·安全技术· 文章编号:1000-3428(2016)01-0128-05 文献标识码:A 中图分类号:TP391

集成电路中硬件木马防御技术研究

赵毅强,何家骥,杨 松,刘沈丰

(天津大学电子信息工程学院,天津 300072)

摘 要: 随着集成电路(IC)设计、制造、测试等环节相分离的趋势进一步增强,使得 IC 中被植入硬件木马的可能性增大。介绍硬件木马概念及危害,研究硬件木马防御技术,并从硬件木马检测和集成电路安全性设计 2 个方面进行阐述,分析硬件木马检测中的旁路分析技术、集成电路安全性设计中的电路增强设计技术。分析结果表明,为最大限度地保障集成电路的安全,设计者在电路设计时需考虑到电路的安全性问题,同时在芯片加工完成后开展硬件木马的检测工作。

关键词: 集成电路;硬件木马;防御技术;旁路分析;安全性设计

中文引用格式: 赵毅强,何家骥,杨 松,等. 集成电路中硬件木马防御技术研究[J]. 计算机工程,2016,42(1):128-132,137.

英文引用格式: Zhao Yiqiang,He Jiaji,Yang Song,et al. Research on Defense Technology Against Hardware Trojans in Integrated Circuits[J]. Computer Engineering,2016,42(1):128-132,137.

Research on Defense Technology Against Hardware Trojans in Integrated Circuits

ZHAO Yiqiang,HE Jiaji,YANG Song,LIU Shenfeng

(School of Electronic Information Engineering,Tianjin University,Tianjin 300072,China)

【Abstract】 With the further improvement of design,manufacture and test separation in Integrated Circuits(IC),hardware trojans can be implemented as modifications to IC,and it raises numerous concerns regarding possible threats. This paper briefly explains the concept of hardware trojans,and explains the countermeasures technology of hardware trojan attacks and the importance of conducting out the countermeasures against hardware trojans. Also it introduces the classification of the state-of-art countermeasures,deeply analyzes the side-channel analysis method and the design for security method. Analysis results show that the designers must consider circuit security problem in designing circuits in onder to the security of integrated circuits,meanwhile they begin test works ensure after chips are completed.

【Key words】 Integrated Circuits(IC);hardware trojans;countermeasures technology;side-channel analysis;security design

DOI: 10.3969/j.issn.1000-3428.2016.01.023

1 概述

自 2007 年硬件木马的概念由 Agrawal D 提出以来[1],国内外学术界对硬件木马相关的技术开展了广泛而深入的研究[2-5],硬件木马是指在集成电路设计或制造过程中对电路的恶意篡改[2],由于目前集成电路设计与制造过程相分离,以及大量第三方设计(IP 等)的使用,使得集成电路在设计或者制造过程中可能被植入硬件木马。一旦硬件木马激活,改变电路的原始功能,破坏电路;或者形成硬件后门,泄露电路中的敏感信息;或者改变电路的工作状态,使电路加速失效等[6-7]。同时硬件木马是一种实体的电路结构,一旦芯片制作完成,硬件木马将会长久存在,因此开展有关硬件木马防御技术的研究显得尤为重要。

目前集成电路的防御技术主要集中在 2 个方面:(1)硬件木马检测技术;(2)集成电路安全性设计技术。本文对硬件木马防御技术进行介绍,分析各种方法的原理、优势及挑战及旁路分析技术和电路增强设计技术,展望硬件木马防御技术的发展

基金项目: 国家自然科学基金资助项目"无参考模型的硬件木马检测技术研究"(61376032);天津市自然科学基金资助重点项目"硬件木马检测技术的研究"(12JCZDJC20500)。

