国际信息工程先进技术译丛

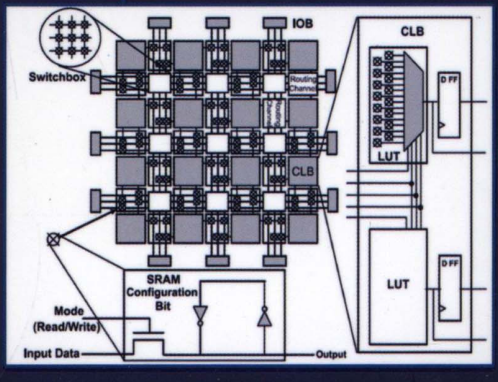
Springer

FPGA安全性设计指南

Handbook of FPGA Design Security

(美) Ted Huffmire
Cynthia Irvine
Thuy D.Nguyen
Timothy Levin
Ryan Kastner
Timothy Sherwood
著

房亮 吴少俊 闫蕾 宫永生 译
夏宇闻 审



机械工业出版社
CHINA MACHINE PRESS

作者简介

本书由泰德.霍夫曼（Ted Huffmire）、辛西亚尔.伊凡（Cynthia Irvine）、秀.阮（Thuy D. Nguyen）、提摩太.莱文（Timothy Levin）、瑞恩.卡思特纳（Ryan Kastner）、提摩西.舍伍德（Timothy Sherwood）等六位有丰富实践工作经验的教授、专家共同编写。他们是美国著名的海军研究生院和加州大学计算机科学系FPGA设计安全领域的资深专家。本书源于他们在FPGA设计安全保障领域研究中多年积累的宝贵经验的总结。本书内容十分广泛，几乎涵盖了FPGA设计安全保障方面的所有问题，本书阐述了造成FPGA设计安全隐患的主要原因，并且提出了解决安全隐患问题的清晰思路。本书所介绍的安全保障思路对中国国防领域的FPGA设计者有很大的参考价值。

国际信息工程先进技术译丛

FPGA 安全性设计指南

Ted Huffmire
Cynthia Irvine
（美）Thuy D. Nguyen 著
Timothy Levin
Ryan Kastner
Timothy Sherwood
房 亮 吴少俊 闫 蕾 宫永生 译
夏宇闻 审

机 械 工 业 出 版 社

现场可编程门阵列（FPGA）已经成为嵌入式系统设计的主要应用技术之一。可重构器件由于融合了硬件和软件的特性，能够在专用集成电路的高性能和 CPU 的可编程性之间找到自己的应用空间，产生更好的应用效果。与此同时，FPGA 安全性设计的问题也日益突出。目前，关于 FPGA 安全性设计的专门著述较少，FPGA 设计者很难针对具体应用进行系统的安全性分析和设计。

本书通过理论阐述并结合实用设计的方式，通过举例说明 FPGA 安全性设计的问题如何进行解决。作者从如何编写顶层设计的形式化说明开始，逐步涉及低层硬件电路的各项强化机制，并分为多个层面对 FPGA 安全性问题和解决方案进行了全面的阐述。作者结合近年来在计算机安全性理论、编程语言、编译器和硬件设计等领域中的最新进展，与 FPGA 设计中的安全性问题作为一个整体予以阐述，创建了一整套静态和动态分析互相配合的多样化设计技术，使得使用商业芯片构建的 FPGA 系统有可能成为一个稳定、可靠和安全的强健系统。

本书旨在为 EDA（电子设计自动化）和 FPGA 领域工作的研究者和实践者们提供一整套 FPGA 安全性设计的管理实用方法。本书适合在公司、工厂和政府研究实验室工作，从事 FPGA 设计的工程师和学术界人士阅读。尤其是对 FPGA 安全性要求较高的领域。同时也适合致力于 FPGA 安全性设计研究的人士，用以提高专业技能。

Translation from English language edition：

Handbook of FPGA Design Security

by Ted Huffmire Cynthia Irvine Thuy D. Nguyen Timothy Levin Ryan Kastner and Timothy Sherwood

北京市版权局著作权合同登记图字：01-2012-1048 号

译 者 序

随着航空、航天等军工领域嵌入式数字系统应用的多元化，可编程逻辑设计技术由于其本身的综合成本优势和灵活性，已经成为核心的支撑技术之一，并在高可靠领域有了大规模的应用。与此同时，如何解决可编程逻辑的安全性设计问题也成为了一项迫切需要进行研究的工作。

