



网络空间安全导论

李琦

清华大学网研院



任课教师简介—李琦



清华大学网研院副教授，博士生导师

研究领域： 互联网和云安全
人工智能和大数据安全
移动和物联网安全

办公地点：FIT楼3区213 办公电话：62603080 电子邮件：qli01@tsinghua.edu.cn

个人主页：<https://sites.google.com/site/qili2012>



认识助教



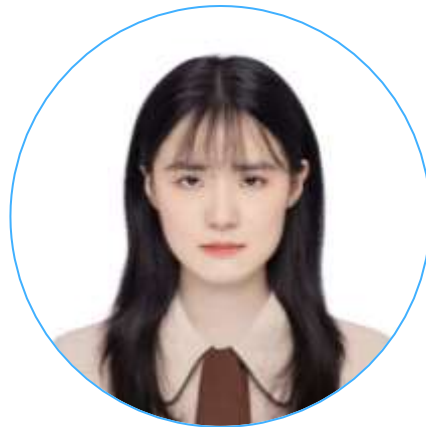
庆语其

qyq21@mails.tsinghua.edu.cn



徐易

y-xu22@mails.tsinghua.edu.cn



王叶

wangye22@mails.tsinghua.edu.cn



车熙嘉

cxj22@mails.tsinghua.edu.cn



课程简介与课程目标



应用实践

practice

- 精心设计实验验证环节，让同学们在动手实践、边学边练中不断加深对网络空间安全问题的理解和领悟



典型用例

Typical cases

- 通过典型安全事件和实例分析，提高同学们的应用思维能力
- 启发同学们进行思考，初步掌握网络空间安全问题分析和防范的方法



基础理论

Basic theory

- 介绍网络空间安全学科基础框架和基础理论
- 全面勾勒网络空间安全全景知识体系
- 认识网络空间安全隐患，提高网络空间安全意识



网络空间安全学科发展



国家批准增设：网络空间安全一级学科

安全是一种依附和伴生技术，
先有这种技术，才有这种技术安全。

先有网络空间，才有网络空间安全！

网络空间安全体系来源于网络空间技术体系。

应用安全

系统
安全

网络
安全

网络空间安全基础

密码学及应用

国务院学位委员会
教 育 部 文 件

学位〔2015〕11号

国务院学位委员会 教育部 关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。



网络空间安全理论支撑

网络空间安全基础

支撑网络空间安全一级学科的基础，为网络空间安全其他研究方向提供理论基础、技术架构和方法学指导

网络空间安全数学理论 (Mathematical theory)
网络空间安全体系结构 (Cyber security architecture)
网络空间安全博弈理论 (Game theory)
网络空间安全治理与策略 (Governance and policies)
网络空间安全标准与评测 (Standard and evaluating)
网络空间中人的安全行为与管理 (Human security behavior and management)
.....

对称密码设计与分析 (Design and analysis of symmetric cryptographic)
公钥密码设计与分析 (Design and analysis of public key cryptography)
安全协议设计与分析 (Security protocol)
侧信道分析与防护 (Channel measurement analysis and protection)
量子密码和新型密码 (Quantum and new cryptography)
.....

密码学及其应用

在有敌手的环境下，研究计算、通信和网络的信息编码和分析，为系统、网络、应用安全提供密码机制



网络空间安全之系统安全

- 研究网络空间环境下计算单元（端系统）的安全
- 计算系统安全是网络空间安全的基础单元

- 芯片安全 (Chip Security)
- 系统硬件及物理环境安全 (System hardware and physical environment Security)
- 系统软件安全 (System software Security)
- 恶意代码分析与防护 (Malicious code analysis and protection)
- 可信计算 (Trust computing)
- 先进计算安全 (Advanced computing security)
-



网络空间安全之网络安全

- **网络是指网络空间环境中连接端系统的中间设备、链路等基础设施以及相关的服务系统和管理系统。网络安全是网络空间安全的重要保障**

- 通信基础设施及物理环境安全 (Communication Infrastructure and physical environment security)
- 互联网基础设施安全 (Internet Infrastructure security)
- 网络安全管理 (Network security management)
- 网络安全防护与主动防御，包括攻防与对抗 (Network security protection and active defense)
- 端到端的安全通信 (End to end security Communication)
-



