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

陈兵,郑嘉琦.轻型的RFID安全认证协议LAP[J].通信学报,2013,(Z1):1~7

轻型的RFID安全认证协议LAP

Lightweight authentication protocol for RFID

投稿时间： 2013-06-29

DOI：10.3969/j.issn.1000-436x.2013.Z1.001

中文关键词：RFID 广义逆矩阵 Gen2标准 认证协议

英文关键词:RFID generalized inverse matrix Gen2 standard authentication protocol

基金项目:国家自然科学基金资助项目(61139002)

作者	单位
陈兵，郑嘉琦	南京航空航天大学 计算机科学与技术学院，江苏 南京 210016

中文摘要:

RFID标签存在着处理能力弱、存储空间小和电源供给有限等局限性，传统的公钥算法或散列函数等复杂运算不能满足实际应用的需求。针对现有轻量级RFID认证协议的不足，设计了基于广义逆矩阵的RFID安全认证协议LAP。该协议采用了硬件复杂度较低的CRC校验及计算量较小的矩阵运算。通过安全隐私和性能分析，LAP协议适用于低成本、存储与计算受限的RFID标签。

英文摘要:

Radio frequency identification (RFID) is a technique using radio frequency to object identification and access to relevant data in the open system enviroment with the limits of process, storage, power and so on. The traditional tag authentication protocols taking complicated algorithms into account can’t meet the demand. In view of the existing security and privacy problems of RFID , a lightweight authentication protocol for RFID named LAP was proposed. LAP is based on the generalized inverse matrix and only uses CRC checksum, some matrix and simple logic operations to satisfy the principles of balancing security, privacy and cost. The comparisons of security, privacy and performance with other authentication protocols show that LAP is feasible for RFID tags with requirements of low cost and resource-constrained.

查看全文 查看/发表评论 下载PDF阅读器

关闭