安全SoC抗功耗攻击研究综述

李 浪[1,2] 李仁发[2] Edwin H. -M. Sha[2,3]
(衡阳师范学院计算机系 衡阳 421008)[1] (湖南大学计算机与通信学院 长沙 410082)[2]
(Department of Computer Science, University of Texas at Dallas, Richardson 75083, USA)[3]

摘 要 功耗攻击目前已成为安全SoC芯片的最大威胁,已经证明是一种非常有效的发现密钥方法。对抗功耗攻击技术研究成为近年来的热点问题。对抗功耗攻击从算法掩码级和电路级两个方面综述,重点对抗功耗攻击国内外有影响的研究成果进行了总结与评述;对抗功耗分析攻击的已有实验方法进行了总结,并给出了较易实现的实验方法,最后提出了安全SoC抗功耗分析攻击的进一步研究方向。

关键词 安全SoC芯片,抗功耗攻击,实验方法
中图法分类号 TP309 **文献标识码** A

Survey on Security SoC against Power Analysis Attack

LI Lang[1,2] LI Ren-fa[2] Edwin H. -M. Sha[2,3]
(Department of Computer, Hengyang Normal University, Hengyang 421008, China)[1]
(School of Computer and Communication, Hunan University, Changsha 410082, China)[2]
(Department of Computer Science, University of Texas at Dallas, Richardson 75083, USA)[3]

Abstract Power analysis attack has become a great threat to security SoC Chips. It has shown to be one of the most effective techniques to discover secret keys. Power analysis attack and its resistant have attracted much study. The paper reviewed various types of power analysis attacks resisted techniques, including algorithm level and circuit-level. The important research results on resisting power analysis attacks were summarized with comments. Power analysis attacks resistant of experimental methods summarized, the proper experimental methods were proposed. In the last, the paper presented the future research directions.

Keywords Security SoC, Against power analysis attack, Experiment methods

1 引言

1998年Paul Kocher给出了一个比较有效的加密SoC功耗分析攻击方法[1],引起了广泛关注。这一方法的主要特点是采用适当仪器对加密设备在加密算法运行时所泄漏出来的能量信息(电磁辐射)进行测量,得到功率曲线,然后对所得到的大量功率曲线进行统计分析,推测出密钥,来实现密钥的破译。这种攻击手段比传统的数学攻击破解方法有更大的威胁性,而且因为实现简单、攻击成功率高等特点,一经提出便引起安全界的高度重视。

在传统的密码分析中,主要是从算法的设计角度来考虑。重点对算法的数学结构进行研究,辅以关于算法输入/输出的某些假设,结合统计测试进行分析,这对高安全强度密码算法的设计是必要的。但是从算法实现的角度来考虑安全问题就有些复杂了,单纯数学结构研究和统计测试理论的应用已经远远不够。在算法实现过程中,磁辐射的物理特性产生了旁路信道,出现了对加密过程的某些中间状态的信息泄漏现象,而测量手段也大大提高,功耗分析正是在这种情况下被提出的。J. R. Rao等人破解了智能卡中的AES算法密钥的过程和结果[3],国内赵强等研究人员也提出了多种功耗分析攻击方法,用来破解加密SoC[4-6]。

现在的集成电路一般采用静态互补CMOS逻辑实现,静态互补CMOS逻辑电路的功耗行为依赖于电路中处理的数据。这种功耗与运算数据的相关性是旁路信息泄漏的原因,这对密码模块的安全应用产生了极大威胁,因此没有考虑功耗攻击的安全加密SoC存在着极大的风险。本文对目前最受关注的SoC抗功耗攻击技术研究成果进行综述。

2 功耗攻击

功耗分析攻击分为简单功耗分析攻击(SPA)与差分功耗分析攻击(DPA)[7]。差分功耗分析攻击又分为一阶差分功耗分析攻击与高阶差分功耗分析攻击。一般把一阶差分攻击简称为差分功耗分析攻击。高阶差分功耗攻击的攻击能力更强,但分析技术更复杂。

到稿日期:2008-07-10 返修日期:2008-10-30 本文受863计划资助项目(2007AA01Z104),国家自然科学基金(60673061,60873074),湖南省自然科学基金(07JJ6108)资助。

