计算机应用 2005 25 (12): 2725-2726 ISSN: 1001-9081 CN: 51-1307/TP

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