计算机工程与应用 2009 45 (7): 32-35 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

NTRUSign无线认证和密钥协商协议

张利华[1,2], 章丽萍[2], 张有光[1], 吕善伟[1]

1.北京航空航天大学 电子信息工程学院，北京 100083
2.华东交通大学 电气与电子学院，南昌 330013

收稿日期 2008-10-7 修回日期 2008-12-16 网络版发布日期 2009-2-28 接受日期

摘要 NTRU是一个快速、低开销的公钥体制，适合在资源受限的应用中使用。NTRUSign是基于NTRU的数字签名算法。基于NTRUSign算法，给出了一个无线认证和密钥协商协议。该协议的安全性基于有限时间内在大维数格计算最短向量的困难性。协议包括三个阶段：用户注册阶段、服务器注册阶段、认证阶段和密钥协商阶段。通过安全性分析和协议性能分析对比，表明该协议是一个安全性和效率比占优的协议。

关键词 无线认证 密钥协商 安全性 NTRUSign

分类号

NTRUSign based wireless authentication and key agreement protocol

ZHANG Li-hua[1,2],ZHANG Li-ping[2],ZHANG You-guang[1],LV Shan-wei[1]

1.School of Electronic and Information Engineering，Beihang University，Beijing 100083，China
2.School of Electrical and Electronic Engineering，East China Jiaotong University，Nanchang 330013，China

Abstract

NTRU is a low cost and fast public key cryptosystem，which is suit to resource constraint applications.NTRUSign is a novel digital signature scheme，which is base on NTRU.A new wireless authentication and key agreement protocol using NTRUSign is also proposed.The security of the protocol relies on the fact that for most lattices，it is very difficult to find extremely short vectors.The protocol has three phases：user registration phase，server registration phase，authentication and key agreement phase.Furthermore，after analyzing the security and performance of the protocol，the proposed protocol is a better scheme with lower cost and strong security.

Key words wireless authentication key agreement security NTRUSign

DOI: 10.3778/j.issn.1002-8331.2009.07.010

通讯作者 张利华 lh_zhang@ee.buaa.edu.cn