李 浪 博士生,副教授,主要研究方向为嵌入式系统安全,E-mail:lilang911@126.com;李仁发 教授,博士生导师,主要研究方向为嵌入式计算与安全;Edwin H. -M. Sha 教授,博士生导师,主要研究方向为嵌入式系统并行计算与安全。

简单功耗攻击是指在算法执行过程中引入的噪声和其它干扰较少，这时所测得的指令和操作数的功耗大小具有明显特征。如果将测量结果绘制成功耗曲线，就可以结合一些指令瞬间功耗经验值来直接推断运行指令顺序，攻击成功的速度快，特别是具有条件选择和跳转的指令表现出很好的 SPA 特性，可以直接反映在所测量的功率曲线上。如果指令或操作数的汉明重量与功耗强烈相关，这就更易攻击。但在一般情况下，操作指令的功耗比较接近，变化较小，测量时不可避免地要产生一定的误差。再加上设备及环境噪声的影响，用简单功耗攻击(SPA)的方法就较难攻击成功。现在 SPA 一般主要是配合差分功耗分析攻击(DPA)使用的，用来辅助确定某些操作执行的起点。

差分功耗分析攻击(DPA)是一种对密码芯片的泄漏功耗进行统计分析而恢复密钥的攻击方法。差分功耗攻击的方法是对大量的曲线样点进行功耗统计测试，即根据大量功耗样本来分析密钥的值，具有比简单功耗攻击更高的强度。

进行差分功耗分析主要有两个步骤：数据采集和数据分析。数据采集需要将功耗波形进行足够采集，在采集同一批数据的时候要求芯片内部的密钥是不变化的。数据分析是利用统计的方法对数据进行处理，得出需要的功耗信息。

总结功耗攻击分析，便可知道功耗攻击要满足以下个条件：

(1)要用相同密钥进行运算。

(2)攻击者能够知道密码运算的明文或密文。

(3)运算过程中某个中间运算结果与密钥位要具有相关性。

(4)密码模块的功耗与被运算处理的数据相关。

3 抗功耗攻击研究综述

目前抗功耗分析攻击方法可分为基于算法级掩码和基于功耗恒定的电路级实现两类技术。其中以算法级掩码最为普遍，这一抗功耗攻击方案主要是利用掩码(Masking)技术，通过引入随机数，对加密 SoC 芯片内部的数据进行掩码，使得电路的功耗、运行时间以及电磁辐射等外界可探测的因素与内部运算数据无关。电路级的抗攻击解决方案是将电路自身设计成没有旁路泄漏的单元，用这些单元来构建安全 SoC 芯片。这种防护方法不改变中间运算结果，而仅改变密码模块的功耗，使功耗恒定或随机化，进而使密码模块的功耗与中间运算结果相互独立，攻击者无法得到功耗与密钥的相关性。

3.1 基于掩码技术的抗功耗攻击

算法级掩码的抗攻击立足点主要是内部处理数据的随机化。具体来说就是用随机数将芯片内部的中间计算结果进行掩码(如异或)。对称钥加密算法的基本运算可以分为两种：一种是线性运算，如移位、混淆等；另一种是非线性运算，如 S-盒的字节替换。对于加掩码来说，前者十分容易实现，而后者是对称钥加密算法级掩码的难点。算法级的抗攻击方案具有易实现、代价低的优点，同时因为没有从电路层来考虑安全问题，所以仍然可能存在如下安全隐患：(1) 代价比较昂贵，需要随机数发生器等硬件；(2)提供的安全性不够高，不能抵抗高阶 DPA 技术的攻击。

M. Bucci 等人提出了密码算法部件的功耗随机化[8]。K. OKeya 等在 ECC 算法中采用随机射影坐标技术来抗 DPA 攻击[9]；H. Chang 等提出基于固定值掩码的 AES 算法实现[10]，可以抗二阶 DPA 攻击。韩军等人提出插入随机伪操作的算法实现[11,12]。毛志刚等提出基于数据掩码的 DES 实现技术[13]，可以防范 DPA 攻击。童元满等人分别从 RSA 和 ECC 算法的细粒度任务调度和基于功耗恒定逻辑单元的半定制设计流程等方面研究抗功耗攻击[14]。

