

<<安全协议模型与设计>>

图书基本信息

书名：<<安全协议模型与设计>>

13位ISBN编号：9787030343260

10位ISBN编号：7030343263

出版时间：2012-8

出版时间：科学出版社

作者：刘天华、朱宏峰

页数：209

字数：290750

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：<http://www.tushu007.com>

<<安全协议模型与设计>>

内容概要

《安全协议模型与设计》介绍了安全协议的整体结构、设计流程与分析方法。

第1~3章介绍了安全协议的基本概念以及采用的数学知识与密码工具，第4章介绍了安全协议的可证明理论，第5~7章探讨了不同环境下安全协议的设计与分析。

针对现有安全协议中出现的问题，提出了一些针对常见协议的改进协议，经过性能测试具有较好的实用性。

《安全协议模型与设计》适合普通高等院校信息安全方向的教师、研究生以及从事安全协议等研究方向的科研人员阅读参考。

<<安全协议模型与设计>>

作者简介

刘天华（1966~），男，博士，沈阳师范大学教授，硕士生导师。

中国计算机学会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、教育信息技术方面的教学及科学研究工作。

主持及参与国家自然科学基金、省自然科学基金等纵向和横向项目10项，在国内外重要学术刊物以及学术会议上发表论文30余篇，撰写和主编专业著作和教材12部，获省部级有关奖励3项。

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。

先后参加省级科研项目6项，在国内外重要学术刊物及学术会议上发表学术论文30余篇，曾获得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，出版教材2部。

<<安全协议模型与设计>>

书籍目录

前言第1章 引言1.1 安全协议的基本概念1.1.1 定义1.1.2 目的1.1.3 游戏角色1.2 安全协议的分类1.2.1 第一种分类方法1.2.2 第二种分类方法1.2.3 其他方法1.3 安全协议的模型与分析方法1.4 安全协议的目标与研究层次1.5 安全协议的设计原则第2章 安全协议的数学基础2.1 数论基础2.1.1 整除及辗转相除2.1.2 算术基本定理2.1.3 同余式2.1.4 费马小定理和欧拉定理2.2 抽象代数基础2.3 离散概率基础2.4 信息论基础2.5 计算复杂性理论基础2.5.1 基本概念2.5.2 计算模型与判定问题2.5.3 复杂性类2.6 计算困难问题及其假设2.6.1 大整数因子分解问题和RSA问题2.6.2 离散对数和Diffie-Hellman问题2.6.3 椭圆曲线和双线性对问题第3章 安全协议的密码学工具3.1 密码学基本概念3.1.1 加密:历史回顾3.1.2 密码演化3.2 古典密码3.3 计算密码3.3.1 对称密钥密码3.3.2 公开密钥密码3.3.3 数字签名3.3.4 Hash函数3.3.5 消息认证与消息认证码3.3.6 伪随机函数第4章 安全协议的可证明理论4.1 密码体制的攻击游戏4.2 随机预言模型下的安全性证明4.3 标准模型下的安全性证明第5章 基本安全协议研究5.1 认证协议5.1.1 认证协议的基本概念5.1.2 认证协议的基本技术5.1.3 常规认证协议5.2 密钥交换协议5.2.1 可信模型5.2.2 安全性讨论5.3 认证及密钥交换协议5.3.1 基于口令的认证及密钥交换协议5.3.2 基于身份的认证及密钥交换协议5.3.3 典型认证及密钥交换协议5.4 抗字典攻击的E-3PAKE协议5.4.1 PAKE中典型字典攻击案例分析——DHEKE协议5.4.2 PAKE中典型字典攻击案例分析——STW-3PAKE5.4.3 PAKE中典型字典攻击案例分析——3PAKE-2'协议5.4.4 抗字典攻击的E-3PAKE协议5.5 基于认证符的高效跨域EV-C2C-PAKE协议5.5.1 相关工作5.5.2 基于认证符的高效跨域EV-C2C-PAKE协议5.5.3 基本工具5.5.4 EV-C2C-3PAKE5.5.5 安全与性能分析5.5.6 实例与结论5.6 一种基于椭圆曲线的无认证表高效鲁棒PAKE方案5.6.1 Juang方案的一种攻击方法5.6.2 一种改进方案5.6.3 效率与安全性分析5.7 基于口令的门限密钥交换协议5.7.1 TPAKE协议模型5.7.2 TPAKE协议描述5.7.3 安全性证明与性能分析第6章 两方安全协议研究6.1 零知识协议6.1.1 零知识思想6.1.2 交互证明系统6.1.3 零知识证明6.2 比特承诺协议6.2.1 比特承诺简介6.2.2 比特承诺实例6.3 掷币协议6.4 电话扑克协议6.5 不经意传输协议6.6 可否认认证协议6.7 同步秘密交换协议6.8 一种P2P网络中的高效隐蔽搜索协议6.8.1 引言6.8.2 隐蔽搜索模型设计6.8.3 安全性与性能分析6.9 一种基于随机预言模型的完全公平签名方案6.9.1 引言6.9.2 预备知识6.9.3 基本模型6.9.4 基于Schnorr signature的FKESS实例6.9.5 FKESS的安全性与效率分析第7章 多方安全协议研究7.1 基本多方协议7.1.1 秘密共享7.1.2 可验证秘密共享7.1.3 BD协议7.1.4 保密的多方计算7.2 电子选举协议7.2.1 电子选举的基本概念7.2.2 安全电子选举模型7.2.3 安全电子选举结构7.2.4 安全电子选举优缺点与实例7.3 数字现金7.3.1 现实场景分析7.3.2 盲签名7.3.3 群签名7.4 一种基于口令的群组密钥协商协议PAGKA7.4.1 群组密钥管理分类7.4.2 基于口令的组通信密钥协商协议7.4.3 一种基于口令的组通信密钥协商协议PAGKA7.4.4 PAGKA属性分析与结论7.5 基于树结构的分布式组密钥协商协议7.5.1 可认证BD协议7.5.2 基于树结构具有认证功能的组密钥协商协议TABD7.5.3 安全性和性能分析7.5.4 结论参考文献

<<安全协议模型与设计>>

编辑推荐

刘天华、朱宏峰编著的《安全协议模型与设计》从内容上可分为基础理论、模型与设计两部分，并在模型与设计部分中穿插作者多年的研究成果。

本书在基础理论部分中按照“全书架构—数学基础—基本工具—设计方法与模型”结构逐步进行阐述。

在模型与设计部分中按照“领域架构—研究现状—问题提出—问题解决—未来研究”进行编写，在每一小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、所采用的模型以及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，使读者对安全协议领域的研究有深刻的认识，从而起到抛砖引玉的作用。

<<安全协议模型与设计>>

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:<http://www.tushu007.com>