计算机工程与应用 2010 46 (5): 69-72 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

RFID系统中基于公钥加密的相互认证协议

张恒山，管会生，韩海强

兰州大学 信息科学与工程学院，兰州 730000

收稿日期 2009-4-28 修回日期 2009-7-2 网络版发布日期 2010-2-8 接受日期

摘要 随着RFID系统能力的提高和标签应用的日益普及，安全问题，特别是用户隐私问题变得日益严重。提出了一种新的RFID认证协议。认为基于公钥加密的RFID认证协议相对基于哈希函数和基于对称密钥加密的RFID认证协议，有较好的安全性。公钥加密算法NTRU被认为是一种效率较高的加密算法，且更适合于RFID系统，因此提出的协议采用了NTRU公钥加密算法。对该协议的安全性和性能进行了比较分析，结果表明该协议可以为RFID系统提供更好的安全性，能为用户提供更好的隐私保护，且性能较佳。

关键词 认证协议 NTRU 安全性 哈希函数 RFID 标签

分类号 TP393.08

Public key based mutual authentication protocol for RFID system

ZHANG Heng-shan，GUAN Hui-sheng，HAN Hai-qiang

School of Information Science & Engineering，Lanzhou University，Lanzhou 730000，China

Abstract

The RFID system has become one of the most important applications.However，this technology may suffer from some security threats，such as secrecy，location privacy，forward secrecy，replay attack，etc.A good way to provide security for RFID system is devising authentication protocol.A new mutual authentication protocol for RFID system is proposed.The authentication protocol based on public key cryptography has more security than the symmetric encryption based protocol and the hash function based protocol in RFID system.The NTRU is a more efficient public key cryptosystem，and it suits for the RFID system，so the proposed authentication protocol has adopted the NTRU public key cryptosystem.Then the security and performance of this protocol are discussed.The result shows that this protocol has provided good security for RFID system，more privacy for users，and has a nice performance.

Key words authentication protocol Number Theory Research Unit（NTRU） security Hash function Radio Frequency IDentification（RFID） tag

DOI: 10.3778/j.issn.1002-8331.2010.05.021

通讯作者 张恒山 wwocgwzhs@126.com

扩展功能

本文信息

Supporting info

PDF(694KB)

[HTML全文](0KB)

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“认证协议”的相关文章

本文作者相关文章

· 张恒山

· 管会生

· 韩海强