3.2 基于电路级抗功耗攻击技术

电路级抗功耗攻击技术主要分为两个方面：一是采用功耗恒定的逻辑单元；二是在芯片内部增加电路以平滑整个芯片的功耗。

K. Tiri 提出 SABL(敏感放大器逻辑)和 WDDL(行波双轨逻辑)运行时功耗几乎恒定[15]，与输入数据及顺序无关，可以用在各种加密电路中提高抵御 DPA 攻击的能力。但是采用 SABL 的芯片，功耗和面积增加约一倍，限制了其在移动设备、独立电源等设备上的使用。Macdonald 等人通过异步电路来达到抗功耗攻击目标[16]，因为双轨的功耗恒定逻辑与异步电路的双轨编码特性可以很好地结合起来。加拿大学者在分析密码运算模块的动态电流特性以及平滑动态电流方面做了较深入研究[17]。在欧洲，SCARD(抗旁路攻击的设计流程)项目主要从功耗恒定逻辑单元入手，研究与之相关的密码算法模块的半定制设计流程，同时研究旁路攻击特别是功耗攻击的基本理论和实施方法。孙义和教授设计实现了功耗平衡加法器，具有与输入数据无关的恒定功耗特性[18]。

文献[19]采用动态双轨与静态单轨逻辑混合设计，用动态双轨代替静态单轨实现关键模块，来提高抵御 DPA 攻击的能力。但是作者认为具体替换哪些模块涉及比较复杂的计算，因此没有给出判断关键模块的方法。复制方法[20]、屏蔽方法[21]、变型的屏蔽方法[22]等能够抵御 DPA 攻击但不能抵御高阶 DPA 攻击。Akkar 等人提出了独特的屏蔽方法(UMM)[23]及改进方法[24]，试图抵御高阶 DPA 攻击 DES(也可应用在 AES 中)。

电路级的安全措施利用了 3 个技术：双轨互补电路、电路级 Masking 以及预充电。比较有代表性的安全电路有 RSL[25]，WDDL[26]以及 MDPL[27]。其中，RSL 采用了预充电和电路级掩码技术。WDDL 采用了双轨电路和预充电技术，MDPL 则将前两者综合在一起，将 3 种技术集于一体。然而，这些电路都存在一个弱点：如果输入信号不同时到达，功耗的泄漏依然存在。

电路级解除功耗与中间运算结果相关性的方法可以分为两类：(1)使密码模块的每个操作均需要相同的功耗，如采用抗功耗分析攻击逻辑实现密码模块；(2)使密码模块任何时候的功耗都是随机的，如在密码模块中加入噪声、随机延迟等。由此可以看出，这种防护方法同样需要昂贵的代价。

实际上，在电路级抗功耗技术当中，无论上述哪一种防护技术，都是以增加硬件的复杂性为代价来换取抗功耗攻击的。

3.3 小结

各种防护方法主要使密码模块不再满足功耗攻击 4 个条件的后两条规则。算法级运算结果就是使密码模块不再满足规则 3，电路级是使密码模块不再满足规则 4。上述两类防护方法中，一种改变中间运算结果，一种改变密码模块的功耗，它们的目的都是减小实际测量功耗与实际的中间运算结果的相关性，从而达到防护目的。

除了上述两类防护方法，Joahn Borst 提出了一种称为临时密钥(Ephemeral Keys)的防护方法[28]。采用这种防护技

术的密码模块，在密码运算过程中，经常改变其密钥值。这种方法不同于上述两种方法，它并不减小实际测量功耗与实际的中间运算结果的相关性。在一般的 DPA 攻击实现中，攻击者必须测量足够多的功耗曲线，才能发现功耗与密钥的相关性。在这种情况下，攻击者不可能得到同一密钥下足够多的功耗曲线，因此使功耗分析方法不可行。

