通信学报
Journal on Communications

李景峰1,潘恒2,郭卫锋1.EPC网络中可证明安全的EPCIS通信方案[J].通信学报,2013,(Z1):235~239

EPC网络中可证明安全的EPCIS通信方案

Provable security EPC information servicecommunication scheme

投稿时间： 2013-07-05

DOI：10.3969/j.issn.1000-436x.2013.Z1.031

中文关键词：EPC信息服务 射频标识 Canetti-Krawczyk模型

英文关键词:EPC Information service radio frequency identification Canetti-Krawczyk model

基金项目:

作者	单位
李景峰1，潘恒2，郭卫锋1	1.解放军信息工程大学 密码工程学院，河南 郑州 450004；2.中原工学院 计算机学院，河南

中文摘要:

针对EPC信息服务存在的安全问题，提出一种EPC信息服务安全通信方案ESCM，方案使用数字签名、消息认证码等安全机制，实现了互认证服务与密钥协商服务，能够保护EPCIS通信的机密性和完整性。利用Canetti-Krawczyk模型证明了ESCM方案是会话密钥安全的，且计销较少，适合EPC网络特性。

英文摘要:

To resolve the security drawbacks of EPC information services, a provable security EPC information service communication scheme—ESCM mechanisms such as the digital signature and the message authentication code, the ESCM could implement mutual authentication and session key and querying application belonging to a different trust domain. Security analysis shows that the session key agreement of ESCM is provably sec ESCM has efficient computation and communication cost.