“Happy New Year of the Rabbit”

密码编码学与网络信息安全

3hrs/week
score 3

Prof Yuesheng Zhu 朱跃生

Ph.D in EE， Msc in EE, Bsc in EE

Room: 6号楼 A1502

Email: zhuys@pku.edu.cn

Dr Guibo Luo 罗桂波

Ph.D in CS， Msc in EE, Bsc in EE

Room: 6号楼 A911

Email: luoguibo@pku.edu.cn

Teaching Assistant:
干皓丞（21级）

Specialty and Interested Area

Information/Network/Data Security

Artificial Intelligent and Security

Intelligent Multimedia Technology

Signal Processing（Audio/Image/Video）

DSP in Communication

Telecommunications

Who will Take?

Research Directions

Information Security (both hardware and Software),

Heterogeneous Network Convergence

Wireless Communications,

Telecommunications,

E-business, E-finance, E-Government

Intelligent information ecological environment

融合先进信息技术的万物互联智能生态环境

（Hot Fields： IMABCDEXS）

网络空间安全-国家一级学科

- 五大空间

  领土
  领空
  领海
  太空
  网络空间

- ✓ 信息安全专业-网络空间安全学院

没有网络安全就没有国家安全

□习近平总书记重要论述

✓ 2013年11月15日关于《中共中央关于全面深化改革若干重大问题的决定》说明）
网络和信息安全牵涉到国家安全和社会稳定

✓ 2014年2月27日在中央网络安全和信息化领导小组第一次会议上讲话）

◆ 网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题
◆ 网络安全和信息化对一个国家很多领域都是牵一发而动全身
◆ 没有网络安全就没有国家安全，没有信息化就没有现代化
◆ 以安全保发展、以发展促安全，努力建久安之势、成长治之业
◆ 总体布局，统筹各方，创新发展，努力把我国建设成为网络强国

✓ 2015年9月23日会见出席中美互联网论坛双方主要代表时的讲话

安全、稳定、繁荣的网络空间，对一国乃至世界和平与发展越来越具有重大意义

网络犯罪成为危害国家政治安全、网络安全、社会安全、经济安全等的重要风险

✓ **2016年4月19日在网络安全和信息化工作座谈会上的讲话**

国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这对世界各国都是一个难题

✓ **2017年2月17日在国家安全工作座谈会上的讲话**

加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护

✓ **2020年11月16日在中央全面依法治国工作会议上的讲话**

网络犯罪已成为危害我国国家政治安全、网络安全、社会安全、经济安全等的重要风险之一

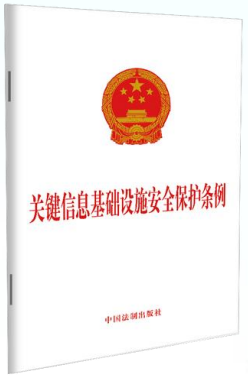
《中华人民共和国网络安全法》

自2017年6月1日起施行

- 全面**规范网络空间安全及管理**的基础性法律
- 规范网络空间法治建设，**依法治网、化解网络风险**，保障互联网在法治轨道上健康运行

《关键信息基础设施安全保护条例》

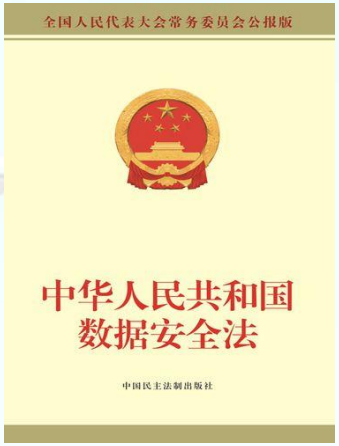
自2021年9月1日起施行



- 根据《网络安全法》制定的条例
- 明确各方责任，建立保障促进措施，**保障关键信息基础设施安全**，及维护网络安全

《中华人民共和国数据安全法》

2021年9月1日起施行



➢ 我国关于“数据安全”首部法律

规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益

数字智能

✓ 以数据开发利用促进数据安全

数据依法合理有效利用，保障数据依法有序流动

✓ 促进数字经济发展创新

数据作为在数字经济的关键生产要素，促进以数据为关键要素的数字经济发展

✓ 提升国家数据安全保障能力

“大物云智移”等新技术应用、全场景、大规模数据应用存在对国家安全造成严重威胁，需要法律来有效维护数据安全，有效提升数据安全的保障能力

✓ 扩大数据保护范围

以电子或非电子形式对信息记录的数据，包括电子数据和非电子形式的数据。《网络安全法》指的是网络数据，明确要求保障网络数据完整性、保密性、可用性能力

✓ 数据监管有法可依

随着数据安全热点事件出现，如数据泄露、勒索病毒、个人信息滥用等，出台针对数据安全保障领域的法律加强对数据监管

数据安全

《中华人民共和国个人信息保护法》

2021年11月1日起施行

➢ 保护个人信息的法律

- ✓ 个人信息处理的基本原则
- ✓ 与政府信息公开条例的关系
- ✓ 对政府机关与其他个人信息处理者的不同规制方式及其效果
- ✓ 协调个人信息保护与促进信息流动关系
- ✓ 个人信息保护法在特定行业的适用问题
- ✓ 关于敏感个人信息问题、法律的执行机构
- ✓ 行业自律机制
- ✓ 信息主体权利
- ✓ 跨境信息交流问题
- ✓ 刑事责任问题

➢ 对个人及行业作用

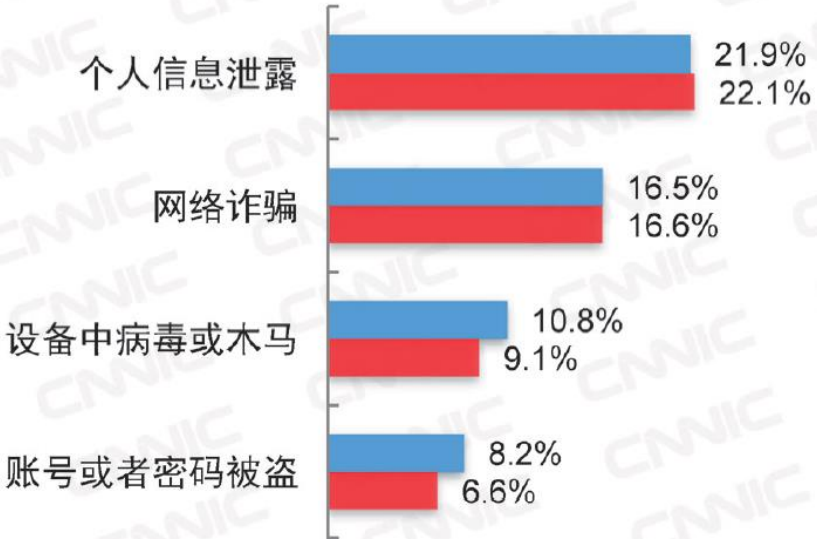
- ✓ 通过数据库安全的技术手段实现核心数据加密存储
- ✓ 通过数据库防火墙实现批量数据防泄漏
- ✓ 通过数据脱敏实现批量个人数据的匿名化
- ✓ 通过数字水印实现溯源处理

