计算机工程　2006 32 (17): 4-6,9　ISSN: 1000-3428　CN: 31-1289/TP

发展趋势/热点技术

公钥密码理论与技术的研究现状及发展趋势

叶生勤

福建移动通信有限责任公司业务支撑中心，福州 350001

收稿日期　修回日期　网络版发布日期 2006-8-28　接受日期

摘要　密码技术是信息安全技术的核心。该文概括介绍了国内外公钥密码的研究现状，特别是近年来国际上相继进行的一系列大型的密码标准化工作，阐述了公钥密码的主要理论基础，介绍了椭圆曲线公钥密码体制及其特点。指出了公钥密码的发展趋势及我国在制定密码的标准化问题上的研究重点。

关键词　公钥密码　大数因子分解问题　有限域　椭圆曲线离散对数问题

分类号　TP309

DOI:

对应的英文版文章：2006-17-002

通讯作者:

作者个人主页: 叶生勤

扩展功能

本文信息

Supporting info

PDF(118KB)

[HTML全文](0KB)

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“公钥密码”的 相关文章

本文作者相关文章

· 叶生勤