网络空间安全之应用安全

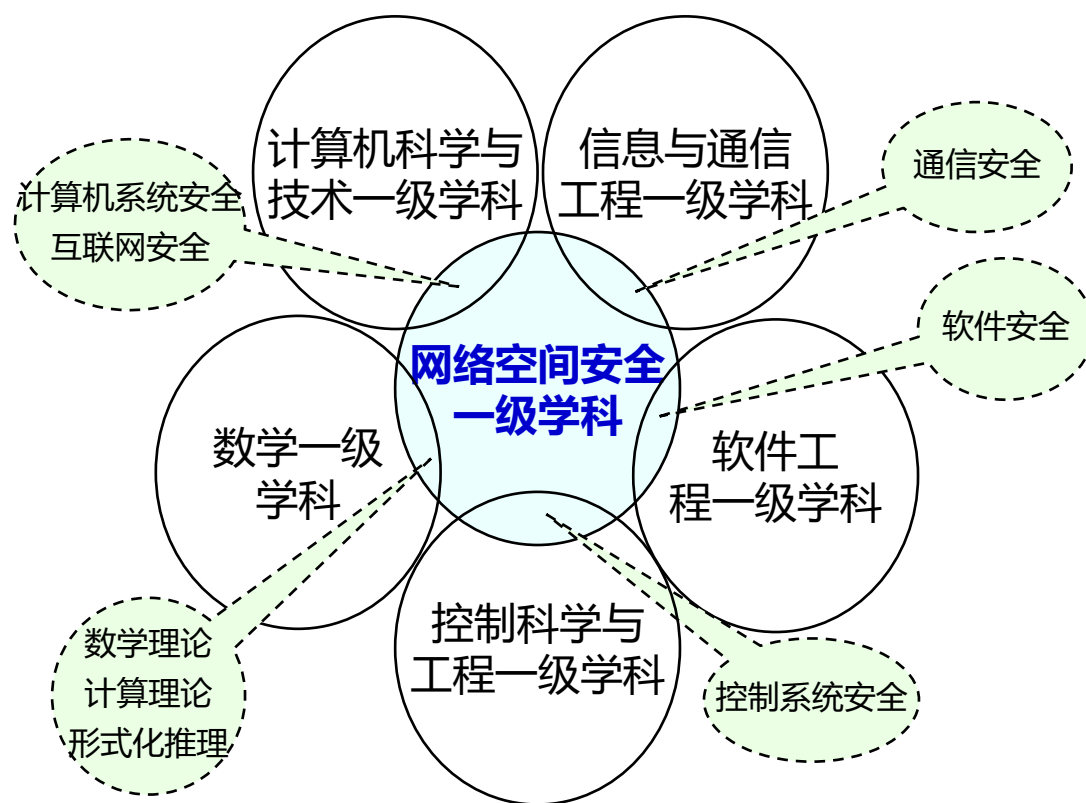
- 应用是指网络空间中建立在互联网之上的应用或服务系统，如国家重要行业应用、社交网络、区块链等
- 应用安全研究各种安全机制在一个复杂系统中的综合应用
 - 关键应用系统安全(Critical application system security)
 - 物联网与工控安全(Internet of things and industrial control system security)
 - 社交网络安全(Social network security)
 - 信息内容安全(Network information content security)
 - 数据安全与隐私保护(Data security and privacy protection)
 -



网络空间安全学科特点

- **网络空间安全渗透于网络空间的各个部分**
 - 互联网安全、系统安全、应用安全、内容安全
 - 网络空间安全基础、密码学及其应用
 - 典型的交叉学科
- **加强网络空间基础研究和掌握核心技术是解决网络空间安全的关键**
- **网络空间安全学科建设关键是培养高层次人才**
 - 硕士生、博士生
- **坚持国际化学科接轨和学术交流**

