第 29 卷 第 4 期
2006 年 4 月
计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS
Vol. 29 No. 4
Apr. 2006

RSA 密码算法的功耗轨迹分析及其防御措施

韩 军 曾晓洋 汤庭鳌
（复旦大学专用集成电路与系统国家重点实验室 上海 201203）

摘 要 针对 RSA 密码算法的电路，提出了一种新的功耗分析攻击方法——功耗轨迹分析. 该方法的基本特点是通过处理电路的功率信号，从信号的轨迹图形中获取 RSA 算法的敏感信息（如密钥），因此，功耗轨迹分析能够有效地攻击现有的多种形式的 RSA 实现方案. 同时还探讨了 RSA 密码电路防御攻击的措施：直接在算法中添加冗余的伪操作能够抵御功耗轨迹分析攻击，但是这会导致电路功耗增大和速度降低. 进而还提出了一种将 RSA 算法中的伪操作随机化的新方法. 该方法能够在保证电路安全性的同时又节省电路功耗和运算时间.

关键词 功耗分析攻击；RSA 密码算法；安全芯片；抗攻击；模幂
中图法分类号 TP309

Power Trace Analysis Attack and Countermeasures for RSA Cryptographic Circuits

HAN Jun ZENG Xiao-Yang TANG Ting-Ao
(*State Key Laboratory of Application Specific Integrated Circuit & System, Fudan University, Shanghai* 201203)

Abstract The first purpose of this paper is to present a new power analysis attack, total power trace analysis, which is a considerable menace to the unprotected RSA chip. And this attack can efficiently extract secret information from the patterns of the processed power signals. Several different version exponentiation algorithms of RSA cipher examined in the authors' research are all vulnerable to this type attack. The second purpose of this paper is to investigate the countermeasures against the power analysis attack mentioned above. The investigation done in this paper indicates that adding dummy operations into the cipher circuits can resist the attack, but result in higher power consumption and slower speed. And a new solution named as randomized dummy operations is proposed, which can also keep the security of the chip but with a lower power consumption level and faster speed.

Keywords power analysis attack; RSA cryptographic algorithm; security chip; anti-attack; exponentiation

1 引 言

从 Kocher 等人提出针对智能卡微处理器的功耗分析方法以来[1]，观测密码算法运行过程中芯片的功耗变化从而获取其密钥的方法得到了深入研究和广泛发展. 在迅速数字化和网络化的信息社会，信息安全芯片如何抵御功耗分析是人们应该十分重视的问题. 目前，公钥制密码算法已经广泛应用于各种嵌入式密码系统，RSA 密码就是其中一个典型例子[2]. 但是，近些年来的研究表明，RSA 有易受功耗分析攻击的弱点. Messerges 等提出了能够有效攻击 RSA 算法的差分功耗分析（Differential Power Analysis, DPA）方法，例如 SEMD, MESD 和 ZEMD[3]. 他们也证明：由于信号受噪声的干扰太大，简单功耗分析（Simple Power Analysis, SPA）难以获

收稿日期：2005-01-19；修改稿收到日期：2006-01-16. 本课题得到国家自然科学基金（90407002，60576024）资助. 韩 军，男，1977 年生，博士研究生，主要研究方向为信息安全芯片设计、芯片防御攻击技术. E-mail：031021025@fudan.edu.cn. 曾晓洋，男，1972 年生，副教授，研究方向为密码系统的 VLSI 设计、测试及信息安全. E-mail：xyzeng@fudan.edu.cn. 汤庭鳌，男，1939 年生，教授，博士生导师，研究领域为防御电路的 IC 设计.

取 RSA 的密钥.

在设计密码系统的安全策略时，必须设法应对可能存在的最强大的攻击方法，因此对攻击方法的研究有助于建构真正合理、有效的安全策略. 本文提出了一种新的功耗分析方法——功耗轨迹分析. 它与以前的攻击方法有很大的不同，具有更好的可行性和有效性. 另外基于对攻击方法的研究，本文还提出了 RSA 密码电路防御攻击的相应措施，对 RSA 算法中的模幂运算进行了改进，以尽量小的代价来提高算法防御攻击的能力.