本书是针对 FPGA 设计安全保障的指南专著，泰德·霍夫曼，辛西亚尔·伊凡等六位作者是 FPGA 设计安全领域的资深专家，对 FPGA 安全性防护有全面深入的研究和独到的见解。本书不仅对 FPGA 设计中可能出现的安全隐患问题进行了全面、细致的分析，并且提出了清晰的解决思路，对相关领域的科研及工程技术人员具有很强的指导意义和借鉴价值。

当夏宇闻教授将本书的英文版《Handbook of FPGA Design Security》推荐给我们时，我们欣喜地发现本书对工程中出现的 FPGA 安全性设计问题给予了系统的分析。当夏宇闻教授建议我们结合工程应用中的实践经验，将本书翻译成中文时，我们立即欣然答应。我们所在的单位是中国科学院空间应用工程与技术中心，主要负责载人航天工程空间应用系统的工程组织管理及总体技术研究工作，成立以来承担了近 300 台（套）有效载荷的工程研制工作，积累了丰富的可编程逻辑设计经验。我们相信本书中文译稿的出版将对国内的 FPGA 安全性设计工作产生积极的影响。

参与本书翻译工作的主要译者是从事载人航天工程空间应用系统中嵌入式系统多年研究的技术专家，他们是中国科学院空间应用工程与技术中心的房亮副研究员、吴少俊副研究员，闫蕾副研究员和宫永生工程师，均为载人航天工程空间应用系统相关型号任务的负责人和核心骨干。本书由夏宇闻教授负责审校。

在《Handbook of FPGA Design Security》中文版即将出版之时，特别向中国科学院空间应用工程与技术中心领导和同事对我们工作的支持、向北京航空航天大学夏宇闻教授和机械工业出版社林春泉编审的悉心指导和帮助表示衷心的感谢！

由于 FPGA 安全性设计技术在国内的相关研究较少，译书中难免有不当之处，敬请读者批评指正。

译者

2014 年 4 月

审 校 者 序

在嵌入式军用数字系统设计领域，FPGA 有着巨大的发展潜力，然而也存在着许多安全隐患。近年来，在推广 Verilog 设计方法学的同时，我也一直在关注着 FPGA 安全性设计方面的文献和书籍。

2011 年底，在中科院空间应用工程与技术中心工作的、我的前硕士生吴少俊向我咨询 FPGA 安全性设计问题时，我立即推荐了我刚读过的一本由 Springer 出版社 2010 年底出版的新书《Handbook of FPGA Design Security》。

该书由泰德·霍夫曼（Ted Huffmire），辛西亚尔·伊凡（Cynthia Irvine）等六位具有丰富实践工作经验的教授、专家共同编写。他们是美国著名的海军研究生院和加州大学计算机科学系 FPGA 设计安全领域的资深专家。该书源于他们在 FPGA 设计安全保障领域研究中多年积累的宝贵经验的总结。书中的内容十分广泛，几乎涵盖了 FPGA 设计安全保障方面的所有问题，该书阐述了造成 FPGA 设计安全隐患的主要原因，并且提出了解决安全隐患问题的清晰思路。我认为该书所介绍的安全保障思路对中国国防领域的 FPGA 设计者有很大的参考价值。

我希望吴少俊和他的同事们能够认真读一读该书，并花点时间把它翻译成通俗易懂的中文。有了好的中文书籍，一定会促进国内 FPGA 设计安全保障工作能更快更健康地开展。所以我答应担任该书译稿的审校。吴少俊征求所在部门意见后同意了我的建议，不久我就把该书和吴少俊介绍给了机械工业出版社的林春泉编审，出版社很快向 Springer 出版社购买了该书的中文版版权，随后签订了翻译合同。

在一年半的翻译过程中，参与翻译工作的人员非常认真，经常通过电子邮件与我切磋难以用通畅中文表达的章节段落，译稿曾经多次反复修改。由于水平和时间有限，我的审校不免存在一些遗漏和错误，敬请细心的读者不吝指教。

在本书出版之际，让我衷心地感谢曾经为本书出版做出过贡献的所有同仁。

夏宇闻
北京航空航天大学电子信息工程学院退休教授
北京至芯科技公司 FPGA 设计培训顾问
2013 年 9 月 18 日

原 书 前 言

本书旨在为 EDA（电子设计自动化）和 FPGA 领域工作的研究者和实践者们提供一整套 FPGA 设计安全性管理的实用方法。本书的读者群包括公司、工厂、政府研究实验室、相关领域的工程师和学术界人士。