网络空间安全与与相近一级学科的关系





网络空间安全学科的理论体系

电子商务/政务安全、物联网安全、信息内容安全等

各种网络空间安全应用技术

芯片安全、可信计算、
操作系统安全、软件安全等

系统安全理论与技术

通信安全、互联网安全、
网络对抗、网络安全管理等

网络安全理论与技术

网络空间安全体系结构、大数据分析、对抗博弈等

网络空间安全理论

对称加密

公钥加密

密码协议

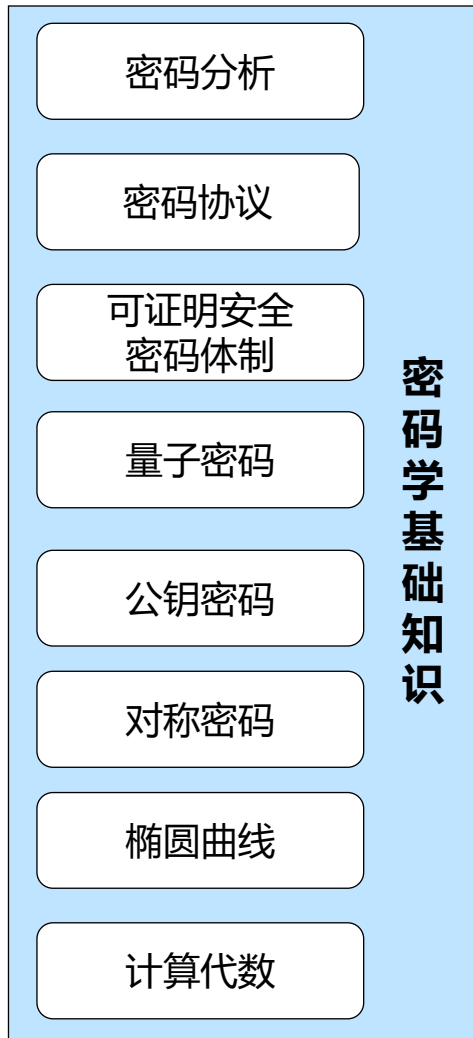
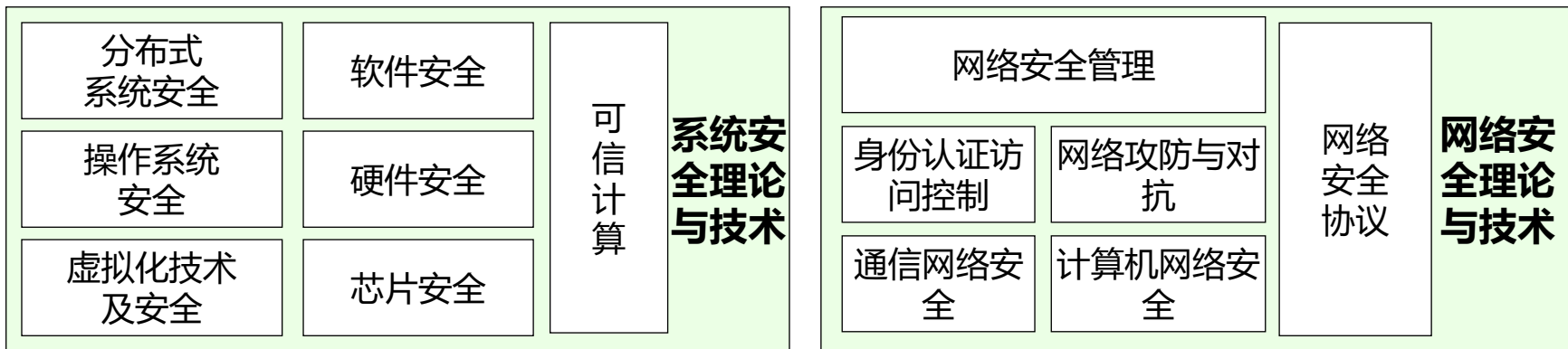
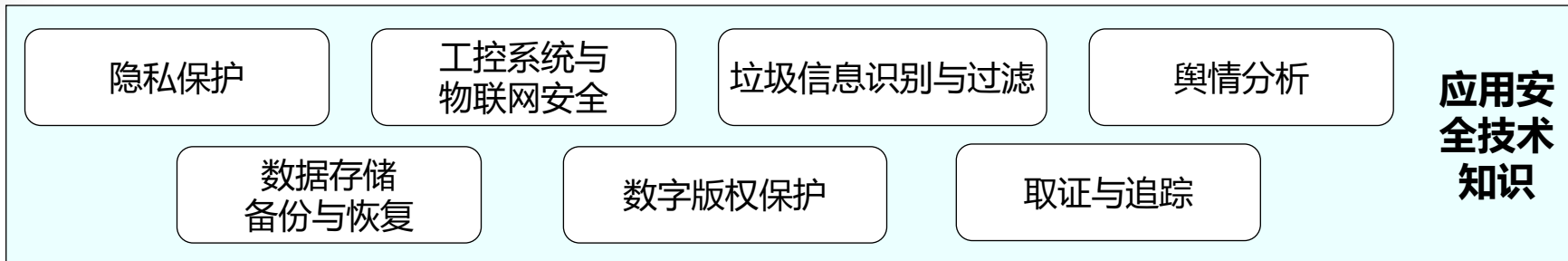
密码分析

