

信息安全

基于掩码的差分能量分析攻击防范对策

周文锦, 范明钰

收稿日期 修回日期 网络版发布日期 接受日期

摘要 介绍了目前比较有效的抗差分能量分析(Differential Power Analysis, DPA)攻击的防范对策——掩码(Masking), 并将改进后的简单固定值掩码方法推广到固定值掩码方法以抵抗二阶差分能量分析(SODPA)攻击。

关键词

分类号

DOI:

对应的英文版文章: [\(25\)2725-2726](#)

通讯作者:

作者个人主页: 周文锦; 范明钰

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(360KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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 无 相关文章](#)
- ▶ 本文作者相关文章
 - [周文锦](#)
 - [范明钰](#)