作者简介: 赵毅强(1964-),男,教授、博士生导师,主研方向为信息安全、集成电路可靠性研究;何家骥、杨 松、刘沈丰,硕士研究生。

收稿日期: 2014-12-04 **修回日期:** 2015-02-03 **E-mail:** yq_zhao@tju.edu.cn

趋势。

2　硬件木马检测技术

由于硬件木马本身具有隐蔽性、功能多样性、难激活等特点[2-3],通过一般的方法往往难以发现硬件木马的存在,硬件木马检测尚未形成成熟的检测体系,是学术界研究的热点。根据是否对待测芯片产生破坏性影响,分为破坏性检测方法和非破坏性检测方法两大类。破坏性检测方法以基于反向解剖技术的检测方法为代表,非破坏性检测方法包括逻辑功能测试、旁路分析技术等方法,如图 1 所示。

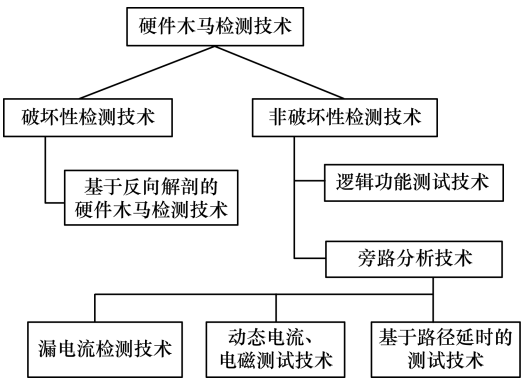
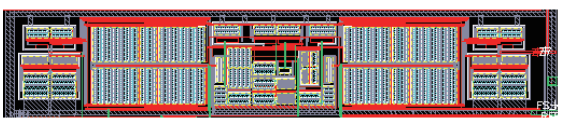


图 1　硬件木马检测技术分类

2.1　基于反向解剖的硬件木马检测

目前绝大多数的芯片都是基于 CMOS 工艺实现的,因而可以通过去除芯片封装后,使用高倍显微镜等对芯片进行拍照,然后借助逆向分析工具对照片进行分析处理,还原实际芯片版图,并与原始版图进行比对分析,判断是否存在硬件木马电路[2,8-9],图 2 为实际芯片版图和原始设计版图的对比。该方法对于规模较小的芯片,硬件木马的检出率理论上可以达到 100% ,但该方法是一种破坏性的检测方法,同时需要耗费大量的人力物力,随着集成电路工艺的飞速发展,工艺尺寸日益减小,甚至超过了现有精密设备的观察范围,无法成为主流的硬件木马检测方法。

(a)去除封装后的版图



(b)原始设计的版图

图 2　去除封装后版图照片与原始设计版图对比

2.2　逻辑功能测试

逻辑功能测试技术,是一种基于自动测试模式生成(Automatic Test Pattern Generation,ATPG)的硬件木马检测方法,该方法通过在电路输入端口输入特定的激励信号,观测电路的输出是否与预期的输出相符合[2],如果发现异常,则判断电路中存在硬件木马[10-11]。由于大部分硬件木马只在特定的条件下才能被激活,同时电路规模越来越大,因此必须要根据一定的算法来产生测试向量,提高测试向量对于电路的覆盖率和硬件木马的激活概率[12]。该方法在检测组合逻辑电路时具有较好的效果,但是对于包含大量时序逻辑的电路,检测效果往往不理想。

2.3　旁路分析

硬件木马的存在,会使原始电路的电路结构发生改变,进而会对电路的旁路信息产生影响,例如漏电流、动态电流、电磁辐射、电路关键路径延迟等,通过一定的算法对获取到的母本电路和待测电路旁路信息进行对比,发现旁路信息间的差异,可以实现硬件木马的检测,由于该方法具有检测精度高、条件限制少等优点,已经成为硬件木马检测领域的研究热点。

(1)漏电流测试技术

硬件木马会使原始的电路结构发生变化,额外电路的增加势必会导致漏电流的增加[13-14]。由于硬件木马一般占原始电路面积比例很小,导致硬件木马对电路漏电流的影响也很小,文献[14]提出一种多芯片同时测量漏电流的方法,测试者将多个芯片的漏电流测试点通过一定的方式进行连接,测量这些芯片的漏电流总和,来放大单个芯片漏电流的变化,如图 3 所示,通过测试电路,将待测芯片上面的漏电流测试点连接起来,统一进行测试。