因此，对付功耗分析攻击的方法主要可以从以下几方面来考虑：

(1)采用可替代的计算技术，比如光学计算，但目前半导体材料还是不易替换的；

(2)从电路的角度，考虑好的滤波电路和物理级防护，使得功耗分析攻击变得困难；

(3)对于有面积和功耗限制的系统，则从减低信息泄漏的数量、测量噪声、使密钥多变且相关性小、加密运算的操作和时间的相关性小等方面来进行研究。

根据上述防 DPA 攻击的主要原理，在研究防止 DPA 模块时，主要有以下几种方法。

方法 1：低功耗设计。实质上就是降低硬件的功耗，使得泄漏信息比较弱。

方法 2：平衡功耗。在设计硬件时，考虑每一个指令的功耗尽可能为常数。

方法 3：功耗随机化。功耗与具体密钥无强相关性，使攻击者无法通过可以测得的功耗来相应地猜测密钥。

各种 DPA 防护技术虽然为密码模块带来了一定的安全防护能力，但同时这种安全性的获取是要付出一定代价的。这些代价包括性能损失、面积增加、运算时间增加、功耗增加等；另外，将各种防护措施加到密码模块中的设计过程同样需要花费一定代价。在实际设计密码模块过程中，设计者需要对多种防护方法进行权衡，以使设计达到较好的抗功耗分析攻击特性。Stofan Mangard 提出了一种统计方法，用来比较各种防护方法的有效性[29,30]。在密码模块的设计过程中，设计者可以根据这种统计方法计算出对密码模块成功实施 DPA 攻击所需要的样本数，从而比较各种防护方法的优劣，避免了重复设计。其中 PhiliPs 研究实验室的研究人员从芯片制造的角度找到了一种抗攻击方案[31]。随着研究的深入，新的抗功耗技术与方法还会不断涌现。

4 实验方法

目前在抗功耗分析攻击的研究中，有两种实验方法：一是仿真实验方法，二是实际的物理测试实验平台。这两种方法各有自己的优缺点。在抗功耗攻击的研究中，研究者可以根据自身实验条件选取相应的实验方法。

4.1 仿真实验方法

功耗分析攻击与防御电路设计和仿真流程为：先完成硬件描述语言(如 Verilog，VHDL)的描述，然后采用工艺库进行综合(综合软件可用 Design Compiler)，将综合后的网表转化为 Hspice 电路，结合工艺库模型参数进行功耗仿真，再对仿真的功率信号完成统计分析。这样做的优点在于：

(1) 能够结合具体的工艺，电路性能十分接近于实际制造出来的电路，所以仿真结果能最大程度地接近真实电路。

(2)能够在制造电路之前，检测出其易受攻击的缺陷，大幅度节省了反复流片测试所花费的时间与成本。能缩短设计周期和减少研发费用。

因此这一设计流程可作为抗功耗攻击研究的一种行之有效的重要途径。本文推荐这一方法作为抗功耗攻击的仿真实验研究方法。

4.2 实际物理测试实验平台

图 1 给出了一个实际的功耗分析攻击与防护测试实验物理平台，分为加密芯片部分、示波器部分、微机处理部分。

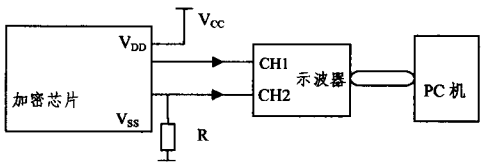

图 1 物理测试平台

加密芯片部分指 IC 卡、SoC、FPGA 等的 PCB 开发板，选择一个合适单片机来模拟加密芯片的功能，它可以执行指定的某种加密或解密。串联在 V_{ss} 与地之间的电阻，测量单片机在指令执行时的功耗波形、示波器的 CH1 接收电阻 R 上的电压波形、CH2 接收触发信号。采样得到的波形数据存储在示波器中，通过通讯软件与微机之间进行数据传输。微机主要完成对示波器的设置及数据的传输，可以用 GPIB 或者 USB 与示波器建立通信。微机同时选用相关的数据处理软件(如 Matlab)，完成数据的处理与分析。另外，加密芯片与微机之间同样存在关联，微机需要控制芯片的工作状态，载入数据。