本文第 2 节介绍本项研究的工作方式和流程；第 3 节简要回顾各种形式的 RSA 模幂运算的实现方案；第 4 节详细论述功耗轨迹分析攻击的原理、实现方法以及相应的分析结果；第 5 节提出防御功耗分析的措施和方法；第 6 节是本文结论.

2　研究方法

RSA 密码算法既可以在通用的微处理器上用高效的软件实现，也可以用嵌入在智能卡上的专用硬件实现. 由于智能卡微处理器能力有限，软件实现的效率比较低，因此采用硬件密码协处理器是目前片上密码系统比较普遍的解决方案. 虽然本文研究工作集中在专用密码协处理器电路上，但是通用微处理器在执行 RSA 算法时也存在类似的缺陷(算法的分支结构)，也易受功耗分析攻击，因此本文研究结果也可以为通用微处理器上运行的密码系统所借鉴.

本文的 RSA 密码协处理器在采用 HDL 语言进行 RTL 级设计以后，基于 SMIC 0.25μm 工艺，利用 Synopsys 公司的 Design Compiler 工具进行综合，得到电路门级网表，然后再将其转化为晶体管级的 spice 网表，用 Hspice 软件实现电路仿真. 在仿真过程中观察和记录电路的功率信号，进而采用功耗轨迹分析方法获取 RSA 算法的密钥. 以上就是本研究中电路实现和功耗特性提取的基本流程. 这一流程的主要优点是：(1)因为结合了具体的工艺库，实现了晶体管级的仿真，所以仿真结果能最大程度地接近真实电路. 根据仿真结果，可以较为精确地分析前端电路设计，鉴定其抗攻击能力. (2)能够在电路进行制造之前，检测出其易受攻击的缺陷，这样就大幅度节省了反复流片测试所花费的时间与成本.

3　RSA 相关算法概述

RSA 密码算法的核心是模幂运算，而实现模幂的基本途径是所谓的“平方-乘积”(“square and multiply”)算法[4]，即将模幂分解成一系列的平方和乘积运算. 对于基本的平方和乘积操作，一般采用 Montgomery 模乘算法来实现[5]. 下面介绍一下各种不同形式的“平方-乘积”算法.

算法 1.　从左到右扫描的模幂(LR).

```
R=M^e mod N
{ R=1
  for (i=n-1 down to 0)
  {
   R=R^2 mod N
   if (ith bit of e is 1)
      R=R·M mod N
  }
  return R
}
```

算法 2.　从右到左扫描的模幂(RL).

```
R=M^e mod N
{ R=1
  S=M
  for (i=0 to n-1)
   {
    if (ith bit of e is 1)
    R=R·S mod N
    S=S^2 mod N
   }
  return R
}
```

算法 3.　随机扫描的模幂(RAD).

```
R=M^e mod N
{ R=1
  S=M
  Z=random number between 1 and n-2
  for(i=Z to n-2)
  {
   if (ith bit of e is 1)
      R=R·S mod N
      S=S^2 mod N
  }
  R=R·S mod N
  for (i=Z-1 down to 0)
  {
   R=R^2 mod N
   if (ith bit of e is 1)
   R=R·M mod N
  }
  return R
}
```

以上算法中 M 为消息，N 为模数，e 为 n 比特

的二进制指数，R 为运算结果. 在算法 2 中，平方、乘积两个运算步骤可用串行和并行两种形式执行. 这就意味着模幂实际上有 4 种实现形式. 算法 3 结合了 RL 和 LR 两种算法，被称为随机扫描(RAD)模幂算法. Messerges 认为随机化的模幂能够显著地抑制所有他列举的功耗分析方法的攻击[6]，包括 SPA、DPA 和相关性攻击(correlation attack)，然而本文的研究表明，随机扫描的模幂算法无法抵御本文提出的功耗轨迹分析方法.

