

李彬,王新梅.高效的R-ate对的参数构造方法[J].通信学报,2010,(1):118-121

高效的R-ate对的参数构造方法

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[李彬](#)

[王新梅](#)

摘要点击次数: 314

全文下载次数: 244

中文摘要:

为进一步提高Tate对的计算效率,在R-ate算法的基础上提出了一种新的(A,B)参数选择方法。与Atei方法相比,该方法将(A,B)参数对选择 (p_i, r) ,使得Atei的方程中域的特征 p_{modr} 代替 p_{mmodr} ,从而大大降低Miller循环的次数。但是在 p 取值不当时,有可能造成系统的可实现性降低,因此最后给出一种 p 的取值规则,以确保本方法应用下的系统成功实施。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

关闭

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/915/917 电子邮件: xuebao@ptpress.com.cn
技术支持: 北京勤云科技发展有限公司