侧信道分析
等

密码理论



网络空间安全学科知识体系

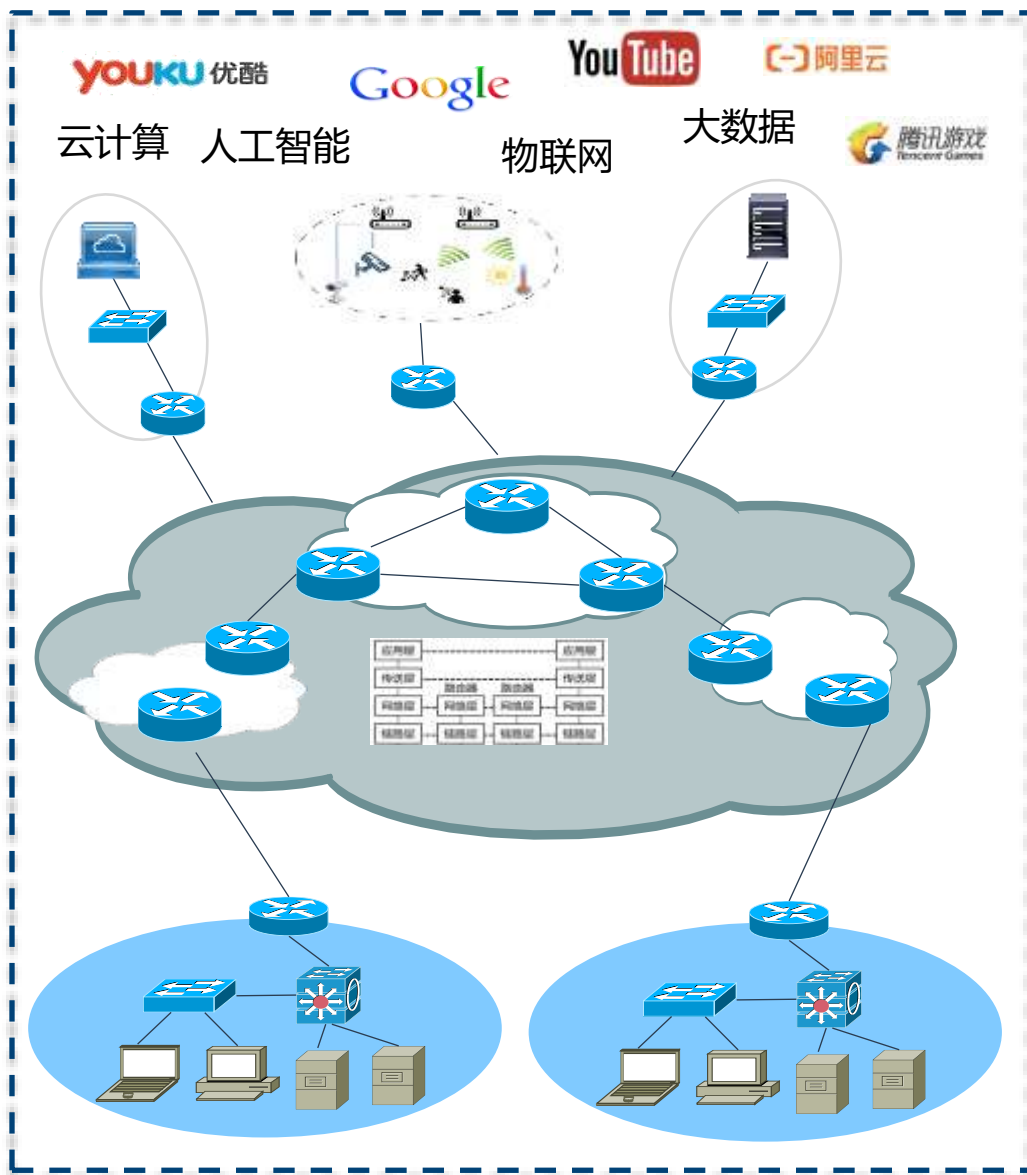
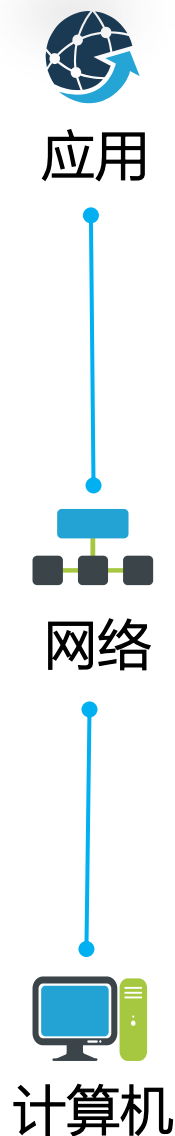




