计算机工程与应用 2007 43 (34): 136-137 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

网络学习系统中代理数字签名算法的研究

王 云

山西师范大学 教育技术与传媒学院，山西 临汾 041004

收稿日期 修回日期 网络版发布日期 2007-11-19 接受日期

摘要 以现有的ElGamal数字签名体制为基础，研究了网络学习系统中的代理数字签名算法：单代理数字签名算法和多代理数字签名算法，与目前用得较多的基于Fiat-Shamir签名体制的代理数字签名算法和基于Guillou-Quisquater签名体制的代理数字签名算法相比，这些算法具有密钥短小、参数规模小、运算速度快和安全性好的优点。

关键词 网络学习系统 数字签名 代理数字签名

分类号

Proxy digital signature algorithms of e-learning system

WANG Yun

College of Educational Technology and Communication，Shanxi Normal University，Linfen，Shanxi 041004，China

Abstract

The proxy digital signature algorithms based on the ElGamal signature scheme in existence are proposed in e-learning system，and they are mono-proxy digital signature algorithm and multi-proxy digital signature.These digital signature algorithms have the strongpoint of short key，small parameter scale，rapid operation，finer security，and contrast with the proxy digital signature algorithms based on the Fiat-Shamir signature scheme and the Guillou-Quisquater signature scheme.

Key words e-learning system digital signature proxy digital signature

DOI:

通讯作者 王 云 wangyun@sxnu.edu.cn