《中华人民共和国反电信网络诈骗法》

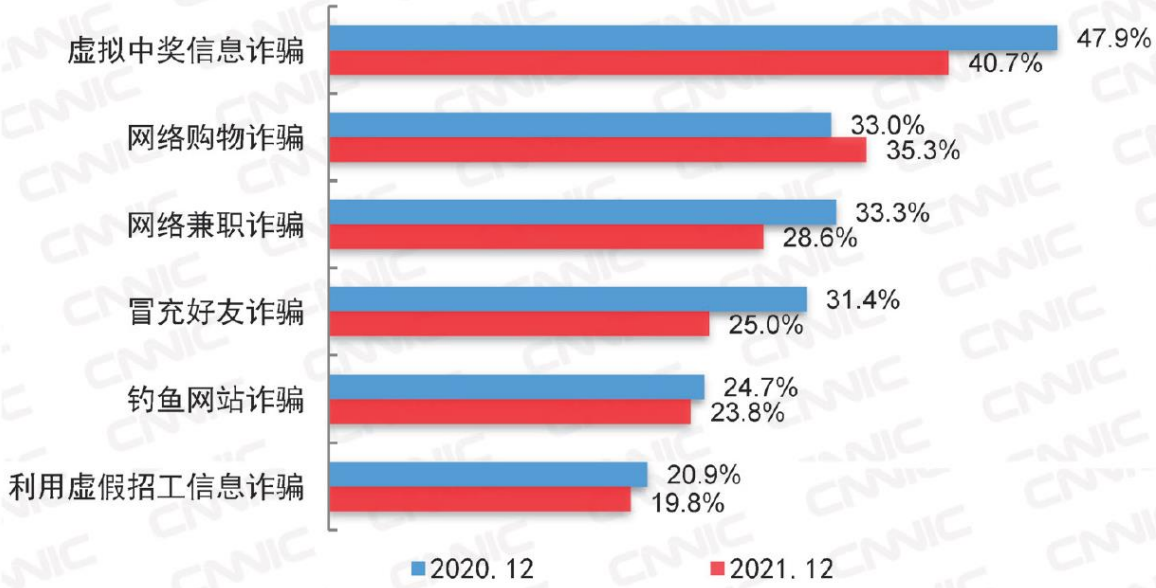
2022年9月2日，十三届全国人大常委会第三十六次会议通过
自2022年12月1日起施行

➢ 预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全的法规

网民遭遇各类网络安全问题的比例



网民遭遇各类网络诈骗问题的比例



来源：CNNIC 中国互联网络发展状况统计调查 2021.12

数据安全与传统网络信息安全的差异性

✓传统网络安全主要关注个人计算机、智能终端机、网络服务器等用户或系统的安全防护

✓大数据环境下，数据服务提供者、云平台、互联网信息中心IDC及虚拟化等技术引入。数据存储/运行在云平台或智能IDC上，数据拥有者无法直接掌控信息的安全性。关注数据不被滥用或损坏的安全管理及防护

✓数据交互及共享与服务是大数据产业的重要应用，提供各种信息安全交互技术及管理措施，防止敏感信息泄露以及信息非法滥用等安全威胁与风险

数据安全与传统信息安全的共异点

- 数据安全与传统信息安全共性问题
  - 病毒、蠕虫、木马等恶意攻击
  - 黑客攻击
  - 软件漏洞引起的信息泄漏
- 大数据时代，应用场景丰富，信息安全原则以及安全需求的内涵得到展开和引申，信息安全更关注于数据全生命周期的内容安全防护及隐私保护

前沿领域：覆盖数据全生命周期的数据安全防护体系

- 在移动计算、云计算及智能 分析的环境下，数据在采集、传输、存储、挖掘、分析、处理、交互、共享及服务各环节可能出现的数据安全问题，上下游产业在数据安全管理及隐私保护等

- 覆盖数据全生命周期的数据安全防护体系，以及支撑该体系关键技术，包括授权、鉴权、密钥共享、加密、脱敏、抗抵赖等数据安全及隐私保护技术。

传统保护信息安全手段（计算机出现前）

traditionally provided by physical and administrative mechanisms

物理手段（physical）：

保险柜：防止被盗窃、毁坏、非法阅读或篡改

图章或签名：表明档的真实性和有效性

铅封：防止文件在传送中被非法阅读或篡改

行政手段（ administrative） (政策)：

文件管理制度：

机密等级

行政级别

密码学手段：

密文

安全隐患

自身缺陷 + 开放性 + 黑客攻击

互联网的特点：

开放性、交互性、分布性、互连性

发明时，根本没有考虑安全问题与 用户的诚信

业务基于公开协议

远程访问

连接基于彼此信任

黑客（Hacker）攻击

“非法入侵者”

目的：

基于兴趣

基于利益

基于捣乱

信息安全的挑战

Copy： 复制后的文件跟原始档没有差别

Modify：对原始档的修改可以不留下痕迹

Signature：无法在文件上直接签名或盖章

Transmit： 在传送中可被非法阅读或篡改

Storage：在保管中可被盗窃、毁坏、非法 阅读或篡改

Method：信息安全无法完全依靠物理手段和行政管理

安全服务 (Security Services)

- 保密 Confidentiality (privacy)
- 鉴别 Authentication (who created or sent the data)
- 完整 Integrity (has not been altered)
- 不可抵赖 Non-repudiation (the order is final)
- 存取/接入控制 Access control (prevent misuse of resources)
- 可用 Availability (permanence, non-erasure)