4 功耗轨迹分析

我们基于 RSA 密码算法设计了密码协处理器，其总体架构如图 1 所示. 协处理器由 Memory(存储单元)，MonPro Unit(蒙哥马利模乘单元)，Data Bridge(数据桥)，Controller(控制器)4 部分构成. 该架构对于公钥制密码协处理器具有一定的通用性，在 512～2048 比特数据宽度的 RSA 密码协处理器中都有较为广泛的应用. 为了缩短冗长的晶体管级 Spice 仿真时间且不失一般性，本文选用的协处理器的数据宽度为 16 比特，逻辑综合结果表明，电路规模约为 2900 个等效门.

图 2 给出了由 Hspice 仿真得到的密码协处理器电路在执行 LR 模幂算法时的功率信号. 如图 2 所示，唯一可以确定的是电路是否工作，但是无法获取电路运行过程中的敏感信息，如密钥.

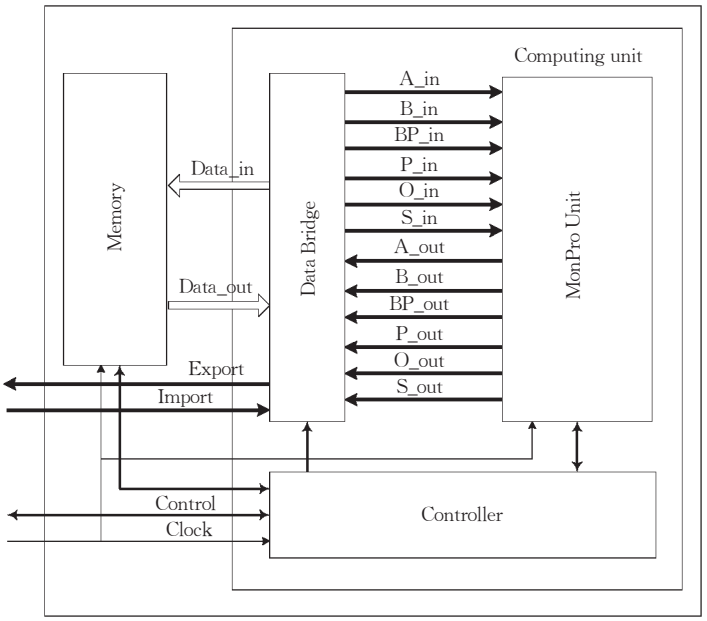

图 1 RSA 密码算法协处理器架构

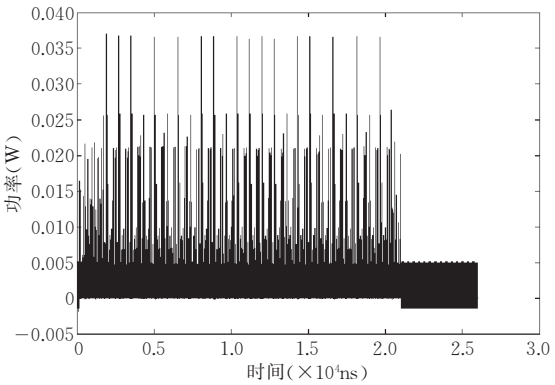

图 2 使用 LR 模幂算法的 16 位 RSA 密码电路的功率信号

在执行算法时，电路在不同时期处于不同的状态，比如存数据、取数据、算术或逻辑运算等. 假设将电路的运行时间分成对应于不同电路状态的时间段，那么在每个时间段中电路功耗不尽相同. 功耗轨迹分析就是通过对一定时间范围内的电路功耗的分析，区分电路的不同状态，从而区分算法的不同步骤.

令原始未作处理的功率信号为 $S_O[j]$，一定时间宽度内的总功耗信号为 $S_P[j]$，简称总功耗信号. $S_P[j]$ 由以下公式计算得到：

$$S_P[j]=\sum_{i=0}^{W}S_O[j+i] \tag{1}$$

其中，W 是一定时间宽度内功率信号的采样数，$W=T_{period}/T$，T_{period} 是时间宽度，T 是采样率，j 为离散的时间点. 假定 $W=200$，由式(1)可以计算 LR 模幂运算的总功耗信号，结果如图 3～5 所示.

