doi:10.3969/j.issn.1000-436x.2012.z1.037

功耗分析攻击中的功耗与数据相关性模型

罗鹏[1,2]，冯登国[1,2]，周永彬[1,2]
(1. 中国科学院 软件研究所，北京 100049；2. 中国科学院 研究生院，北京 100049)

摘 要：在对密码设备进行功耗分析攻击时，攻击者需要建立密钥或者与密钥关联的数据值与被攻击设备的功耗相关性模型，藉此通过对功耗的分析破解出敏感信息。从攻击者的角度对器件功耗物理特性分析的基础上，重构了汉明距离模型和汉明重量模型，并从理论上证明了汉明重量模型的正确性，并建立起 MCU 功耗采集平台，验证了汉明重量模型的有效性和实用性。

关键词：信息安全；密码学；边信道攻击；功耗分析攻击；相关性模型
中图分类号：TN918.1;TP309.1 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0276-06

Power model in power analysis attack

LUO Peng[1,2], FENG Deng-guo[1,2], ZHOU Yong-bin[1,2]
（1. Institute of Software, Chinese Academy of Sciences, Beijing 100049, China;
2. Graduate University of Chinese Academy of Sciences, Beijing 100049, China）

Abstract: A mapping relation model should be established between data value and power value which is collected from device under attack when the power analysis attack accuse. The sensitive information can be fund through the power trace analysis using this type of relation. Hamming distance model and hamming weight model were described based on device's physical characteristics. Furthermore, the correctness of hamming weight model was proved not only by Formula Derivation, but also by experiment under power consumption collection platform based on MCU. The experimental results show that hamming weight model is a valid and practicable model in power analysis attack.

Key words: information security; cryptography; side channel attack; power analysis attack; power model

1 引言

随着电路等分析技术的发展，密码破解已经不再单纯地停留在数学手段之上，还可从密码芯片运算时的功耗入手。通过对密码芯片运算时的功耗分析发现，密码芯片在进行运算时的功耗波形与所使用的密钥有着一定的关系，当使用密钥不同时，密码芯片运算时的功耗也会表现出不同的特性，于是，攻击者利用这种密钥和功耗间的关系，对密码芯片运算过程的功耗进行分析，分析出密码芯片运算所使用的密钥，对于这种利用密钥和运算时的功耗间的关系来进行密钥分析的方法称为功耗分析攻击[1~5]。

为了使功耗分析攻击得以实现，必须建立功耗与密钥或与密钥紧密相关的数据之间的关系模型，这样才能通过分析功耗，破解出密码芯片上的密钥或者与密钥相关的信息。

2 器件功耗与数据相关性的物理基础

2.1 CMOS 反相器电路

CMOS 逻辑门电路是在 TTL 电路问世之后，所开发出的第 2 种广泛应用的数字集成器件，从发展趋势来看，由于制造工艺的改进，CMOS 电路的性能超越了 TTL 而成为占主导地位的逻辑器件，它的

收稿日期：2012-08-20

功耗和抗干扰能力则远优于 TTL。此外，几乎所有的超大规模存储器件以及 PLD 器件都采用 CMOS 工艺制造，且费用较低。目前主流的加密、解密设备均使用 CMOS 电路，研究其功耗情况对使用功耗分析技术对设备进行攻击有重大意义。

本以 CMOS 反相器为例，主要讨论与功耗分析攻击相关的 CMOS 电路功耗问题。

CMOS 反相器电路如图 1 所示，它由 2 只增强型 MOSFET 组成，其中，一个为 N 沟道结构，另一个为 P 沟道结构。其总功耗 P_{inv} 可看成静态功耗 P_{stat} 和动态功耗 P_{dyn}2 部分功耗之和。

$$P_{\text{inv}} = P_{\text{stat}} + P_{\text{dyn}} \tag{1}$$

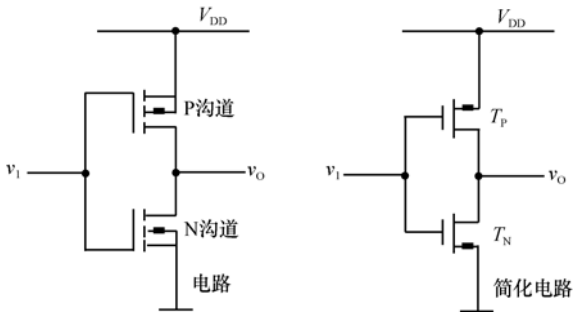


图 1　CMOS 反相器电路

2.2　静态功耗分析

当反相器输入 V_i 稳定时器件所产生的功耗为静态功耗 P_{stat}。V_i 不论其为高还是低电平，2 个 MOS 管中必定是一个处于导通，另一个处于截止，因此在 V_{DD} 到 GND 之间处于截止的 MOS 管上仅有一个很小的泄露电流 I_{leak}，则静态功耗 P_{stat} 可以用以下公式计算得到：

