计算机工程　2009 35 (23): 138-140　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

GF(p)上安全椭圆曲线产生算法

侯爱琴1，辛小龙2，杨世勇3

(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1;辛小龙2;杨世勇3