图 4 和图 5 分别示出了两种不同图形，这两种图形反复出现在图 3 的总功耗信号的变化轨迹中. 对比电路中算法的执行过程，我们发现当电路仅执

行$R=R^2 \bmod N$ 操作时，总功耗信号的变化轨迹显示为图形(1)；而当电路顺序执行 $R=R^2 \bmod N$ 操作和 $R=R\cdot M \bmod N$ 操作时，总功耗信号的变化轨迹显示为图形(2). 由 LR 模幂算法可知，图形(1)和(2)实际上指示了幂指数相应的比特位值是 0 还是 1，因此通过区分不同的总功耗信号的轨迹图形，就可以破解 RSA 算法的密钥. 这种方法本文称之为功耗轨迹分析.

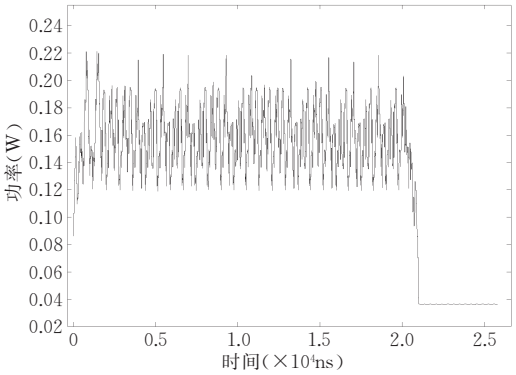

图 3　使用 LR 模幂算法的 16 位 RSA 密码电路的总功耗信号

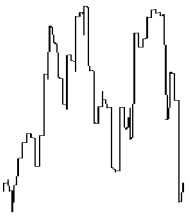

图 4　出现在图 3 信号轨迹中的图形(1)

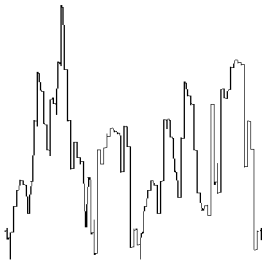

图 5　出现在图 3 信号轨迹中的图形(2)

功耗轨迹分析比目前报道的针对 RSA 的 DPA 方法更容易实现和操作. 在现实环境下完成功耗轨迹分析可能需要让电路重复执行模幂算法多次，从而获得一组总功耗轨迹信号，然后利用取均值的办法去除噪声. 尽管如此，与 Messerges 等的 DPA 方法相比，所需执行的模幂运算的次数是十分少的.

当然，在执行功耗轨迹分析时也需要解决一些困难. 首先，如何在总功耗信号的轨迹中确定模幂运算的起点和终点，因为 RSA 密码算法在模幂扫描之外，还有一些预处理和后处理步骤. 其次，如何确定相应的图形表征的是 0 还是 1，因为攻击者只知道不同的图形对应不同的值. 但是上述问题并不会对功耗轨迹分析造成太多的麻烦. 幂指数实际上是一个二进制比特位串，只要在功耗轨迹中确定了它的主体部分，剩余部分可以采用枚举法来进行搜索，最终得到整个指数. 对于第二个问题，如果一种图形代表了 0，那另一种图形就必然代表 1，反之亦然，因此实际上只需尝试两种可能性，这样的工作量是可以接受的.

RL 模幂算法同样是易受功耗轨迹分析攻击的. 如图 6、图 7 所示，分别采用串行和并行架构的 RSA 电路(执行 RL 模幂算法)都在总功耗信号的轨迹中显示出一些特定的图形，它们表征了不同的算法操作，从而泄漏了密钥信息.

