

《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

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《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研人员参考，信息安全领域的研究生可将本书作为补充读物。

书籍目录

前言

第1章 信息安全简介

1.1 信息安全基础知识

1.2 密码学

1.2.1 对称加密与公钥加密

1.2.2 分组密码与流密码

1.2.3 密码算法的保密与密钥的保密

1.3 密码设备

1.4 侧信道分析技术

参考文献

第2章 通用密码算法

2.1 对称算法

2.1.1 DES算法

2.1.2 AES算法

2.2 公开密钥算法

2.2.1 RSA算法

2.2.2 ECC算法

参考文献

第3章 侧信道分析的分类与半导体物理基础

3.1 侧信道攻击分类

3.1.1 非侵入式

3.1.2 侵入式

3.1.3 半侵入式

3.2 侧信道攻击的半导体物理基础

3.3 侧信道攻击防御技术的半导体物理基础

3.3.1 异步双轨逻辑

3.3.2 差分动态逻辑技术

参考文献

第4章 时序攻击

4.1 模型

4.2 对RSA的时间攻击

4.3 对ECC的时间攻击

4.3.1 ECC的简介

4.3.2 对ECC的时间攻击

参考文献

第5章 功耗攻击

5.1 功耗分析技术简介

5.1.1 简单功耗分析

5.1.2 差分功耗分析

5.1.3 高阶差分功耗分析

5.1.4 相关性功耗分析

5.1.5 互信息分析

5.2 智能卡功耗分析的实验环境

5.3 简单功耗分析示例

5.3.1 DES智能卡的简单侧信道功耗分析示例

5.3.2 AES算法的简单功耗分析示例

5.3.3 ECC算法的简单功耗分析示例

5.3.4 ECC简单功耗攻击的防御技术

参考文献

第6章 电磁攻击

6.1 麦克斯韦方程

6.2 电磁场传播

6.2.1 电偶极子的空间场

6.2.2 磁偶极子的空间场

6.3 电磁场探头

6.4 电磁分析攻击

6.4.1 直接辐射

6.4.2 调制辐射

6.5 电磁分析示例

参考文献

第7章 侧信道技术与其他密码分析技术的结合应用

7.1 侧信道技术与选择明文技术的结合应用

7.1.1 “侧信道+选择明文”攻击硬件DES协处理器

7.1.2 “侧信道+选择明文”攻击RSA

7.1.3 “侧信道+选择明文”攻击ECC

7.2 侧信道与故障攻击技术的结合应用

7.2.1 故障引入的方法

7.2.2 基于故障的密码分析原理

参考文献

第8章 侧信道技术的研究热点及未来发展趋势

8.1 安全芯片的检测认证及量化评估

8.1.1 国外密码安全设备的检测认证标准简介

8.1.2 安全芯片侧信道安全性的量化评估方法

8.2 侧信道技术在硬件木马检测中的应用

8.3 侧信道技术在云计算中的应用

8.3.1 云计算的定义

8.3.2 侧信道技术攻击虚拟机

8.4 总结

参考文献

《密码安全芯片与侧信道技术》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com