信息安全技术丛书

隐私保护安全协议研究

朱宏峰　刘天华　著

科学出版社

信息安全技术丛书

隐私保护安全协议研究

朱宏峰　刘天华　著

科学出版社

北京

内 容 简 介

本书主要分为三篇：第一篇是基础篇，主要介绍安全协议的概念、数学基础、密码学工具、可证明理论以及隐私保护安全协议；第二篇是进阶篇，提出多个概念与协议，如 OTIP（one-time identity password）、完全公平匿名签名、混沌映射构造的两方和三方隐私保护认证密钥协商、完备电子优惠券系统等；第三篇是高级篇，主要探讨普适化形式的概念与协议，如面向多服务器体系结构的单向 AKE 协议、多密钥隐私保护协议和多方隐私保护协议等。

本书可供信息安全、计算机等相关专业教师、研究生阅读，也可供相关领域工程技术人员阅读参考。

图书在版编目 (CIP) 数据

隐私保护安全协议研究/朱宏峰，刘天华著. —北京：科学出版社，2015.6

(信息安全技术丛书)

ISBN 978-7-03-044707-8

Ⅰ. ①隐… Ⅱ. ①朱… ②刘… Ⅲ. ①计算机网络－安全技术

Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 123168 号

责任编辑：任 静 / 责任校对：郭瑞芝

责任印制：张 倩 / 封面设计：迷底书装

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

铭浩彩色印装有限公司 印刷

科学出版社发行 各地新华书店经销

*

2015 年 6 月第 一 版 开本：720×1 000 1/16

2015 年 6 月第一次印刷 印张：15 1/4

字数：291 000

定价：68.00 元

（如有印装质量问题，我社负责调换）

作 者 简 介

朱宏峰（1978～），男，博士，沈阳师范大学副教授。研究方向为分布式网络、网络工程、计算机系统结构、网络安全等。曾参与省级科研项目 5 项，目前主持辽宁省自然科学基金计划一项（立项编号：20102202），沈阳师范大学实验中心主任基金项目一项（立项编号：SY200906）。曾获辽宁省自然科学学术成果奖一等奖，辽宁省自然科学学术成果奖论文类三等奖。在 SCI 期刊、EI 期刊以及学术会议上发表论文 50 余篇，主编教材两部，合著专著一部。

刘天华（1966～），男，博士，沈阳师范大学教授，CCF、YOCSEF 沈阳副主席，中国电子学会高级会员。长期从事计算机网络、网络安全、信息安全、嵌入式系统领域的教学及科研工作。主持及参与国家自然科学基金、省级自然科学基金等纵向和横向项目 8 项，在国内外重要学术刊物以及学术会议上发表论文 40 余篇，先后主持、参与沈阳师范大学、辽宁大学、沈阳建筑大学、鞍山科技大学等新校园计算机网络工程建设和设计评审工作。

前　言

随着 Internet 的迅猛发展，以及搜索引擎和数据挖掘等技术的广泛应用，Internet 上的隐私问题已越来越被关注。隐私不仅意味着信息的机密性，而且意味着信息发布者身份的机密性。从更高级别的角度来看，甚至服务器为用户提供的各种服务，也均要保证机密性。

匿名技术是 Internet 上保护用户隐私的一种有效手段，主要通过三个方面来体现。

（1）解决“谁和谁”问题。匿名技术通过一定的方法将通信流中的通信关系加以隐藏，使攻击者无法获知“谁和谁”在通信、通信的时间以及通信流的多少等。对许多应用来说，匿名已成为不可缺少的要求。

（2）解决“谁做什么”问题。该问题是针对服务器对某个用户提供服务时，将服务结果加以隐藏，除了用户本身，任何人均不知道该用户通过服务器得到的结果是什么，如可搜索加密等。

（3）解决“公平服务”问题。当服务器对用户某种服务加以存储时，用户和其存储结果不能一一对应。对服务器来说，不能分辨某个用户与该用户存储的数据的对应关系，即对存储的结果加以隐藏，防止管理员随意删除普通用户（加密）的数据，如纠缠云存储等。