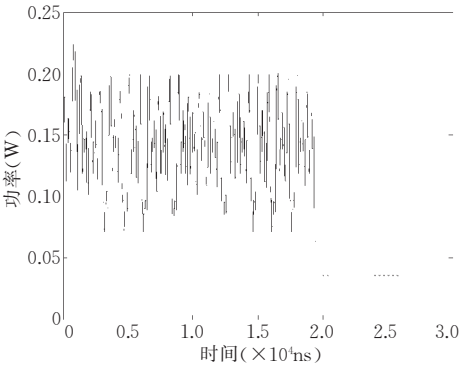

图 6　使用 RL 模幂算法的 16 位 RSA 密码电路(串行架构)的总功耗信号

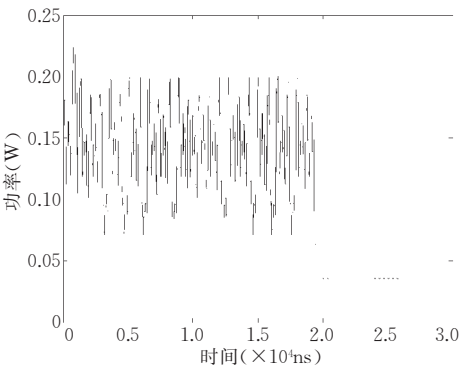

图 7　使用 RL 模幂算法的 16 位 RSA 密码电路(并行架构)的总功耗信号

本文也研究了随机扫描的模幂算法，Messerges 将该算法作为防御功耗分析攻击的有效措施，但是本文研究表明：该算法无法防御功耗轨迹分析的攻击，其总功耗信号如图 8 所示.

随机扫描(RAD)模幂算法结合了 LR 和 RL 两种模幂算法，也就是说一部分的模幂运算是采用从左到右扫描幂指数，另一部分的模幂运算是采用从右到左扫描幂指数，两种扫描所涉及的幂指数(n 比特二进制数)的位数则是随机的，这样就可以导致目

前的 DPA 攻击失效. 但是如图 8 所示,功耗轨迹分析却可以找到 LR 和 RL 两种模幂运算的分界点,因为两种运算的各自的总功耗信号的幅度具有明显的区别(左侧为 RL,右侧为 LR). 因此攻击者可以先分别分析 LR 和 RL 模幂运算的幂指数信息,然后两者合并得到整个密钥. 由此可见随机扫描(RAD)模幂算法并不能为 RSA 密码电路提供足够的安全保障.

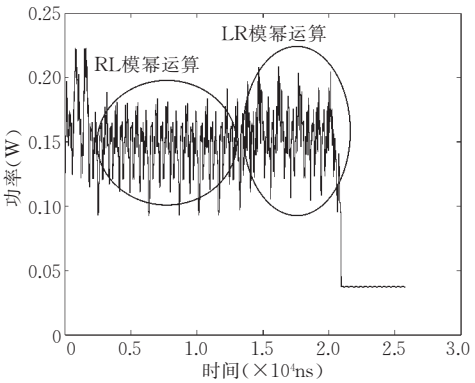

图 8 使用 RAD 模幂算法的 16 位 RSA 密码电路的总功耗信号

下面讨论功耗轨迹分析能够成功攻击 RSA 密码电路的内在机理.

数字集成电路一般采用有限状态机来控制电路运转的流程,状态机状态的转换导致相应寄存器和组合逻辑的跳变和翻转. 另外,状态机的状态还对应着功能性的操作,比如取数据、存数据和算术逻辑运算等,因此电路功耗的变化和状态机状态是相互关联的. 如果电路周期性地在一些特定状态之间跳转,那么相同的功耗变化轨迹也会反复出现. 为进一步深入研究,本文给出一个电路总功耗信号的数学模型.

