计算机工程　2006 32 (23): 153-155,173　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于Brier-Joye的Elgamal 椭圆曲线密码体制研究

李宗秀，鲍皖苏，汪 翔

（解放军信息工程大学电子技术学院，郑州 450004）

收稿日期　修回日期　网络版发布日期 2006-11-23　接受日期

摘要　对二元域上基于Brier-Joye公式的Elgamal椭圆曲线密码体制的安全性进行了分析，给出了抵抗碰撞点攻击的方法，介绍了Brier-Joye公式抵抗信道攻击的椭圆曲线选择标准。

关键词　侧信道攻击　碰撞点　异常点　Elgamal型椭圆曲线密码　Brier-Joye公式

分类号

DOI:

对应的英文版文章：2006-23-056

通讯作者:

作者个人主页: 李宗秀;鲍皖苏;汪 翔