匿名技术所搭载的最佳载体是“安全协议”（secure protocol）。安全协议是建立在密码体制基础上的一种高互通协议，运行在计算机通信网或分布式系统中，为安全需求的各方提供一系列步骤，借助密码算法来实现密钥分配、身份认证、信息保密以及安全地完成电子交易等。安全协议的研究已经历近三十年，取得了丰硕的成果，但强调隐私保护的安全协议最近几年才迅猛发展，大量的隐私泄露，使用户成为攻击靶心：垃圾短信、骚扰电话、账户泄露等一系列隐私泄露问题呈指数级增长，导致用户不得不关注隐私的问题。安全协议是信息安全领域中理论通向应用的“桥梁”，好比是信息安全领域的“操作系统”，也像软件与硬件结合的“指令系统”。安全协议是为互联网时代数以万计应用提供安全服务的通用形式，在安全协议的设计过程中，加入匿名技术后，其打造的匿名应用是呈指数级扩展的。此外，本书以“隐私保护安全协议研究”来命名的主要原因为：①安全协议可作为应用的通用基点，既具有理论价值，又可大面积推广应用；②构造安全协议虽然极其复杂，但对极微本原（即困难问题）不做研究，只需证明协议安全，因为安全协议的安全性归约到极微本原（计算复杂度类领域）；③安全协议变化多端，研究领域非常多。

本书对隐私保护安全协议采用对比分析设计方法，明确安全所依赖的基本工具，

清晰地阐述建模与设计流程，最终给出安全的可证明性，这些研究将为网络信息系统的隐私保护奠定坚实的基础。

需求是科研的原动力，为此，本书在隐私保护安全协议的选材方面，强调设计通用、普适化形式的设计思想，不强调多、全、杂，而注重少、精、新，在安全协议中融合隐私保护的属性，同时引入可证明安全、可组合安全和量子纠缠传统应用等新模式。

本书在基础理论模块中按照“全书架构→数学基础→基本工具→设计方法与模型→隐私概述”结构逐步进行阐述。在模型与设计模块中严格遵照作者的研究顺序（领域架构→研究现状→问题提出→问题解决→未来研究）进行编写，在每一节中提出问题并给出相应的解决方案。各章内容既相互联系又相对独立，紧紧围绕解决安全协议中针对不同服务环境的设计思想、设计方法、采用的模型和折中效率与安全等实际问题，并给出安全性证明、通信量和计算量等参数的横向对比结果，使读者对隐私保护安全协议领域的研究有全面的认识。

特此，作者将 5 年多来的研究进行回顾和总结，对有关方面的工作加以介绍，与国内同行进行交流，使隐私保护安全协议的研究更加深入，真诚希望从事相关研究的同仁为本书提出宝贵意见，以便推动我国这项事业的进一步发展。

作者对在研究过程中的合作者（沈阳师范大学的郝新、张一峰、夏宇、张妍）和所有提供过帮助的人员表示诚挚的谢意。

作　者

2015 年 1 月于沈阳

目　录

第二篇 进 阶 篇

第三篇　高　级　篇

第一篇　基　础　篇

第 1 章　安全协议概述

如果把一封信锁在保险柜中，把保险柜藏在纽约的某个地方，然后告诉你去看这封信，这并不是安全，而是隐藏。相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全的概念。隐藏是攻击者不知道从何下手，安全是你知道也没办法下手。

上述类比中，可以如此理解安全体系中的各个部件：数学是保险柜的材质，坚固可靠。密码学是锁，利用符合条件的数学知识构造。安全协议是保险柜，其完美整合的设计是实践化的最佳载体。保险柜保护的内容就是安全协议保护的互联网上的各种应用。

1.1　安全协议的基本概念

信息安全是一个没有尽头的任务，信息社会存在一天，信息安全就会存在一天。攻防共生共存，魔高一尺，道高一丈，反之亦然。完美的理论，并不一定能够解决信息安全的实际问题，理论到实践是一个系统工程，而安全协议的模型与设计是这个工程的核心，是承载信息安全体系的脊梁，是应用选择理论的载体：设计安全协议不单单是基于技术本身，也要考虑应用的成本、代价和体验。

1.1.1　定义

所谓协议（protocol），就是两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。这包含三层含义：①协议自始至终是有序的过程，每一个步骤必须依次执行。在前一步没有执行完之前，后面的步骤不可能执行。②协议至少需要两个参与者。一个人可以通过执行一系列的步骤来完成某项任务，但它不构成协议。③通过执行协议必须能够完成某项任务。

协议还有其他特点。

（1）协议中的每个人都必须了解协议，并且预先知道所要完成的所有步骤。

（2）协议中的每个人都必须同意遵循它。

（3）协议必须是不模糊的，每一步必须明确定义，并且不会引起误解。

（4）协议必须是完整的，对每种可能的情况必须规定具体的动作。

安全协议（security protocol）是建立在某种体系（密码体制、量子禀性）基础上

且提供安全服务的一种交互通信的协议，它运行在计算机通信网络或分布式系统中，借助于特定算法来达到密钥分配、身份认证等目的。安全协议的密码基础是由三类基石构造的，如图 1.1 所示。