本书将理论基础的阐述与实用设计方法的介绍紧密结合，通过举例说明了 FPGA 设计的安全性问题是如何解决的。为了透彻理解 FPGA 系统在运行中的风险和生命周期等一系列问题，本书从如何编写顶层设计的形式化说明书开始，一直讲到低层硬件电路的强化机制，分多个层面对 FPGA 安全性问题和解决方案进行了全面的阐述。在这一过程中，作者将近年来在计算机安全性理论、语言、编译器和硬件等领域中的进展，与 FPGA 设计中安全性的考虑作为一个整体予以阐述，从而创建了一整套静态和动态分析互相配合的多样化设计技术，使得用商业化芯片构建的 FPGA 系统有可能成为一个稳定、可靠、经得起考验的强健系统。

在本书出版之际，我们要感谢那些曾经给我们提供帮助的人们，他们的支持是这本可重构硬件安全性著作之所以能取得成功的关键。我们要特别感谢路易斯安那州立理工大学的 Andrei Paun 和 Jason Smith，他们为我们提供一个 Linux 兼容版的 Grail + 软件。我们还要感谢帕德伯恩大学（the University of Paderborn）的 Marco Platzner 和加州大学圣地亚哥分校（the University of California，San Diego）的 Ali Irturk 和 Jason Oberg，他们给本书的初稿提供了宝贵的意见和建议。

本课题研究经费部分源于美国国家科学基金会，编号为：CNS-0524771 和 NSF Career Grant CCF-0448654 的两项拨款，在此表示感谢。

Ted Huffmire
Cynthia Irvine
Thuy D. Nguyen
Timothy Levin
Ryan Kastner
Timothy Sherwood

作 者 简 介

泰德·霍夫曼（Ted Huffmire） 博士

海军研究生院 计算机科学系 美国 加利福尼亚州 蒙特雷坎宁安路（Cunningham） 1411 号 邮编：93943

电子邮箱：tdhuffmi@ nps. edu

美国加利福尼亚州海军研究生院计算机科学系的助理教授，他的研究领域跨计算机科学的两个专业方向，即计算机安全性和计算机体系结构。他的研究重点是面向硬件的安全性，以及专用芯片实施机制的研发。他在加利福尼亚大学圣芭芭拉分校，计算机科学系获得博士学位。他是美国 IEEE 和 ACM 的成员。

辛西亚尔·伊凡（Cynthia Irvine） 博士

海军研究生院 计算机科学系 美国 加利福尼亚州 蒙特雷 坎宁安路（Cunningham）1411 号 邮编：93943

美国加利福尼亚州蒙特雷海军研究生院信息系统安全学和研究中心（CISR）主任，计算机科学系教授。她的研究兴趣包括高保险度安全性。她在凯斯西储大学获得天文学科博士学位。她是 IEEE、ACM 和太平洋天文学会的成员。

秀·阮 （Thuy D. Nguyen）

海军研究生院 计算机科学系 美国 加利福尼亚州 蒙特雷 坎宁安路（Cunningham）1411 号 邮编：93943

美国加利福尼亚州蒙特雷海军研究生院计算机科学高级研究员，她的研究兴趣包括高保险平台、可信任的操作系统、动态安全性服务、多级安全性、安全性评价和安全性需求工程。她在加利福尼亚大学圣地亚哥分校获计算机科学学士学位。

提摩太·莱文（Timothy Levin）

海军研究生院 计算机科学系 美国 加利福尼亚州 蒙特雷 坎宁安路（Cunningham）1411 号 邮编：93943

美国加利福尼亚州蒙特雷海军研究生院副教授。他的研究兴趣包括高保险安全性体系结构和动态安全性策略的设计、分析和验证。他在加利福尼亚大学圣克鲁斯分校获得计算机科学学士。他是 IEEE 和 ACM 学会的成员。

瑞恩·卡思特纳（Ryan Kastner） 博士

加利福尼亚大学 圣地亚哥分校 计算机科学与工程系。美国 加利福尼亚州拉乔拉 格立曼大道（Gilman Drive） 9500 号 邮编 92093

电子邮箱：kastner@ cs. ucsd. edu

加利福尼亚大学圣地亚哥分校计算机科学与工程系副教授。他的研究兴趣集中在嵌入式计算机系统，包括可重构计算体系结构，数字信号处理和安全性等许多方面。他在加利福尼亚大学洛杉矶分校计算机科学系获得博士学位。