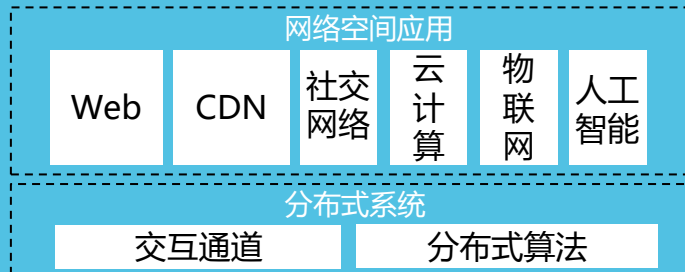
课程体系及教学安排



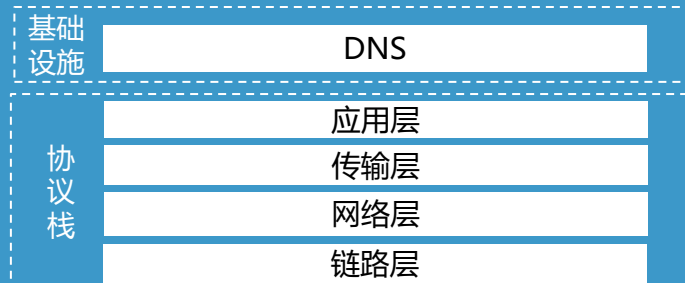
网络空间安全研究体系架构



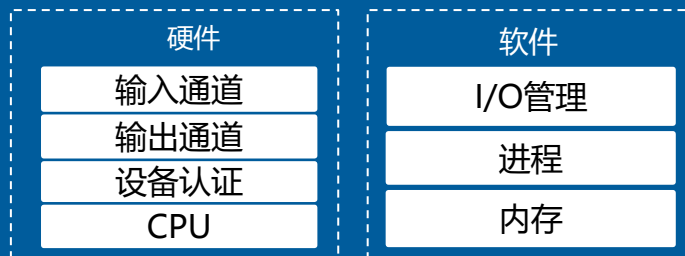
分布式系统与应用安全



网络安全



系统安全



算法

数据加密

隐私保护

机制

沙箱
入侵容忍

零信任网络

真实地址

理论

图论

控制论

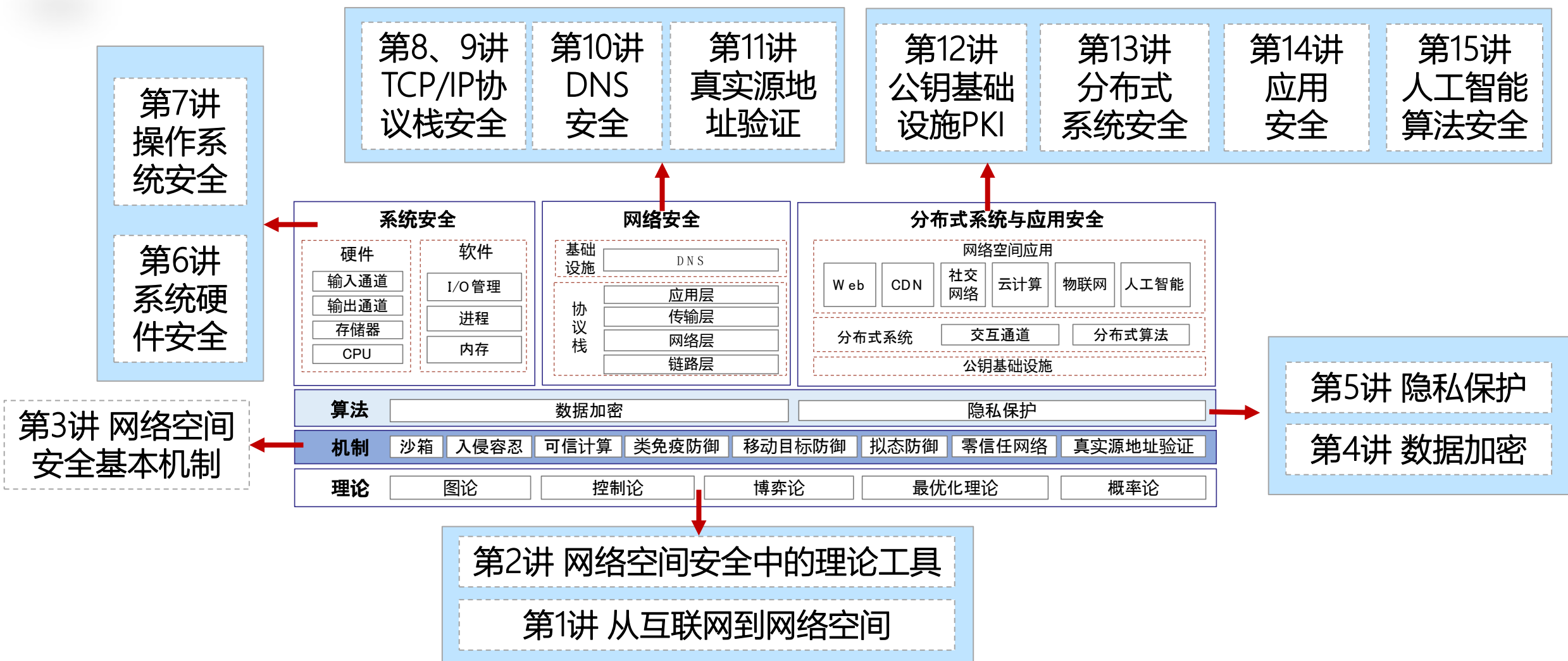
博弈论

最优化理论

概率论



课程安排





课程教材



在线题库

https://www.qingline.net/book-detail?book_id=478

内容简介

“没有网络安全就没有国家安全”。随着网络空间的迅速发展，网络空间安全成为信息技术领域关注的焦点。本书从“网络空间安全”学科体系出发，以网络空间的发展历程为起点，首先介绍网络空间安全领域涉及的基础理论、机制与算法；接着在此基础上围绕网络空间的系统安全、网络安全及应用安全展开，具体介绍数据加密、隐私保护、系统硬件安全、操作系统安全、协议安全、DNS安全、应用安全等网络空间安全领域的核心安全问题；最后介绍真实源地址验证、公钥基础设施PKI、分布式系统安全及人工智能安全等最新研究进展。

