

一种基于电磁分析的硬件木马旁路检测方法

张 鹏, 王新成, 周 庆

(信息保障技术重点实验室, 北京 100072)

摘 要: 为了应对集成电路在制造过程中可能被嵌入非法硬件木马所导致的安全性威胁, 提出一种利用芯片电磁旁路泄漏信息的硬件木马检测技术. 在对芯片表面进行区域划分的基础上, 采用随机选优算法生成硬件木马测试所需要的输入向量集; 利用相关性电磁分析技术, 有效分辨硬件木马电路与原始电路之间的旁路信号差异. 针对示例性 AES 硬件木马电路的检测实验表明, 该检测技术利用 9 000 个电磁信号样本, 成功地对硬件木马进行了存在性判定及区域定位.

关键词: 集成电路词; 硬件木马; 电磁分析; 木马检测

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2013)12-0014-04

A Hardware Trojans Detection Method Based on Electromagnetic Emission Analysis

ZHANG Peng, WANG Xin-cheng, ZHOU Qing

(Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: A novel hardware Trojans detection technique is proposed. This technique divides the surface of tested chip into some smaller sub-blocks, and generates a suitable input vector set with a special selection algorithm. Then the electromagnetic signals from hardware Trojan and genuine circuits could be distinguished effectively with correlation analysis. The detection experiment against an exemplary AES hardware Trojan circuit showed that the technique proposed in this paper could detection the existence of the hardware Trojan and locate the region most responsible for the Trojan successfully with 9 000 samples.

Key words: integrate circuit; hardware Trojans; electromagnetic analysis; Trojans detection

1 引言

当前, 集成电路芯片已经渗透到现代科技的各个领域. 与此同时, 针对芯片的攻击行为也越来越普遍. 例如, 攻击者可以通过对芯片的原始设计进行更改, 嵌入所谓的“硬件木马”电路, 并在特定的激活条件下实现破坏性功能或泄漏芯片内部秘密信息^[1]. 一般来说, 硬件木马(以下简称木马)最可能的设计者有两类: 芯片原始设计者与芯片制造商. 对于前者, 其在正常设计阶段就留下后门, 并且受制于知识产权保护, 其硬件设计细节并不公开. 因此, 除非出现不良后果, 对这种木马的检测几乎不可进行. 此

外, 为了追求经济利益, 芯片的设计与制造过程分离事实上不可避免, 芯片在外包制造过程中, 部分不可信制造商可能更改设计并嵌入木马. 由于原始电路与木马电路之间存在功能与结构差异, 因此可能通过这些差异来检测木马.

木马检测是一项困难的工作, 一般使用三种方法^[2]: 一是利用电子显微扫描等复杂的故障分析技术. 对设备要求高, 代价昂贵, 有些是破坏性检测并且对于纳米级的芯片可能失效. 二是利用标准的VLSI故障检测工具, 例如自动检测模式生成器(ATPG)进行仿真测试以发现木马. 但是对于激活条件非常独特的木马来说, 很难生成激活模式. 而未

收稿日期: 2013-02-20; 修回日期: 2013-04-07

基金项目: 中国博士后科学基金项目(2012M512073)

激活的木马电路同原始电路仿真功能完全相同,无法分辨.并且对于不改变正常输出(例如通过隐蔽通道泄漏信息)的木马来说完全失效.三是通过旁路(Side Channel)信号分析.利用原始电路与木马电路之间旁路测量信号的差异来检测木马.例如,利用子空间映射技术来检测旁路信号差异^[3],利用功耗分析^[4]、路径延迟分析^[5]进行木马检测等.这是当前最有前途的一类检测方法^[6].

本文提出一种新的硬件木马旁路检测技术.采用芯片区域划分方式,对每个区域利用有效的测试激励向量生成技术来增强木马激活或部分激活效果,并利用相关性电磁旁路分析技术对木马电路进行辨别,从而检测并精确定位木马.

2 区域划分与测试向量生成

一般对于检测者来说,木马的完全激活非常困难.但是许多木马需要监控激活条件,因此有部分电路始终处于激活状态.由于木马电路一般结构小巧,其产生的旁路效应往往淹没在整个电路的效应之中.本节采用分而治之的方式,对芯片区域进行划分,尝试对木马进行分离,并生成特殊的激励向量,在增强木马部分旁路信号的同时,抑制其它电路部分的旁路信号,从而最大化木马的旁路效应.

