通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会



叶青1,2,杨赟3,郑世慧2,常利伟2,肖达2,杨义先2,4.公平的多方并发签名方案[J].通信学报,2014,(3):140~149

# 公平的多方并发签名方案

# Fair multi-party concurrent signature scheme

投稿时间： 2013-01-11

**DOI**：10.3969/j.issn.1000-436x.2014.3.016

中文关键词：多方并发签名 公平性 双线性对 随机预言模型

英文关键词:multi-party concurrent signature fairness bilinear pairing random oracle model

基金项目:国家自然科学基金资助项目(61003285, 61202082)；中央高校基本科研业务费专项基金资助项目(BUPT2012RC0219, BUPT2012RC0218)

| 作者 | 单位 |
| --- | --- |
| 叶青1,2，杨赟3，郑世慧2，常利伟2，肖达2，杨义先2,4 | 1. 河南理工大学 计算机科学与技术学院，河南 焦作454000；2. 北京邮电大学 信息安全中心，北京100876； 3. 铁道部信息技术中心，北京 100010；4. 北京邮电大学 灾备技术国家工程实验室，北京100876 |



中文摘要:

Tonien等在ISC2006上首次提出了多方并发签名体制，但Xie和谭指出Tonien等的方案并不满足公平性，进而分别重新构造了多方并发签名方案。分别对Xie和谭的多方并发签名方案进行了分析，指出他们的方案也不满足公平性，进而正式定义了公平多方并发签名的安全模型，并基于双线性对及多方密钥协商技术重新构造了一个多方并发签名方案。分析表明，在随机预言模型下，假设CDH问题是难解的，新方案同时满足正确性、不可伪造性、模糊性、并发性和公平性，并且与同类方案相比，新方案在签名长度、计算量、通信代价方面效率较高。

英文摘要:

Multi-party concurrent signatures were first proposed by Tonien et al at ISC2006, but Xie and Tan pointed Tonien et al’s scheme doesn’t satisfy fairness and they reconstructed multi-party concurrent signature schemes respectively. Through analysis, the multi-party concurrent signature schemes proposed by Xie and Tan don’t satisfy fairness either, so a formal security model of fair multi-party concurrent signatures was proposed and a multi-party concurrent signature scheme based on bilinear pairing and multi-party key agreement was also reconstructed. Analysis shows that the new scheme satisfies correctness, unforgeability, ambiguity, concurrency and fairness in the random oracle model assuming the CDH problem is intractable and highly efficient in signature size, computation cost and communication cost compared with other schemes of its kind.

查看全文 查看/发表评论 下载PDF阅读器

关闭