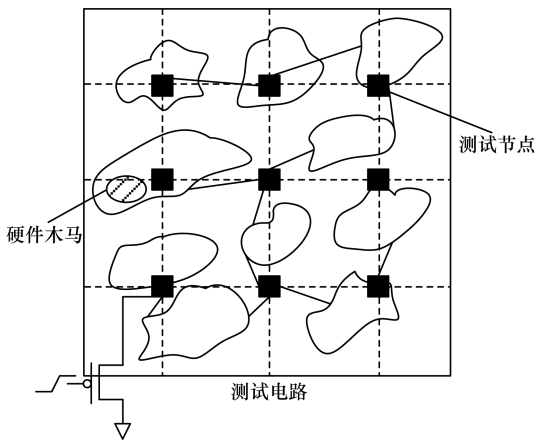


图 3　多芯片串联漏电流测试

(2)动态电流、电磁测试技术

动态电流测试技术关注电路在运行过程当中的动态电流(I_{DDT})变化,用来反映电路内部的活动情况。利用该方法进行硬件木马检测,需要硬件木马在电路的运行过程中激活,为了提高测试过程中硬件木马的电流贡献比,研究者开展了相关的研究,可以通过电源门控等技术[15],减小原始电路的电流,进而放大硬件木马电流的影响;硬件木马在正常电路当中所占的比重较小,其功耗占整个电路的功耗

也非常有限,文献[16]将电路划分为 5 个部分,对于选定的区域电路,通过选取特定的激励向量,最大程度激活所选取的电路区域,提高硬件木马功耗在其中的比重。同时研究者开发了多种数据处理算法,用来提高信噪比同时提取测试数据当中的电流主要特征[17]。

由于硬件木马的存在,电路在运行过程中的电磁辐射会发生变化,国内外研究者在利用电磁旁路信号进行硬件木马检测方面做出了较深入的研究[18]。文献[18]提出一种基于区域划分的硬件木马检测的方法,如图 4 所示,首先将电路平均划分成 M 部分,针对每个部分单独产生测试向量并进行电磁测试,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,从而使当前区域的电磁辐射效应在整个电路效应中凸显出来,来实现硬件木马检测。

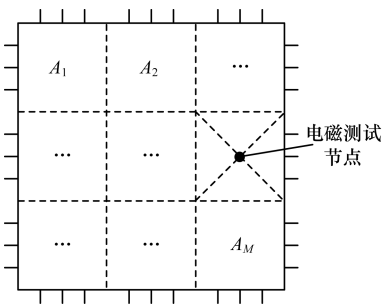


图 4 分块电磁测试

(3)基于路径延迟的检测

由于硬件木马的植入会对原始电路结构造成影响,电路中某些路径的时间延迟会因此而发生改变,基于路径延迟的硬件木马检测方法也成为了研究的热点[2,19]。文献[19]首先根据母本电路整体的延时,形成其指纹信息,然后与待测芯片的电路延时信息进行比对,发现了电路中硬件木马的存在。文献[20]通过在电路当中插入“影子寄存器”,采用与母本电路相同频率但不同相位的时钟 CLK2 进行驱动,在电路末端通过一个比较器进行比较,对比母本电路和“影子寄存器”的延时信息,用来判断母本电路是否受到了硬件木马的影响,如图 5 所示。

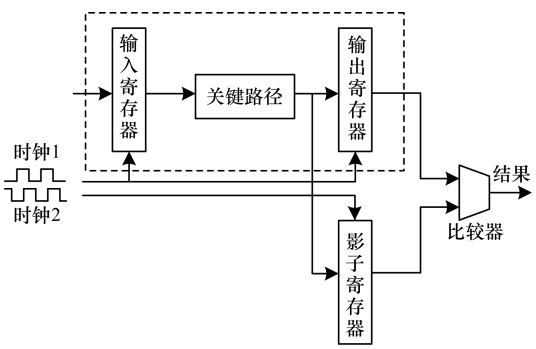


图 5 影子寄存器结构

旁路分析的硬件木马检测方法最终都要进行旁路信息的对比分析,发现不同数据之间的差异。目前研究者提出的处理方法主要分为 2 类:一类是基于降维和特征提取的方法,主要包括投影寻踪技术、K-L 变换、主成分分析等方法;另一类是基于判别和分类决策的方法,包括相关性分析、支持向量机、马氏距离等方法。第 1 类方法能够实现高维数据的降维、压缩,完成数据主要特征的提取,第 2 类方法通过衡量数据的特征属性,区分不同的数据样本,实现硬件木马的检测。

