计算机工程 2009 35 (22): 155-158 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

Eisenstein环上的圆锥曲线公钥密码系统

潘 瑞，王丽君，李端端，李 旭

(辽宁科技大学计算机科学与工程学院，鞍山 114051)

收稿日期 修回日期 网络版发布日期 接受日期

摘要

为了实现安全有效的曲线密码系统，引入Eisenstein环 。论述剩余类环 上圆锥曲线 的基本性质，证明 中分别用映射方式和坐标方式定义的2种加法运算的一致性，以 构成一个有限的Abel群。验证在 上寻找基点的算法适用于 ，给出ElGamal密码系统在 上的数值模拟，结果表明改进后的圆锥曲线密码系统具有明文嵌入方便、运算速度快、易于实现的优点。

关键词 剩余类环；不可分数；圆锥曲线离散对数；公钥密码系统；数值模拟

分类号 TP309.2

DOI:

通讯作者:

作者个人主页: 潘 瑞;王丽君;李端端;李 旭