通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

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

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(pi, r),使得Atei的方程中域的特征pmodr代替pmmodr，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：