3 安全性设计技术

在芯片加工完成之后,开展硬件木马的检测工作,可以在一定程度上保证集成电路的可靠,但是不能防止硬件木马的植入,为了进一步增强集成电路的安全性,需要电路设计者在开展芯片设计的同时兼顾硬件木马的抗植入等技术,即集成电路安全性设计技术,主要分为 3 个方向:(1)安全性设计以防止硬件木马植入;(2)安全性设计片上实时监测结构;(3)安全性设计电路增强技术。

3.1 防止硬件木马植入的安全性设计

硬件木马的植入主要发生在代工厂或者一些不可信的第三方设计(IP 核)当中,针对以上 2 种情况,防止硬件木马植入的安全性设计主要分为电路模糊技术以及后版图填充技术。电路模糊技术是一种通过对电路的功能或结构进行模糊处理[21-22],使得攻击者很难发现原始电路的特征,提高了植入硬件木马的难度。后版图填充技术是一种通过填充版图当中没有用到的空余空间,来降低硬件木马植入的可能性。文献[23]提出一种 BISA 技术,可以填满芯片当中未被利用的空间,使得硬件木马的植入变得尤其困难,如图 6 所示。其中,图 6(a)表示原始的电路布局布线,很明显电路当中存在较多的空余空间,图 6(b)表示通过一定的算法识别出版图当中的空余空间,通过将图 6(c)所示的电路结构填充到原始设计的空余位置,最终形成图 6(d)所示的版图。