$$P_{\text{stat}} = I_{\text{leak}} V_{\text{DD}} \tag{2}$$

2.3　动态功耗分析

当输入信号 V_i 发生变化时，输出信号会随之发生变化，此时器件会产生动态功耗 P_{dyn}。表 1 给出当输入信号（或输出信号）发生变化时，反相器的功耗情况。

表 1　　输入信号与反相器功耗对应情况

初态	终态	功耗	功耗类型
0	0	P_{00}	静态功耗
0	1	P_{01}	静态功耗+动态功耗
1	0	P_{10}	静态功耗+动态功耗
1	1	P_{11}	静态功耗

影响动态功耗 P_{dyn} 的主要因素有 2 个：对负载电容 C_{L} 充放电所产生的功耗 P_{chrg} 和 MOS 管在翻转过程中的短路电流所产生的功耗 P_{sc}。令α为加权因子，f 为器件翻转的时钟频率，t_{sc} 为 MOS 器件短路时间，则功耗计算如式(3)和式(4)所示。

$$P_{\text{chrg}} = \frac{1}{T}\int_0^{\text{T}} p_{\text{chrg}}(t)\text{d}t = \alpha f C_{\text{L}} V_{\text{DD}}^2 \tag{3}$$

$$P_{\text{sc}} = \frac{1}{T}\int_0^{T} p_{\text{sc}}(t)\text{d}t = \alpha f V_{\text{DD}} t_{\text{sc}} \tag{4}$$

图 2 所示为一个 CMOS 反相器的模拟仿真示意图。从图中可以看出，当输入信号 V_i 发生翻转（0 到 1 或 1 到 0）时，电源电流 i_{DD} 均出现正向脉冲，且 2 种脉冲波形、高度都不相同。由此可看出，当 CMOS 单元中有不同数据通过的时候，会产生相应的功耗波动，即为动态功耗与数据的相关性。

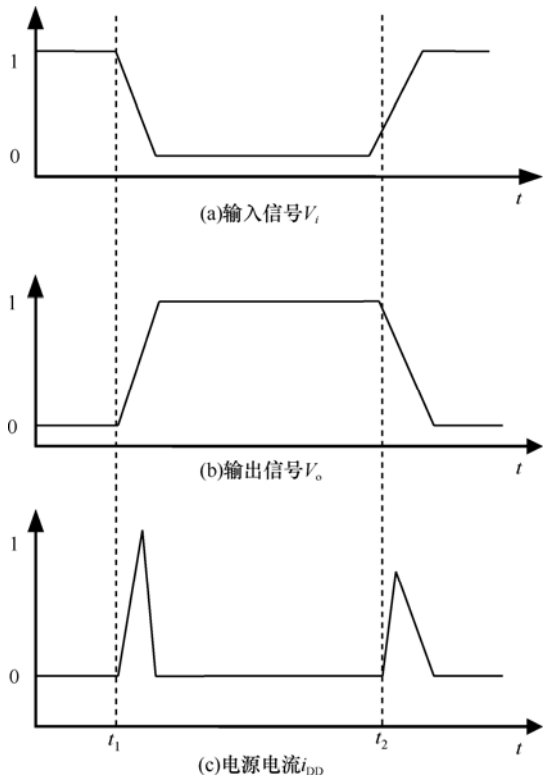


图 2　CMOS 反相器输入、输出与 i_{DD} 间关系仿真

同理，对于由 CMOS 器件构成的异或门、与非门等基本逻辑门电路均存在类似的数据相关性。

在实际的电路网络中，存在延迟、竞争、反馈、毛刺等各种复杂情况。当信号通过这样的网络时，由状态翻转而产生的各个脉冲之间呈现非线性的作用关系，电路单元某时刻功耗与数据的相关性并不是简单的线性叠加。但对于功耗分析攻击者来

