

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 and 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

前言

第一部分 理论基础

第 1 章 数理逻辑基础	3
1.1 基本概念	3
1.2 命题逻辑	5
1.2.1 命题逻辑语法	5
1.2.2 命题逻辑语义	6
1.2.3 命题逻辑推演系统	7
1.2.4 命题逻辑的可靠性	8
1.3 谓词逻辑	9
1.3.1 谓词逻辑语法	9
1.3.2 谓词逻辑的语义	11
1.3.3 谓词逻辑推演系统	13
1.3.4 谓词逻辑的可靠性	13
1.4 模态逻辑	13
1.4.1 命题模态逻辑	14
1.4.2 谓词模态逻辑	17
1.4.3 知识逻辑与信念逻辑	19
1.5 Hoare 逻辑	20
1.6 本章小结	21
参考文献	21
第 2 章 现代密码学基础	23
2.1 概述	23
2.1.1 加密方案	23
2.1.2 对加密方案的攻击	24
2.1.3 信息论安全	24
2.1.4 现代密码学	25

2.2	计算复杂性	26
2.2.1	图灵机	26
2.2.2	时间复杂性	27
2.2.3	P 与 NP	28
2.2.4	多项式时间归约	28
2.2.5	概率图灵机与 BPP	29
2.3	计算安全	30
2.3.1	计算安全的概念	30
2.3.2	安全假设	31
2.3.3	几个安全相关概念	32
2.4	私钥加密	33
2.4.1	私钥加密方案	33
2.4.2	私钥加密方案的 CPA 安全	34
2.4.3	私钥加密方案的 CCA 安全	35
2.5	公钥加密	35
2.5.1	公钥加密方案	36
2.5.2	公钥加密方案的 CPA 安全	36
2.5.3	公钥加密方案的 CCA 安全	37
2.6	数字签名	37
2.6.1	数字签名方案	38
2.6.2	数字签名方案的安全性	38
2.7	安全性证明	39
2.7.1	概率多项式时间归约	39
2.7.2	混合论证	40
2.7.3	标准模型与随机应答器模型	40
2.8	本章小结	41
	参考文献	42

第二部分 密码协议分析概述

第 3 章	密码协议	45
3.1	密码协议的概念与意义	45
3.2	密码协议的属性与分类	46
3.3	对密码协议的攻击	47
3.4	密码协议的表示法	50

3.5	密码协议实例	51
3.6	本章小结	59
	参考文献	60
第 4 章	密码协议分析	61
4.1	形式化方法	61
4.1.1	形式化方法概览	61
4.1.2	DY 模型	64
4.1.3	Woo-Lam 模型及其扩展	66
4.2	计算方法	67
4.2.1	计算方法概览	67
4.2.2	BR 模型	68
4.2.3	其他模型	71
4.3	密码协议形式化分析的计算可靠性	71
4.3.1	基于映射的方法	72
4.3.2	基于模拟的方法	73
4.3.3	已有形式化方法的计算可靠性	73
4.3.4	计算方法的直接形式化	74
4.4	可复合密码协议分析	75
4.5	密码协议逻辑	76
4.6	本章小结	77
	参考文献	77

第三部分 密码协议逻辑

第 5 章	BAN 逻辑	87
5.1	BAN 逻辑的语法	87
5.2	推理规则	88
5.3	协议及其目标的描述	92
5.3.1	协议理想化	92
5.3.2	协议注解	93
5.3.3	认证目标的形式化	94
5.4	协议分析实例	95
5.4.1	NSSK 协议及其形式化分析	95
5.4.2	Kerberos 协议及其形式化分析	98
5.5	对 BAN 逻辑语义的简单讨论	101

5.6	对 BAN 逻辑的不同意见	103
5.6.1	Nessett 的评论	103
5.6.2	Snekkenes 的评论	105
5.7	本章小结	107
	参考文献	107
第 6 章	BAN 逻辑的扩展	108
6.1	GNY 逻辑	108
6.1.1	模型	108
6.1.2	GNY 逻辑的语法	109
6.1.3	推理规则	111
6.1.4	协议形式化	117
6.1.5	协议分析实例	118
6.2	VO 逻辑	123
6.2.1	语法扩展	123
6.2.2	公理与规则扩展	125
6.2.3	通用的形式化目标	125
6.2.4	通用的形式化假设	127
6.2.5	STS 协议分析	127
6.3	MB 逻辑	130
6.3.1	公式	131
6.3.2	推理规则	132
6.3.3	协议消息理想化	134
6.3.4	协议分析	135
6.4	本章小结	136
	参考文献	137
第 7 章	类 BAN 逻辑的语义	138
7.1	AT 逻辑	138
7.1.1	AT 逻辑对 BAN 逻辑的改进	138
7.1.2	语法	141
7.1.3	公理系统	142
7.1.4	模型	143
7.1.5	AT 逻辑的语义	145
7.2	SVO 逻辑	148
7.2.1	SVO 逻辑语言	148
7.2.2	公理系统	149