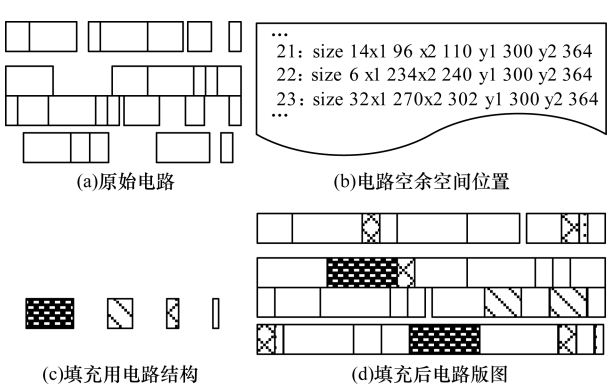


图 6 版图填充技术

3.2　实时监测技术

利用 SM 结构对电路行为进行的实时监测如图 7所示。

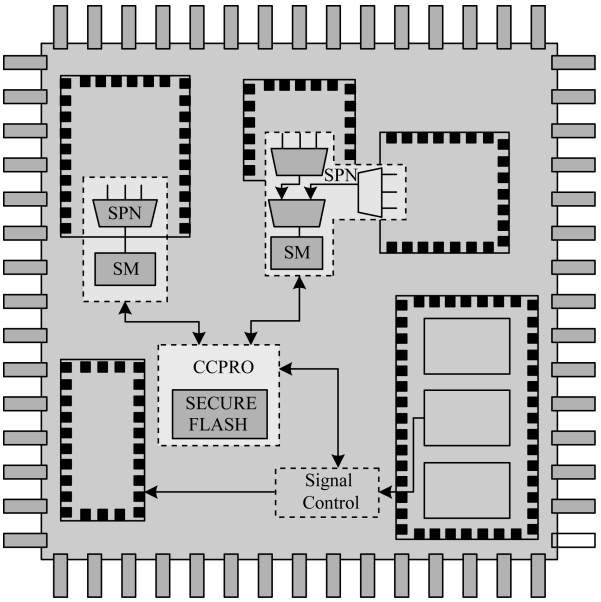


图 7　基于 SM 结构的实时监测

实时监测技术通过在芯片当中植入一定的安全结构,对电路状态进行实时监测,一旦发现电路的异常动作,将会采取封闭电路信息通道、关闭电路等安全措施,防止硬件木马的危害进一步扩大。文献[24]提出一种在 SoC 芯片上植入安全监控(Security Monitor,SM)的结构,不仅可以监控电路在运行过程中出现的异常状态,而且可以监测内存的非正当存取等功能,实现对电路行为的实时监测,如图 7 所示,首先通过信号探测网络(Signal Probe Network,SPN)模块选择待监测的信号,然后将该信号传递给 SM 结构,最后通过配置和控制处理器(Configuration and Control Processor,CCPRO)模块进行监测信号的整合和分析。

3.3　电路增强设计技术

利用片上安全结构,可以进行硬件木马检测,或者借用安全结构增强其他检测方法的有效性。基于路径延时等旁路分析的方法受测试噪声等的影响较大,阻碍测试精度的进一步提高,文献[25]提出一种基于片上环形振荡器环形振荡器(Ring Oscillator,RO)的电路安全结构,如图 8 所示。

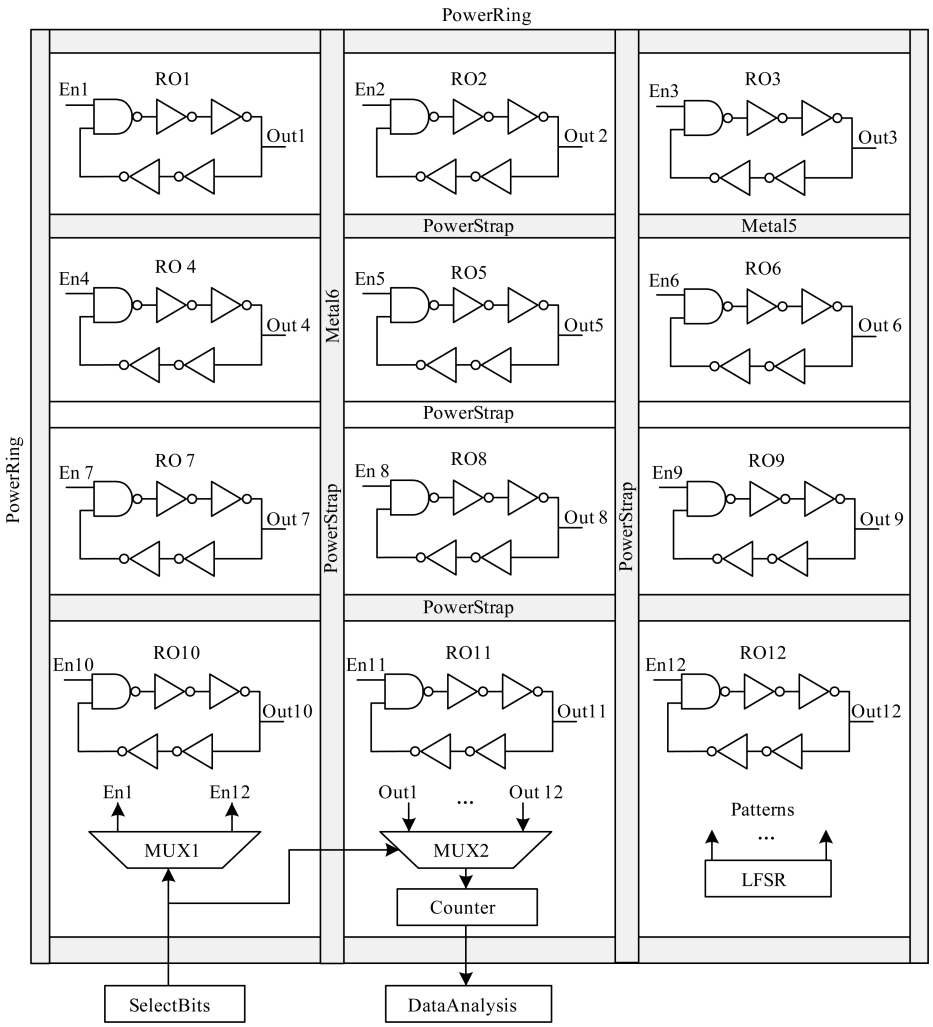
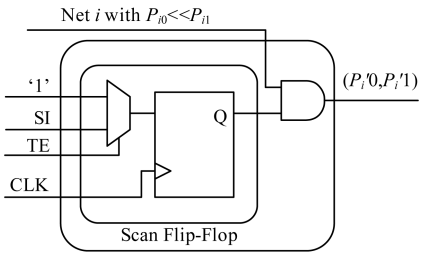