说，通过简单的线性相关性模型就可分析出被处理数据的很多信息，甚至直接还原出数据，因此线性相关性模型具有很强的实用意义。

3 功耗与数据相关性模型

在功耗分析攻击中，攻击者需要将数据值与被攻击设备的功耗建立一定的映射关系。在具体实施攻击的技术中，这种关系不必是一种严格的值对应，攻击者只需要知道功耗值的相对差别而不必了解功耗的绝对值情况就可实施攻击。因此针对功耗分析攻击所建立的功耗与数据相关性模型要比设计一个密码设备所进行的功耗分析仿真模型简单得多。在本节将着重描述当前功耗分析攻击中基础的模型——汉明距离模型。在此基础上，建立更实用的模型——汉明重量模型，并分析该模型的正确性和适用环境。

3.1 汉明距离模型

由上节讨论可知，某时刻在数字电路中有器件发生翻转就会产生动态功耗，并且翻转的器件越多，则功耗越大，那么只需计算数据值导致的翻转个数，就可和功耗值的相对大小建立联系，这个就是汉明距离模型（HDM, hamming-distance model）的基本原理。

在信息论中，2 个等长二进制数串之间的汉明距离(HD, hamming-distance)是这 2 个二进制数串对应位置的不同字符的个数。而一个二进制数串的汉明重量(HW, hamming-weight)就是该数串中“1”的个数。

令 V_0 为电路翻转前二进制数据，V_1 为电路翻转后的二进制数据，则有

$$HD(V_0,V_1)=HW(V_0\oplus V_1)=HW(E) \tag{5}$$

其中，⊕运算为按位异或，差错图案 $E=V_0\oplus V_1$ 也是一个相同长度的二进制数串，差错图案中的“1”标识了 V_0 和 V_1 在哪些位置是不相同的。因此，2 个等长二进制数串的汉明距离即为它们之间差错图案的重量。

在 HDM 中，假设器件翻转（无论是从“0”到“1”，还是“1”到“0”）都产生相同的功耗；而“0”到“0”和“1”到“1”也可产生相同的功耗，但与翻转产生的功耗完全不同。再假设忽略各个电路单元中分布式电容的差异，这时可得结论：器件翻转前后的功耗大小与前后二进制数值的汉明距离近似成线性相关，即

$$\tilde{P}\approx kHD(V_0,V_1)+d \tag{6}$$

其中，k 和 d 为由器件特性决定的常数。

HDM 模型一般用于对总线和寄存器的功耗进行描述。通过该模型，攻击者建立了数据传输存储时始、终态间器件翻转个数与功耗之间的相对关系，从而获得数据的信息：从简单功耗分析攻击（SPA, simple power analysis attack）的角度，只需检测出功耗的相对大小，既可获得数据的汉明距离的信息；而从差分功耗分析攻击（DPA, differential power analysis）的角度，可用汉明距离作为区分（又称为选择）函数对功耗曲线进行分类实施攻击。

HDM 模型必须同时知道初态值和终态值，以此才能正确计算出汉明距离，而在实践中，攻击者往往无法做到 2 个值都明确。

3.2 汉明重量模型

汉明重量模型（HWM, hamming-weight model）要比 HDM 模型简单。在这个模型中，攻击者假设功耗的大小与正在处理的数据 V_1 中被置位成“1”的个数成正比，也就是和 V_1 的汉明重量成正比，而在这个数据之前、之后所处理数据产生的影响忽略不计。即

$$\tilde{P}\approx kHW(V_1)+d \tag{7}$$

其中，k 和 d 为由器件特性决定的常数。

该模型的优势在于并不需要对被攻击的电路单元所有状态值都有所了解，只需知道某个状态值的汉明重量，就可构造功耗与数值间相对关系。

乍看这个模型并不能很好地用来描述上一节所讨论的 CMOS 电路，因为它的功耗取决于数据的翻转个数，而不是数据的置位成“1”的个数。然而通过下面的分析可以看到，在特定的实际攻击环境中，HWM 模型是一个非常有实用价值的模型。下文假定某 n 位电路单元的数据初态值为 V_0，终态值为 V_1。

