0839 网络空间安全一级学科研究生核心课程指南

01 复杂网络基础与应用

一、课程概述

本课程主要包括复杂网络的属性、模型及功能和行为的基本方法和理论，其中网络属性是指各种复杂网络的聚集系数、度分布等静态特征；网络模型包括规则网络、小世界网络、随机网络、无标度网络等实际应用中的各类网络拓扑结构；网络功能和行为包括挖掘复杂网络中的重要节点和社团、动力学建模、攻击策略和抗毁策略、可视化建模等动态特征行为。本课程是支撑网络空间安全一级学科的基础课程，为信息内容安全原理、社交网络分析、高级网络安全技术等课程提供基础理论和方法指导。

二、先修课程

大学计算机基础、数据结构。

三、课程目标

本课程旨在系统介绍复杂网络的基础知识和最新研究进展，使学生了解复杂网络在相关学科的应用，掌握复杂网络研究的一般性方法，具备针对特定复杂网络开展网络属性、网络结构、网络功能和行为研究的能力，为社交网络、交通网络、电力网络、物联网等领域的复杂网络技术研究、工程应用提供理论和技术准备。

四、适用对象

本课程适用于网络空间安全一级学科的博士研究生或硕士研究生。

五、授课方式

在教学活动上，本课程采用理论和实践相结合的方式，一方面注重对复杂网络本身的基本概念、基础理论和主要模型的全貌讲解和深入剖析，如随机图理论、小世界网络、无标度网络以及演化网络理论等；另一方面注重理论联系实际和对理论应用方法的介绍，以实际案例出发，以复杂网络理论为指导，分析和解决实际问题，如复杂网络中的数据挖掘问题、动力学问题、安全问题和可视化问题。