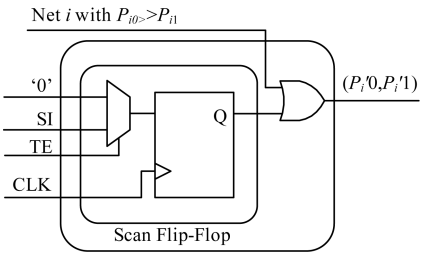
图 8　环形振荡器监测功耗变化

如果电路当中存在硬件木马,一旦木马激活,会导致功耗的增加,通过在电路的电源环上加入 RO 结构,可以直接有效地测得电路的功耗变化,进而判断是否存在硬件木马。

硬件木马多是利用电路当中的稀有翻转节点进行触发的,如果能够在设计阶段减少电路中的稀有翻转节点,有助于防止硬件木马的植入或者提高硬件木马的激活概率。文献[26]提出一种“虚拟触发器”,在电路设计完成后,通过分析找出电路当中的稀有翻转节点,然后植入该结构,能够有效地提高电路当中稀有节点的翻转概率,如图 9 所示。其中,图 9(a)为当电路节点出现 0 的概率远远小于 1 的情况;图 9(b)为当电路节点出现 1 的概率远远小于 0 的情况。



(a)与-虚拟触发器



(b)或-虚拟触发器

图 9 虚拟触发器提高节点翻转概率

4 结束语

在硬件木马检测技术中,基于旁路分析的检测方法已成为重要的研究方向,但是该方法无法脱离对于母本电路的依赖,因此,需开展无参考模型的检测技术研究。安全性设计技术在防止硬件木马植入和电路增强方面起到了一定的作用,但是安全性设计的结构普遍存在对电路覆盖率较低、需要引入较大额外面积等问题。本文介绍硬件木马概念及危害,研究硬件木马防御技术。研究结果表明,为保障集成电路的安全,在设计阶段考虑电路的安全问题,加入安全性结构,同时在芯片加工完成后进行硬件木马检测工作。

参考文献

[1] Agrawal D,Baktir S,Karakoyunlu D,et al. Trojan Detection Using IC Fingerprinting[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C. ,USA:IEEE Press,2007:296-310.

[2] Tehranipoor M, Koushanfar F. A Survey of Hardware Trojan Taxonomy and Detection[C]//Proceedings of IEEE Conference on Design & Test of Computers. Washington D. C. ,USA:IEEE Press,2009:10-25.

[3] Bhunia S,Hsiao M S,Banga M,et al. Hardware Trojan Attacks: Threat Analysis and Countermeasures[J]. Proceedings of the IEEE,2014,102(8):1229-1247.

[4] 刘长龙,赵毅强,史亚峰,等. 基于相关性分析的硬件木马检测方法[J]. 计算机工程,2013,39(9):183-185,189.

[5] 冯紫竹,赵毅强,刘长龙. 一种基于时序型硬件木马的 IP 版权保护结构[J]. 计算机工程,2014,40(9):19-22.

[6] Rostami M, Koushanfar F, Rajendran J, et al. HardwareSecurity:Threat Models and Metrics[C]//Proceedings of International Conference on Computer-aided Design. Washington D. C. ,USA:IEEE Press,2013:819-823.