2.1 区域划分

根据电磁测量时探头可以在芯片表面进行精确定位的特点,将整个芯片表面划分成不同区域,如图1所示.

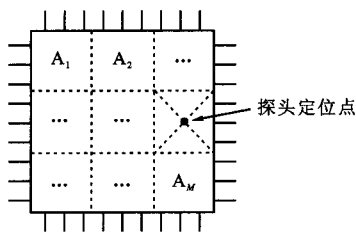


图1 芯片表面区域划分示意图

图1将整个芯片表面共划分为M个区域,硬件木马可能分布在其中1个或多个区域之中.每个区域的中心位置作为电磁探头的测量定位点.

2.2 测试向量生成

对于每一个芯片区域,我们选择一组测试需要的激励向量.选取原则是使得当前区域的电磁辐射信号与其他区域相比差别较大,从而导致当前区域的电磁辐射效应在整个电路效应中凸显出来.如果当前区域中存在硬件木马,硬件木马信号效应相应得以增强.

测试向量集详细生成步骤描述如下:

Step 1. 随机选择D个不同输入,记为向量 $\mathbf{d} = (d_1, d_2, \dots, d_D)^T$,在每一个区域,分别测量芯片在进行D次运算时的电磁泄漏.令 $\mathbf{t}_{a,i} = (t_{a,i,1}, t_{a,i,2}, \dots, t_{a,i,T})$ 表示在区域a,输入 d_i 对应的电磁泄漏轨迹,其中T代表轨迹长度.则全部电磁轨迹可表示为 $M(M$ 为区域总数)个 $D \times T$ 的矩阵 $\mathbf{T}_a = (t_{a,1}, t_{a,2}, \dots, t_{a,D})^T$.

Step 2. 对于区域a,输入 d_i 计算当前电磁信号与其他区域同输入对应电磁信号的差异如下:

$$\text{dif}_{a,i} = \sum_{\substack{a'=1 \\ a' \neq a}}^M \sum_{t=1}^T (t_{a,i,t} - t_{a',i,t})^2 \quad (i = 1, 2, \dots, D) \quad (1)$$

对于所有区域,可得到 $M \times D$ 的矩阵 $\mathbf{DIF} = (\text{dif}_1, \text{dif}_2, \dots, \text{dif}_M)^T$,其中 $\mathbf{dif}_a = (\text{dif}_{a,1}, \text{dif}_{a,2}, \dots, \text{dif}_{a,D})$.

Step 3. 从矩阵 $\mathbf{DIF}$ 的每个行向量中分别选取最大的n个元素,其对应输入作为相应区域的测试向量集.

通过上述步骤,最终可以生成 $M \times n$ 个元素组成的测试向量集,每个芯片区域分别对应n个输入.

3 相关性电磁分析

电磁分析(Electromagnetic analysis, EMA)^[7]作为一种有效的旁路攻击(Side Channel Attacks)技术,已经得到了较为广泛的应用.其中相关性电磁分析(Correlation EMA)^[8]一般是指利用芯片在运行密码算法时实际测量的电磁信号与通过密钥猜测获得的电磁信号之间的相关性大小来判断获取密钥.本文将这种思想进行延伸,利用原始电路与待测试电路之间的电磁信号相关性来判断测试电路之中是否存在木马.其思路是:对于原始电路与测试电路的相同区域,应用相同的激励向量进行测试并分别记录电磁辐射信号曲线,如果测试电路该区域中不存在木马,则两次电磁曲线应该具有很高的相关性,否则由于木马电路的影响,两者的相关性会很低.

为了量化两次电磁曲线之间的相关性,可以应用Pearson相关系数法.若令 $\mathbf{o} = (o_1, o_2, \dots, o_l)$ 和 $\mathbf{t} = (t_1, t_2, \dots, t_l)$ 分别表示对原始电路与测试电路的电磁辐射进行离散采样形成的电磁轨迹曲线,其中l为轨迹长度,则两者的相关性可估计如下:

$$\text{COR} = \frac{\sum_{i=1}^l (o_i - \bar{o}) \cdot (t_i - \bar{t})}{\sqrt{\sum_{i=1}^l (o_i - \bar{o})^2 \cdot \sum_{i=1}^l (t_i - \bar{t})^2}} \quad (2)$$

式中, $\bar{o}$ 和 $\bar{t}$ 分别表示 o 与 t 的均值.