六、课程内容

第一章　复杂网络概述

1.1　复杂性科学概述

主要内容：复杂性科学的概念、发展阶段和主要特征。

1.2　图论简介

主要内容：图的概念、结构、应用。

1.3　复杂网络的概念和特性

主要内容：复杂网络的概念、特性、主要研究内容。

1.4　复杂网络的应用和挑战

主要内容：复杂网络的应用案例、挑战性问题、未来趋势。

■ 重点：复杂性科学的主要特征、复杂网络的概念和特性。

■ 难点：复杂网络的挑战性问题。

第二章　复杂网络结构属性和建模

2.1　网络的基本静态几何特征

主要内容：节点、边、网络规模、节点度数、网络直径、最短路径、聚集系数、介数等。

2.2　复杂网络的常见类型

主要内容：无向网络、有向网络、加权网络。

2.3　复杂网络结构建模

主要内容：规则网络、随机网络、小世界网络、无标度网络、层次网络、自相似网络。

2.4　复杂网络结构分析工具

主要内容：NetworkX、Ucinet。

■ 重点：聚集系数、度分布、小世界等网络静态特征；小世界网络和无标度网络模型的重构方法。

■ 难点：针对目标网络分析其结构属性特征；针对目标网络特点设计合适的复杂网络结构进化模型，并分析其结构属性。

第三章　复杂网络的数据挖掘

3.1　重要节点挖掘方法及评价指标

主要内容：影响节点重要性的特征因素及测度方法。

3.2　常见重要节点挖掘方法

主要内容：基于网络结构的重要节点挖掘、基于网络内容的重要节点挖掘、综合多因素的重要节点挖掘。

3.3　社团结构挖掘研究现状及评价指标

主要内容：社团结构稳定性的影响因素及评价测度。

3.4　常见社团挖掘方法

主要内容：非重叠社团发现算法、重叠社团发现算法。

■ 重点：重要节点挖掘方法、社团挖掘方法。

■ 难点：设计节点重要性测度和社团测度，在动态网络环境下设计快速的社团挖掘算法。

第四章　复杂网络动力学

4.1　复杂网络同步动力学

主要内容:复杂网络同步的概念、理论模型、应用。

4.2　复杂网络传输动力学

主要内容:复杂网络信息传输模型、路由策略、应用。

4.3　复杂网络传播动力学

主要内容:复杂网络传播模型、应用。

4.4　复杂网络级联动力学

主要内容:复杂网络中的级联失效模型、应用。

■ 重点:复杂网络同步动力学模型、复杂网络传输动力学模型、复杂网络传播动力学模型、复杂网络级联动力学模型。

■ 难点:结合实际复杂网络讲解动力学模型的理论,应用复杂网络动力学模型解决实际问题。

第五章　复杂网络安全问题

5.1　复杂网络结构脆弱性分析

主要内容:复杂网络脆弱性的概念和评估指标。

5.2　复杂网络的攻击策略

主要内容:随机攻击、蓄意攻击、树形攻击、近似最长路径攻击、最短路径攻击、邻居节点攻击。

5.3　复杂网络的抗毁性指标

主要内容:连通度、坚韧度、完整度、粘连度、离散度、膨胀系数。

5.4　复杂网络抗毁模型

主要内容:基于统计物理的复杂网络抗毁性、基于特征谱的复杂网络抗毁性。

■ 重点:复杂网络的攻击模型、复杂网络抗毁模型。

■ 难点:不同攻击策略下的复杂网络结构脆弱性分析;结合实际复杂网络部分可见的特点,设计鲁棒的网络抗毁方法。

第六章　复杂网络可视化

6.1　网络结构分析

主要内容:可视化聚类算法的原理和应用。

6.2　网络信息展示

主要内容:网络节点布局算法的原理、多尺度网络压缩算法、高密度网络的精确展示。

■ 重点:可视化聚类算法、网络节点布局算法、网络压缩算法。

■ 难点:利用可视化聚类算法发现高阶依赖关系,高维数据的快速网络压缩展示。

七、考核要求

考核成绩由课程实验成绩和课程研究论文成绩组成。

课程实验主要考查学生对复杂网络理论、方法及模型的理解程度和编程实践能力,要求学生能够复现已有复杂网络方法和模型的效果,并形成实验文档。

课程研究论文主要考查学生对复杂网络的理论、方法及模型的应用能力和创新研究能力,

要求学生能够针对具体复杂网络场景的特点和约束条件提出新方法，解决新问题，形成研究论文。

八、编写成员名单

卢凯（国防科技大学）、马行空（国防科技大学）、王清贤（中国人民解放军战略支援部队信息工程大学）、袁坚（清华大学）、童超（北京航空航天大学）、樊瑛（北京师范大学）。

02 现代密码学

一、课程概述

本课程以可证明安全等现代密码设计和分析理论视角讲授密码学相关知识，是在本科阶段密码学基础知识学习后对密码学的原理、方法和前沿方向的进一步学习。本课程对培养网络空间安全方向的硕士研究生和博士研究生在密码理论、网络安全、信息内容安全的领域研究提供重要支撑，为安全协议设计与分析、密码算法分析、密码应用与安全等课程提供基础理论。

二、先修课程

信息安全数学基础、概率论与数理统计、密码学基础、计算复杂性理论。

三、课程目标

通过本课程的学习，研究生应熟知现代密码设计与分析的基本原理，熟练掌握密码原语和体制的形式化描述、安全目标的图灵归约等分析方法，具备应用密码方法和技术解决数据、信息所面临的安全问题的能力。

四、适用对象

本课程适用于网络空间安全一级学科密码学及其应用方向的博士研究生和硕士研究生。

五、授课方式

现代密码学是一门内容较为广泛和深入的课程，同时又具备实际的应用背景，要求学生能够将抽象的概念和结论与其背景和发展历史结合起来理解，了解其在网络信息安全中的应用，并掌握密码学中丰富的实践思想。本课程采用讲授和研讨相结合的方式授课。

六、课程内容

第一章 现代密码学概论

1.1 密码学发展史

主要内容:密码学的起源、发展历史以及最新研究进展。

1.2 现代密码学的基本原则

主要内容:现代密码学的基本设置,密码体制设计与分析的基本原则,包括形式化定义、精确的数学假设、基于图灵规约的计算安全性证明。

1.3 可证明安全理论

主要内容:概率多项式时间 PPT,选择明文攻击 CPA、选择密文攻击 CCA 等攻击类型,可忽略概率、攻击成功概率,攻击游戏、语义安全、不可区分性等概念,随机预言模型与标准模型,完美加密体制的形式化定义和安全性证明。

- 重点:攻击游戏定义,随机预言模型。
- 难点:各种形式化定义中涉及的概率空间。

第二章 对称加密

2.1 对称加密算法

主要内容:计算安全的对称加密算法形式化定义。

2.2 伪随机生成器和序列密码

主要内容:伪随机生成器的基本定义和性质,伪随机置换的定义和构造,序列密码的实际构造及安全性规约证明。

2.3 CPA 安全的对称加密方案构造

主要内容:CPA 安全的对称加密算法,伪随机函数和分组加密,基于伪随机函数的安全对称加密算法构造方法和规约证明,以及 CBC、OFB 和 CTR 计算模型的安全规约分析和性质。

