

<<计算机密码学>>

图书基本信息

书名：<<计算机密码学>>

13位ISBN编号：9787121066580

10位ISBN编号：7121066580

出版时间：1970-1

出版时间：电子工业出版社

作者：田园

页数：314

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>

## <<计算机密码学>>

### 内容概要

《计算机密码学：通用方案构造及安全性证明》阐述计算机密码方案与密码协议的安全性证明理论，包括基于计算复杂度概念的计算密码学方法和基于符号演算的形式分析与验证方法。安全性证明是一个技术复杂而思想活跃的领域，作者并不打算对此做面面俱到式的阐述，而只打算选择少数典型、普适、有发展前途同时又不特别复杂艰涩的方法进行论述。在选择这些方法时，作者也充分考虑到这些方法所解决的问题本身都有着相当的理论与应用价值，从而使读者通过仔细学习这些安全证明而能更深入地理解这些密码方案。

## 书籍目录

第1章 导论 1.1 Needham-Schoeder协议 1.2 更多的例子 1.3 更复杂的协议和攻击 1.4 一些符号约定 第2章 消息认证与数字签名方案 2.1 消息认证方案及其抗伪造性质 2.2 数字签名方案及其抗伪造性质 2.3 数字签名方案与身份鉴别协议：Fiat-Shamir变换 第3章 对称加密方案 3.1 各种保密性质及其相互关系 3.2 一些典型对称加密方案的保密性质 3.3 加密—认证方案：明文完整性与密文完整性 3.4 加密—认证方案的几个一般性构造 3.5 时变对称加密方案及其前向保密性质 第4章 公钥加密方案( )：保密性质和PA性质 第5章 公钥加密方案( )：一些通用构造及其保密性条件 第6章 公钥加密方案( )：匿名性质 第7章 身份鉴别协议 第8章 密码协议的UC—理论及应用 第9章 Dolev-Yao理论( )：自由消息代数strand—图模型 第10章 Dolev—Yao理论( )：自动分析技术 第11章 Dolev-Yao理论( )：带交换群算术的非自由消息代数 第12章 密码协议形式模型的计算语义( )：被动攻击情形 第13章 密码协议形式模型的计算语义( )：主动攻击情形 附录A 一些必要的数学事实 附录B 进程代数模型：spi—演算 参考文献

## <<计算机密码学>>

### 编辑推荐

《计算机密码学:通用方案构造及安全性证明》由电子工业出版社出版。

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>