prevent

Virus that deletes files

Denial of Service Attacks

为什么需要密码算法

- 信息存储:存放在公开的地方
- 信息交换:使用非隐秘介质
- 信息传输:通过不安全通道

密码学

- 密码学：

  研究与信息安全相关的方面如机密性、完整性、实体鉴别、抗否认等的数学理论。

  由**密码编码学**和**密码分析学**构成。

- 密码**编码学**的基本目标：
  - 机密性、数据完整性、鉴别、抗否认
- 基本的密码工具：

  加密、散列函数、数字签名

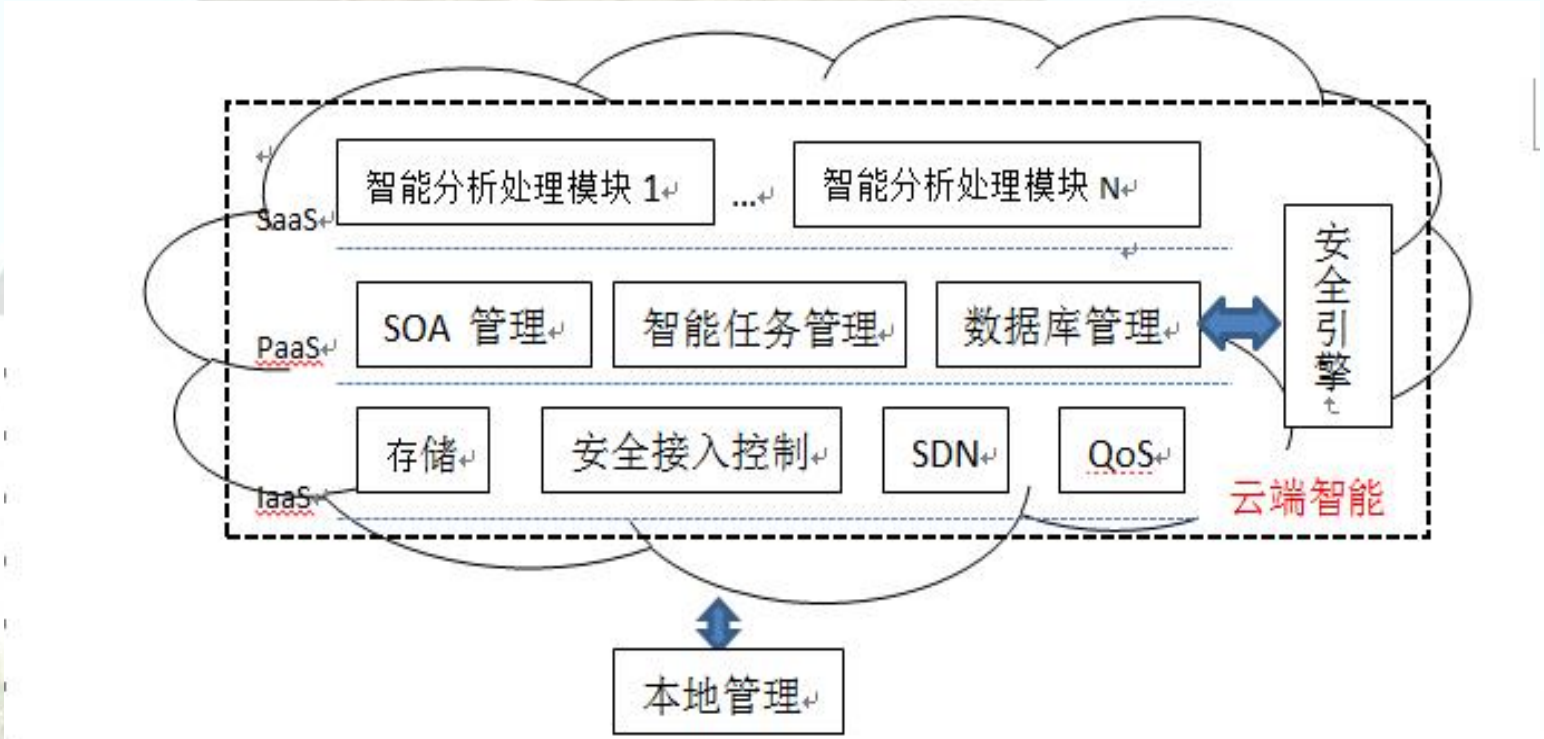
智能生产/机器人

- 云计算：数据和服务管理、虚拟化、和跨域共享模式特点
- 信息汇集，分析处理，存取共享，智能控制/生产及服务
- 服务器端隐私及控制的安全问题面临安全隐患及挑战

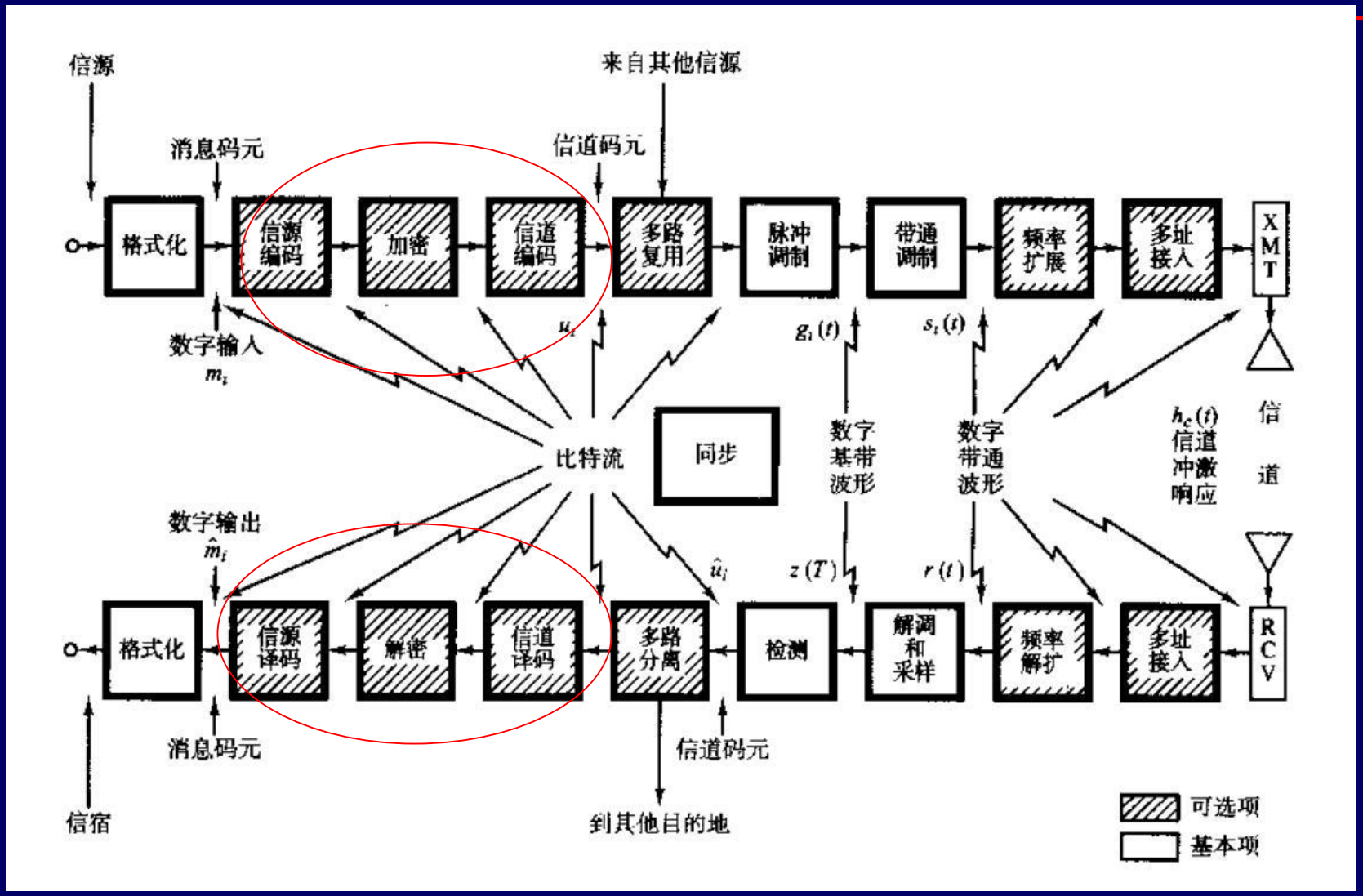
➢ 2015年德国钢铁厂熔炉控制系统
被黑客通过网络攻击，渗透到系统的业务网络，控制关键系统，使钢铁熔炉无法正常关闭，损失惨重