物理测试平台的搭建也比较容易实现，且所需仪器设备并不复杂也不昂贵，一般的实验室很容易购买和组建。

结束语 综合起来，目前国内外的相关研究成果也存在诸多的不足。也正是由于目前研究成果或多或少存在一些缺陷，大力开展创新的抗功耗攻击技术研究才具有重要的理论价值和应用前景。进一步的研究应该包括：

(1)功耗模型的定量研究。具体算法实现的功耗模型定量研究是一件比较困难的事情，如果能够在通用性上做出一点突破，无疑对功耗分析攻击与防护研究起极大的推动作用。

(2)某一类加密算法的通用防护技术，目前都是针对具体算法、具体实现的防护，这无疑不利于防护的通用设计。

(3)研究量化评估密码算法部件的抗功耗攻击防护能力方法，比如如何确定成功实施功耗攻击所需的最少样本数。

(4) 功耗分析攻击与计时攻击甚至与错误导入攻击是否存在相关性[32]。如果能从实际和理论上证明之间存在强相关，那么在防御上就可以综合进行设计，同时防御多种攻击。

(5) 在实际的抗功耗攻击应用中，如何对资源受约束的安全 SOC 芯片采取何种有效的抗功耗攻击技术，既能保证面积或能耗优先，又能起到安全保证，还值得进一步的研究。

(6)功耗分析攻击与防护实验平台的整合。如何开发能够在一个平台上就可以有效完成整个功耗攻击分析实验研究的仿真软件，并且在普通的现有 PC 资源下有比较高的分析效率。

参 考 文 献

[1] Kocher P, Jaffe J, Jun B. Introduction to differential power analysis and related attacks[EB]. http://www.cryptography.com/dpa/technical, 1998

(下转第 25 页)

Media Access Protocol for Wireless Sensor Networks[C]//Proceedings of the International Conference on Mobile Adhoc and Sensor Networks. 2005

[26] Navrati S, Abhishek R, Jitae S. Dynamic duty cycle and adaptive contention window based QoS-MAC protocol for wireless multimedia sensor networks[J]. Computer Networks, 2008, 52(13): 2532-2542

[27] Schaar M V D, Shankar S. Cross - layer wireless multimedia transmission: Challenges, principles and new paradigms [J]. IEEE Wireless Commun, 2005, 12(4): 50-58

[28] Pynadath E S, Kondi L P. Cross-layer Optimization with Power Control in DS-CDMA Visual Sensor Networks[C]// IEEE International Conference on Image Processing (ICIP). 2006: 25-28

[29] Setton E, Yoo T, Zhu X, et al. Cross layer design of ad hoc networks for real-time video streaming[J]. IEEE Wireless Communications, 2005, 12(4): 59-65

(上接第 18 页)

[2] Rao J R, et al. Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards[C]// IEEE Symposium on Security and Privacy. 2002: 31-41

[3] Schuster A. Differential Power Analysis of an AES Implementation[R]. IAIK-TR2004/06/25. Http: // www. iaik. tu-graz. ac. at/research/sca-lab/index. php, 2004

[4] Chu jie, Zhao qiang, et al. Differential Power Analysis for Cryptographic ICs[C]// ICEMI'2007. 2007: 291-295

[5] 邓高明，陈开颜，张鹏，等. 差分功率分析仿真中的功率消耗模型[J]. 计算机工程，2007，33(14)：239-246

[6] 陈开颜，赵强，褚杰，等. 差分功耗分析单片机 DES 加密实现的旁路攻击[J]. 计算机科学，2007，34(11)：58-61

[7] Kocher P, Jaffe J, Jun B. Differential power analysis[A]// Advanced in Cryptology-CRYPTO' 99 [C]. California, USA: Springer Verlag, 1999: 388 - 397

[8] Bucci M, et al. A Power Consumption Randomization Coun- termeasure for DPA-Resistant Crypto- graphic Processors[C]// Integrated Circuit and System Design, LNCS 3254. 2004: 481- 490

[9] OKeya K, Miyazaki K, Sakurai K. A Fast Scalar Multipli- cation Method with Randomized Projective Coordinates on a Montgomery-Form Elliptic Curve Secure against Side Channel Attacks[C]// ICICS 2002. LNCS 2288. 2002: 428-439

