

《门级信息流分析理论及应用》

图书基本信息

书名：《门级信息流分析理论及应用》

13位ISBN编号：9787030423704

出版时间：2014-11

作者：胡伟,慕德俊

页数：224

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《门级信息流分析理论及应用》

内容概要

本书属于信息安全领域，旨在解决物联网和信息物理系统环境下高可靠系统所面临的信息安全问题。但本书同时涵盖了网络信息安全、数字电路、设计自动化以及算法复杂性理论等相关学科。其中，在网络信息安全领域主要涉及基于格模型的信息流安全理论及方法；在数字电路方面主要涉及信息流模型的形式化描述以及设计优化问题；在设计自动化领域主要利用了一些相关的电路设计、评估与验证方法；在算法复杂性理论方面主要涉及一些相关算法的设计与复杂度分析。

《门级信息流分析理论及应用》

作者简介

胡伟，男，1982年10月生，分别于2005年、2008年和2012年获得西北工业大学“信息对抗技术”专业学士、“模式识别与智能系统”专业硕士和“控制科学与工程”专业博士学位，2009年9月—2011年9月赴加州大学圣迭戈分校计算机科学与工程系学习，2012年7月入西北工业大学“计算机科学与技术”博士后流动站，主要从事硬件安全、高可靠系统安全、嵌入式安全、可重构计算等方面的研究。

慕德俊，男，1963年6月生，西北工业大学自动化学院教授、博士生导师，主要研究方向包括网络与信息安全、控制理论与应用、网络化控制、无线传感器网络等。

书籍目录

前言

第1章绪论1

1.1信息安全问题的起源与发展1

1.1.1信息安全问题的起源1

1.1.2信息安全问题的发展历程1

1.1.3信息安全问题的发展方向4

1.2高可靠系统信息安全6

1.2.1高可靠系统面临的信息安全问题6

1.2.2高可靠系统的信息安全需求8

1.2.3高可靠系统安全研究概述8

1.3常用信息安全机制9

1.3.1密码算法10

1.3.2访问控制10

1.3.3信息流控制12

1.4本书主要研究内容14

1.5本书主要特点和读者对象15

第2章信息流安全相关理论16

2.1信息和数据16

2.2信息流的定义16

2.3信息流的分类16

2.3.1显式流16

2.3.2隐式流17

2.3.3时间信息流18

2.3.4间接流19

2.4信息流安全策略19

2.4.1信息流安全主体和客体19

2.4.2信息流安全等级20

2.4.3信息流的格模型20

2.5常用信息流安全模型23

2.5.1军用模型23

2.5.2Bell—LaPadula模型24

2.5.3Biba模型25

2.5.4无干扰模型25

2.6信息流控制机制26

2.6.1基于编译的机制27

2.6.2基于执行的机制27

2.7信息流跟踪技术29

2.7.1信息流跟踪29

2.7.2程序语言层的信息流跟踪技术30

2.7.3操作系统层的信息流跟踪技术31

2.7.4体系架构层的信息流跟踪技术31

2.7.5逻辑门级的信息流跟踪技术31

2.8本章小结32

第3章二级安全格下的GLIFT理论33

3.1基本概念和原理33

3.2GLIFT逻辑函数的基本性质36

3.3基本门GLIFT逻辑的形式化描述38

- 3.3.1缓冲器38
- 3.3.2非门39
- 3.3.3触发器39
- 3.3.4与门和与非门40
- 3.3.5或门和或非门41
- 3.3.6异或门和同或门42
- 3.3.7三态门43
- 3.4基本门GLIFT逻辑的复杂度分析44
 - 3.4.1与门44
 - 3.4.2或门45
 - 3.4.3与非门和或非门45
 - 3.4.4异或门46
- 3.5GLIFT逻辑的不精确性46
 - 3.5.1GLIFT逻辑潜在的不精确性46
 - 3.5.2不精确性根源的分析与证明48
- 3.6实验结果与分析52
 - 3.6.1复杂度分析52
 - 3.6.2精确性分析53
- 3.7本章小结55
- 第4章多级安全格下的GLIFT理论57
 - 4.1多级安全格模型57
 - 4.2多级安全格下的GLIFT问题59
 - 4.2.1三级线性安全格59
 - 4.2.2四级线性安全格60
 - 4.2.3任意级线性安全格61
 - 4.2.4非线性安全格64
 - 4.3多级安全格下的相关运算和运算律65
 - 4.3.1安全类的边界运算65
 - 4.3.2安全类边界运算的运算律66
 - 4.3.3点积运算66
 - 4.3.4点积运算的运算律67
 - 4.4基本门GLIFT逻辑的形式化描述68
 - 4.4.1缓冲器68
 - 4.4.2非门68
 - 4.4.3触发器69
 - 4.4.4与门和与非门69
 - 4.4.5或门和或非门72
 - 4.4.6异或门和同或门73
 - 4.4.7三态门74
 - 4.5GLIFT逻辑的布尔描述75
 - 4.5.1安全类的编码75
 - 4.5.2运算符的布尔实现76
 - 4.5.3GLIFT逻辑的布尔实现78
 - 4.6多值逻辑系统下的GLIFT逻辑79
 - 4.6.1四值逻辑79
 - 4.6.2四值逻辑系统下的污染传播80
 - 4.6.3四值逻辑系统下的GLIFT逻辑81
 - 4.6.4九值逻辑系统下的GLIFT逻辑82
 - 4.7实验结果与分析84