本书力图全面反映“网络空间安全”学科体系的概况，让读者能够理解“网络空间安全是整体性的，不可分割的”。网络安全具有很强的实践性，本书还注重通过典型的应用案例来讲解网络空间安全的基本机制和原理，并且精心设计了一系列实验，让读者通过实际动手操作进一步加深对网络空间安全的理解和掌握。

本书是清华大学本科核心课程“网络空间安全导论”的配套教材，面向计算机科学与技术 and 网络空间安全等相关专业的本科生，也可供广大相关专业的网络工程技术人员和科研人员参考。

课件下载·样书申请



书 图

清华大学出版社

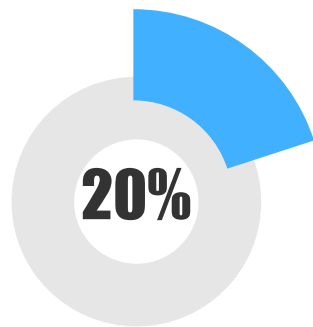


官 方 微 信 号

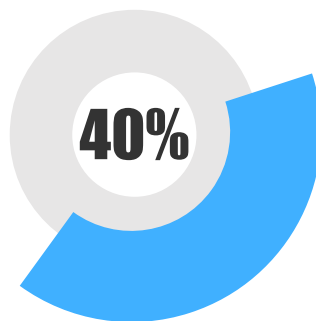




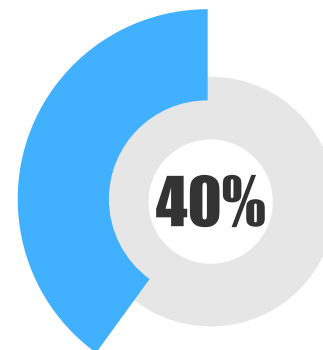
考核要求



作业



实验



期末考试 (开卷)

作业：实验：期末考试=1:2:2

两次作业：10分*2

三次实验：★5分，★★10分，★★★15分

(必须选择2个★★★ 实验，另外10分可选1个★★ 实验或者2个★实验)

期末考试：40分



Q and A