[7] Sunar B. Rise of the Hardware Trojans[C]// Proceedings of the 17th IEEE International On-line Testing Symposium. Washington D. C., USA: IEEE Press,2011:138-138.

[8] Moore T,Jarvis J. FailureAnalysis and Stress Simulation in Small Multichip BGAs[C]//Proceedings of the 38th IEEE International Reliability Physics Symposium. Washington D. C. ,USA:IEEE Press,2000:217-224.

[9] 罗宏伟. 集成电路芯片安全隐患检测技术[J]. 半导体技术,2008,32(12):1094-1097.

[10] Chakraborty R S,Wolff F,Paul S,et al. MERO:AStatistical Approach for Hardware Trojan Detection[C]//Proceedings of CHES'09. Berlin,Germany:Springer,2009:396-410.

[11] Jha S. Randomization Based Probabilistic Approach to Detect Trojan Circuits[C]//Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium. Washington D. C. ,USA:IEEE Press,2008:117-124.

[12] Banga M,Chandrasekar M,Fang L,et al. Guided Test Generation for Isolation and Detection of Embedded Trojans in Ics[C]//Proceedings of the 18th ACM Great Lakes Symposium on Very Large Scale Integration. New York,USA:ACM Press,2008:363-366.

[13] Cao Yuchen, Zhou Yongbin, Yu Zhenmei. On the Negative Effects of Trend Noise and Its Applications in Side-channel Cryptanalysis[J]. Chinese Journal of Electronics,2014,23(2).

[14] Aarestad J,Acharyya D,Rad R,et al. Detecting Trojans Through Leakage Current Analysis Using Multiple Supply Pads[J]. IEEE Transactions on Information Forensics and Security,2010,5(4):893-904.

[15] Narasimhan S,Du D,Chakraborty R S,et al. Hardware Trojan Detection by Multiple-parameter Side-channel Analysis[J]. IEEE Transactions on Computers,2013,62(11):2183-2195.

[16] Banga M,Hsiao M S. ARegion Based Approach for the Identification of Hardware Trojans[C]//Proceedings of IEEE International Workshop on Hardware-oriented Security and Trust. Washington D. C., USA: IEEE Press,2008:40-47.

(下转第 137 页)

由实验结果可以看出,当丢失率为 80% 时,本文方法的检测效率均高于 IIPS-CM 协议;当丢失率为 0.1% 时,2 种方法检测效率差别不大。在相同丢失率的情况下,本文方法的检测效率是稳定的,不随丢失标签数量变化而变化。

综上分析,在不同的标签丢失率和丢失数量下,本文方法中单个标签的平均检测时间减少,具有更高的检测效率,且检测性能具有较好的稳定性。

7　结束语

通过对历史检测信息进行迭代识别,本文提出一种丢失 RFID 标签的快速检测方法。实验结果证明,相比于已知最高检测效率的 IIPS-CM 协议,本文方法具有更高的性能。下一步工作将探索如何进一步提高丢失 RFID 标签检测方法的效率。

参考文献

[1] 颜　元,武岳山,熊立志. RFID 系统多标签碰撞检测方法探索与测试[J]. 移动通信,2011,35(15):35-39.

[2] 刘　丹,魏　鹏,谭　杰,等. 一种 RFID 多标签碰撞检测方法[J]. 小型微型计算机系统,2009,30(9):1890-1894.

[3] 胡玲敏. RFID 系统的防碰撞算法研究[D]. 杭州:杭州电子科技大学,2012.

[4] Luo Wen, Chen Shigang, Qiao Yan, et al. Missing-tag Detection and Energy-time Tradeoff in Large-scale RFID Systems with Unreliable Channels [J]. IEEE/ACM Transactions on Networking, 2014, 22(4): 1079-1091.

[5] Khanam S, Mahbub M, Mandal A, et al. Improvement of RFID Tag Detection Using Smart Antenna for Tag Based School Monitoring System [C]//Proceedings of International Conference on Electrical Engineering and Information & Communication Technology. Washington D. C., USA: IEEE Press, 2014: 1-6.

