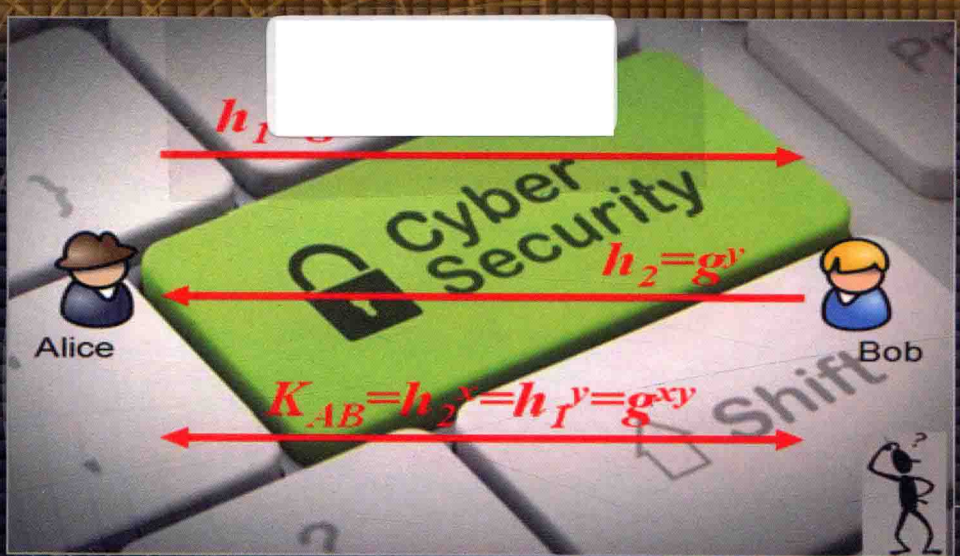
国防科技图书出版基金

网络与信息安全前沿技术丛书

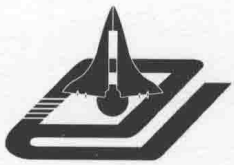
安全协议设计与分析

张文政 王立斌 李益发 郑东 董新锋 编著

Design and Analysis of Security Protocols



国防工业出版社
National Defense Industry Press



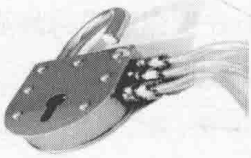
国防科技图书出版基金

网络与信息安全前沿技术丛书

张文政　王立斌　李益发　郑东　董新锋　编著

安全协议
设计与分析

Design and Analysis of Security Protocols



你想了解网络世界怎样进行安全通信的吗？其中安全协议的设计是非常重要的。安全协议是利用安全的密码算法在两个或两个以上的通信者之间规定一系列通信步骤，达到通信者预期的安全目标。本书全面给出了安全协议的设计准则，以及逻辑化分析方法、串空间方法及可证明安全性方法，并给出了应用实例。本书可作为工程技术人员及大学师生的学习参考书籍。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

安全协议设计与分析 / 张文政等编著. —北京：国防工业出版社，2015.11
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-10339-7

Ⅰ.①安… Ⅱ.①张… Ⅲ.①计算机网络-安全技术-通信协议-研究 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 268695 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）
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　**印张** 14　**字数** 255 千字
2015 年 11 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 78.00 元

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需

要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	杨崇新	
秘书长	杨崇新			
副秘书长	邢海鹰	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

计算机技术及通信技术的快速发展，使人们的生活发生了极大的变化。人们在利用先进的通信技术时，也面临着许多问题，其中信息安全技术是重要问题之一。信息安全主要研究在攻击者能够参与通信的环境中，如何保证信息的安全性，主要包括信息的保密性、完整性、可用性等。它是计算机科学、数学、通信等多门学科的综合学科。安全协议是信息安全中的重要分支之一，它是研究利用安全的密码算法如何能够达到通信者的安全目标。

自从有了安全协议的应用，就有了安全协议的安全性分析。安全协议是利用安全的密码算法在两个或两个以上的通信者之间规定一系列通信步骤，达到通信者预期的安全目标。最初人们是靠密码工作者的经验和手工分析对安全协议进行安全性分析。之后人们发现有些协议通过人工分析结果是安全的，但在使用多年之后却又发现这些协议是存在安全漏洞的。这使得密码工作者更加重视安全协议的分析与设计，同时也意识到分析安全协议是一件非常困难的事情。通过20余年的发展，人们已经寻找了一些分析安全协议的方法。这些方法可以使人们在设计协议时降低安全漏洞的风险，也可以对设计出的安全协议进行安全检测。近年来，安全协议分析无论在理论研究，还是在实际应用方面，都得到了人们的重视。在人才培养方面，国内外高校的相关专业都设置了安全协议分析研究方向。目前，关于安全协议分析的书籍很少，能够用于相关人员系统阅读的书更是寥寥无几。无论是高校相关专业的学生和老师，还是相关研究人员和工程人员，都需要一本涵盖最新研究成果并有一定深度的教材，使得读者能够了解安全协议分析的基本内容，又能够为希望了解安全协议分析深奥理论的读者提供一条快速通道。

本书作者是保密通信重点实验室的张文政研究员和几所高校长期从事安全协议研究的教师合作完成。本书所有作者都是从事安全协议分析长达十多年的一线教师或科研人员。他们长期从事“密码学”“安全协议”

等专业的教学和科研。作者注意到现代社会对信息安全人员需求的持续增长和现有专业人员明显短缺这一现象、了解相关学者对安全协议分析与设计的浓厚兴趣，书中内容正是基于作者的研究、教学经验并参考相关文献编写而成。

本书按照安全协议研究背景、安全协议设计准则、安全协议分析方法及实例分析等合理顺序编排章节。本书可以作为大学计算机、信息安全专业高年级本科生选修教材，也可作为计算机和信息安全专业的研究生教材，还可作为相关工程技术人员学习安全协议的参考书籍。

本书共分7章，内容包括安全协议背景、逻辑化分析方法、串空间分析方法，可证明安全性分析方法、基于中心服务器认证的密钥交换协议分析、基于口令的认证密钥交换协议、RFID协议设计与分析等。与本书相关的科研工作受到国家自然科学基金61070249、保密通信重点实验室基金资助。

限于我们的水平和经验不足，书中的错误和缺憾在所难免，诚恳地希望读者对书中的错误和问题能够及时指出。我们欢迎对本书的批评和建议，以便我们以后对本书进行修改。

编著者

2015年9月

于保密通信重点实验室

目　录

Contents