- 重点:伪随机函数,伪随机置换,CPA 安全的对称加密构造。
- 难点:CPA 安全的对称加密构造及安全性证明。

第三章 消息认证码

3.1 消息认证码

主要内容:针对消息认证码 MAC 的各类攻击和安全需求,计算安全的消息认证码的形式化定义。

3.2 消息认证码的构造

主要内容:消息认证码的构造及安全性证明,包括基于伪随机函数的安全 MAC 构造、固定长度安全 MAC 拓展到任意长度安全 MAC 的方法等。

3.3 认证加密

主要内容:计算安全的认证加密形式化定义、典型构造方法及其安全性证明。

- 重点:消息认证码的构造,认证加密的构造。
- 难点:各种构造方法的安全性证明。

第四章 杂凑函数

4.1 杂凑函数

主要内容:针对杂凑函数的各类攻击和安全需求,抗碰撞攻击计算安全的杂凑函数形式化定义。

4.2 杂凑函数的构造

主要内容:Merkle-Damgard 变换,MD5 类、SHA3 等典型杂凑函数的构造方法及安全性证

明,针对杂凑函数的攻击。

4.3 杂凑函数的应用

主要内容:基于杂凑函数的消息认证码构造及安全性证明,杂凑函数的应用。

- 重点:杂凑函数的构造方法。
- 难点:杂凑函数构造方法的安全性证明。

第五章 公钥密码

5.1 公钥加密的形式化定义

主要内容:计算安全的公钥加密形式化定义,公钥加密的语义安全、不可区分安全、不可延展安全等定义及不同安全定义之间相互归约。

5.2 公钥加密体制的构造

主要内容:经典公钥加密体制的构造及其安全性证明概要,ElGamal 公钥加密体制的 IND-CPA 安全性证明,Crame-Shoup 公钥加密体制的 CCA2 安全性证明,RSA-OAEP 的 CCA 安全性证明,基于格的公钥密码体制及可证安全性介绍。

- 重点:公钥加密体制的不同安全定义及相互规约,公钥加密体制的构造。
- 难点:公钥加密体制的构造方法和安全性证明。

第六章 数字签名

6.1 数字签名的形式化定义

主要内容:数字签名的形式化定义,数字签名的攻击类型及安全性定义。

6.2 数字签名体制的构造

主要内容:Hash-and-Sign 框架及其安全性,基于 RSA 的签名方案及其安全性证明,基于离散对数的签名方案 DSA 和 ECDSA 构造及其安全性证明,基于双线性对的签名方案及其安全性证明,签名与加密的组合,签密概要。

- 重点:数字签名体制的构造。
- 难点:数字签名体制的构造方法和安全性证明。

七、考核要求

1. 硕士研究生考核要求:

考核成绩由期末考试成绩和研究论文成绩组成。

期末考试采用闭卷考试方式,主要考查学生对现代密码学中对称加密、杂凑函数、消息认证码、公钥加密及签名体制等基本原理和方法的掌握。

研究论文主要考查学生对现代密码学中研究内容的掌握程度和总结能力,要求能够写出综述性论文;或者要求学生能够针对具体密码算法设计提出新方法,解决新问题,形成研究论文。

2. 博士研究生考核要求:

考核成绩由研究论文确定。要求学生能够针对具体密码算法设计提出新方法并进行安全性证明,形成研究论文。

八、编写成员名单

祝跃飞(中国人民解放军战略支援部队信息工程大学)、王小云(清华大学)、王明生(中国

科学院信息工程研究所)、吴铤(杭州电子科技大学)、陈晓峰(西安电子科技大学)、魏福山(中国人民解放军战略支援部队信息工程大学)。

03 安全协议设计与分析

一、课程概述

安全协议是建立在密码体制基础上的一种交互式通信协议,它运用密码算法和协议逻辑来实现认证和密钥协商以及加密通信等目标。本课程主要讲授安全协议设计、形式化分析和安全性归约证明等理论和方法以及安全协议的应用,使学生能较全面地理解和掌握安全协议设计和分析的一般原理、核心思想和关键技术,培养学生在网络安全方面的研究能力。

二、先修课程

现代密码学、算法设计与分析、计算复杂性理论、计算机网络。

三、课程目标

通过本课程的学习,研究生应能很好地理解安全协议设计和分析中的基本概念、原理、模型、方法和技巧,初步具备安全协议的设计和分析能力,从而掌握网络信息安全的基本分析技术和方法,同时熟练掌握常用网络安全协议以及各个应用实现版本的安全缺陷,从而能够较好解决与网络安全协议相关的技术难题和实际问题。

四、适用对象

本课程适用于网络空间安全一级学科密码学及应用方向的博士研究生和硕士研究生。

五、授课方式

安全协议的研究成果涉及面广、难度大、内容丰富,可根据具体需要来选择重点核心内容对学生进行理论知识讲授和实践能力培养,本课程采用理论和实践相结合的方式授课。

六、课程内容

第一章 安全协议形式化分析

1.1 安全协议设计

主要内容:安全协议的基本概念和分类,安全协议面临的威胁,安全协议的常见攻击方法,攻击者能力及刻画,攻击者成功概率,安全协议的模型与分析方法,安全协议的目标与研究层次,安全协议的设计原则。

