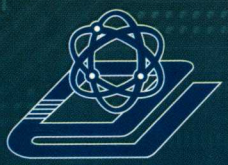

装备科技译著出版基金

Secure Integrated Circuits and Systems

安全集成电路与系统

[比利时] 因格里德·M·R· 维鲍维迪 主编

李雄伟 陈开颜 张阳 谢方方 李艳 王晓晗 译

国防工业出版社
National Defense Industry Press

Springer

装备科技译著出版基金

安全集成电路与系统

Secure Integrated Circuits and Systems

[比利时]因格里德·M·R·维鲍维迪 主编

李雄伟 陈开颜 张 阳 谢方方 李 艳 王晓晗 译

国防工业出版社

著作权合同登记　图字:军-2016-058 号

图书在版编目(CIP)数据

安全集成电路与系统/(比) 因格里德·M·R·维鲍维迪主编;李雄伟等译. —北京:国防工业出版社,2019.4
书名原文:Secure Integrated Circuits and Systems
ISBN 978-7-118-11752-3

Ⅰ. ①安… Ⅱ. ①因… ②李… Ⅲ. ①集成电路 Ⅳ. ①TN4

中国版本图书馆 CIP 数据核字(2019)第 025440 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
天津嘉恒印务有限公司印刷
新华书店经售
*
开本 710×1000　1/16　印张 15¼　字数 270 千字
2019 年 4 月第 1 版第 1 次印刷　印数 1—2000 册　定价 85.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

译 者 序

随着信息时代的到来，基于嵌入式设备的移动支付、物联网等已经渗透到工作生活中的各个方面。在给人们带来便捷的同时，其安全受到了越来越严重的威胁。通常采用密码算法构筑安全堡垒，密码算法具有较高的数学强度，在实践中取得了良好的应用效果。然而，以旁路攻击、物理攻击等为代表的新攻击方式针对密码算法的实现环节展开攻击，呈现出了强大的攻击能力，对嵌入式系统的安全性造成了严重威胁。

嵌入式系统安全性涉及密码学和系统设计两个方面。对于传统嵌入式系统设计人员而言，关注的要点在于使用更少的资源实现更快的运算，从而达到高效实现的目标。然而，系统设计人员对于密码算法的安全特点了解较少，难以达成安全实现的目标。本书尝试在高效实现和安全实现之间搭建桥梁，使得系统设计人员能够做到两者兼顾。本书从密码算法的基本原理入手，讨论了密码算法的各个基本模块和安全设计的基本方法，并进行了实际案例分析。本书涵盖了嵌入式系统安全从理论到实践的各个环节，提纲挈领地把各环节要点呈现出来，引领读者逐步进入嵌入式系统安全设计的殿堂。

本书原著出版较早，难以涵盖最新的安全技术。然而，作为嵌入式系统安全设计的入门教程，本书所涵盖的主题较广，能够为读者进一步深入学习安全技术奠定良好的基础。同时，本书各个章节分别由 Christof Paar、Elisabeth Oswald 等业内知名学者撰写，对相关技术的脉络把握更为精准，起到了很好的引领作用。因此，在承担国家自然科学基金、河北省自然科学基金等相关项目的过程中，我们组织项目组主要成员翻译了本书，以期培养更多的嵌入式系统安全设计人员，从而推动我国信息安全的整体发展。

参加本书翻译的主要成员有李雄伟、陈开颜、张阳、谢方方、李艳、王晓晗等，李雄伟对全书进行了统稿和校对。

本书的翻译工作得到国家自然科学基金(编号:61271152、51377170、61602505)、河北省自然科学基金(编号:F2012506008)、装备科技译著出版基金的资助,深表感谢。

需要说明的是,本书涉及内容多、专业性强,且由多人翻译,限于水平和经验,加之有些概念译法本身就有难度,故而不妥之处在所难免,敬请读者见谅,并提出宝贵意见。

译 者

2018 年 6 月

前　言

密码系统中的薄弱环节决定了其整体安全强度。自20世纪70年代末公钥密码学出现以来，几十年间密码算法的数学设计与分析取得了长足进步。密码算法的数学强度已经足够安全，攻击者转而将“实现”环节作为攻击目标。目前已经报道了很多针对软件和硬件实现进行攻击的案例。实际上，人为因素经常是最薄弱环节，因为人们经常忘记密码，或使用简单密码。

越来越多的信息处理使用嵌入式便携设备完成，使得密码系统的脆弱实现问题变得尤为突出。这些小巧设备通常价格低廉、轻便易携，但也容易丢失。人们对嵌入式安全的需求涵盖了生活中的方方面面，如手机、PDA、医疗设备、自动驾驶、消费电子、智能卡、RFID标签、传感器节点等。

另外，计算和存储敏感信息的设备从个人计算机迁移到了中央服务器以及云端。在此情况下，高效安全的密码实现是保护安全与隐私的基础。

本书主要面向集成电路(IC)或嵌入式系统设计人员，使其从实现的角度了解安全与密码学的基本原理。设计人员在考虑高效实现(优化功耗、面积、吞吐量等)的同时，也应关注安全实现(抗攻击能力，尤其是抗旁路攻击①)，因而，本书同时涵盖了提高效率和抗旁路攻击的相关技术。

