基于 PayTV-AES 智能卡平台实现建模及求解，通过对结果的比较分析，提出并证明了两点结论：最小二乘估计比最小一乘估计更适合用于泄露模型的线性回归分析；可以基于线性回归分析对测量数据进行预处理，以提高泄露模型建模及攻击效率. 本文的建模、求解方法及以上两点结论为差分侧信道密码分析的泄露模型的研究提供了理论基础及工程应用参考.

参考文献：

[1] Kocher P C, Jaffe J, Jun B. Differential power analysis[C]// Advances in Cryptology—CRYPTO'99, LNCS 1666. Berlin: Springer, 1999: 388-397.

[2] 中国密码学会. 2009—2010 密码学学科发展报告[R]. 北京：中国科学技术出版社，2010.
Chinese Association for Cryptologic Research (CACR). 2009—2010 Cryptography discipline development report[R]. Beijing: Chinese Science and Technology Press, 2010.

[3] Stefan M, Elisabeth O, Thomas P. Power analysis attacks—revealing the secrets of smart cards[M]. Berlin: Springer, 2007.

[4] Mangard S, Oswald E, Standaert F X. One for all—all for one: unifying standard differential power analysis attacks[J]. IET Information Security, 2011, 5:100.

[5] Schindler W, Lemke K, Paar C. A stochastic model for differential side channel cryptanalysis [C] // Cryptographic hardware and embedded systems—CHES 2005. Berlin: Springer, 2005, 3659: 30-46.

[6] Prouff E, Rivain M, Bévan R. Statistical analysis of second order differential power analysis[J]. IEEE Transactions on Computer, 2009, 58(6): 799.

[7] Doget J, Prouff E, Rivian M, et al. Univariate side channel attacks and leakage modeling[J]. Journal of Cryptographic Engineering, 2011, 1(2): 123.

[8] Moradi A, Poschmann A, Ling S. Pushing the limits: a very compact and a threshold implementation of AES[C]// Advances in Cryptology—EUROCRYPT 2011. Berlin: Springer, 2011, 6632: 69-88.