电子与信息学报 2001 23 (4): 321-326 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于数字签名的交互式用户身份鉴别方案

唐韶华, 韦岗

华南理工大学计算机系, 广州, 510640

收稿日期 1999-6-11 修回日期 1999-11-8 网络版发布日期 2008-10-13 接受日期

摘要
该文首先利用Harn数字签名方案建立了基于身份的交互式用户认证与双向认证方案, 并首次将这种基于身份的交互式用户认证方案推广为基于身份的交互式共享认证方案, 使得认证系统的n名验证者中t名以上验证者才能验证用户身份的有效性, 从而可以有效地防止认证系统个别管理人员的作弊行为, 提高了认证系统的安全级别与可用性。

关键词 数字签名 用户认证 共享认证 基于身份的密码系统

分类号 TN918.1

ID-Based Interactive User Authentication Schemes Using Digital Signature

Tang Shaohua, Wei Gang

Dept. of Computer Sci. and Eng., South China Univ. of Tech.,Guangzhou 510640 China

Abstract
A kind of ID-based interactive user authentication and two-way authentication schemes are presented in this paper and extended to form a new ID-based interactive shared authentication scheme, which enables more than t out of n verifiers in authentication system to validate a user s identity, such that the cheating trick of few administrators in the authentication system can be prevented, thus the security class and the availiability of the authentication system are improved.

Key words Digital signature User authentication Shared authentication ID-based cryptosystem

DOI:

通讯作者

作者个人主页 唐韶华; 韦岗