计算机工程 2010 36 (7): 153-155,158 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

基于完全平方数的RSA密码分析算法机理

孙克泉

(南开社区学院计算机系，天津 300100)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 给出基于完全平方数的RSA密码分析算法的机理，分析满足同余式x2≡y2 (mod n)的完全平方数x和y的数域选择与算法效率的关系。通过数学证明和相关分析方法，定义RSA公钥n的素因子特征c，证明当c>2时，如果数域范围选择和构造的算法得当，则分解n的效率较高，当c<2时，使算法的运算数域增大，可以降低分解n的效率和有效性，即构造的RSA密码是安全的。

关键词 RSA密码分析；平方数；筛法；特征；数论

分类号 TP309

DOI:

通讯作者:

作者个人主页: 孙克泉