3.2.1 V_0 中各比特均相等

众多实际电路设计中，为保证稳定性，在传输、存储某个数据 V_1 前，会先将电路状态全部置位或全部复位。此时，HWM 就成了 HDM 的简化形式。

当 V_0 为 n 位全“0”数据时，有

$$HD(V_0,V_1)=HW(V_0\oplus V_1)=HW(V_1) \tag{8}$$

由 HDM 模型（式(6)）得

$$\tilde{P} \approx kHW(V_1) + d \tag{9}$$

同理，当 V_0 为 n 位全“1”数据时，有

$$HD(V_0, V_1) = HW(V_0 \oplus V_1) = HW(\overline{V_1}) \tag{10}$$

$$\tilde{P} \approx kHW(\overline{V_1}) + d \tag{11}$$

由式(9)和式(11)可知，功耗的大小与 V_1 或 V_1 反码的汉明重量近似成线性相关。

3.2.2　V_0 为一个常数

电路每次都将 V_0 设置成某个常数，但该常数并不为攻击者所知。这时，对整个数串用 HWM 进行建模明显与 HDM 模型得到的结果不同，但对 V_0 到 V_1 转换过程中的某一位用 HWM 建模则总是和 HDM 一致的，其原理如 3.2.1 节中所述，可将该位看成是 n=1 时 V_0 中各比特位均相等情况的特例。而在实际功耗分析攻击中，经常会利用运算中间值的某位来对密钥进行猜测、攻击，此时，就可对该位使用 HWM 模型。

还可通过对每一比特位用 HWM 进行建模，先获取 V_0 所有位的信息，然后就可使用 HDM 模型对电路单元进行功耗分析攻击。

3.2.3　V_0 为一个与 V_1 独立的均匀分布随机变量

HWM 模型应用中最坏的情况是，在攻击者进行测试攻击时 V_0 的各个比特是随机变化的，且与 V_1 是独立的。这时，HW（V_1）明显与 HD（$V_0 \oplus V_1$）相互独立的。这意味着对相同的电路单元用 HWM 建模和用 HDM 建模会得到完全独立的结果。

但实际情况中，HDM 假设的电路单元翻转所产生的功耗均相同这点并不完全正确，从对图 2 的分析中已经看到，“0”到“1”翻转的功耗要比“1”到“0”翻转的功耗大，在这样的情况下，当 V_0 为均匀分布的随机变量，而 HW（V_1）越大时，电路单元中“0”翻转到“1”的位数多的可能性就越大，那么从统计平均的角度看，大汉明重量对应的功耗就会比小汉明重量的要大。因此，只需用相同的数据 V_1 对电路单元进行反复测试，然后进行平均，即可获得与 HWM 相对应的功耗分布。

由上述可知，汉明重量在实践中是一个非常实用的功耗分析模型，从当前的功耗分析攻击发表的文献中亦可发现，绝大部分功耗分析攻击都是基于汉明重量模型的攻击。

4　MCU 功耗统计特性与汉明重量分析

根据图 3 显示的原理图搭建功耗采集平台，该平台主要包括示波器、PC 机、MCU 智能运算模块和电源。

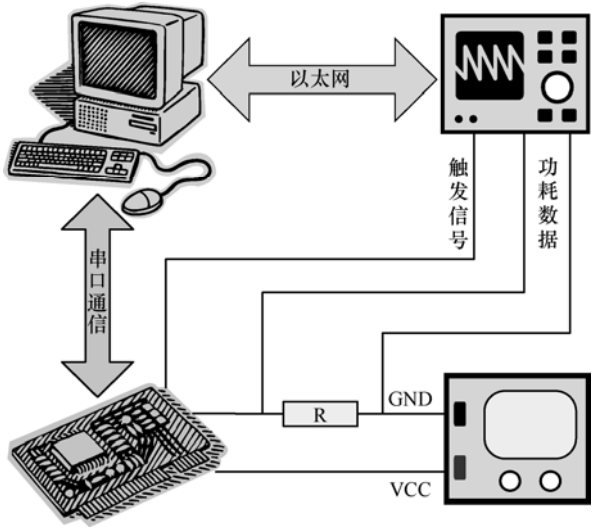


图 3　功耗采集平台原理

MCU 智能运算模块是整个功耗采集平台的核心，智能运算模块 MCU 选用宏晶科技的 STC89C52。STC89C52 可用于工业控制等方面，并且市场上大多数智能卡读写器的控制芯片是与 STC89C52 同系列的 MCU，因此这对以后研究智能卡密码系统的功耗分析攻击有很强的参考性。

4.1　电子噪声

在实际应用中，电子噪声是不可避免的。要想研究电子噪声 $P_{\text{el-noise}}$ 的概率分布，需要密码设备执行相同的操作，处理相同的数据，例如重复移动数据 0 从它的内存到寄存器。图 4 显示了 MCU 执行赋值操作 ucData=0x00 时的功耗轨迹。

