密码协议分析的逻辑方法

雷新锋　薛　锐　著

科学出版社

密码协议分析的逻辑方法

雷新锋　薛　锐　著

本书得到中国科学院科学出版基金、国家自然科学基金(No.61170280)和中国科学院先导专项研究计划(XDA 06010701)资助

科学出版社

北京

内 容 简 介

本书对密码协议分析的逻辑方法进行了系统详尽和深入的介绍，全书共四部分，第一部分是理论基础，第二部分是密码协议分析概述，第三部分介绍密码协议逻辑，第四部分介绍计算可靠的密码协议逻辑.

本书的内容包括密码协议分析相关数理逻辑和现代密码学理论的基础知识、密码协议分析的主要方法综述、各种密码协议逻辑、协议分析实例以及密码协议逻辑分析方法的计算可靠性等. 内容涵盖了所有迄今为止重要的密码协议分析逻辑系统，其中包括作者在密码协议分析方面的工作.

本书的读者对象为信息安全专业高年级本科生及研究生，也可供从事信息安全专业的教学、科研人员和工程技术人员参考.

图书在版编目(CIP)数据

密码协议分析的逻辑方法/雷新锋，薛锐著. —北京：科学出版社，2013
ISBN 978-7-03-037096-9

Ⅰ.密… Ⅱ. ①雷… ②薛… Ⅲ.密码协议－逻辑方法 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字 (2013) 第 049259 号

责任编辑：余 丁／责任校对：李 影
责任印制：张 倩／封面设计：蓝 正 薛凯文

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏杰印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2013 年 3 月第 一 版 开本：B5(720×1000)
2013 年 3 月第一次印刷 印张：25
字数：480 000

定价：98.00 元

(如有印装质量问题，我社负责调换)

前　言

密码协议是使用密码机制的协议, 是保障信息安全的手段. 密码协议在信息社会凸显出日益重要的作用, 但其设计和分析一直是信息安全中的难点. 为了保证密码协议的安全性, 自 20 世纪 80 年代以来, 人们提出了各种各样的分析方法. 在这些方法中, 基于逻辑的方法扮演了非常重要的角色. 本书首次把文献中常用的逻辑方法进行总结, 对其作了系统详尽而深入的阐述.

数理逻辑是计算机科学的基础, 计算机领域的科学问题大都或多或少地与数理逻辑有着千丝万缕的联系, 基于逻辑的方法在密码协议形式化分析中的位置不可替代. 当前在国内外还没有专门针对密码协议逻辑分析方法的论著, 大部分论著仅限于简要地介绍一两种方法, 使得读者一叶障目, 难以根据自己的需求进行有选择性的学习和应用, 导致的结果是, 对于初学者, 相关理论基础缺乏, 掐头去尾的介绍使得内容难以理解和掌握; 对于具有理论基础的读者, 没有任何新意, 而技术上以点概面的介绍容易产生误导; 对于希望作为一种工具进行查阅的研究者来说, 内容又显得不够全面, 不足为据.

从学科内容上说, 密码协议分析是一门典型的交叉学科, 它不但需要形式化方法背景, 而且需要密码学的知识. 但是目前面世的文献还没有见到一本把形式化方法与密码学结合起来, 完整介绍密码协议分析方法的论著. 大部分论著要么仅从纯形式化的角度进行阐述, 要么仅把密码协议分析作为密码学的一部分进行阐述.

鉴于此, 本书把论述的范围限定在密码协议分析的逻辑方法内, 以便对该范围内的密码协议分析作全面和深入的阐述. 在内容方面, 充分体现了逻辑分析方法和密码学方法的有机结合, 凸显了密码协议分析学科交叉的特点, 还其全貌.

全书共分为以下四部分.

(1) 第一部分为理论基础, 主要针对数理逻辑和密码学的初学者, 同时也为书中其他内容的展开做好铺垫. 熟悉数理逻辑或现代密码学的读者可跳过本部分.

(2) 第二部分为密码协议分析概述, 主要针对密码协议形式化分析的初学者, 使其对密码协议的概念、密码协议的安全威胁、密码协议实例以及主要的密码协议分析方法有基本的了解.

(3) 第三部分为密码协议逻辑, 是本书的重点阐述内容. 它对近年来有代表性的密码协议分析逻辑从语法、语义及可靠性等方面作了系统深入的阐述, 同时给出一些协议分析实例. 本部分内容难易适中, 注重理论的读者可选择感兴趣的逻辑进

行阅读, 注重应用的读者可略去逻辑语义及可靠性分析的相关章节.

(4) 第四部分为计算可靠的密码协议逻辑, 本部分可作为高级专题部分, 供希望进一步了解密码协议分析逻辑的读者参考. 同时对当前本领域的一些最新成果进行介绍.

在内容编排上, 本书注重由浅入深, 适合各层次读者参阅. 全书从基础理论和基本概念入手, 涵盖了主要的密码协议分析逻辑以及该领域的一些前沿理论, 其中包括作者在密码协议分析的逻辑方面所做的工作. 这些内容对于初学者有着重要的启发和引导作用, 对于研究者具有一定的参考价值, 对于密码协议的分析和设计人员具有重要的指导意义.