➢ 中石化华东公司，内鬼通过网络在油管监控系统中，嵌入破坏性程序，按需让系统正常、出错甚至瘫痪，影响系统正常运行，后果特别严重。

云端智能的机器人安全保障方案

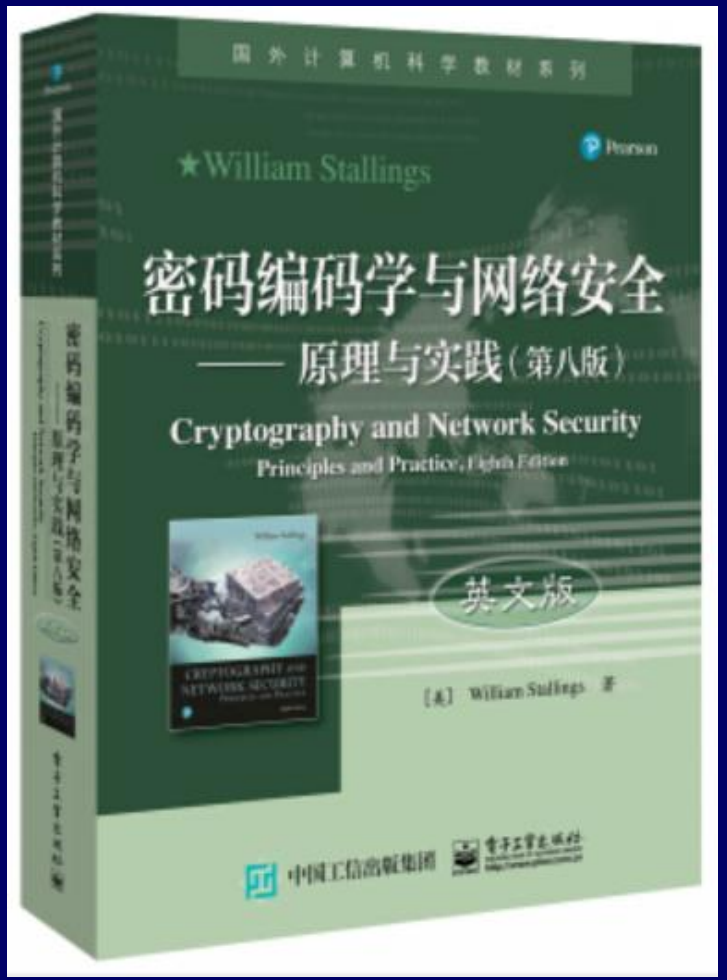


数字通信系统基本模型(完整系统)



TEXT Book

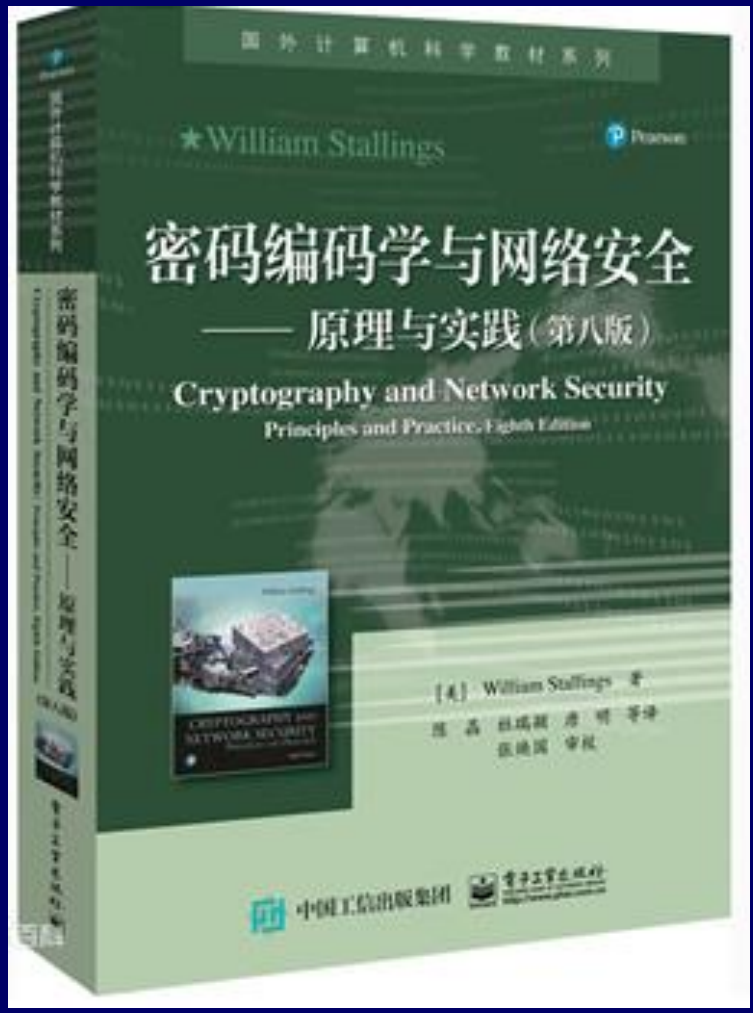
密码编码学与网络安全——原理与实践（第八版）（英文版）William，Stallings, 2020-05



