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

冯涛,彭伟,马建峰.安全的无可信PKG的部分盲签名方案[J].通信学报,2010,(1):128~134

安全的无可信PKG的部分盲签名方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
冯涛	
彭伟	
马建峰	

中文摘要：

利用Gap Diffie-Hellman(GDH)群，在部分盲签名机制的基础上，提出了一个有效的基于身份的无可信私钥生成中心(PKG，private key generator)的部分盲签名方案。方案中PKG不能够伪造合法用户的签名，因为它只能生成一部分私钥。在随机预言模型下，新方案能抵抗适应性选择消息攻击和身份攻击下的存在性伪造，其安全性依赖于CDHP问题。该方案满足正确性和部分盲性，与Chow方案相比具有较高的效率。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