7.2.3	模型	152
7.2.4	SVO 逻辑的语义	154
7.2.5	SVO 逻辑的可靠性	158
7.2.6	基于 SVO 逻辑的协议分析	159
7.3	本章小结	162
	参考文献	163
第 8 章	BAN 逻辑的进一步扩展	164
8.1	Kailar 逻辑	164
8.1.1	可追责性	164
8.1.2	分析框架	165
8.1.3	分析假设	166
8.1.4	逻辑规则	167
8.1.5	协议目标	169
8.1.6	分析实例	169
8.2	BSW 逻辑	171
8.2.1	模型	172
8.2.2	BSW 逻辑语言	173
8.2.3	推理规则	174
8.2.4	定理	175
8.2.5	合成规则	175
8.2.6	协议分析与设计的实例	177
8.3	本章小结	181
	参考文献	181
第 9 章	非单调逻辑	182
9.1	引言	182
9.2	Moser 逻辑	182
9.2.1	知道与相信公理	183
9.2.2	unless 谓词	184
9.2.3	关于 unless 的例子	185
9.3	Rubin 逻辑	186
9.3.1	khat 协议	186
9.3.2	协议描述与分析概述	187
9.3.3	全局集	188
9.3.4	本地集	189
9.3.5	信任矩阵	190

9.3.6	行为描述	191
9.3.7	更新函数	193
9.3.8	推理规则	194
9.3.9	对 khat 协议的描述与分析	195
9.4	本章小结	199
	参考文献	200
第 10 章	引入时间的协议逻辑	201
10.1	CKT5 逻辑	201
10.1.1	CKT5 逻辑术语	202
10.1.2	安全性定理	205
10.2	CS 逻辑	208
10.2.1	语法	208
10.2.2	公理与推理规则	209
10.2.3	实例分析	211
10.3	GS 逻辑	213
10.3.1	扩展术语及规则	214
10.3.2	协议分析实例	215
10.4	本章小结	218
	参考文献	218
第 11 章	时间相关密码协议逻辑及其形式化语义	220
11.1	TCPL 的引入	220
11.2	TCPL 的语法	222
11.3	公理与规则	225
11.4	TCPL 的语义	228
11.4.1	模型	228
11.4.2	语义	232
11.5	TCPL 的可靠性	233
11.6	基于 TCPL 的密码协议形式化建模方案	238
11.6.1	密码协议建模	238
11.6.2	安全属性建模	241
11.7	基于 TCPL 的密码协议分析	243
11.7.1	定时发布协议	243
11.7.2	NSPK 协议	249
11.8	进一步讨论	250
11.9	本章小结	252

参考文献	252
第 12 章 协议复合逻辑	255
12.1 协议编程语言	255
12.1.1 PPL 的语法	255
12.1.2 PPL 的语义	258
12.2 协议及其属性	259
12.2.1 协议执行模型	259
12.2.2 协议属性	260
12.3 PCL 的语法与语义	261
12.3.1 PCL 的语法	261
12.3.2 PCL 的语义	262
12.4 证明系统	264
12.5 PCL 的可靠性	267
12.6 协议分析实例	270
12.6.1 弱认证	270
12.6.2 强认证性	271
12.7 协议复合	272
12.7.1 并行复合	272
12.7.2 顺序复合	273
12.7.3 协议复合实例	274
12.8 PCL 协议存在的问题	275
12.9 本章小结	276
参考文献	276

第四部分 计算可靠的密码协议逻辑

第 13 章 AR 逻辑	281
13.1 形式化加密与消息等价	281
13.1.1 形式化消息	281
13.1.2 消息等价	282
13.2 加密方案与不可区分性	284
13.2.1 加密方案的安全性	284
13.2.2 加密方案安全性的定义	285
13.3 形式等价的计算可靠性	286
13.3.1 总体关联	287

13.3.2 等价性蕴涵不可区分性	287
13.4 不完备性	293
13.5 完备性定理	295
13.5.1 无混淆加密与认证加密	296
13.5.2 完备性定理	297
13.6 本章小结	305
参考文献	306
第 14 章 对 AR 逻辑的扩展	307
14.1 形式化模型	308
14.1.1 消息	308
14.1.2 模式	310
14.1.3 等价	313
14.2 计算模型	315
14.3 计算可靠性	317
14.4 本章小结	324
参考文献	325
第 15 章 计算可靠的 PCL	327
15.1 协议语法	327
15.2 逻辑语法	328
15.3 证明系统	329
15.4 证明实例	330
15.5 协议的执行	331
15.6 计算语义	333
15.7 本章小结	336
参考文献	336
第 16 章 IK 逻辑	337
16.1 T 系统	338
16.1.1 语法	340
16.1.2 T 系统的公理	341
16.1.3 T 系统的可靠性	345
16.2 基于 T 系统的实例证明	345
16.3 计算不可区分系统	348
16.3.1 语法	348
16.3.2 证明规则	349
16.4 基于 IK 逻辑的证明实例	350

16.5 IK 逻辑的可靠性	351
16.6 本章小结	352
参考文献	353
第 17 章 计算不可区分逻辑	354
17.1 应答器系统	354
17.1.1 应答器系统与敌手	354
17.1.2 语义	357
17.1.3 事件	358
17.2 CIL 的语句与基本规则	359
17.2.1 语句	359
17.2.2 基本规则	359
17.3 上下文	360
17.4 互模拟	362
17.5 确定性	364
17.6 CIL 的规则与可靠性	364
17.6.1 上下文与应答器规则	364
17.6.2 派生规则与外部前提	365
17.7 概率签名方案	366
17.7.1 随机应答器	367
17.7.2 形式化证明	368
17.8 本章小结	372
参考文献	373
结束语	374
索引	377

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.