该模型假定电路在运行过程中存在 4 个状态: state1, state2, state3 和 state4,而且每个状态占据的时间都是 τ. 在一个状态所占据的时间段里,瞬态功率信号围绕一个平均值波动,因此对应于 4 个不同状态有 4 个不同功率平均值,命名为 P_1, P_2, P_3 和 P_4. 为了描述功率平均值在时间域里的变化,定义分段函数 $E(P(t))$ 如下:

$$E(P(t))=\begin{cases}P_1, t\in\{t\mid state(t)=\text{state1}\}\\ P_2, t\in\{t\mid state(t)=\text{state2}\}\\ P_3, t\in\{t\mid state(t)=\text{state3}\}\\ P_4, t\in\{t\mid state(t)=\text{state4}\}\end{cases} \tag{2}$$

考虑电路状态的一组跳转序列: state1→state2→state1→state2→state1→state2→state3→state4→state1→state2→state3→state4→state1. 令原始的瞬态功率信号为 $P(t)$,一定时间窗口 τ 内的总功耗信号为 $P_{\text{total}}(t)$,计算 $P_{\text{total}}(t)$ 可以将式(1)变形为

$$P_{\text{total}}(t)=\int_t^{t+\tau}P(t)\mathrm{d}t \tag{3}$$

由式(2)已知功率平均值函数,因此式(3)可化简为

$$\begin{aligned}P_{\text{total}}(t)&=E(P(t))\tau=P_f(\tau-t')+P_s t'\\&=(\tau-t')(P_f-P_s)+\tau P_s\\ t'&=t-n\tau,\ 0\le t'\le\tau,\ n=0,1,2,3,\cdots\end{aligned} \tag{4}$$

其中,P_f 为两个前后相继的状态中的前一个状态的功率平均值,P_s 则为后一个状态的功率平均值. P_f 和 P_s 的值从 P_1, P_2, P_3 和 P_4 中选取. 假定 τ 为 200 个时间单位,P_1 为 3 个功率单位,P_2 为 2 个功率单位,P_3 为 4 个功率单位,P_4 为 1 个功率单位,由式(4)计算可得到总功耗信号(如图 9 所示).

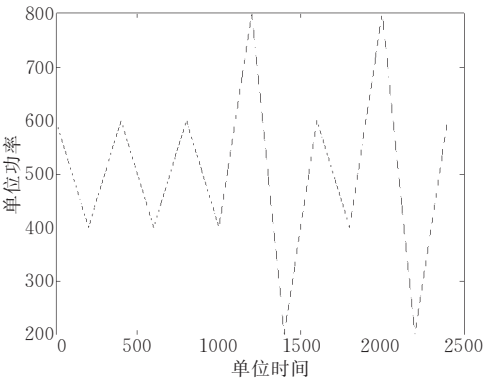

图 9 由数学模型计算得到的总功耗信号

图 9 表明总功耗信号的轨迹反映了电路在不同状态之间的转换,实际上也表征了电路不同的运行过程. 对于 RSA 密码协处理器电路,由算法可知,电路必须进行模平方、模乘等运算,再加上一些相应的加载和存储操作,就构成了一系列在一定条件下互相切换的状态. 由于不同状态下功耗的差异,总功耗轨迹信号就能反映出电路状态的变化,从而揭示算法步骤.

功耗轨迹分析不仅是一种有效的功耗分析攻击方法,而且是功率信号图形具有数据相关性的很好例证. 我们认为,要进一步增强功耗轨迹分析的功能,具有机器学习能力的图形识别技术可应用到功耗轨迹分析中,这样就可以利用特定设备更加自动和更加精细地分析功率信号的轨迹图形. 功耗轨迹分析也体现了信号处理在旁道攻击(side-channel attack)中的应用,先进的信号处理技术有助于推动新的数据分析技术的发展.

5 RSA 电路抵御功耗分析的方法

未进行保护的 RSA 密码电路容易受到功耗分

析方法的攻击. 研究各种攻击方法的目的在于设计和制定足够强的防御措施，以保证芯片安全. 我们认为，只有密码算法及其电路实现都得到改进和提高，才能有效地遏制针对密码芯片的功耗分析.

功耗分析攻击利用了 RSA 密码电路的一个基本特点：密钥的每个比特位值不同，就会导致电路不同的运算操作. 因此一个直接的办法就是在算法中添加多余的伪操作，从而平衡不同的操作步骤，下面给出改进以后的 LR 模幂算法.

