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

李继国,孙 刚,张亦辰.实用的本地验证者撤销群签名方案[J].通信学报,2011,(10):67~77

实用的本地验证者撤销群签名方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者 **单位**

李继国，孙 刚，张亦辰

中文摘要：

本地验证者撤销是一种有效的群成员撤销方法，该方法只需将撤销信息发给验证者而无需签名者的参与。目前本地验证者撤销群签名方案中普遍存在不能防止陷害攻击以及撤销验证计算量与撤销列表长度呈线性增长等问题。为了解决这些问题，并针对群签名在隐私保护证明方面的应用，基于q-SDH假设和DLDH假设，提出一种实用的本地验证者撤销群签名方案，并在随机预言模型下证明了方案的安全性。分析了方案的效率，并与现有的本地验证者撤销群签名方案进行了比较，分析表明方案的撤销验证计算量与撤销列表长度无关，同时还具有防陷害性和向后无关联性。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