中文版：

《密码编码学与网络安全—原理与实践（第八版）

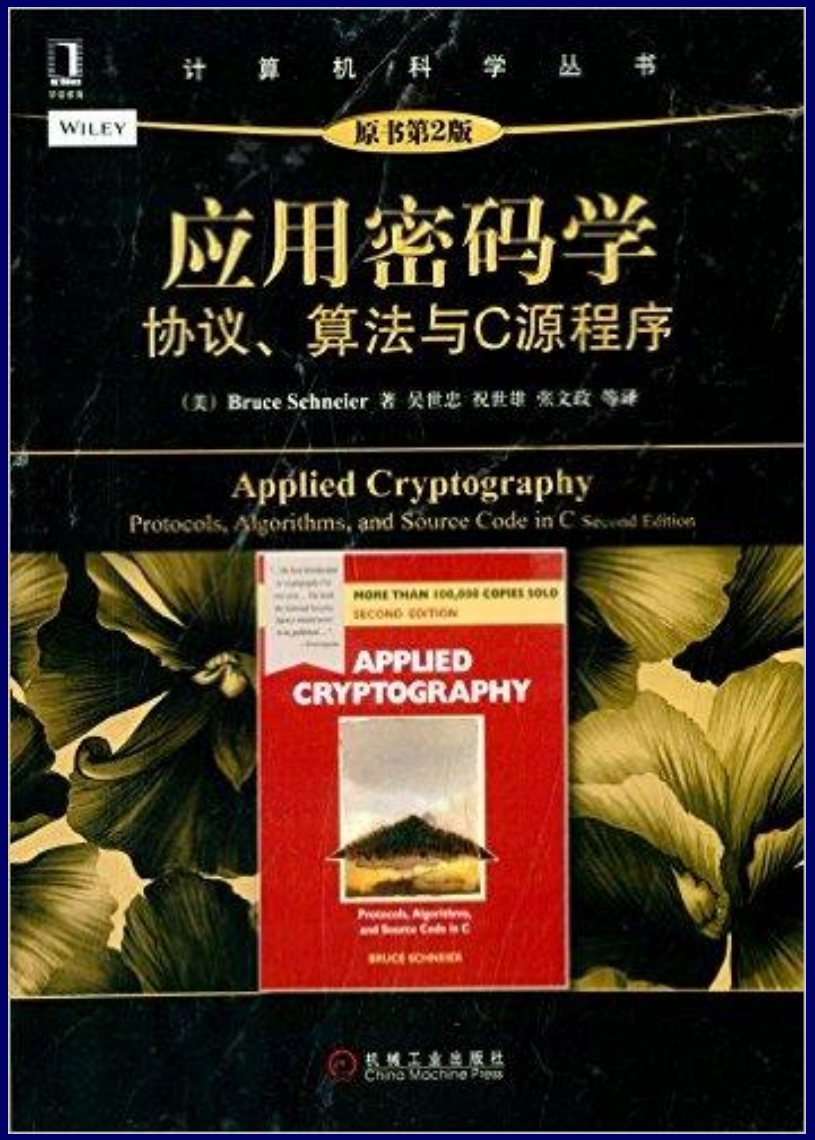
2021年电子工业出版社



Reference Books

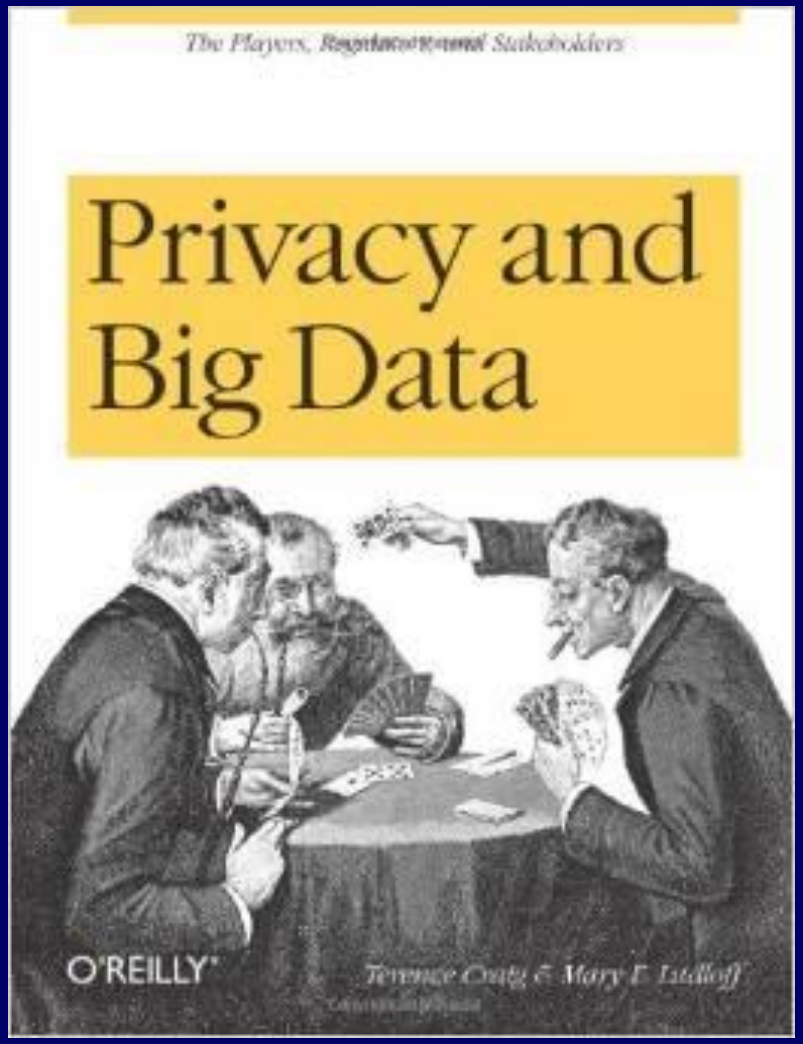
Bruce Shneier, “**Applied cryptography: protocols, algorithms, and source code in C**”, Second Edition.

吴世忠等译，《应用密码学 - 协议、算法与C源程序，》机械工业出版社，2014，1



Privacy and big data

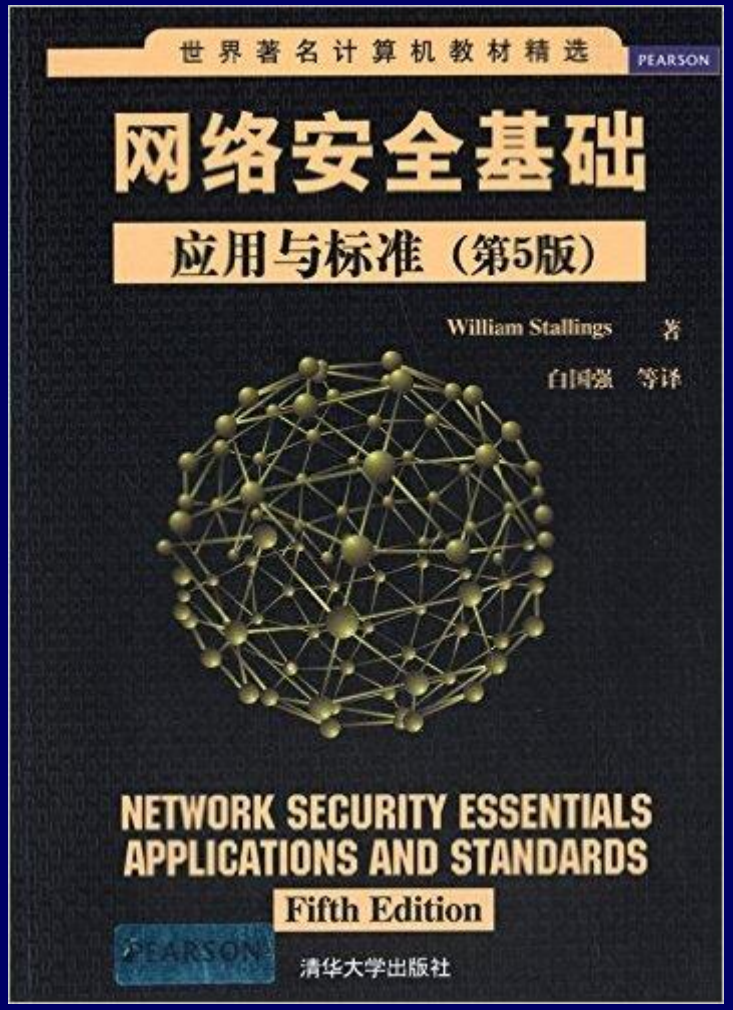
- by Terence Craig, Mary E. Ludloff
- Publisher:
  O'Reilly Media