算法 4.　添加伪操作后的从左到右扫描的模幂(LR).

```
R=M^e mod N
{ R=1
  for (i=n-1 down to 0)
  {
    R=R^2 mod N
    if (ith bit of e is 1)
      R=R · M mod N
    else
      R=R · M mod N (should not be stored)
  }
  return R
}
```

算法 4 中的 M，N 和 e 的定义与算法 1 中一致. 在算法 4 中 e(密钥)比特位值为 0 和 1 时，算法的运算步骤相同. 我们对于改进后的 LR 模幂的运行过程也进行了功耗轨迹分析. 其结果如图 10 和图 11 所示.

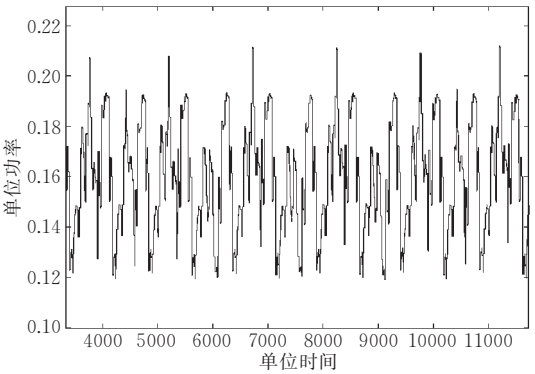

图 10　使用添加伪操作后的 LR 模幂算法的 16 位 RSA 密码电路的总功耗信号

与图 3 相比，图 10 中反复出现的轨迹图形之间的差异显著减小，几乎是周期性地出现十分类似的轨迹图形. 由此可见，由于轨迹图形之间互相区分的难度增加，功耗轨迹分析的攻击效能被很大程度地削弱了.

但是，如果更细微地考察图 10 总功耗信号的轨迹图形(如图 11 所示)可以发现：算法 4 不足以使 RSA 密码电路抵御功耗轨迹分析. 图 11 中尽管左边的轨迹图形(对应于密钥比特位的值为 0 时)与右边的轨迹图形(对应于密钥比特位的值为 1 时)十分相似，但是在部分位置仍有微小的差别，这足以将两者区别开来. 当然在实际条件下的攻击中，这样的差别可能因为噪声干扰的存在而变得十分不明显，但是目前信号处理的工具和技术发展迅速，去除噪声找到这些微小的差别并不是很困难的问题. 导致这些微小的差别原因是，虽然伪操作的运算过程和真正算法步骤的运算过程一致，但是伪操作运算结果是不存储到存储器里的，因此电路也就跳过了存储数据的状态直接继续下面的操作，而真正的算法步骤在模乘运算结束后必须将结果先存到存储器中. 目前密码芯片处理的数据宽度和数据总量都很大，数据存取会占据相当长时间，其功耗特征也会明显地反映到功率信号的轨迹图形中. 如果要更完全地平衡不同算法步骤的轨迹图形，必须再添加数据存取的伪操作.

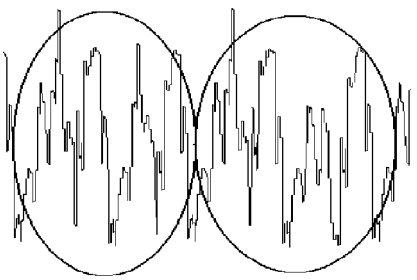

图 11　轨迹图形的对比

诚然，添加伪操作能够有效地抵御功耗分析攻击，但是这将导致电路浪费相当多的功耗和运行时间. 对于智能卡和各种移动设备，低功耗和高效率是十分关键的. 鉴于此，算法 4 仍需进行改进. 改进的新算法如下.

