

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 $x^2 \equiv y^2 \pmod{n}$ 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](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(325KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [参考文献 \[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“RSA密码分析; 平方数; 筛法; 特征; 数论”的 相关文章](#)
- ▶ [本文作者相关文章](#)