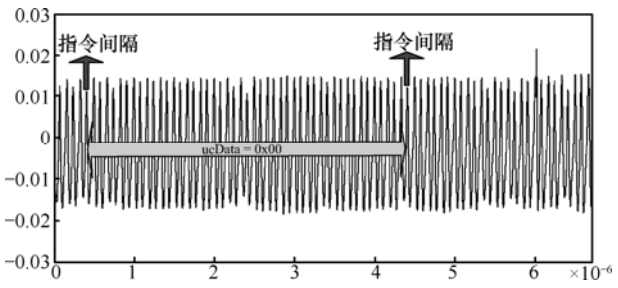


图 4　执行赋值操作 ucData=0x00 时 MCU 的功耗轨迹

重复上述过程 6 000 次，得到 6 000 组数据。这 6 000 组数据均是随时间变化的，这里只使用了样本点 2 328ns 处的功耗。对于这 6000 个点，得到电压与发生频率的分布直方图，如图 5 所示。

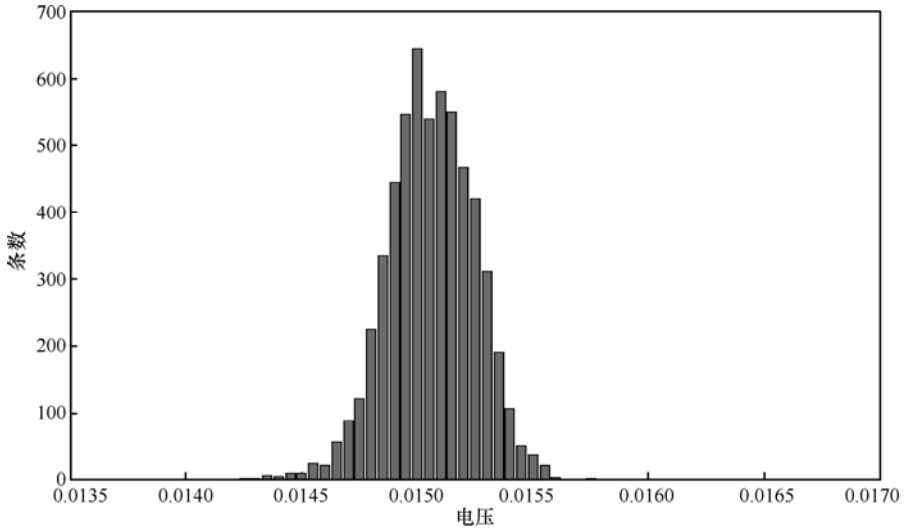


图 5　2 328ns 点的功耗分布直方图

实验显示大多数 2 328ns 点的电压分布在 15.1mV 左右，只有很少的点分布于 14.5mV 和 15.7mV。不仅 2 328ns 点的功耗分布情况如图 5 所示，如果统计其他时刻点的功耗分布情况，将会得到和图 5 极其相似的分布，而图 5 显示概率分布近似服从正态分布。

实验中对 2 328ns 点的 6 000 组数据进行统计分析，得到样本均值 $\bar{X}$ =15.1mV，样本标准差 S=0.186 65mv。因此，可以说 2 328ns 点的功耗服从均值 μ=15.1mV，σ =0.18665mV 的正态分布，记为 $X \sim N(15.1, 0.18665)$。利用 matlab 仿真产生一个均值 μ=15.1mV，σ=0.186 65mV 的正态分布，如图 6 所示，对比图 5 和图 6 可知，两者显示的统计特性是相一致的，模型匹配的很好。这进一步验证了 2 328ns 点的功耗分布逼近正态分布。

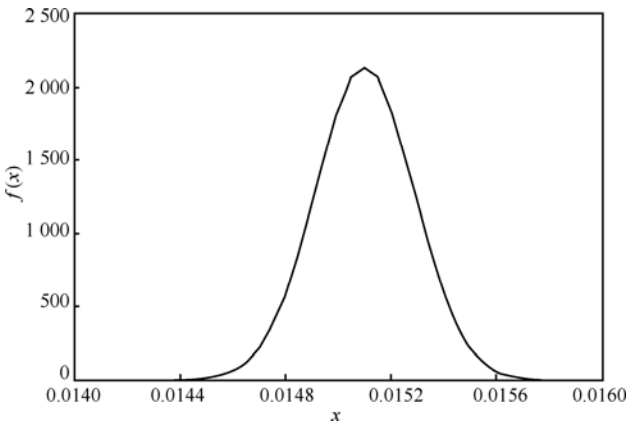


图 6　均值为 15.1mV、方差为 0.186 65 的正态分布

4.2　与数据相关功耗

对于与数据相关的功耗 P_{data}，最关注的是当密码设备处理不同的数据时，P_{data} 与数据的汉明重量（或汉明距离）之间的关系。为此，设计如下实验。

重新测量对 MCU 累加器进行赋值的过程。与先前实验不同的是这次实验使用了 256 个不同的数据值，每个数据各测量 150 次。对于 8bit 的数据共计有 9 个汉明重量。将得到的 256×150 个数据分成 9 组，汉明重量相同的数据分为一组。