算法 5.　添加随机伪操作后的从左到右扫描的模幂(LR).

```
R=M^e mod N
{
  R=1
  D=random number between 1 and 2K
  for (i=n-1 down to 0)
  {
    R=R^2 mod N
    if (ith bit of e is 1)
      R=R · M mod N
    else if (D<K)
      R=R · M mod N
```

}
return R
}

算法 5 中的 M,N 和 e 的定义与算法 1 中一致,K 为整数. 在算法 5 中,伪操作的执行是随机的. 如果扫描到幂指数比特位的值为 0,那么由随机数发生器决定是否执行伪操作. 假定二进制幂指数宽度为 n 位,且每一位为 0 和为 1 的概率是相等的. 这样对于未添加伪操作的 LR 模幂算法,平均来说其运行一次所需执行的模乘运算的次数为 $1.5n$,而对于直接添加伪操作的算法 4,所需执行的模乘运算为 $2n$,这样算法 4 所浪费的功耗和时间就相当可观,因为目前 RSA 密码算法的密钥宽度已经超越了 1000 比特,算法 4 需要增加至少 500 次模乘. 伪操作随机化的算法 5 则不同,一次模幂所需模乘的次数为 $(1.5+0.5p)n$,p 是由随机数发生器和一定的判决条件所决定的概率. 如果 $p=0.5$,那么与算法 4 相比就节约了至少 250 次模乘,而增加一个伪随机数发生器的硬件开销非常小,而且对于那些本身就具有随机数发生器的密码系统来说就更不成问题. 综合考虑,添加随机伪操作是 RSA 密码电路十分可行的防御措施,利用伪操作抵抗了功耗分析攻击,而通过将其随机化则能够在不影响安全性的前提下,大幅度地节约功耗和时间.

6 结 论

本文提出的功耗轨迹分析方法是一种既容易实施又十分有效的功耗分析方法. 它能够成功攻击 LR、RL 和 RAD 等 RSA 模幂算法. RAD 模幂算法 (randomized exponentiation) 被认为是抵御功耗分析攻击的重要方法,但是本文研究表明其并不能抵抗功耗轨迹分析. 在防御攻击技术方面,本文指出:在算法中直接添加伪操作能够使 RSA 密码电路有效地抵御功耗轨迹分析攻击,但是会引起功耗和运行时间的大幅度增加,而添加随机化伪操作可以在保证安全性的前提下,节约大量功耗和运行时间.

参 考 文 献

1 Kocher P., Jaffe J., Jun B.. Differential power analysis. In: Proceeding of the Advances in Cryptography (CRYPTO'99), Santa Barbara, USA, 1999, 388～397

2 Rivest R. L., Shamir A., Adleman L.. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120～126

3 Messerges T. S., Dabbish E. A., Sloan R. H.. Power analysis attacks of modular exponentiation in smartcards. In: Proceeding of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'99), Worcester, USA, 1999, 144～157

4 Brickel E. F.. A survey of hardware implementations of RSA. In: Proceedings of the Advances in Cryptology (CRYPTO'89), Santa Barbara, USA, 1990, 368～370

5 Montgomery P. L.. Modular multiplication without trial division. Mathematics of Computation, 1985, 44(170): 519～521

6 Messerges T. S.. Power analysis attacks and countermeasures for cryptographic algorithms[Ph. D. dissertation]. Graduate College of the University of Illinois at Chicago, 2000

HAN Jun, born in 1977, Ph. D. candidate. His research interests include information security chip design, anti-attack technologies for chip.

ZENG Xiao-Yang, born in 1972, associate professor. His research interests include VLSI design of cryptosystem, design testing, and information security.

TANG Ting-Ao, born in 1939, professor. His research interests include semiconductor device, IC design for anti-attack circuits.

Background

This paper focuses on power analysis attack against RSA cryptosystem and its countermeasures. The project is supported by the National Natural Science Foundation of China under the grant No. 90407002 and 60576024. The research goal of this project is to improve the algorithm and circuit design of cryptosystem, considering the stronger power analysis attack on security chip. During recent years, power analysis attack has been a considerable menace for information security applications. And a lot of research works are involved in this type attack in order to develop the reasonable security strategies. This paper presents a new powerful attack (total power trace analysis) that will challenge our cryptographic hardware. And the countermeasures against power analysis attack are also discussed and developed in this paper.