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

甄鸿鹄,陈越,谭鹏许,郭渊博.基于非对称双线性对的直接匿名认证方案[J].通信学报,2010,(8A):37~43

基于非对称双线性对的直接匿名认证方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
甄鸿鹄	
陈越	
谭鹏许	
郭渊博	

中文摘要：

根据国产可信密码模块(TCM, trusted cryptography module)的直接匿名认证需求，基于非对称双线性对(ABP, asymmetric bilinear pairing)，提出了一种全新的DAA方案——ABP-DAA方案，与已有DAA方案相比，其不仅能够适用于TCM的直接匿名认证，而且更加安全、简单、高效。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