计算机应用研究
Application Research Of Computers



友情链接
>> 中国期刊网
>> 万方数据资源库
>> 台湾中文电子期刊
>> 四川省计算应用研究中心
>> 维普资讯网

# 优化的匿名电子现金支付协议及其形式化验证*

## Optimization of anonymous e-cash payment protocol and its formal verification

摘要点击：11 全文下载：4

查看全文 查看/发表评论 下载PDF阅读器

中文关键词：安全属性 形式化验证 密钥保密性 非否认性 公平性 原子性

英文关键词：security property formal verification key confidentiality non-repudiation fairness atomicity

基金项目：国家“863”计划资助项目（2007AA01Z471);国家自然科学基金资助项目（60473021）；河南省重点科技攻关项目（072102210029）；河南省科技攻关项目（0624260017）;河南省教育厅自然科学研究计划项目（2010A520004）

| 作者 | 单位 |
| --- | --- |
| 陈莉， 刘军 | (河南财经学院 计算中心， 郑州 450002) |

中文摘要：

针对匿名电子现金支付协议存在的缺陷，提出了一种能够满足多种安全属性的优化协议。将会话密钥的协商与使用分为两个阶段进行，确保协议密钥保密性的实现；引入电子证书证明交易主体的身份，确保协议非否认性的实现；借助可信方传递付款收据，避免交易主体不诚实所导致的公平性缺失；引入FTP传输方式传送电子货币和付款收据，确保实现可追究性与公平性，进一步增强协议的鲁棒性。对优化协议进行形式化验证，结果表明，优化协议满足密钥保密性、非否认性、公平性、可追究性、原子性等安全属性。

英文摘要：

In response on the existing problems of anonymous e-cash payment protocol, the paper proposed an optimal protocol, which could meet a variety of security properties. To ensure the realization of its key confidentiality, the agreement and use of the session key were divided into two stages. To realize its non-repudiation, the certificates were used to prove the identities of the transaction entities. To avoid unfairness arisen by the dishonest transaction entities, the transmission of payment receipt was achieved by the trusted party. The proposed protocol used FTP to transmit electronic cashes and payment receipts, which ensured achievement of accountability and fairness, and enhanced the robustness of the protocol. Formal verification results indicate that the optimal protocol satisfies key confidentiality, non-repudiation, accountability, fairness and atomicity.

开放期刊联盟 http://www.oajs.org

您是第2827724位访问者

主办单位：四川省计算机研究院 单位地址：成都市武侯区成科西路3号

服务热线：028-85249567 传真：028-85210177邮编：610041 Email：arocmag@163.com

蜀ICP备05005319号 本系统由北京勤云科技发展有限公司设计