计算机工程与应用 2009 45 (30): 118-120 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

具有消息自恢复的ECC认证加密方案

侯爱琴[1]，杨世勇[2]，葛建华[2]

1.西北大学 信息科学与技术学院，西安 710069
2.西安电子科技大学 ISN国家重点实验室，西安 710071

收稿日期 2008-5-29 修回日期 2008-8-19 网络版发布日期 2009-11-6 接受日期

摘要 给出一种新的基于椭圆曲线密码的具有消息恢复功能的数字签名加密方案。Shao的基于椭圆曲线的具有消息恢复的数字签名改进方案，克服了Tzeng方案的缺乏不可否认性和前向安全性的弱点。但Shao算法中对椭圆曲线点与整数求hash值，实际中无法实现。针对Shao方案的这一缺陷作了改进；并在签名中加入时间戳，增加了抵御重发攻击的能力。

关键词 认证加密 椭圆曲线数字签名 消息恢复 哈希函数 重发攻击

分类号 TP309

Authenticated encryption scheme with message recovery based on ECC

HOU Ai-qin[1]，YANG Shi-yong[2]，GE Jian-hua[2]

1.School of Information Science & Technology，Northwest University，Xi’an 710069，China
2.ISN National Lab，Xidian University，Xi’an 710071，China

Abstract

A new digital signature encryption scheme with message recovery based on elliptic curve cryptography is presented.Shao proposes an improved digital signature scheme with message recovery based on ECC.It has overcome the weakness of Tzeng’s scheme that lacks nonrepudiation and forward security.But Shao’s algorithm which tries to achieve the hash value of a point on elliptic curve and an integer，cannot be realized.It has improved the weakness of Shao’s scheme.Furthermore，the new scheme appends time stamp to signature，and it can resist against replay attack.

Key words authenticated encryption Elliptic Curve Digital Signature（ECDSA） message recovery hash replay attack

DOI: 10.3778/j.issn.1002-8331.2009.30.036

通讯作者 侯爱琴 houaiqin@eyou.com