计算机工程　2007 33 (20): 148-149,152　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

RSA密钥对高效生成算法

姚国祥，林良超

(暨南大学信息科学技术学院，广州 510632)

收稿日期　修回日期　网络版发布日期 2007-10-11　接受日期

摘要　RSA是公钥密码体系中十分重要的加解密算法，RSA的效率瓶颈主要在大素数的寻找和指数模幂运算上。RSA密钥对的生成过程直接地涉及以上两大瓶颈计算问题。该文分析了RSA密钥对生成过程中涉及到的各种算法，并且通过修改随机数的生成方法来达到进一步改进预筛选算法的目的。

关键词　RSA算法；大素数寻找；指数模幂运算；密钥对

分类号　TP309

DOI:

对应的英文版文章：072048c

通讯作者:

作者个人主页: 姚国祥;林良超