提摩西·舍伍德（Timothy Sherwood）博士

加利福尼亚大学 圣芭芭拉分校 计算机科学系 美国 加利福尼亚州 圣芭芭拉 邮编：93106

加利福尼亚大学圣芭芭拉分校计算机科学副教授。他的研究兴趣包括计算机体系结构、专门研究可构造、监视和分析系统的新型高通量方法。他在加利福尼亚大学圣芭芭拉分校计算机科学和工程系获得哲学博士学位。他是 IEEE 和 ACM 学会的成员。

目　　录

第1章 概 述

摘要：从蓝牙收发器到美国宇航局的火星探测器，现场可编程门阵列（FPGA）已经成为了嵌入式系统设计的主要方式之一。这种可重构器件，由于融合了硬件和软件的特性，因而能够在专用硬件的高性能和CPU的可编程性之间找到自己的应用空间，产生更好的效果。尽管这种灵活性可以让开发人员快速设计出原型机，并使设计性能接近于专用集成电路（ASIC）的嵌入式系统，但其可编程性可能会被敌方利用来中断关键的功能、窃听加密的通信内容，甚至摧毁芯片。构建高效灵活的系统，并确保其具有足够的安全性，是研究人员以及业内人士必须面对的艰难挑战。由于在可重构系统的设计过程中，通常要在设计末期才能发现其面临的安全问题，这就导致相关的系统只能通过系统深奥的难懂性㊀得到保护。本章将从安全性角度对现场可编程门阵列（FPGA）进行概述，重点说明这类器件在过去十年内为什么并如何成为现代计算机系统中最值得信赖和最重要的器件之一。本章还将讨论这类器件的角色转换（即如何从原型机平台转变成可应用的解决方案），介绍现代FPGA的架构，阐述由日益增加的用途而导致的安全衍生问题，以及可能适用于此领域的安全性方面的经验教训。

1.1 对FPGA日益增加的依赖

FPGA是很多领域关键设备的核心，在从无线接入点（WAP）到商用面部识别系统等几乎所有领域都有广泛的应用。与通用处理器的顺序执行方式不同，现代的现场可编程门阵列器件在每个循环中可以执行数百次乘法运算以及数千次加法运算，使其具有能够同时处理很多不同逻辑模块的计算能力。例如，采用FPGA的无线接入点（WAP）中，可能需要使用一个信号处理器、一个协议处理器，以及一个包调度器，所有这些可以集成在一个芯片中。另外，可重构硬件能同时在实验室及现场重新写入，因此可以保证较快的设计周期，相关的补丁甚至可以下载到已经开发完成的设备中（例如，可以根据需要，将错误修正或者功能增强补丁通过网络向手机或者无线接入点推广）。

由于集成了灵活性和计算能力，可重构器件已经推动了很多性能优异的嵌入式系统的发展[9,15,19,40,51,62]。很多可重构器件单位面积的速度和性能能够达到类似的

㊀ 这种难懂性源于非设计者对于设计的不了解。——译者注

微处理器的 100 倍[12,18,75]。卫星、机顶盒、入侵探测系统、电网、加密装置、飞机甚至火星探测器都需要通过现场可编程门阵列（FPGA）来实现相应的功能。据估计，仅仅在 2005 年一年内，就启动了超过 80000 项不同的商用 FPGA 设计项目[53]。这些器件在比特（bit）级上的可重构能力能够被用来实现所有高度优化的电路，从加密技术到快速傅里叶变换，甚至到完全自定义的多处理器系统。在本节中，我们将对其中几个领域进行介绍，并讨论 FPGA 器件在这些领域中的使用情况。

设计提示：FPGA 器件的优点。FPGA 非常适合用于嵌入式设计以及新型计算机体系结构开发过程中原型机的快速开发。随着专用集成电路（ASIC）生产成本的增加，FPGA 相对于通用型处理器的性能优势，以及 FPGA 和 ASIC 之间的较小的性能差异，都使得在实际系统中 FPGA 的应用日益增加。对于一些份额不大的市场（如高可靠系统），与专用集成电路相比，FPGA 同时具有成本优势和安全优势。例如，对于 FPGA 而言，敏感的设计绝对不会被送到可能造成设计失窃的晶圆代工厂中。另外，FPGA 器件提供的并行性使其能够用做由吞吐量推动的应用领域中的通用型 CPU 的替代产品。