本书是在中国科学院科学出版基金、国家自然科学基金 (No.61170280) 和中国科学院先导专项研究计划 (XDA 06010701) 的资助下完成的, 在此对科学出版社和国家自然科学基金委员会表示感谢, 同时感谢信息安全国家重点实验室为本书的完成提供了良好的工作环境, 感谢实验室各位老师与同学的大力支持, 感谢解放军理工大学肖军模教授、刘军副教授对本书部分内容的支持与帮助, 感谢作者的家属在本书编写过程中所给予的默默支持, 感谢科学出版社余丁编辑为本书出版所付出的辛勤劳动.

限于作者水平, 书中疏漏之处在所难免, 敬请读者指正.

作者联系方式：leixinfeng@iie.ac.cn, xuerui@iie.ac.cn.

目　　录

第二部分　密码协议分析概述

第三部分 密码协议逻辑

第四部分　计算可靠的密码协议逻辑

第一部分　理论基础

天地之变, 寒暑风雨
水旱螟蝗, 率皆有法

—— 沈括《梦溪笔谈 · 象数一》

在深入学习密码协议分析的逻辑方法之前, 有必要掌握一定的基础理论. 本部分主要就是以此为目的而编写的, 其主要内容包括数理逻辑与现代密码学的相关知识.

(1) 第 1 章对数理逻辑的基础概念以及与本书密切相关的逻辑系统进行简要介绍. 首先介绍了逻辑系统的组成以及一些语法和语义层次的概念, 其次分别介绍了命题逻辑、谓词逻辑、模态逻辑以及 Hoare 逻辑. 其中命题逻辑和谓词逻辑是最基本的内容, 几乎每种逻辑都是以它们为基础的; 模态逻辑 (尤其是知识逻辑和信念逻辑) 是许多密码协议逻辑的基础; Hoare 逻辑主要用于程序正确性证明, 本书所介绍的 PCL 中将会涉及.

(2) 第 2 章对现代密码学的基本概念以及与本书密切相关的内容进行了简要介绍. 首先从信息论安全与计算安全的主要思路入手, 然后从安全假设、安全定义以及安全证明 3 方面对现代密码学进行简要论述. 其中安全假设部分主要从计算复杂性理论的角度进行阐述; 安全定义包含加密方案和签名方案的一些主要安全性定义; 安全证明主要介绍了几种在可证明安全中常用的方法. 这些内容是为掌握密码协议逻辑计算可靠性奠定基础的.

第 1 章　数理逻辑基础

通俗地说, 数理逻辑将一些概念符号化, 将一些公认的思维规律公理化, 然后通过一定的推理由已知的事实得出未知的事实. 计算机的主要功能是符号运算, 如果赋予这些符号一定的语义, 那么就可以将现实中需要处理的一些问题符号化, 由计算机通过运算得到结果, 然后根据符号的语义, 将结果解释为现实中对该问题的解答. 可见, 数理逻辑是计算机科学天然的理论基础, 甚至可以毫不夸张地说, 所有形式化方法都直接或间接以数理逻辑为基础. 在信息安全领域, 尤其是密码协议分析领域, 数理逻辑发挥着非常重要的作用. 本章简要对书中将用到的一些逻辑进行介绍, 这些逻辑包括命题逻辑、谓词逻辑、模态逻辑以及 Hoare 逻辑等.

1.1　基 本 概 念

数理逻辑①也称现代逻辑或符号逻辑 (以下简称逻辑), 它通常由以下 3 部分组成[1].

(1) **语言**. 逻辑语言是一种形式化语言, 它与自然语言的不同之处在于它是人工定义的语言. 逻辑语言通常包括**符号表**和**语法**, 其中符号表规定了逻辑语言中所使用的符号, 由符号表和相关语法可生成**项**和**公式**. 直观上说, 逻辑语言中的符号、项、公式分别类似于自然语言中的字、词、句. 逻辑语言中的公式并不是符号的任意组合, 而是由符号表中的符号按照给定的语法规则构造的表达式, 通常将这种表达式称为**良构公式**(well-formed formulas)或**合式公式**, 简称**公式**.

(2) **语义**. 逻辑语言中的语句是由抽象符号构成的公式, 它本身并没有具体的含义, 要使其有意义, 必须给出相应的解释, 通过解释而得到的意义称为**语义**. 如将逻辑语言中的语句解释为关于一定对象的描述, 可反映对象的属性或对象之间的关系. 这些对象可以是数学对象, 如群、图、自然数等, 也可以是日常生活中的对象, 如汽车、计算机、员工等. 类似于自然语言中很多句子有正确与否之分, 逻辑语言中的语句有真假之分, 这种真假取值简称**真值**. 通过语义的定义可以确定一个逻辑语句的真值.

(3) **推演系统**. 推演系统由一组公理或推理规则组成. 其中, **公理**是一些公式,

① 此处所说的数理逻辑是一种狭义的理解, 主要是指命题逻辑、谓词逻辑以及其他一些相关的逻辑. 从广义上来说, 除以上逻辑系统, 数理逻辑研究的内容还包括公理集合论、证明论、递归论和模型论等内容.