1.2 安全协议形式化分析

主要内容:安全协议符号化分析方法,基于复杂性理论形式化分析方法,基于实现代码形式化分析方法,安全协议的通用工具和专用工具验证方法。

■ 重点:密码协议的设计原则,安全协议的各种形式化分析方法,安全协议可证安全的思想和基本方法。

■ 难点:安全协议各种形式化分析的原理和方法。

第二章　认证密钥交换协议

2.1　密钥交换协议的安全模型

主要内容:认证密钥交换协议的形式化定义及安全目标,Canetti-Krawczyk 模型、扩展 Canetti-Krawczyk 模型以及 Bellare-Pointcheval-Rogaway 模型等典型基于公钥或口令的认证密钥交换协议的安全模型建立。

2.2　密钥交换协议的设计与安全性证明

主要内容:基于公钥的密钥交换协议的设计与安全性证明,基于口令的认证密钥交换协议的设计和安全性证明。

■ 重点:认证密钥交换协议的安全模型,认证密钥交换协议的设计方法。

■ 难点:认证密钥交换协议的安全证明。

第三章　高级协议

3.1　比特承诺协议

主要内容:比特承诺协议概述,比特承诺协议的定义和性质,比特承诺的安全模型,基于对称密码算法、单向函数及伪随机序列发生器的比特承诺的典型方案设计及其安全证明。

3.2　零知识证明协议

主要内容:零知识证明协议的定义和安全模型,交互式零知识证明的基础理论和设计方法,非交互式零知识证明的基础理论和设计方法。

3.3　秘密共享协议

主要内容:秘密共享协议的定义,秘密共享协议的安全模型,Shamir、Feldman 及 Peterson 等经典秘密共享协议的设计方法及其安全性证明。

3.4　不经意传输协议

主要内容:不经意传输协议的定义和性质,不经意传输协议的安全模型,典型不经意传输协议的设计方法和安全性证明。

3.5　安全多方计算

主要内容:安全两方/多方计算的定义,两方/多方计算中的半诚实服务器模型和恶意服务器模型,安全两方计算的基本定理、构造方法和经典协议。

■ 重点:比特承诺协议、零知识证明协议、秘密共享协议、不经意传输协议、安全多方计算协议及各协议的形式化定义、安全模型定义、设计思想和典型实现方案。

■ 难点:零知识证明协议的形式定义和方案证明,安全多方计算协议的形式定义和相关存在性结论的证明思想。

第四章　网络安全协议

4.1　链路层安全协议

主要内容:链路层安全认证协议 PAP、CHAP 以及 L2TP 协议的原理和实现。

4.2 IP 层安全协议

主要内容:IPsec 协议概述,ISAKMP 协议,IKEv1、IKEv2 协议,IPsec 协议应用与实现。

4.3 传输层安全协议

主要内容:SSL 协议概述,SSLv2、SSLv3、TLS 协议,SSL 和 TLS 协议应用与实现。

4.4 会话层安全协议

主要内容:SSH 协议概述,SSH 传输协议、SSH 身份认证协议、SSH 连接协议,SSH 协议应用与实现。

4.5 移动与无线通信协议

主要内容:2G/3G/4G 认证协议,Wi-Fi 认证协议等。

■ 重点:各主要网络安全协议的安全目标、设计思想、协议体系、协议流程、报文规范和典型实现,各版本的应用方法和缺陷。

■ 难点:网络安全协议的设计与分析原理及配置实现。

七、考核要求

考核成绩由研究论文成绩和课程实验成绩组成。

研究论文主要考查学生对安全协议设计与分析原理和方法的理解和应用能力,要求学生针对具体复杂网络场景设计安全协议并给出安全性分析或证明,形成研究论文。

课程实验主要考查学生对 L2TP、PAP、CHAP、IPsec、SSL、SSH 等网络安全协议的理解和实践应用能力,要求学生能够对网络安全协议的常用实现进行有效配置,并形成实验文档。

八、编写成员名单

祝跃飞(中国人民解放军战略支援部队信息工程大学)、程光(东南大学)、陈晓峰(西安电子科技大学)、顾纯祥(中国人民解放军战略支援部队信息工程大学)。

04 密码算法分析

一、课程概述

密码学包括对立统一的密码编码学和密码分析学,密码算法分析是密码分析学的核心内容。本课程主要学习密码学中主要类型密码算法的基本分析原理、基本分析方法和密码分析计算复杂度的估计等。通过本课程学习,学生能理解密码分析思想,掌握基本的分析原理和经典分析方法,具备运用相关理论进行密码算法分析的能力和密码分析的思维。本课程的学习同时培养学生的密码算法设计能力,为培养具有较强的密码算法设计与分析能力的高层次人才打下基础。