1.1.1 航空航天用 FPGA

由于 FPGA 能够兼顾性能、成本以及灵活性等诸多方面，很多航空航天电子设备中都开始使用这种器件。例如，在联合打击战斗机[56]中、新的波音 787 梦幻客机[20]中、美国宇航局火星探测器[23,57]中都使用 FPGA 来实现重要功能。在这些应用领域中，FPGA 被用在驾驶员座舱显示装置、飞行管理装置、航空电子设备、武器制导设备以及飞行雷达设备中[2]。

设计提示：FPGA 基础。通过比特流来确定 FPGA 内部结构的配置位设置方式，FPGA 中的核是更大型嵌入系统的组成模块。反熔丝 FPGA 采用熔丝作为配置位，因此这种器件只能进行一次编程，之后数据不会丢失。SRAM（静态随机访问存储器）型 FPGA 采用 SRAM 存储单元作为配置位。Flash（闪存）型 FPGA 采用电可擦除可编程只读存储器（EEPROM）作为配置位。

电路可以是反熔丝电路、Flash 电路或者 SRAM 电路。其中基于反熔丝电路的 FPGA 为一次性写入器件，而 SRAM 型和 Flash 型的 FPGA 可以多次写入，可以在实验室写入或者在现场写入。Flash 型的 FPGA 还具有低功耗的优点。

设计提示：FPGA 选型。SRAM 型 FPGA、Flash 型 FPGA 以及反熔丝 FPGA 具有不同的安全性能[76]。反熔丝性 FPGA 的缺点是只能写入一次，优点是窃取设计时十分费力，必须采用破坏性的研磨及扫描破译技术（Sand-And-Scan Attack）。这包括拆除器件的封装、逐层研磨和剥离蚀刻的微电路，以及电子显微摄影，并通过这些来创建芯片的 3D 图像。由于反熔丝具有非易失性，比特流不需要由外部存储器载入，可以避免板级探测的破译，防止针对比特流加密机制的破译攻击。Flash 型 FPGA 同样可以将比特流存储在芯片中，这种设计方式也不需要从外部存储器载入比特流。因此，同样可以避免上述方式的攻击。尽管如此，和反熔丝 FPGA 相比，由于 Flash 存储器可以被修改，因此设计可能被改变。另外，与反熔丝型 FPGA 相比，Flash 型 FPGA 很容易被芯片探测技术破译，而芯片探测破译的成本比研磨及扫描破译的成本低得多。SRAM 型 FPGA 在上电之后，必须重新载入比特流，同时软存储错误[28]或者比特流解密机制实现过程中产生的缺陷会为破译者提供窃取设计信息的机会。在不断电的情况下，SRAM 型 FPGA 类似于非易失性的 FPGA 器件，此时不需要从非易失性的外部存储器中加载设计信息。

以军用航空电子设备为例，在这种设备中，单片机需要同时处理机密的目标信息，以及非机密的燃料和维护信息。航空电子设备涉及的其他多级安全（MLS）问题还包括传感器-发射器问题。与接到命令攻击相关目标的士兵相比，决定攻击目标的情报分析师具有更高级别的指挥决策权。在另一个多级安全（MLS）问题中，如果联军飞行员和其盟军组成编队一起飞行，则必须明确相关指令，确定哪些信息可以共享。在多级系统中，可以用 CPU 进行分配，使其处理某个特定秘密级别（或者某个秘密级别范围）的数据，同时为其设置一个安全标记（或者安全标记范围）。如果为每个秘密级别设置一个单独的器件，则会大大增加飞机的重量。为了降低飞机重量，可以考虑采用单一器件处理多个秘密级别数据。但是，如果对器件的安全性能没有经过仔细考虑，这种处理方式可能会非常危险。将不同秘密级别的信息分开需要经过仔细的设计。由于可重构系统常常缺乏存储保护、虚拟内存以及其他通用系统中经常采用的传统隔离方式，因此需要采取必要的安全措施来防止机密数据和非机密数据之间发生混淆。另外，同软件更新机制一样，在对器件进行远程更新时，保证安全十分重要，这能够有效阻止破坏行为。最后，由于所涉及的知识产权的敏感性，如何防止竞争对手或者敌人轻易地对芯片实施逆向工程也至关重要。