

<<软件保护新技术>>

图书基本信息

书名：<<软件保护新技术>>

13位ISBN编号：9787307100015

10位ISBN编号：7307100010

出版时间：2012-9

出版时间：武汉大学出版社

作者：查先进 编

页数：172

字数：282000

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：<http://www.tushu007.com>

## <<软件保护新技术>>

### 内容概要

《软件保护新技术》是一部关于软件保护理论与实践相结合的著作。全书共分6章，第1章对软件保护的现状、应用领域进行了综述性的说明；第2章介绍软件保护的基础知识；第3章介绍软件中的数据保护方法；第4章介绍软件中的计算保护方法；第5章介绍软件版权保护；第6章介绍软件保护中的密钥管理。

《软件保护新技术》适合从事软件工程、信息安全和通信领域的科研和工程技术人员阅读参考，也可作为计算机及相关专业的研究生教材与辅导书。

## <<软件保护新技术>>

### 书籍目录

#### 第1章 软件保护概述

- 1.1 引言
- 1.2 软件保护技术
  - 1.2.1 基于硬件的保护方法
  - 1.2.2 基于软件的保护方法
- 1.3 软件保护的应用
  - 1.3.1 当前保护技术的局限
  - 1.3.2 软件保护技术的应用
- 1.4 软件的知识产权保护
  - 1.4.1 软件知识产权概述
  - 1.4.2 软件知识产权的保护措施

#### 第2章 软件保护的技术基础

- 2.1 加密算法
  - 2.1.1 加密算法分类
  - 2.1.2 软件保护中的加密算法
- 2.2 HASH算法
  - 2.2.1 HASH算法原理
  - 2.2.2 SHA算法
  - 2.2.3 MD5算法
- 2.3 签名算法
  - 2.3.1 签名算法概述
  - 2.3.2 数字签名原理
  - 2.3.3 非对称密钥密码算法进行数字签名
  - 2.3.4 对称密钥密码算法进行数字签名
  - 2.3.5 HASH算法进行数字签名
- 2.4 认证算法
  - 2.4.1 口令共享认证算法
  - 2.4.2 基于散列树的广播认证

#### 第3章 软件中的数据保护

- 3.1 数据保护的任务
  - 3.1.1 数据保护定义
  - 3.1.2 存储介质上数据保护分类
  - 3.1.3 数据保护应用
- 3.2 数据混淆
  - 3.2.1 数据混淆原理
  - 3.2.2 数据混淆方法
  - 3.2.3 数据混淆实现
- 3.3 同态数据混淆

#### 第4章 软件中的计算保护

- 4.1 计算保护的任务
- 4.2 计算保护技术
  - 4.2.1 防篡改硬件
  - 4.2.2 环境密钥生成
  - 4.2.3 黑箱安全
  - 4.2.4 加密函数计算

## &lt;&lt;软件保护新技术&gt;&gt;

- 4.2.5 滑动加密
- 4.2.6 代码混淆
- 4.3 基于RSA同态加密函数计算
  - 4.3.1 整数环上的同态加密机制
  - 4.3.2 基于RSA的幂同态
  - 4.3.3 同态加密函数计算CHEF
  - 4.3.4 CHEF小结
- 4.4 基于ElGamal算法的同态加密函数计算
  - 4.4.1 ElGamal加密
  - 4.4.2 基于更新的ElGamal的代数同态加密机制
  - 4.4.3 AHBE小结
- 4.5 计算保护在移动代理中的应用
  - 4.5.1 移动代理概述
  - 4.5.2 移动代理的安全性问题
  - 4.5.3 基于计算保护的移动代理的安全
- 第5章 软件的版权保护
  - 5.1 软件版权保护的任务与进展
    - 5.1.1 软件版权保护的任务
    - 5.1.2 研究进展
  - 5.2 软件防篡改
    - 5.2.1 软件防篡改的任务
    - 5.2.2 评价指标
    - 5.2.3 软件防篡改技术分类
  - 5.3 软件水印
    - 5.3.1 软件水印研究现状及任务
    - 5.3.2 扩频软件水印
    - 5.3.3 动态图软件水印
    - 5.3.4 软件零水印
  - 5.4 数字版权管理
    - 5.4.1 DRM的起源与发展
    - 5.4.2 DRM定义与分类
    - 5.4.3 DRM工作原理以及模型
    - 5.4.4 主要的DRM技术标准分析
- 第6章 软件保护中的密钥管理
  - 6.1 密钥管理概述
    - 6.1.1 密钥管理定义
    - 6.1.2 密钥管理分类
    - 6.1.3 密钥管理流程
  - 6.2 软件保护中的密钥协商
    - 6.2.1 密钥协商概述
    - 6.2.2 密钥协商协议
    - 6.2.3 经典的证书基密钥协商协议
  - 6.3 软件保护中的密钥更新
    - 6.3.1 密钥更新
    - 6.3.2 密钥更新方案
    - 6.3.3 密钥更新效率分析
  - 6.4 软件保护中的密钥隔离

<<软件保护新技术>>

6.4.1 密钥隔离概述

6.4.2 密钥隔离的模型

6.4.3 基于IBE的密钥隔离

6.4.4 IR-KIE的方案

6.5 基于HIBE的密钥更新与隔离机制

6.5.1 HIBE

6.5.2 HIBE-IKE机制

6.5.3 HIBE-IKE模型安全分析

6.5.4 HIBE-IKE应用

附录 《计算机软件保护条例》

参考文献

## <<软件保护新技术>>

### 编辑推荐

软件保护是近几年来信息安全领域的一个新兴研究分支。

在软件保护的研究中，需要借鉴计算机安全方面的技术，还会用到计算机科学其他领域的知识：密码学、软件水印、软件混淆、防篡改技术、密钥管理等。

计算机软件可以简单地抽象为两个部分：数据和计算。

向广利、朱平、钟欣、鲁晓成所著的《软件保护新技术》主要是讨论软件中的数据保护和计算保护方法。

从软件的版权保护角度，考虑到软件分发的途径和软件运行环境的多样性，本书也论述软件的版权保护和适合软件保护的密钥管理体系。

<<软件保护新技术>>

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:<http://www.tushu007.com>