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

崔永刚,刘玉军.可公开验证的短密钥公钥加密方案[J].通信学报,2010,(3):45~50

可公开验证的短密钥公钥加密方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
崔永刚	
刘玉军	

中文摘要：

利用一个选择身份安全的基于身份加密方案（IBE）和2个目标抗碰撞散列函数，构造了一个可公开验证的公钥加密方案。在判定性BDHI假设的基础上，证明了新方案在标准模型下是适应性选择密文安全的。相比现有可公开验证的公钥加密方案，新方案的公私钥长度较短且与安全参数相互独立。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