计算机工程　2007 33 (13): 179-181,184　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于MYK-NTRUSign签名的用户认证方案

张利华1,2，朱成九2，郭 强1，范晓红3，吕善伟1

(1. 北京航空航天大学电子信息学院，北京 100083；2. 华东交通大学电气与电子学院，南昌 330013； 3. 北京电子科技学院电子学院，北京 10070)

收稿日期　修回日期　网络版发布日期 2007-7-3　接受日期

摘要　基于修复了延展性缺陷的NTRUSign算法，给出了一个使用智能卡的远程用户认证方案。该方案的安全性是基于单向Hash函数和在有限时间在大维数格计算最短向量的困难性。该方案包括4个阶段：注册阶段，登陆阶段，认证阶段和更改口令阶段。允许用户自主选择并更改口令，实现了双向认证；能够抵御中间人攻击，抗DoS攻击，具备前向安全性、强安全修复性和“黑名单”拒绝服务机制。是一个低开销、强安全性的方案。

关键词　身份认证　口令　智能卡　NTRUSign　延展性

分类号　TP393.08

DOI:

对应的英文版文章：13-68D

通讯作者:

作者个人主页: 张利华1;2;朱成九2;郭 强1;范晓红3;吕善伟1