《密码安全芯片与侧信道技术》

图书基本信息

书名：《密码安全芯片与侧信道技术》

13位ISBN编号：9787030393252

出版时间：2014-1-1

作者：李慧云,李大为,罗鹏,尹旭程

页数：104

《密码安全芯片与侧信道技术》

内容概要

李慧云、李大为、罗鹏、尹旭程编著的《密码安全芯片与侧信道技术》着重探讨密码安全芯片受到的侧信道攻击以及相应的安全措施与安全评估方法。第1章为信息安全简介；第2章介绍通用密码算法，包括对称算法（DES、AES）和公开密钥算法（RSA、ECC），这些算法实现是侧信道分析攻击的对象；第3章介绍侧信道分析的分类与半导体物理基础；第4章介绍时序攻击；第5章介绍功耗攻击；第6章介绍电磁攻击；第7章讲述侧信道技术与其他密码分析技术的结合应用；第8章讨论侧信道技术的研究热点及未来发展趋势。《密码安全芯片与侧信道技术》可供密码安全芯片领域的工程技术人员与科学研究人员参考，信息安全领域的研究生可将本书作为补充读物。

《密码安全芯片与侧信道技术》

书籍目录

《密码安全芯片与侧信道技术》

版权说明