二、先修课程

信息安全数学基础、概率论与数理统计、计算复杂性理论、现代密码学。

三、课程目标

通过本课程的学习，研究生应深入理解密码算法分析的思想，重点掌握序列密码、分组密码、杂凑函数和公钥密码等主流密码算法攻击的原理、理论和方法，具备从事挖掘密码算法非随机性质、设计密码分析模型、编程实验验证分析效果、评估密码分析复杂度等与密码算法分析相关工作的能力。

四、适用对象

本课程适用于网络空间安全一级学科密码学及其应用方向的博士研究生和硕士研究生。

五、授课方式

本课程的授课方式以讲授为主，重视交互式、研讨式和研究式教学方法的运用，突出密码分析创新能力的培养，将一些分析方法编程实现作为辅助教学内容。本课程涉及内容较深，一些需要较深的代数和数论基础的内容难度较大，可以选择性讲授。

六、课程内容

第一章　计算代数和数论基础

主要内容：

代数数域：代数整数、Dedekind 整环、order、类群和类数等数学对象的概念、性质和计算方法。

椭圆曲线：椭圆曲线群结构、除子类群、同种映射、Tate 模和 Weil 对、有限域上椭圆曲线的算术等数学对象的概念、性质和相关计算方法。

格：格和格基，格中求解困难的问题，LLL 算法。

- 重点：代数整数环的构造和性质，有限域上椭圆曲线的性质和算术，LLL 算法。
- 难点：类群结构，Weil 对的构造和性质，有限域上椭圆曲线的群结构，格基约化方法。

第二章　密码算法分析基础

主要内容：密码算法分析基础方法和变换的原理与复杂度分析，方法和变换包括穷举攻击、时空折中攻击、生日攻击、中间相遇攻击、Fourier 变换、Hadamard-Walsh 变换。

- 重点：基础分析方法的思想和原理。
- 难点：Hadamard-Walsh 变换的数学原理。

第三章　序列密码算法分析

主要内容：序列密码算法的主要分析方法，包括最佳仿射逼近攻击、相关攻击、猜测确定攻击、代数攻击、立方攻击等，并以对 Grain、Trivium 等典型序列密码算法的攻击作为示例进行讲授。

- 重点：各攻击方法的适用对象、原理、方法、成功概率和复杂度分析。

■ 难点:统计量的分布,关于密钥的代数方程组的构建与求解。

第四章　分组密码算法分析

主要内容:分组密码算法的主要分析方法,包括差分攻击、线性攻击、高阶差分攻击、截断差分攻击、积分攻击、不可能差分攻击、零相关线性攻击、中间相遇攻击、插值攻击、相关密钥攻击等,并以对 AES、SIMON 等典型分组密码算法的攻击作为示例进行讲授。

■ 重点:各攻击方法特别是差分攻击和线性攻击的原理。

■ 难点:中间相遇攻击、积分攻击。

第五章　杂凑算法分析

主要内容:杂凑算法的主要分析方法,包括长度扩展攻击、代数攻击、固定点攻击、模差分攻击、比特追踪技术、多碰撞攻击、长消息第二原像攻击、集群攻击、中间相遇原像攻击、反弹攻击等,以对 MD4-族、SHA-3 等典型杂凑算法的攻击为示例进行讲授。

■ 重点:各分析方法的原理。

■ 难点:模差分攻击、中间相遇原像攻击。

第六章　公钥密码算法分析

主要内容:

大数分解算法:$p-1$ 算法、Pollard-ρ 算法、$p+1$ 算法、椭圆曲线因子分解算法、二次筛法、数域筛法和特殊数域筛法。

有限域上离散对数求解算法:Pollard-ρ 算法、Shank 算法(小步-大步法)、指标算法、P-H 算法。

椭圆曲线上的离散对数求解算法:椭圆曲线公钥密码,MOV 约化、FR 约化、SSSA 约化等算法。

LLL 算法在密码分析中的应用:背包问题求解、针对 RSA 算法的小解密指数攻击等。

■ 重点:各求解方法的数学原理、能力分析和应用条件。

■ 难点:椭圆曲线因子分解、因子分解数域筛法、基于格的密码分析方法。

七、考核要求

对硕士研究生的考核建议采用课程作业形式,重点考查学生对基本的密码算法分析原理、理论、方法的掌握情况;对博士研究生的考核建议采用研究论文形式,重点考查学生对某一分析方法的综合理解与评估能力。