本书主要包含4个部分内容。

第一部分为基本原理，介绍了公钥密码算法的数学基础，并对旁路攻击进行了概述。

第二部分介绍了密码系统的基本模块。构建片上系统(SOC)等复杂系统时，设计者通常采用知识产权模块(IP)。这些模块包括对称密码算法、公钥密码算法、哈希函数等，也包括随机数生成器、不重数生成器以及物理不可克隆函数(PUF)等。

第三部分介绍了安全设计的基本方法。安全观念应贯穿于整个设计过程。从寄存器转移级(RTL)描述到布局的后端设计需要考虑安全，高层设计同样如此，如GEZEL设计环境可促进安全的软硬件协同设计。

---

① 旁路攻击，side channel attack，也译为侧信道攻击。——译者注

第四部分是案例介绍，包括 RFID 安全、FPGA 终端安全以及 Flash 存储安全。

本书的主要读者为集成电路或嵌入式系统设计者，包括 ASIC、FPGA、嵌入式处理器以及嵌入式系统等设计人员。本书并未涵盖所有方面，只是设计者的入门教程，尝试为密码学的理论数学与设计之间搭建桥梁，从而使得安全实现更为可行。感谢本书的各位撰稿人，也感谢间接提供帮助的业内人士。

2009 年 7 月

Ingrid M. R. Verbauwhede

撰 稿 人

Lejla Batina 荷语天主教鲁汶大学,比利时鲁汶-海弗莱;内梅亨大学,荷兰。电子邮箱:lejla. batina@ esat. kuleuven. be

Guido Marco Bertoni 意法半导体公司,意大利阿格拉德布里昂扎蒂雷松纳勒科莱奥尼中心,20041。电子邮箱:guido. bertoni@ st. com

Tim Güneysu 波鸿鲁尔大学嵌入式安全讲座教授,德国波鸿。电子邮箱:gueneysu@ crypto. rub. de

Helena Handschuh 荷语天主教鲁汶大学电子工程系计算机安全与工业密码研究组(ESAT/COSIC),比利时鲁汶-海弗莱 KasteelparkArenberg 大街 10 号,B-3001。电子邮箱:helenahandschuh@ yahoo. fr

Miroslav Knežević 荷语天主教鲁汶大学 ESAT/COSIC,比利时鲁汶-海弗莱 KasteelparkArenberg 大街 10 号,B-3001。电子邮箱:miroslav.knezevic@ esat.kuleuven. be

Yong Ki Lee 加州大学洛杉矶分校电子工程系,美国加利福尼亚州洛杉矶市西木区 420 号,CA 90095-1594。电子邮件: jfirst@ ee. ucla. edu

Roel Maes 荷语天主教鲁汶大学 ESAT/COSIC,比利时鲁汶-海弗莱 Kasteelpark Arenberg 大街 10 号,B-3001。电子邮箱:roel.maes@ esat.kuleuven.be

Stefan Mangard 英飞凌科技公司,德国诺伊贝格市坎比昂 1-12 号,85579。电子邮箱:stefan. mangard@ infineon. com

Filippo Melzani 意法半导体公司,意大利阿格拉德布里昂扎蒂雷松纳勒科莱奥尼中心,20041。电子邮箱:filippo. melzani@ st. com

Elisabeth Oswald 布里斯托大学计算机科学系,英国布里斯托市 Woodland 路 Venturers 大楼,BS8 1UB;格拉茨技术大学应用信息处理与通信研究所,奥地利格拉茨市英飞街 16 号,8010 Graz。电子邮箱:elisabeth. oswald@ bristol. ac. uk

Christof Paar 波鸿鲁尔大学嵌入式安全讲座教授,德国波鸿。电子邮箱:christof. paar@ rub. de

Kazuo Sakiyama 电气通信大学,日本东京。电子邮箱:saki@ ice. uec. ac. jp

Patrick Schaumont 弗吉尼亚理工大学电子与计算机工程系,美国布莱克斯堡,VA 24061。电子邮箱: schaum@ vt. edu

Dries Schellekens 荷语天主教鲁汶大学 ESAT/COSIC,比利时鲁汶-海弗莱 KasteelparkArenberg 大街 10 号,B-3001。电子邮箱:dries.schellekens@ esat.kuleuven.be

Eric Simpson 弗吉尼亚理工大学电子与计算机工程系,美国布莱克斯堡,VA 24061.

Francois-Xavier Standaert 法语天主教鲁汶大学(UCL)密码研究组,比利时新鲁汶市黎凡特 3 号,B-1348。电子邮箱:fstandae@ uclouvain. be

Berk Sunar 伍斯特理工学院电气与计算机工程系,美国伍斯特,MA 01609-2280。电子邮箱: sunar@ wpi. edu

Kris Tiri 加州大学洛杉矶分校。电子邮箱:kris. tiri@ gmail. com

Elena Trichina 意法半导体公司(罗塞特) 先进系统科技部,法国。电子邮箱:

elena. trichina@ st. com

Pim Tuyls Intrinsic-ID 公司,荷兰埃因霍温。电子邮箱:pim. tuyls@ intrinsic-id. com

Ingrid M. R. 荷语天主教鲁汶大学 ESAT/COSIC,比利时鲁汶-海弗莱 Kasteelpark Arenberg 大街 10 号,B-3001。电子邮箱:ingrid.verbauwhede@ esat.kuleuven.be

Pengyuan Yu 弗吉尼亚理工大学电子与计算机工程系,美国布莱克斯堡,VA 24061.

目　录

第一部分　基本原理

第二部分 加密模块与数学运算

第三部分　安全设计方法

第四部分 应　用