

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

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(126KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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“侧信道攻击”的 相关文章](#)
- ▶ [本文作者相关文章](#)

- [李宗秀](#)
- [鲍皖苏](#)
- [汪 翔](#)