八、编写成员名单

祝跃飞(中国人民解放军战略支援部队信息工程大学)、王小云(清华大学)、谷大武(上海交通大学)、李超(国防科技大学)、王鹏(中国科学院信息工程研究所)、段明(中国人民解放军战略支援部队信息工程大学)。

05 密码应用与安全

一、课程概述

密码技术是网络空间安全的核心支撑技术。面向应用的安全需求和具体环境，保护网络信息安全需要综合运用各种密码技术设计并实现安全的密码系统。本课程围绕密码应用系统的设计、实现和安全性分析这一主题，内容包括体系、原理、技术和实现等方面的相关知识，并以典型密码系统为例进行解析。通过课程学习，学生能够理解、掌握密码系统设计和安全性分析的思想方法，具备密码系统设计和分析的综合素养和能力。

二、先修课程

现代密码学、网络安全协议、计算机网络、信息系统。

三、课程目标

通过本课程的学习，学生应理解密码系统设计和分析的体系化问题，掌握各种密钥管理的原理、方法和技术，熟悉密码工程实现的主要软硬件方法及其安全问题，掌握侧信道攻击的基本思想、方法、技术和防御的基本手段，理解和掌握 VPN 和区块链中密码系统的要素、体系、功能和安全保障；学生应具备密码系统设计和安全性分析的系统化思维方式以及工程化实现和测试的能力，为开展密码系统设计和分析方向课题研究和成为密码系统设计和分析专门研究人才打下坚实基础。

四、适用对象

本课程适用于网络空间安全一级学科密码学及应用方向的博士研究生和硕士研究生。

五、授课方式

由于课程内容丰富、涉及面广，建议采用专题研讨式教学，在学生充分研读相关材料的基础上，教师基于合理预定的内容体系组织研讨，重点是解析逻辑、解析难点、纠正理解偏差和指导深入理解并掌握知识点。

六、课程内容

第一章 密码应用与安全概要

主要内容：面向应用的密码系统的适应性、安全性和有效性要求，突出适应应用环境的密码系统的快速实现和安全性评估主线，解析课程思维、内容体系和体系逻辑。

- 重点：综合密码系统的安全性和有效性需求体系。
- 难点：密码系统安全性综合评估的体系和思维。

第二章　密钥管理方案

主要内容:密钥类型、密钥体系和典型密钥系统,伪随机生成器技术与标准,公钥基础设施(PKI)体系、技术与标准,基于身份公钥密码体系的原理、技术与标准,白盒密码设计的思想、方法和技术。

- 重点:各类密钥管理模式的基本思想、方法、优缺点分析和适用条件。
- 难点:PKI 体系,密钥混淆。

第三章　密码软件工程

主要内容:密码软件工程问题概要;密码软件工程编程基础,包括主流操作系统密码服务(如 Windows 系统 Crypto-API 和 CSP 机制),主流编程语言或平台(MFC、.NET、Java、Python 等)密码编程概要,密码中间件概要,XML 密码机制);密码算法的快速软件实现,密码软件安全问题分析和防范。

- 重点:密码软件工程基本机制。
- 难点:密码软件工程中的安全性分析。

第四章　密码硬件工程

主要内容:专用芯片、FPGA 等硬件平台密码算法快速、安全实现的基本问题和对策,TPM 安全芯片设计、实现和应用。

- 重点:各类密码算法特点对硬件实现的需求和技巧。
- 难点:密码硬件工程中的安全性分析。

第五章　侧信道分析

5.1　侧信道分析概要

主要内容:信息泄露产生的基本机理,侧信道分析的基本概念,经典侧信道分析方法及技术原理,密码实现信息泄露和侧信道攻击的基本概念,计时攻击、能量分析攻击以及电磁分析攻击等技术原理。

5.2　能量分析攻击

主要内容:差分能量分析、相关能量分析、简单能量分析等典型攻击方法,特征点、预处理等基本概念与关键技术等。

5.3　高级侧信道分析

主要内容:模板攻击、高阶侧信道攻击以及多源融合攻击等方法和技术。

5.4　侧信道攻击防御

主要内容:掩码防护、随机延迟、乱序执行等主要防御技术的原理和基本方法,信息泄露评估的基本理念和体系。

- 重点:信息泄露泛在形式与内在机理,信息泄露特征刻画与有效利用,信息泄露防御方法与检测评估。
- 难点:泛在信息泄露的基本特征与信息泄露利用的微妙性,信息泄露的可靠防御方法与有效性评估技术。

第六章　典型密码应用系统

主要内容:虚拟专用网(VPN)、区块链、可信计算等系统或平台中的密码技术综合应用解析;围绕满足安全需求和适应应用环境,结合适当的标准或产品,解析密码技术的综合应用和实

