计算机工程　2009 35 (19): 161-163　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

基于ECC数字签名的实现及优化

蔡 冰，叶 玲

(南京邮电大学通信与信息工程学院，南京 210003)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　为满足无线传感器网络对信源端身份认证的需求，在TelosB硬件节点上实现椭圆曲线加密机制(ECC)数字签名算法，并对ECC的点乘运算模块进行优化。改进算法的运算复杂度和实际节点运行情况都优于已有的功能软件。实验结果表明，在硬件平台和加密强度相同的情况下，改进后的ECC算法可以有效提高数字签名的运算速度。

关键词　椭圆曲线加密机制；无线传感器网络；数字签名

分类号　TP311.52

DOI:

通讯作者:

作者个人主页: 蔡 冰;叶 玲