Reference Books

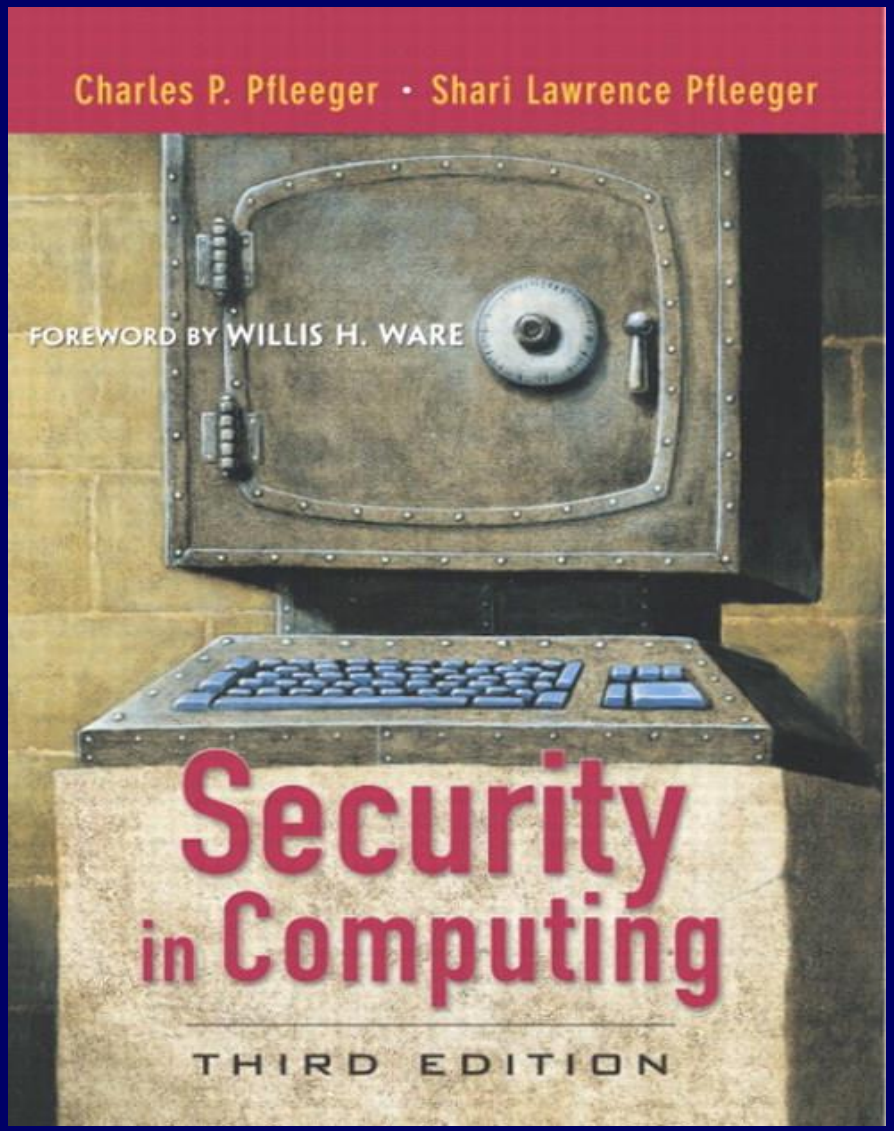
网络安全基础:应用与标准 (第5版) – 2014年5月1日

斯托林斯 (William Stallings) (作者), 白国强 (译者)



Reference Books

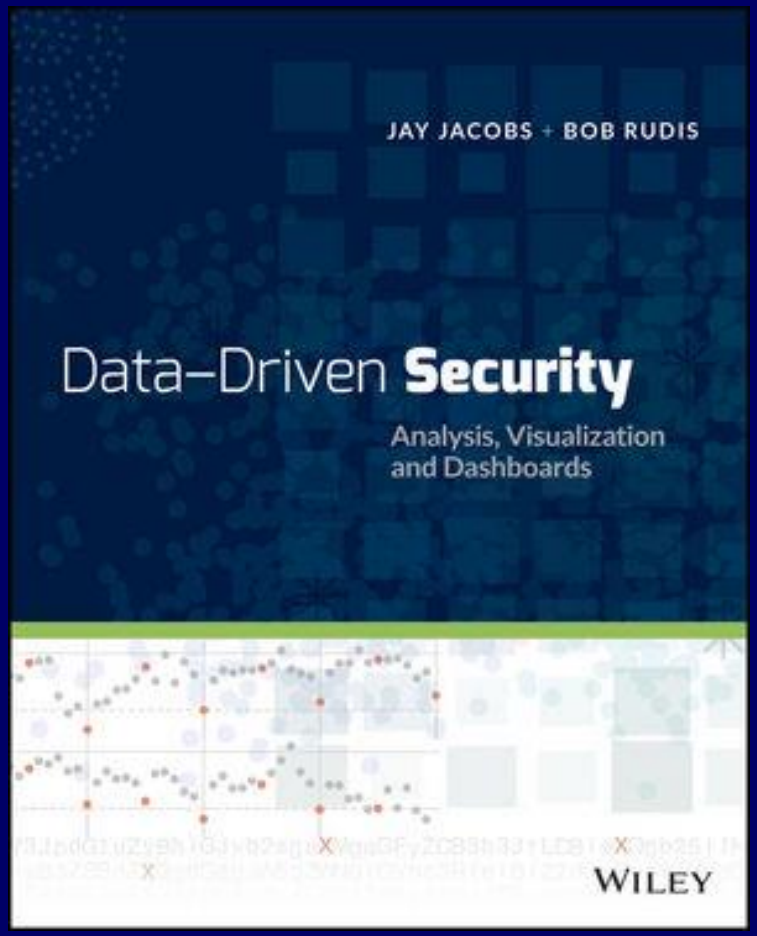
Charles P. Pfleeger, Shari Lawrence Pfleeger,
"**Security in Computing**",
Third Edition, Prentice Hall PTR 2003



Data-Driven Security: Analysis, Visualization and Dashboards

- By Jay Jacobs, Bob Rudis

- http://as.wiley.com/WileyCDA/WileyTitle/productCd-1118793722.html



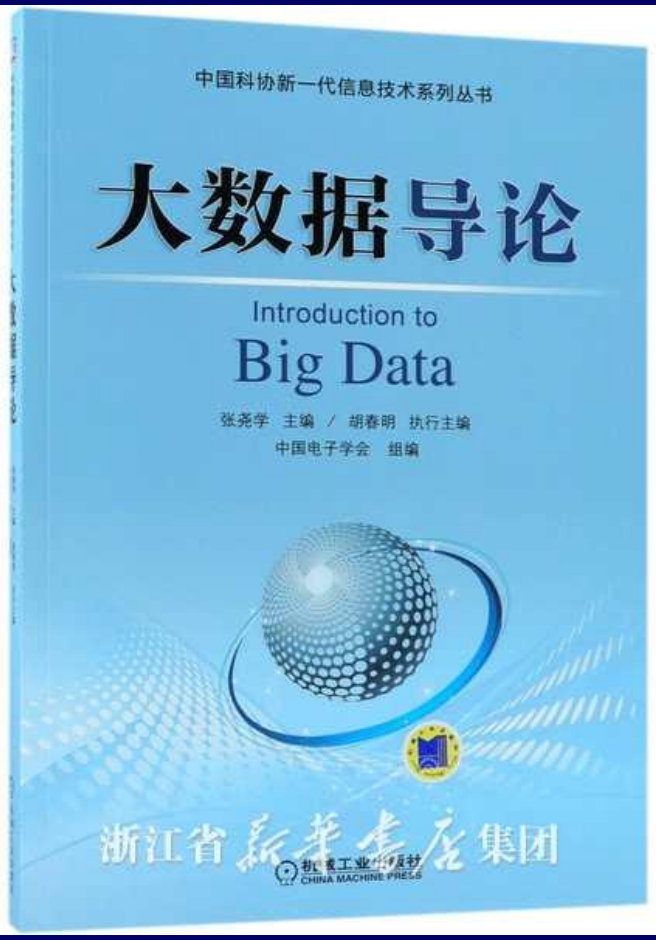
大数据导论　机械工业出版社，2018-08-01

- 张尧学等 中国电子学会
- 中国科协新一代信息技术系列丛书

参编:

- 王宏志　哈尔滨工业大学
- 唐　杰　清华大学
- 王建民　清华大学
- 袁晓如　北京大学
- 朱跃生　北京大学
- 吴中海　北京大学
- 吕金虎　北京航空航天大学
- 王　晨　清华大学
- 陈恩红　中国科学技术大学
- 刘　闯　中国科学院
- 王德庆　北京航空航天大学
- 马民虎　西安交通大学

