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

李大伟,杨 庚,苏弘逸,陈燕俐.基于身份的泛在通信隐私保护方案[J].通信学报,2011,(9):44~50

基于身份的泛在通信隐私保护方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
李大伟	
杨 庚	
苏弘逸	
陈燕俐	

中文摘要：

针对泛在通信应用场景中数据传输的私密性要求，基于IBE公钥加密算法和Shamir门限秘密共享，提出了一种泛在通信隐私保护方案。方案以不同信任域身份标识为公钥，加密后的影子密钥可通过广播信道分发，满足门限条件的节点可以重构隐私会话密钥。方案具有随机预言模型下可证明的IND-sID-CPA安全性，支持安全的新成员加入策略，具有较小的计算复杂度和存储、通信开销。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