

博士论文

## Paillier-Pointcheval公钥概率加密体制的改进

姜正涛<sup>1</sup>, 刘建伟<sup>2</sup>, 王育民<sup>3</sup>

(1. 北京航空航天大学计算机学院, 北京 100083; 2. 北京航空航天大学电子信息工程学院, 北京 100083; 3. 西安电子科技大学综合业务网国家重点实验室, 西安 710071)

收稿日期 修回日期 网络版发布日期 2008-1-29 接受日期

**摘要** 分析P. Paillier等提出的公钥概率加密体制的安全性, 证明它的单向性与几类问题的等价关系, 进一步证明了在不降低安全性的前提下, 可以通过选取适当的参数, 提高体制的效率, 减少通信量, 在此基础上给出改进的加密体制, 加密和解密的效率比以往的体制有了很大的提高。

**关键词** [安全性分析](#); [公钥概率加密体制](#); [参数选择](#)

**分类号** [TP309+.7](#)

**DOI:**

对应的英文版文章: [3-12](#)

通讯作者:

作者个人主页: [姜正涛<sup>1</sup>](#); [刘建伟<sup>2</sup>](#); [王育民<sup>3</sup>](#)

### 扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(138KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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“安全性分析: 公钥概率加密体制: 参数选择”的 相关文章](#)
- ▶ [本文作者相关文章](#)

- [姜正涛](#)
- [刘建伟](#)
- [王育民](#)