数据安全与隐私保护



大数据与人工智能技术丛书

教育部-阿里云产学合作协同育人项目支持

人工智能安全

◎ 曾剑平 编著

教学课件　程序代码

独特的安全视角

构建人工智能安全观，阐述人工智能的安全属性与安全原理，理解人工智能安全的本质。

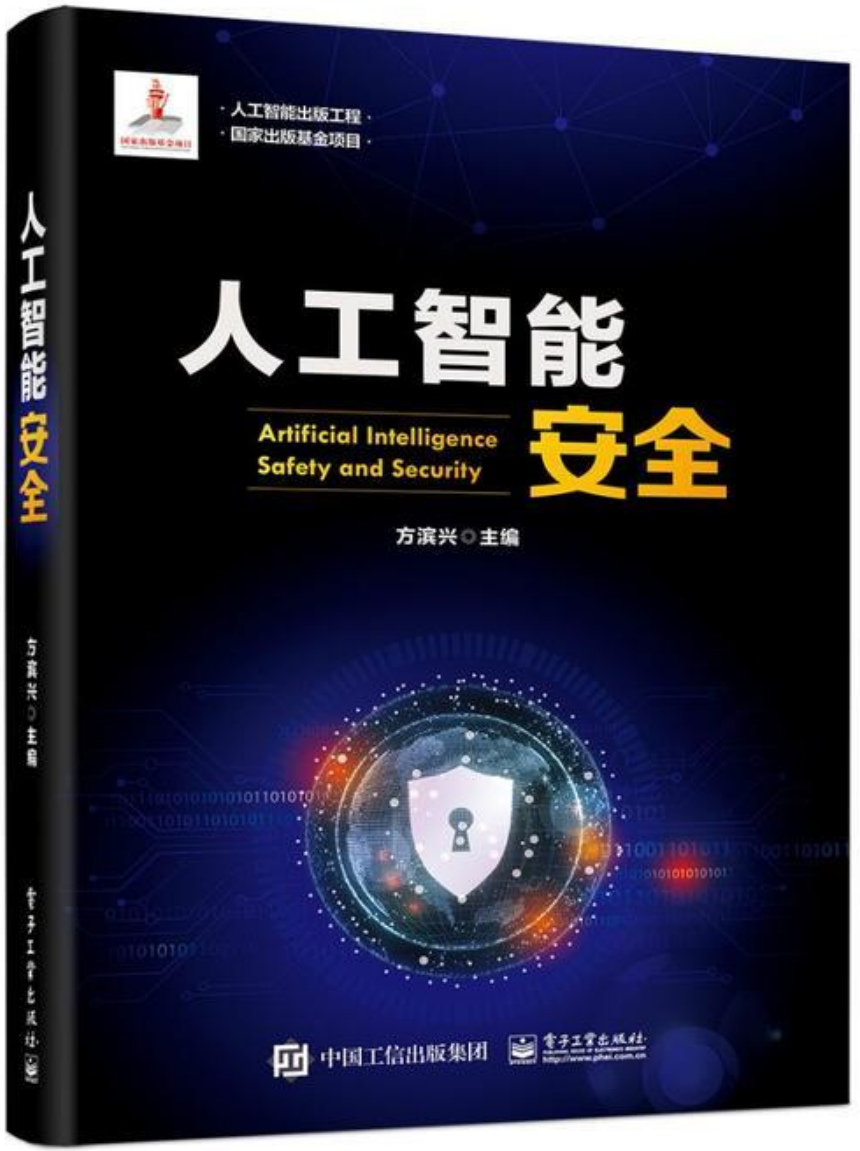
完整的知识体系

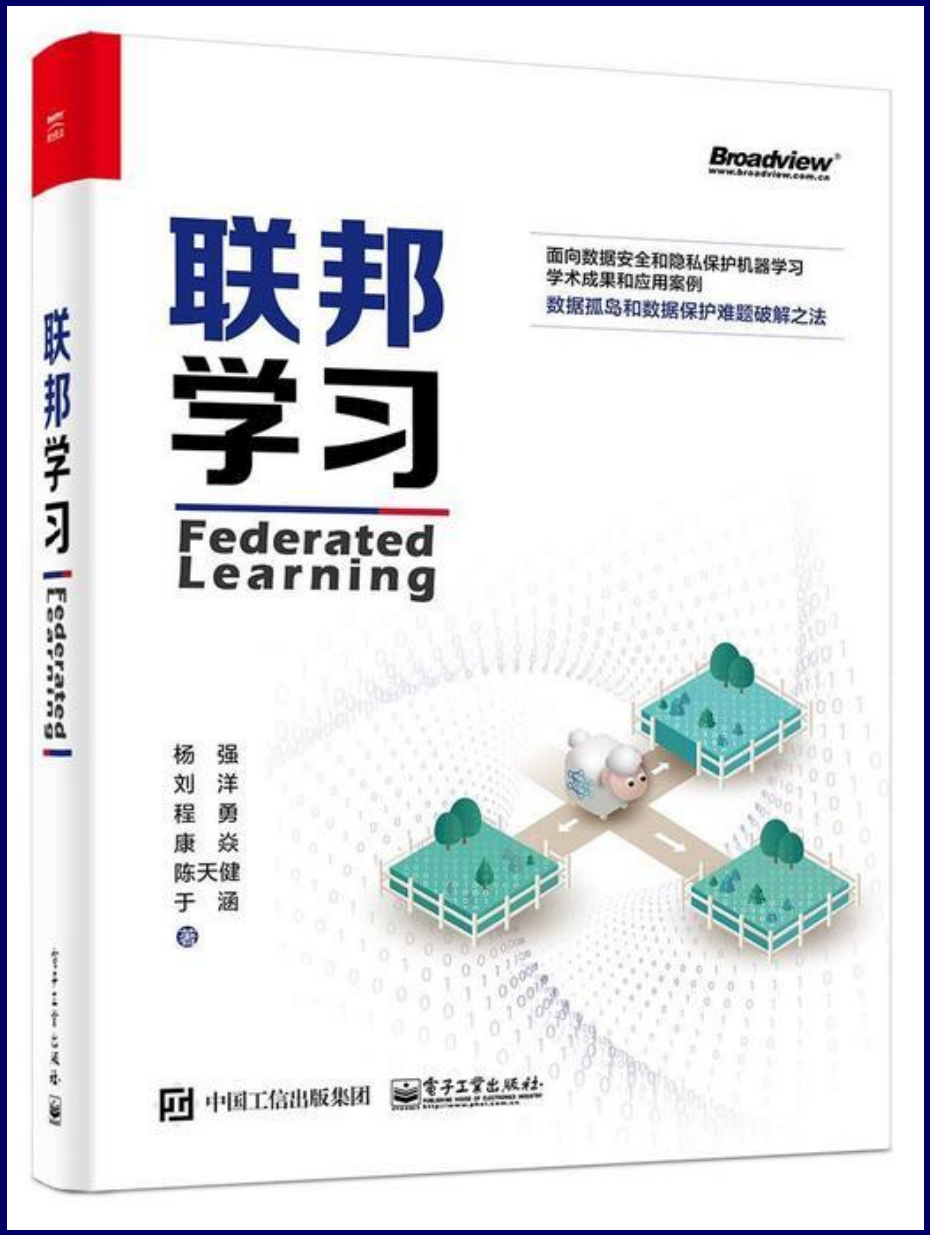
涵盖人工智能安全技术及应用的四大方面：数据处理、网络攻防、模型攻防、平台安全与工具。