分别对 9 组数据进行统计处理。得到某个时刻点所对应的功耗，绘制该点功耗与汉明重量之间的关系图，如图 7 所示。为了精确化得到的结论，需要尽量排除电子噪声对于功耗的影响。根据 4.2 节的介绍，电子噪声 $P_{\text{el-noise}}$ 服从正态分布，因此可以选择相应的信号处理技术尽量减小 $P_{\text{el-noise}}$ 的均方差，不过完全消除 $P_{\text{el-noise}}$ 的影响是不可能的。

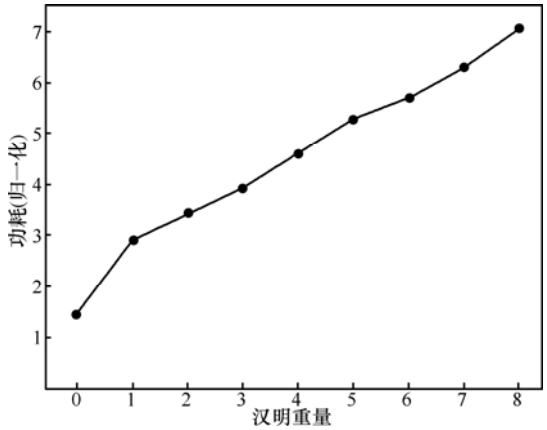


图 7　汉明重量与功耗的关系

图 7 显示，汉明重量为 0 时对应的功耗最小，汉明重量为 8 时导致功耗最高。由于实验的前提条件是假设电子噪声全部消除，并且对数据操作相同的步骤，因此，图 7 所示功耗与汉明重量的功耗轨迹，也正反映了 P_{data} 与汉明重量的关系，即对于密码设备 MCU 来说， P_{data} 与处理数据的汉明重量成正比。

5　结束语

在功耗分析攻击中，攻击者需要将数据值与被攻击设备的功耗建立一定的映射关系。本文在器件功耗与数据相关性的物理基础上详细阐述了汉明距离模型和汉明重量模型，从理论上证明了汉明重量模型的正确性。并建立 MCU 功耗采集平台，验证了汉明重量模型的有效性和实用性。

参考文献：

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. Proceedings of the 19th Annual International Cryptology Conference[C]. Cryptology, 1999. 388- 397.

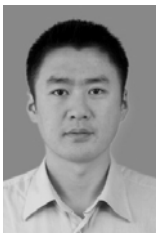
[2] KOCHER P C. Timing attacks on implementations of Diffie- Hellman, RSA, DSS, and other systems[A]. CRYPTO' 96[C]. 1996.104-113.

[3] WU Z, CHEN Y, CHEN J, *et al*. Exponential information's extraction from power traces of modulo exponentiation implemented on FPGA[J]. Journal on Communications, 2010,31(2):17-21

[4] WU Z, CHEN Y, WANG M , *et al*. Improvement of equivalent power consumption coding secure against power analysis attacks[J]. Journal on Communications, 2010,31(8):26-30

[5] WANG M, WU Z. Simple power analysis attack on random pseudo operations[J]]. Journal on Communications, 2012,31(5):138-142.

作者简介：



罗鹏（1978-），男，四川遂宁人，中国科学院博士生，主要研究方向为信息安全。

冯登国（1965-），男，陕西靖边人，中国科学院研究员、博士生导师，主要研究方向为信息安全。

周永彬（1973），男，山东人，博士，中国科学院软件研究所副所长、副研究员，主要研究方向为信息与网络安全、互联网技术、电信技术、计算机软件及计算机应用。

ISSN 1000-436X

发行代号：国内2-676 / 国外M395

(2012)京新出报刊增准字第(493)号

2012 年 9 月 25 日出版　定价：58.00 元

通信学报　第三十三卷　第Z2期　二〇一二年十一月