为了降低噪声的影响,采用平均化去噪技术,包括两个层次:一是选择多个测试向量;二是对每个测试向量多次重复实验采样,取均值后再求相关性.对某个区域进行的电磁分析见算法 1.在算法 1 中,计算轨迹平均值函数 $MEAN()$ 是把多条电磁轨迹上的点对应相加然后分别求均值.若对于所有的区域,算法 1 给出的输出均为 NO(不存在木马),则认定测试电路是安全的,否则判定存在木马,并可定位该区域.

算法 1 相关性电磁分析 CorrelationEMA

输入:当前区域测试向量 $VectorSet[1..n]$, 单向量样本量 $SampleNum$,

相关性阈值 $CorrelationThreshold$

输出: YES/NO

Function $CorrelationEMA (VectorSet[1..n],$

$SampleNum, CorrelationThreshold)$

{ for ($i=1; i \leq n; i++$)

{ for ($j=1; j \leq SampleNum; j++$)

{ $OriginalEMTrace[j] = MonitorOriginalCircuitRun (VectorSet[i]);$

$TestEMTrace[j] = MonitorTestCircuitRun (VectorSet[i]);$

} //以上获取 $SampleNum$ 条原始电路与测试电路运行的电磁轨迹矩阵

$OriginalMean[i] = MEAN(OriginalEMTrace[SampleNum]);$

$TestMean[i] = MEAN(TestEMTrace[SampleNum]);$ //计算轨迹平均值

$CorrelationCoefficient[i] = COR(OriginalMean[i], TestMean[i]);$

} //以上计算第 i 个测试向量得到的相关性

$FinalCorrelation=0;$

for ($i=1; i \leq n; i++$)

$FinalCorrelation = FinalCorrelation + CorrelationCoefficient[i];$

$FinalCorrelation = FinalCorrelation/n;$ //通过 n 个向量得到的平均相关性

if $FinalCorrelation > CorrelationThreshold$

//阈值判断

RETURN(NO);

else RETURN(YES);

}

4 木马电路检测实验

4.1 木马电路

实验针对一个示例性木马电路,如图 2 所示.原始电路是一个 AES-128 加密器,木马部分核心是一个比较器,当明文输入为“F0F0F0F0F0F0F0F0”(可任选)时,木马激活并将密钥直接写入密文,此时敌手可直接通过输出端得到密钥.由于木马激活基于特定的明文输入,因此在功能测试时无意激活木马的概率($1/2^{128}$)很低.

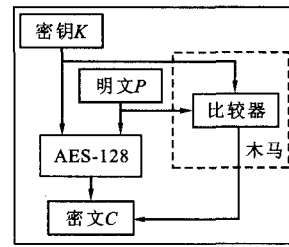


图 2 木马电路示意图

所有电路运行于 Xilinx 公司的 XC3S400 型 FPGA 上,设定运行频率 50 MHz.芯片表面积约 $3\text{ cm} \times 3.5\text{ cm}$,被划分为 9 个区域.测试芯片中的硬件木马通过区域约束技术约束到其中一个区域中.每个区域生成 20 个测试激励向量.

4.2 电磁信号采集

为进行电磁信号的采集,搭建了实验平台,如图 3 所示.在计算机上用 LabView 编写了虚拟仪器(VI),控制实验流程:首先通过 RS232 接口给 FPGA 提供选择的检测输入,当运行 AES 时,触发示波器记录磁场探头接收的电磁信号(采样率 1.25 G/s,采样时间 80 ns,每条轨迹共采样 100 个点),并控制示波器实时向计算机传输电磁波形数据.重复上述过程,控制输入所有的测试向量,直到采集到足够的样本.然后更改探头位置,从而实现所有区域的电磁信号数据采集.

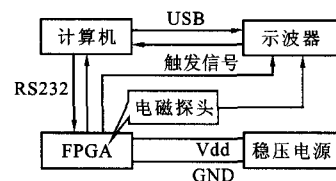


图 3 实验平台原理图

4.3 电磁信号分析

为了确定相关性阈值,首先对两个完全相同的原始电路进行多次实验,计算得到各个区域对应的相关性最小值.为了减少“不存在木马,而误报存在木马”这类错误的发生,确定相关性阈值为该最小值

的3/4.当测试电路与原始电路的电磁相关性小于相关性阈值时,判定电路中存在木马.