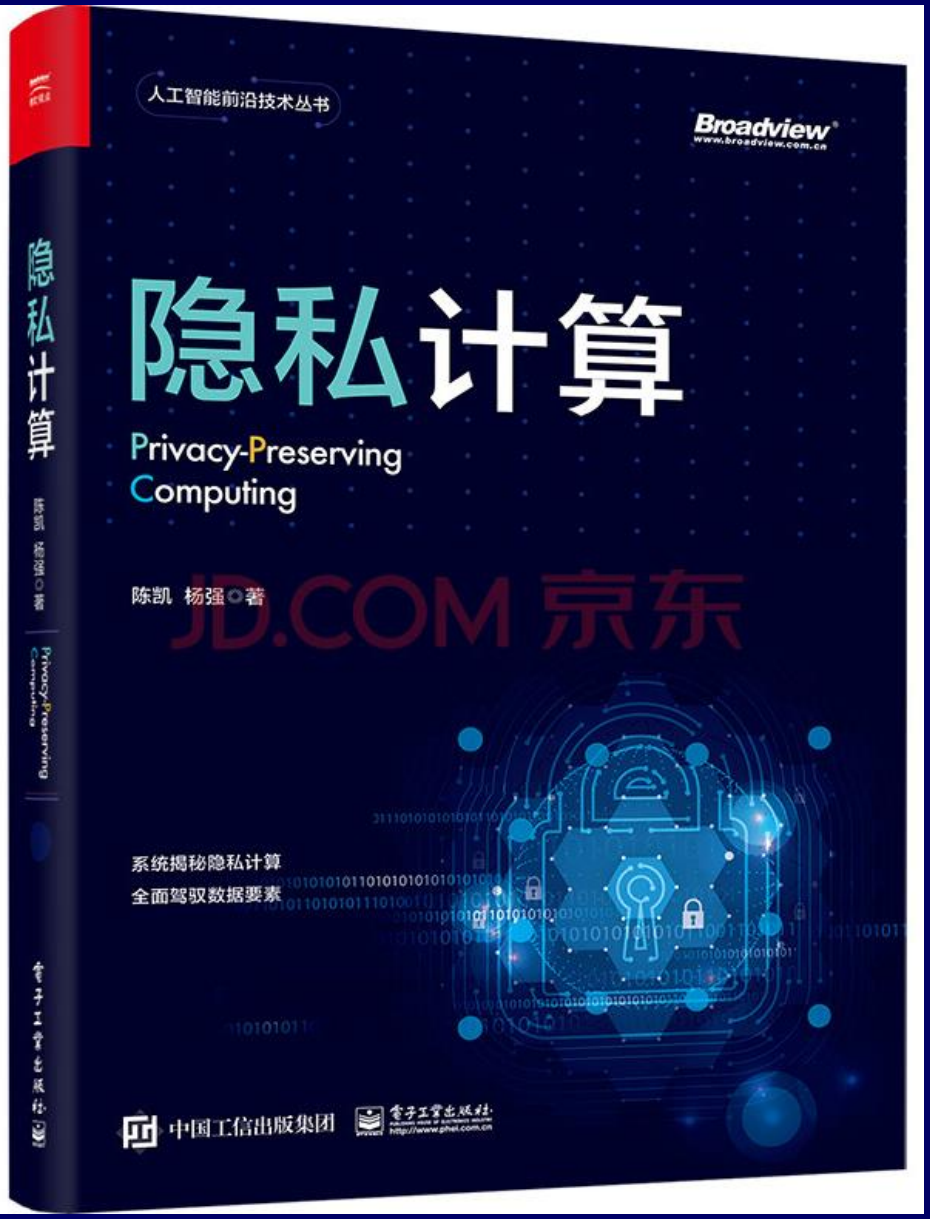
丰富的实践案例

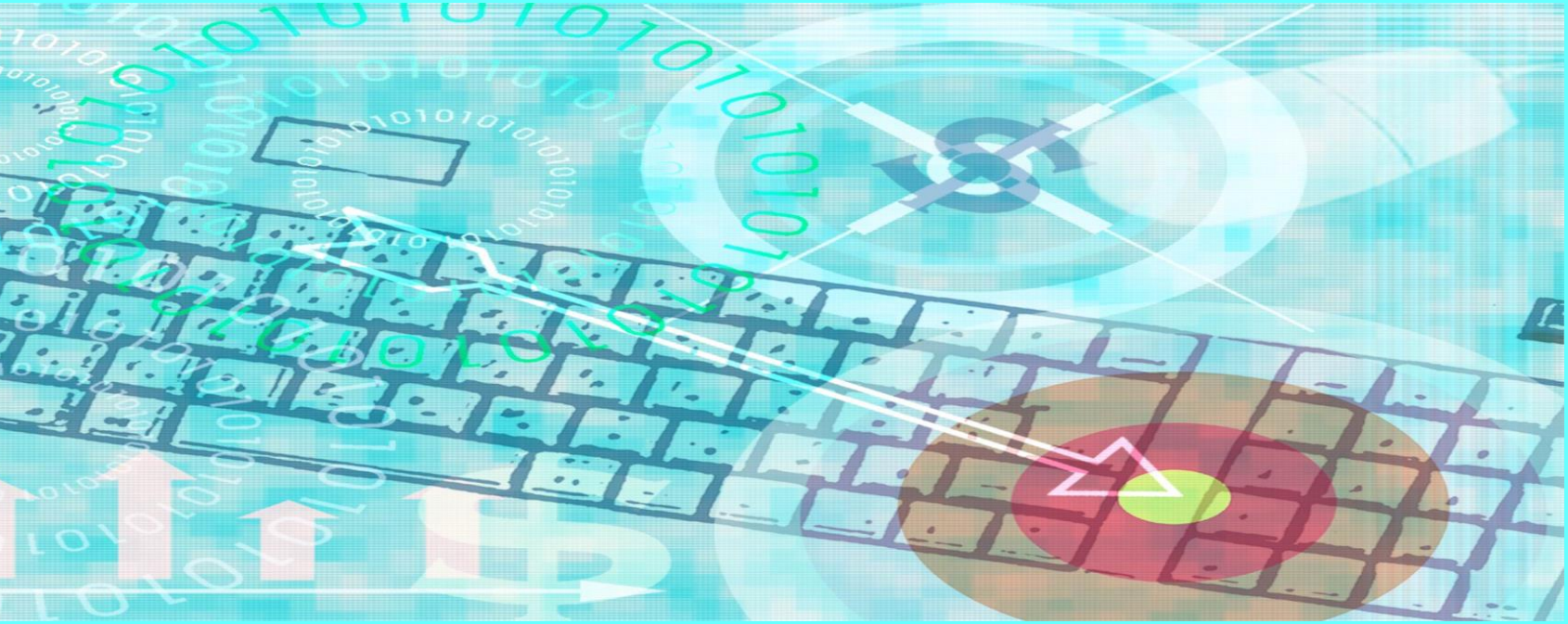
提供10个案例及代码，包括入侵检测、虚假新闻检测、多种分类器的投毒和逃避攻击、聚类算法的攻击等。

清华大学出版社




Broadview
www.broadview.com.cn
联邦学习
面向数据安全和隐私保护机器学习
学术成果和应用案例
数据孤岛和数据保护难题破解之法
Federated Learning
杨 强
刘 洋
程 勇
康 焱
陈天健
于 涵
著
中国工信出版集团
电子工业出版社
联邦学习 Federated Learning


人工智能前沿技术丛书
Broadview
www.broadview.com.cn
隐私计算
Privacy-Preserving Computing
陈凯 杨强 著
JD.COM 京东
系统揭秘隐私计算
全面驾驭数据要素
中国工信出版集团
电子工业出版社
http://www.phei.com.cn



Internet Industry Standards/Open resource

www.ietf.org: RFC (Request for Comments)

www.rsasecurity.com

www.openssl.org

web.mit.edu/kerberos/www/

www.nist.gov

Examination & Grading System

Grading System：

Assignments 50%

Mini projects and Research Reports: 50%