[10] Chang H, Kim K. Securing AES against Second-order DPA by Simple Fixed-Value Masking[C]// CSS- 2003. 2003(15): 145-150

[11] 韩军，曾晓洋，汤庭鳌. RSA 密码算法的功耗轨迹分析及其防御措施[J]. 计算机学报，2006，29(4)：590- 596

[12] 赵佳，曾晓洋，韩军，等. 抗差分功耗分析攻击的 AES 算法的 VLSI 实现[J]. 计算机研究与发展，2007，44(3)：378-383

[13] 蒋惠萍，毛志刚. 一种抗差分功耗攻击的改进 DES 算法及其硬件实现[J]. 计算机学报，2004，27(3)：334- 338

[14] 童元满，戴葵，陆洪毅，等. 基于细粒度任务调度的防功耗分析模幂方法[J]. 计算机工程，2006，32(24)：15-16

[15] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential logic with signal independent power consumption to withstand differential power analysis on smartcards[C]// Proc. of the 28th European Solid State Circuits Conf. 2002: 403-406

[16] Macdonald. A balanced-power domino-style standard cell library for fine-grain asynchronous pipelined design to resist differential power analysis attacks [D]. Boston: Master thesis of Boston Univesity, 2005

[17] Ratanpal G B, Williams R D, Blalock T N. An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks[J]. IEEE Tran on Dependable and Secure Computing, 2004, 1(3): 179-189

[18] 李翔宇，孙义和. 用于密码芯片抗功耗攻击的功耗平衡加法器[J]. 半导体学报，2005，26(8)：1629- 1634

[19] 童元满，王志英，戴葵，等. 基于动态双轨逻辑的抗功耗攻击安全芯片半定制设计流程[J]. 小型微型计算机系统，2007，28(5)：935-939

[20] Goubin L, Patarin J. DES and differential power analysis: the duplication method[A]// CHES[C]. 1999: 158-172

[21] Messerges T S. Securing the AES finalists against power analysis attacks[C]// Fast Software Encryption (FSE2000). New York, 2000: 150-164

[22] Akkar M L, Giraud C. An implementation of DES and AES, Secure against Some Attacks[A]// CHES2001[C]. Paris, France: Springer-Verlag, 2001: 309-318

[23] LAkkar M, Goubin L. A generic protection against high-order differential power analysis [C]// Fast Software Encryption (FSE2003) 2003. LNCS 2887. Springer-Verlag, 2003: 192-205

[24] Akkar M L, Bevan R, Goubin L. Two power analysis attacks against one mask methods [C]// Fast Software Encryption (FSE2004). LNCS3017. Springer-Verlag, 2004: 332-347

[25] Suzuki D, Saeki M, Ichikawa T. Random Switching Logic: A Countermeasure Against DPA Based on Transition Probability [EB/OL]. IACR eprint Archive (http: // eprint. iacr. org/). report 2004/346, 2004

[26] Tiri K, Verbauwhede I. Securing Encryption Algorithms Against DPA at the Logic Level Next Generation Smart Card Technology[C]// CHES 2003. LNCS2779. Springer, 2003: 125-136

[27] Popp T, Mangard S. Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints [C]// CHES 2005. Springer, 2005: 172-186

[28] Borst J. Block Ciphers: Design, Analysis and Side-chanel Analysis[D]. Katholieke Universiteit Leuven, September 2001

[29] Mangard S. Hardware Countermeasures Against DPA-A Statistical Analysis of Their Effectiveness [C]// CT-RSA 2004. LNCS2964. 2004: 222-235

[30] Mangard S. Securing Implementations of Block Ciphers against Side-channel Attacks[D]. IAIK. Graz University of Technology, 2004

[31] Tuyls P, et al. Read-proof Hardware from Protective Coatings [C]// CHES06. LNCS 4249. 2006: 369-383

[32] Bar-El H, Choukri H, Naccache D, et al. The Sorcerer's Apprentice Guide to Fault Attacks. Proceedings of the IEEE, 2006, 94(2): 370-382