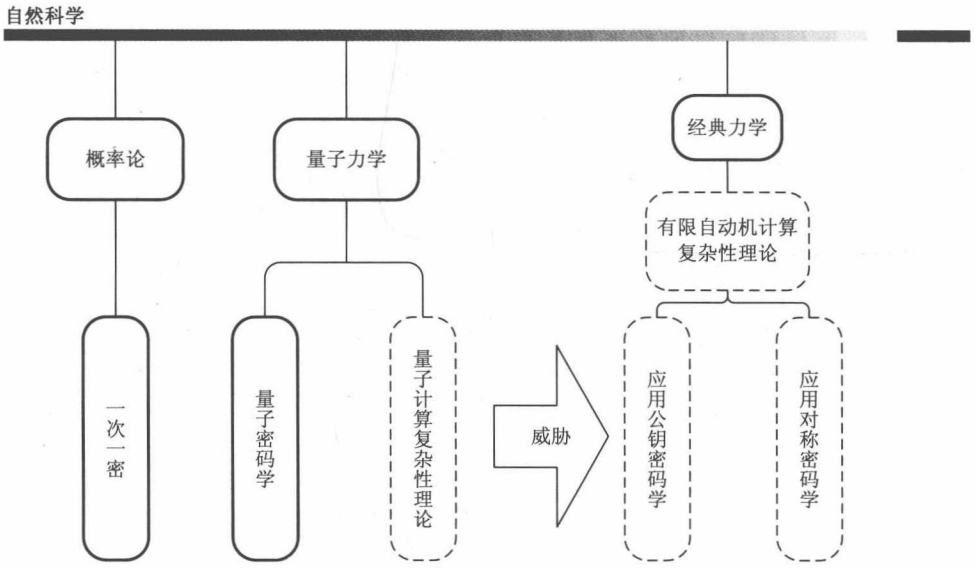

图 1.1　三类密码学的理论基础

安全协议的通信系统基本安全模型如图 1.2 所示。

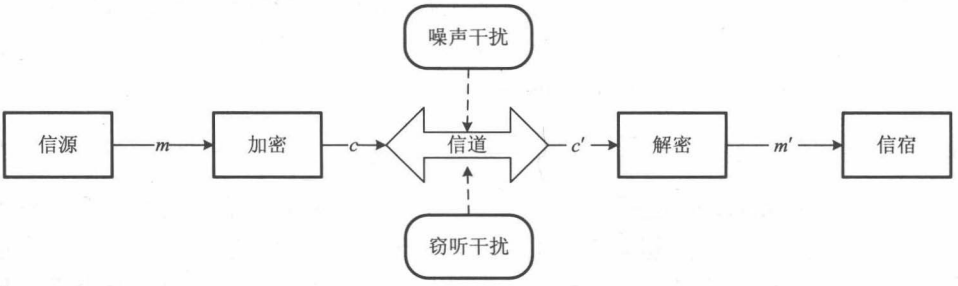

图 1.2　通信系统的安全模型

安全协议的参与者可能是可以信任的实体，也可能是攻击者和完全不信任的实体。安全协议的目标不只是实现信息的加密传输，参与协议的各方可能希望通过分享部分秘密来计算某个值、生成某个随机序列、向对方表明自己的身份或签订某个合同等。解决这些安全问题就需要在协议中采用密码技术，因为它们是防止或检测非法用户对网络进行窃听和欺骗攻击的关键技术措施。对于采用这些技术的安全协议，如果非法用户不可能从协议中获得比协议自身所体现的更多的、有用的信息，那么可以说协议是安全的。安全协议中采用了多种不同的密码体制，其层次结构如表 1.1 所示。

表 1.1　安全协议层次结构

高级协议	身份认证、不可否认、群签名；量子密钥分发、博弈量子密钥协商
基本协议	数字签名、零知识、秘密共享；量子签名
基本算法	对称加密、非对称加密、Hash 函数；量子 Hash 函数
基础	核心断言、数论、抽象代数、数学难题；不可克隆、真随机性

从表 1.1 可看出，安全协议建构在数学或量子信息科学基础和基本算法之上，并且往往涉及秘密共享、加密、签名、承诺、零知识证明等许多基础协议，因此安全协议的设计比较庞大且复杂，设计满足各种安全性质的安全协议成为一项具有挑战性的研究工作。