现机制及其中的安全因素。

- 重点：虚拟专用网中密码技术系统应用的原理与模式。
- 难点：虚拟专用网的安全体系需求和密码系统的功能对应性，密码技术综合应用的基本模式。

第七章　密码系统安全性分析

主要内容：针对密码系统攻击的基本思路和可能方法，密码系统安全性综合分析的背景、思维、主要内容和系统思路，密码系统综合安全性的主要因素和主要实现思路。

- 重点：安全性综合分析的基本思路和模式。
- 难点：安全性综合分析的理论框架。

七、考核要求

本课程建议采用“通专结合”的方式考核，“通”考核学生对课程内容体系和各方面基本知识的掌握情况，可采用闭卷考试或课程作业方式实施考核；“专”考核学生在课程整体思想和体系指导下对课程内容某一专题深入学习研究的成果，以研究论文方式实施考核。

八、编写成员名单

祝跃飞（中国人民解放军战略支援部队信息工程大学）、赵波（武汉大学）、周永彬（中国科学院信息工程研究所）、程光（东南大学）、丁勇（桂林电子科技大学）、王磊（中国人民解放军战略支援部队信息工程大学）。

06　计算系统安全

一、课程概述

计算系统安全是关于设计和实现安全计算系统、分析计算系统安全性的专业核心课程。课程涵盖了与计算系统安全相关的主流技术，包括硬件辅助的计算系统安全机制、虚拟化及其安全、操作系统安全、计算系统软件保护与逆向工程、计算系统中的信息与故障隔离技术、编译器辅助的计算系统安全、计算系统安全监控技术、移动智能终端系统安全和 IoT 设备安全。通过课程学习，学生能够理解、掌握设计实现安全计算系统、计算系统安全性分析的思想方法，具备计算系统设计和分析的科研能力。

二、先修课程

操作系统原理、密码学原理、程序设计基础。

三、课程目标

本课程的教学目标是使研究生全面地学习计算系统安全领域的基础理论和最新实用技术，

系统地掌握设计和开发安全计算系统、分析计算系统安全性的基本方法和高级技术,并且能够自己动手解决与计算系统安全相关的技术难题和实际问题。本课程将提升研究生在计算系统安全领域的科研能力、创新能力和实践能力,为其将来从事与计算系统安全相关的科学研究和开发工作打下坚实的基础。

四、适用对象

本课程适用于网络空间安全一级学科系统安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用理论讲授和实践相结合的方式授课。