[6] Chawla V, Dong Sam-Ha. An Overview of Passive RFID[J]. IEEE Communications Magazine, 2007, 45(9): 11-17.

[7] 张士庚,刘光亮,刘　璇,等. 大规模 RFID 系统中一种能量有效的丢失标签快速检测算法[J]. 计算机学报,2014,37(2):434-444.

[8] Zhang Rui, Liu Yunzhong, Zhang Yanchao, et al. Fast Identification of the Missing Tags in a Large RFID System [C]//Proceedings of the 8th Annual Communication Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks. Washington D. C., USA: IEEE Press, 2011: 278-286.

[9] 刘金艳,冯全源. 无线射频识别多标签防碰撞算法综述[J]. 计算机集成制造系统,2014,20(2):440-451.

[10] 周　清. 射频识别(RFID)技术中防碰撞算法的研究[D]. 无锡:江南大学,2012.

[11] 吴　楠. 一种树型结构的 RFID 防碰撞算法研究[D]. 长春:吉林大学,2014.

[12] Li Tao, Chen Shigang, Ling Yibei. Identifying the Missing Tags in a Large RFID System [C]//Proceedings of the 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York, USA: ACM Press, 2010: 1-10.

[13] Tan C C, Sheng Bo, Li Qun. How to Monitor for Missing RFID Tags[C]//Proceedings of the 28th International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2008: 295-302.

[14] Ma Cunqing, Lin Jingqiang, Wang Yuewu. Efficient Missing Tag Detection in a Large RFID System[C]// Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK: [s. n.], 2012: 185-192.

[15] NXP Semiconductors. I-code Smart Label RFID Tags[EB/OL]. (2004-01-30). http://www.nxp.com/documents/data_sheet/SL092030.pdf.

编辑　顾逸斐

(上接第 132 页)

[17] 刘长龙,赵毅强,史亚峰,等. 基于侧信道分析的硬件木马建模与优化[J]. 华中科技大学学报:自然科学版,2013,41(2):53-57.

[18] 张　鹏,王新成,周　庆. 基于电磁辐射信号分析的芯片硬件木马检测[J]. 电子学报,2013,42(2):341-346.

[19] Kumar P, Srinivasan R. Detection of Hardware Trojan in SEA Using Path Delay [C]//Proceedings of IEEE Conference on Electrical, Electronics and Computer Science. Washington D. C., USA: IEEE Press, 2014: 1-6.

[20] Li J, Lach J. At-speed Delay Characterization for IC Authentication and Trojan Horse Detection [C]// Proceedings of IEEE International Workshop on Hardware-oriented Security and Trust. Washington D. C., USA: IEEE Press, 2008: 8-14.

[21] Chakraborty R S, Bhunia S. Security Against Hardware Trojan Attacks Using Key-based Design Obfuscation[J]. Journal of Electronic Testing, 2011, 27(6): 767-785.

[22] Schrittwieser S, Katzenbeisser S, Kieseberg P, et al. Covert Computation——Hiding Code in Code Through Compile-time Obfuscation[J]. Computers & Security, 2014, 42(1): 13-26.

[23] Xiao K, Tehranipoor M. BISA: Built-in Self-authentication for Preventing Hardware Trojan Insertion[C]//Proceedings of IEEE International Workshop on Hardware-oriented Security and Trust. Washington D. C., USA: IEEE Press, 2013: 45-50.

[24] Bhunia S, Abramovici M, Agrawal D, et al. Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution[J]. IEEE Design & Test, 2013, 30(3): 6-17.

[25] Zhang X, Tehranipoor M. RON: An On-chip Ring Oscillator Network for Hardware Trojan Detection[C]// Proceedings of DATE'11. Washington D. C., USA: IEEE Press, 2011: 1-6.

[26] Salmani H, Tehranipoor M, Plusquellic J. A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time[J]. IEEE Transactions on Very Large Scale Integration Systems, 2012, 20(1): 112-125.

编辑　索书志