

安全技术

## GF(p)上安全椭圆曲线产生算法

侯爱琴<sup>1</sup>, 辛小龙<sup>2</sup>, 杨世勇<sup>3</sup>

(1. 西北大学信息科学与技术学院, 西安 710069; 2. 西北大学数学系, 西安 710069; 3. 西安电子科技大学ISN国家重点实验室, 西安 710071)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 研究素数域GF(p)( $p > 3$ )上的椭圆曲线, 讨论阶为素数的椭圆曲线的产生算法, 在此基础上, 分析阶为2个素数之积的椭圆曲线产生问题, 并提出一种GF(p)上安全椭圆曲线的产生算法, 给出椭圆曲线及其全体有理点的随机产生实例。仿真实验结果表明, 该算法是有效可行的。

**关键词** [椭圆曲线群](#); [阶](#); [基点](#)

**分类号** [TP309](#)

**DOI:**

通讯作者:

作者个人主页: 侯爱琴<sup>1</sup>; 辛小龙<sup>2</sup>; 杨世勇<sup>3</sup>

### 扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#)(307KB)

▶ [\[HTML全文\]](#)(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“椭圆曲线群; 阶; 基点”的 相关文章](#)

▶ [本文作者相关文章](#)