

安全技术

NTRU参数选择方法的研究

步山岳1, 冯万利1, 王汝传2

(1. 淮阴工学院计算机工程学院, 淮安 223001; 2. 南京邮电大学计算机学院, 南京210003)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 NTRU算法是一种基于环的公开密钥体制, 与RSA和ECC等典型的加密算法相比, 在安全性和速度方面具有明显的优势。分析目前比较成熟的攻击NTRU方法, 从安全的角度, 根据不同的应用场合, 给出NTRU加密参数选择方法, 减少选择NTRU参数的盲目性, 达到提高算法的执行速度、减少占用系统资源的目的。

关键词 [NTRU算法](#); [选择参数](#); [阶元](#); [安全](#)

分类号 [TP309.7](#)

DOI:

通讯作者:

作者个人主页: [步山岳1](#); [冯万利1](#); [王汝传2](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(183KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“NTRU算法; 选择参数; 阶元; 安全”的 相关文章](#)
- ▶ [本文作者相关文章](#)