

《电子商务交易协议理论与验证方法》

图书基本信息

书名：《电子商务交易协议理论与验证方法》

13位ISBN编号：9787306035004

10位ISBN编号：7306035002

出版时间：2010-7

作者：王茜

页数：181

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《电子商务交易协议理论与验证方法》

内容概要

《电子商务交易协议理论与验证方法》是对国家自然科学基金资助项目“基于离线可信第三方的电子现金交易系统理论与方法”的一个全面总结。全书围绕电子商务交易协议相关理论和协议验证方法展开，从保护交易双方利益的角度出发，针对电子商务交易协议，尤其是电子现金支付理论研究和实际应用中存在的瓶颈问题，以电子商务交易安全框架为主线，对电子商务交易协议的底层安全技术、交易协议属性、交易协议的模型以及交易协议验证的理论和方法进行了系统的阐述。

书籍目录

第一章 电子商务交易系统	1.1
1.1 电子商务交易系统发展	1.1.1
1.1.1 电子商务交易的网上支付发展	1.1.1.1
1.1.2 电子现金交易系统发展	1.1.1.2
1.1.3 电子商务交易的个性化推荐系统发展	1.1.1.3
1.2 电子商务交易系统安全体系	1.2.1
1.2.1 电子商务安全技术体系	1.2.1.1
1.2.2 加密技术层	1.2.1.2
1.2.3 安全认证层	1.2.1.3
1.3 电子商务交易协议属性及分析	1.3.1
1.3.1 电子商务交易协议特殊性	1.3.1.1
1.3.2 电子商务交易协议属性	1.3.1.2
1.3.3 电子商务交易协议比较分析	1.3.1.3
第二章 电子现金交易协议研究进展	2.1
2.1 交易协议的公平性	2.1.1
2.1.1 渐进式互换实现公平性	2.1.1.1
2.1.2 On—line TTP方法实现公平性	2.1.1.2
2.1.3 Off—line TTP方法实现公平性	2.1.1.3
2.2 交易协议的原子性研究	2.2.1
2.2.1 原子性解决方案	2.2.1.1
2.2.2 匿名原子交易协议	2.2.1.2
2.3 交易协议的匿名性研究	2.3.1
2.3.1 无条件的电子现金方案	2.3.1.1
2.3.2 有条件的电子现金方案	2.3.1.2
2.4 交易协议的电子现金可分性研究	2.4.1
2.4.1 基于二叉树的可分电子现金方案	2.4.1.1
2.4.2 不使用二叉树的可分电子现金方案	2.4.1.2
2.5 数据压缩k-spensible电子现金方案	2.5.1
2.5.1 数据压缩k-spensible电子现金方案的效率研究	2.5.1.1
2.5.2 数据压缩k-spensible电子现金方案的可分性研究	2.5.1.2
2.5.3 数据压缩k-spensible电子现金方案的其他研究方向	2.5.1.3
第三章 匿名原子的电子现金交易协议模型	3.1
3.1 交易协议模型研究进展	3.1.1
3.2 E-Cash交易协议电子商务系统模型化	3.2.1
3.2.1 协议模型假设	3.2.1.1
3.2.2 电子商务系统的模型化	3.2.1.2
3.3 离线可信第三方匿名原子的电子现金交易协议模型	3.3.1
3.3.1 数据类型及映射函数	3.3.1.1
3.3.2 消费者本地协议模型	3.3.1.2
3.3.3 商家本地协议模型	3.3.1.3
3.3.4 离线可信第三方本地协议模型	3.3.1.4
3.4 交易协议模型的原子性分析	3.4.1
3.4.1 协议模型的原子性表示	3.4.1.1
3.4.2 对于原子性分析	3.4.1.2
3.4.3 原子性分析	3.4.1.3
第四章 匿名原子的电子现金交易协议研究	4.1
4.1 扩展的CEMBS可验证加密算法	4.1.1
4.1.1 系统建立	4.1.1.1
4.1.2 消息的加密	4.1.1.2
4.1.3 CEMBS可验证加密的生成	4.1.1.3
4.1.4 CEMBS验证	4.1.1.4
4.1.5 TTP对加密消息m解密	4.1.1.5
4.2 ICSP交互确认协议设计	4.2.1
4.2.1 注册	4.2.1.1
4.2.2 ICSP交互协议	4.2.1.2
4.2.3 不可否认数字签名的转换	4.2.1.3
4.2.4 ICSP协议的安全性分析	4.2.1.4
4.3 离线可信第三方的匿名原子电子现金交易协议	4.3.1
4.3.1 交易协议设计思想	4.3.1.1
4.3.2 E-Cash提取	4.3.1.2
4.3.3 Transaction协议	4.3.1.3
4.3.4 Cresolve协议	4.3.1.4
4.3.5 Mresolve协议	4.3.1.5
4.3.6 Abort协议	4.3.1.6
4.4 匿名原子交易协议分析比较	4.4.1
4.4.1 原子性分析	4.4.1.1
4.4.2 匿名性分析	4.4.1.2
4.4.3 终止性分析	4.4.1.3
4.4.4 安全有效性分析	4.4.1.4
4.4.5 不可否认性分析	4.4.1.5
4.5 交易协议的比较分析	4.5.1
4.5.1 协议执行效率比较	4.5.1.1
4.5.2 交易时限和终止性	4.5.1.2
4.5.3 数据存贮	4.5.1.3
第五章 安全协议验证分析方法研究	5.1
5.1 BAN逻辑	5.1.1
5.1.1 BAN逻辑概述	5.1.1.1
5.1.2 BAN逻辑的缺陷	5.1.1.2
5.1.3 BAN逻辑研究的发展方向	5.1.1.3
5.2 BAN类逻辑	5.2.1
5.2.1 BAN类逻辑概述	5.2.1.1
5.2.2 SVO逻辑概述	5.2.1.2
5.3 Kailar逻辑	5.3.1
5.3.1 Kailar逻辑概述	5.3.1.1
5.3.2 Kailar逻辑的缺陷	5.3.1.2
5.4 定理证明方法	5.4.1
5.4.1 串空间	5.4.1.1
5.4.2 Schneider秩函数	5.4.1.2
5.5 模型检测分析方法	5.5.1
5.5.1 通信顺序进程CSP	5.5.1.1
5.5.2 SMV型检测系统	5.5.1.2
5.5.3 基于分支时态逻辑CTL及有限状态机模型	5.5.1.3
5.6 其他的协议分析方法	5.6.1
第六章 电子商务交易协议形式化验证方法	6.1
6.1 SVO形式化验证方法	6.1.1
6.1.1 SVO形式化验证方法的缺陷	6.1.1.1
6.1.2 SVO分析方法存在的局限性	6.1.1.2
6.2 电子商务交易协议新形式化验证方法	6.2.1
6.2.1 基本符号	6.2.1.1
6.2.2 协议运行环境及语义	6.2.1.2
6.2.3 推理规则	6.2.1.3
6.2.4 协议分析步骤	6.2.1.4
6.3 新形式化方法的应用实例	6.3.1
6.3.1 Zhou Gollmann协议形式化验证	6.3.1.1
6.3.2 ISI支付协议形式化验证	6.3.1.2
6.3.3 匿名原子电子商务交易协议形式化验证	6.3.1.3
6.3.4 离线可信第三方匿名原子电子现金交易协议验证参考文献	6.3.1.4

《电子商务交易协议理论与验证方法》

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:www.tushu111.com