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

张俊伟,马建峰,杨力.UC安全的基于一次签名的广播认证[J].通信学报,2010,(5):31~36

UC安全的基于一次签名的广播认证

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
张俊伟	
马建峰	
杨力	

中文摘要：

研究了基于一次签名的广播认证协议的可证明安全问题。在通用可组合安全框架下，提出了基于一次签名的广播认证的安全模型。首先，形式化定义了一次签名理想函数FOTS和广播认证理想函数FBAUTH。其次，设计了一次签名算法HORS+。然后，在(FOTS, FREG)-混合模型下设计了广播认证方案πBAUTH。组合协议HORS+，在πBAUTH的基础上可以构造出新的基于一次签名的广播认证协议。结果表明，HORS+能够安全实现FOTS；在(FOTS, FREG)-混合模型下πBAUTH安全实现理想函数FBAUTH的广播认证方案πBAUTH。根据组合定理，新的广播认证协议具有通用可组合安全性适用于能量受限网络中广播消息的认证。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