当前存在着大量的实现不同安全服务的安全协议，其中最常用的基本安全协议按照其完成的功能可分类起名，如电子支付协议、分布式环境下的身份鉴别协议、不可否认协议、密钥协商协议等。

1.1.2　目的

在日常生活中，几乎所有的事情都有非正式的协议：电话订货、玩扑克、选举中投票，人们都知道怎样使用它们，而且它们也很有效。随着信息技术的高速发展，将这些现实的协议功能转化为数字，从而在计算机世界中实现是顺理成章的事情。越来越多的人通过计算机网络交流代替面对面的交流，计算机需要正式的协议来完成人们不用考虑就能做的事情，虽然方便大众，但也不是很容易就能实现的：如果你从一个城市迁移到另一个城市，可能会发现投票亭与你以前使用的完全不同，你会很容易去适应它，但计算机就不那么灵活了。

许多面对面的协议依靠人的现场存在来保证公平和安全。你会交给陌生人一叠现金去为你买食品吗？如果你没有看到他洗牌和发牌，那么你愿意和他玩扑克吗？如果没有匿名的保证，那么你会将秘密投票寄给政府吗？

那种假设使用计算机网络的人都是诚实的想法，是天真的。天真的想法还有：假设计算机网络的管理员是诚实的，假设计算机网络的设计者是诚实的。当然，绝大多数人是诚实的，但是不诚实的少数人可能招致很多损害。通过规定协议，可以查出不诚实者企图欺骗的把戏，还可开发挫败这些欺骗者的协议。

除了规定协议的行为，还根据完成某一任务的机理，抽象出完成此任务的过程。由于基本底层通信协议是相同的，对于高层的安全协议是一个黑盒子，所以我们专注设计协议流程与分析，而不用受限于具体的实现。

1.1.3　游戏角色

为了帮助说明协议，通常选出几个人作为助手：Alice 和 Bob 是开始的两个人。他们将完成所有的两人协议。按规定，由 Alice 发起所有协议，Bob 响应。如果协议需要第三或第四人，那么 Carol 和 Dave 将扮演这些角色。由其他人扮演的专门配角，如表 1.2 所示。

表 1.2　剧中人

Alice	所有协议中的第一个参加者	Mallory	恶意的主动攻击者
Bob	所有协议中的第二个参加者	Trent	值得信赖的仲裁者
Carol	在三、四方协议中的参加者	Walter	监察人：在某些协议中保护 Alice 和 Bob
Dave	在四方协议中的参加者	Peggy	证明人
Eve	窃听者	Victor	验证者

游戏角色可以扩展为 N 方，其行为可以分为外部攻击和内部攻击，攻击参与方可以分为个体或团体。因此，四组攻击方式可分为：个体外部攻击、个体内部攻击、团体外部攻击和团体内部攻击。四种攻击方式因目标和意义不同而不同。但通常来说，四种攻击从前往后越来越复杂。

经典案例　内部团体协作之拜占庭将军问题

问题描述如下。

（1）1982，Lamport(SRI), Pease, Shostak。

（2）几个将军围困一座城池，大家必须协商一种策略，进攻还是撤退。

（3）如果有的进攻，有的撤退就有可能打败仗。

（4）条件：有的将军叛国，希望爱国的将军打败仗（破坏达成一致）。

（5）目标：有什么办法使爱国的将军在这种环境下达成一致？

问题抽象如下。

（1）消息的传送是可靠的。

（2）所有的将军可以互相发消息，也可以传递消息。例如，一个叛变的将军可以告诉将军 A“B 要攻城”，并告诉将军 C“B 要撤退”。

（3）口头消息模型和书写消息模型。

（4）目标是达成一致，而不是找背叛的将军。

口头消息如下。

（1）解决的办法：每个爱国者都采用多数人的意见一致算法。

（2）这要求每个爱国者得到相同的表决。

（3）面临的问题就变为：每个爱国的将军获得的其他将军的观点是相同的（每个将军都有一个其他将军的决策）。如果将军 i 是爱国的，则其他将军必须得到将军 i 的真实决策。

解决方案为采用多数投票表决方式。

例 1.1　3 个忠诚将军，1 个叛变将军。Lamport 递归算法，共 4 步，如图 1.3 所示。

(a)对外报告　(b)收集向量　(c)报告向量　(d)生成结果向量：（1，2，未知，4）。

例 1.2　若三个将军中，有两个忠诚将军，一个叛变将军，则不能判断出哪个将军叛变，如图 1.4 所示。

最终结论如下。