实际的木马电路测试中,对于9个区域,每个测试激励向量重复采样50次,全部电磁信号样本量为9 000.通过算法1得到木马电路与原始电路之间,除木马存在的区域外,其余区域的电磁相关性均大于预先确定的相关性阈值,从而成功判断存在木马并进行了区域定位.

5 结束语

通过分区域的测试激励向量生成技术,可以分离木马电路并相对增强木马的旁路信号活跃性;利用相关性电磁分析技术,可以有效分辨木马电路与原始电路之间的旁路信号差异.本文提出的硬件木马检测技术要求检测者拥有符合原始设计、安全可信的基准芯片,这可通过侵入式检测技术来实现.

参考文献:

- [1] Tehranipoor M, Koushanfar F. A survey of hardware trojan taxonomy and detection[J]. IEEE Design & Test of Computers, 2010, 27(1):10-25.
- [2] Wang X, Tehranipoor M, Plusquellic J. Detecting malicious inclusions in secure hardware: challenges and solutions[C]// 1st IEEE International Workshop on Hardware-Oriented Security and Trust (HOST). Anaheim, CA: IEEE Press, 2008:15-19.
- [3] Agrawal D, Baktir S, Karakoyunlu D, et al. Trojan

detection using IC fingerprinting[C]//IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Press, 2007: 296-310.

- [4] Koushanfar F, Mirhoseini A. A unified framework for multimodal submodular integrated circuits trojan detection[J]. IEEE Transactions on Information and Security, 2011, 6(1):162-174.
- [5] Jin Y, Makris Y. Hardware trojan detection using path delay fingerprint [C]//1st IEEE International Workshop on Hardware-Oriented Security and Trust (HOST). Anaheim, CA: IEEE Press, 2008:51-57.
- [6] 王晨旭,姜佩贺,喻明艳. 芯片级木马检测技术研究综述[J]. 半导体技术, 2012, 37(5):341-346.
- [7] Quisquater J J, Samyde D. Electromagnetic analysis (EMA): measures and counter-measures for smard cards [C]// Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001. Berlin/ Heidelberg, Springer, 2001:200-210.
- [8] 张鹏,邓高明,陈开颜,等. 针对 AES 密码芯片的远场相关性电磁分析攻击[J]. 华中科技大学学报:自然科学版, 2009:37(8):31-34.

作者简介:

张 鹏 男,(1976—),博士后,工程师.研究方向为芯片安全防护技术.

王新成 男,(1969—),博士,高级工程师.研究方向为集成电路芯片设计.

周 庆 男,(1964—),高级工程师.研究方向为信息安全技术.

(上接第13页)

- [2] Mahapatro J, Misra S, Manjunatha M, et al. Interference mitigation between WBAN equipped patients[C]// Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on. India: Indore, 2012:1-5.
- [3] Ameen M A, Liu J, Ullah S, et al. A power efficient MAC protocol for implant device communication in wireless body area networks[C]// Consumer Communications and Networking Conference (CCNC) USA: Nevada, IEEE, 2011:1155-1160.
- [4] IEEE standard for local and metropolitan area networks - Part 15. 6: wireless body area networks[S]. IEEE Std 802.15.6, 2012(29):1-271.
- [5] 孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社, 2005.
- [6] BaniYassein M, Al-zoubi A, Khamayseh Y, et al. Improvement on LEACH protocol of wireless sensor network (VLEACH)[J]. International Journal of Digital Content Technology and its Applications, 2009, 3(2):

132-136.

- [7] Wairagu G Richard. Extending LEACH routing algorithm for wireless sensor network[D]. Makerere University, Data Communications Engineering, 2009.
- [8] Meenakshi Sharma, Kalpana Sharma. An energy efficient extended LEACH (EEE LEACH)[C]// CSNT, 2012 International Conference on Communication Systems and Network Technologies. India: Gujarat, 2012: 377-382.
- [9] 刘铁流,巫咏群. 一种新的基于分簇的无线传感器网络多跳节能路由协议[J]. 信息与控制, 2012, 41(1):27-32.
- [10] 尚凤军. 无线传感器网络通信协议[M]. 北京:电子工业出版社, 2011.

作者简介:

孔令淑 女,(1989—),硕士研究生.研究方向为无线传感器网络.

姚向华 男,(1973—),博士,副教授.研究方向为无线传感器网络、现代检测技术.