- 4.7.1GLIFT逻辑的复杂度分析84
- 4.7.2GLIFT逻辑的性能分析85
- 4.8本章小结87
- 第5章GLIFT逻辑生成算法理论88
- 5.1基本概念与理论88
- 5.1.1相关概念88
- 5.1.2NP完全性理论90
- 5.2精确GLIFT逻辑生成问题的NP完全性92
- 5.2.1非定常GLIFT逻辑的存在条件92
- 5.2.2污染传播判定问题93
- 5.2.3污染传播搜索问题94
- 5.3GLIFT逻辑生成算法95
- 5.3.1暴力算法96
- 5.3.20—1算法97
- 5.3.3构造算法99
- 5.3.4完全和算法101
- 5.3.5SOP—POS算法102
- 5.3.6BDD—MUX算法104
- 5.3.7RFRR算法106
- 5.3.8GLIFT逻辑生成算法的比较108
- 5.4结果与分析109
- 5.4.1实验流程109
- 5.4.2实验结果与分析110
- 5.5本章小结112
- 第6章GLIFT逻辑的设计优化问题113
- 6.1二级安全格下GLIFT逻辑编码方式及其不足113
- 6.1.1二级安全格下GLIFT逻辑编码方式113
- 6.1.2二级安全格下GLIFT逻辑编码方式的不足114
- 6.2二级安全格下GLIFT逻辑编码方式的改进115
- 6.2.1GLIFT逻辑现有编码方式的改进115
- 6.2.2基本门GLIFT逻辑118
- 6.2.3新旧编码方式下GLIFT逻辑的比较120
- 6.2.4新GLIFT逻辑用于硬件冗余123
- 6.3多级安全格下GLIFT逻辑的设计优化问题125
- 6.3.1编码方式的优化125
- 6.3.2利用无关项优化GLIFT逻辑127
- 6.4实验结果与分析131
- 6.4.1静态验证效率分析131
- 6.4.2动态实现性能分析132
- 6.5本章小结136
- 第7章GLIFT方法的应用137
- 7.1GLIFT方法应用原理137
- 7.2静态信息流安全测试与验证140
- 7.3动态信息流跟踪143
- 7.4GLIFT在开关电路设计中的扩展应用145
- 7.4.1静态逻辑冒险检测145
- 7.4.2X—传播146
- 7.4.3可控性分析148
- 7.4.4错误检测149

7.5本章小结	149
第8章测试与验证方法	150
8.1测试与验证内容	150
8.1.1GLIFT逻辑精确性分析	150
8.1.2GLIFT逻辑复杂度分析	151
8.1.3GLIFT逻辑静态测试与验证分析	152
8.2测试与验证流程	152
8.2.1精确性分析流程	152
8.2.2复杂度分析流程	153
8.2.3静态测试与验证流程	154
8.3测试与验证环境	154
8.3.1ABC工具	155
8.3.2SIS工具	158
8.3.3ESPRESSO工具	159
8.3.4ModelSim工具	160
8.3.5DesignCompiler工具	161
8.4测试信号源	163
8.4.1计数器	163
8.4.2ModelSim内置随机数发生器	164
8.4.3线性反馈移位寄存器	164
8.4.4非线性反馈移位寄存器	167
8.5本章小结	167
第9章测试与验证实例	168
9.1I2C总线控制器的测试	168
9.2AES密码算法核的测试与验证	173
9.3ALU的测试与验证	176
9.4本章小结	182
第10章结束语	183
10.1本书的主要工作	183
10.2后续工作与展望	185
参考文献	187
附录1CLASS标准单元库相应的GLIFT逻辑库	196
附录2软件工具和测试基准集	204
附录3ModelSim仿真工具参考脚本	205
附录4DesignCompiler综合工具参考脚本	206
附录5缩略词表	208
附录6符号对照表	211

《门级信息流分析理论及应用》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com