六、课程内容

第一章　概述

1.1　计算系统安全的定义及内涵

1.2　计算系统安全的发展历史

1.3　计算系统面临的安全挑战和主要攻击类型

1.4　计算系统安全设计

1.5　计算系统安全主流技术

1.6　计算系统安全标准

■ 重点:主要攻击类型的基本原理、计算系统安全主流技术的比较。

■ 难点:典型系统攻击和防御的工程化方法。

第二章　硬件辅助的计算系统安全机制

2.1　TPM/TCM 与可信计算

2.2　安全协处理器与加密芯片

2.3　Intel SGX 技术

2.4　AMD 内存加密技术

2.5　ARM TrustZone 技术

■ 重点:可信根与可信计算的内涵、Intel SGX、AMD 内存加密技术和 ARM TrustZone 技术的基本原理。

■ 难点:可信计算体系架构的构建、Intel SGX 与 AMD 内存加密技术的比较。

第三章　虚拟化及其安全

3.1　主机虚拟化技术介绍

3.2　主机虚拟化的主要安全威胁

3.3　虚拟化安全防御架构

3.4　Hypervisor 自身安全

3.5　虚拟机隔离机制

■ 重点:硬件与软件虚拟化技术的基本原理、Hypervisor 自身安全保护方法、虚拟机隔离中的指令改写与转换。

■ 难点：基于代码转化和硬件安全特性的虚拟机隔离。

第四章　操作系统安全

4.1　安全操作系统的国内外研究现状

4.2　访问控制机制

4.3　可追究机制

4.4　连续保护机制

4.5　安全模型

4.6　安全操作系统设计

■ 重点：操作系统访问控制机制的基本原理和关键技术、强制访问控制技术、命名空间及容器技术、操作系统连续保护机制的基本原理和关键技术。

■ 难点：操作系统访问控制机制的安全性分析、容器隔离技术的安全性分析、操作系统连续保护机制的安全性分析。

第五章　计算系统软件保护与逆向工程

5.1　计算系统软件保护技术介绍

5.2　代码混淆

5.3　软件防窜改

5.4　二进制代码分析与逆向工程技术

■ 重点：代码混淆与软件防窜改关键技术原理、逆向工程分析工具。

■ 难点：代码混淆与软件防窜改主流技术方法分析、逆向工程技术所面临的技术难题。

第六章　计算系统中的信息与故障隔离技术

6.1　计算节点间隔离

6.2　数据存储隔离

6.3　应用系统之间数据流转的管控

6.4　计算系统物理边界和逻辑边界隔离

6.5　计算系统中的软件故障隔离

■ 重点：基于任务的计算节点信息按需隔离、面向租户的卷/文件细粒度数据隔离、隔离能力动态描述、软件故障隔离中的指令改写与转换方法。

■ 难点：原子任务抽取与组合抽象描述、逻辑边界安全性形式化验证、基于代码转化和硬件安全特性的软件故障隔离。

第七章　编译器辅助的计算系统安全

7.1　编译器在计算系统安全中的作用

7.2　GCC 和 LLVM 编译器

7.3　基于编译器的代码插桩与指令转换

7.4　典型的编译器辅助安全技术方案

■ 重点：使用编译器实现主流的计算系统安全机制。

■ 难点：编译器修改。

第八章　计算系统安全监控技术

8.1　系统安全监控类型与简介

8.2 基于硬件或系统管理模式的系统安全监控
8.3 基于 Hypervisor 的虚拟机自省技术
8.4 基于系统调用的安全监控
8.5 主机防病毒软件与系统内安全监控

- 重点:各种系统安全监控技术的基本原理与优缺点比较。
- 难点:带外监控的语义间隙问题。

第九章 移动智能终端系统安全

9.1 移动智能终端系统面临的安全威胁
9.2 恶意移动应用检测与防御
9.3 移动用户数据隐私保护
9.4 移动智能终端安全与隐私风险评估
9.5 Android 系统安全特性和应用安全模型

- 重点:恶意移动应用检测主流技术的基本原理和比较、移动用户数据隐私保护主流技术的比较。
- 难点:Android 系统中 Hook 机制的实施。

第十章 IoT 设备安全

10.1 RFID 标签攻击和防御
10.2 RFID 标签指纹
10.3 SIM 卡安全
10.4 无人机、智能汽车和智能摄像头安全
10.5 其他 IoT 设备安全

- 重点:各种 IoT 设备面临的安全问题分析。
- 难点:RFID 标签攻击和防御的实施、物信跨域攻击和防御。

七、考核要求

考核成绩由期末考试成绩和课程作业成绩组成。

期末考试采用闭卷考试形式,主要考查学生对计算系统安全相关基础知识和高级技术的掌握程度。

课程作业由学生任选一个课程作业题目,实现该题目所要求的功能并提交报告,主要考查学生的计算系统安全设计、实现与分析能力,运用所学知识分析解决具体问题的能力。

八、编写成员名单

马建峰(西安电子科技大学)、李金库(西安电子科技大学)、李凤华(中国科学院信息工程研究所)、周亚金(浙江大学)、张超(清华大学)、姚青松(西安电子科技大学)、罗林波(西安电子科技大学)、杨力(西安电子科技大学)。

07 软件安全

一、课程概述

软件安全是关于设计和实现安全软件、分析软件安全性的专业核心课程，涵盖了与软件安全相关的主流技术，包括主流的软件漏洞类型及典型攻击方法、软件漏洞挖掘与利用、代码安全与代码完整性保护、控制流完整性保护、数据流与数据完整性保护、软件随机化保护技术、污点分析技术以及软件安全形式化证明等。通过本课程的学习，学生应具备软件安全设计和安全分析的综合素养和能力。

二、先修课程

操作系统原理、程序设计基础、汇编语言、编译原理。

三、课程目标

本课程的教学目标是使研究生全面地学习软件安全领域的基础理论和实用技术，系统地掌握设计和开发安全软件、分析软件安全性的基本方法和高级技术，并且能够自己动手解决与软件安全相关的技术难题和实际问题。本课程将提升研究生在软件安全领域的科研能力、创新能力和实践能力，为他们将来从事与软件安全相关的科学研究和开发工作打下坚实的基础。

四、适用对象

本课程适用于网络空间安全一级学科系统安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用理论讲授和实践相结合的方式授课。

六、课程内容

第一章 软件安全概述

1.1 软件安全的定义及内涵

1.2 软件面临的安全挑战

1.3 软件安全技术的发展历程

1.4 软件安全学科的主要内容

1.5 确保软件安全的工程化方法

■ 重点：围绕软件安全对抗的博弈演进；软件安全与系统安全、网络安全的关系；软件安全主流技术。

■ 难点：软件的安全开发生命周期与内构安全。

第二章　主流的软件漏洞类型及典型攻击方法

2.1　空间错误类内存漏洞及攻击方法

主要内容:堆/栈缓冲区溢出攻击、格式化字符串攻击等。

2.2　时间错误类内存漏洞及攻击方法

主要内容:double-free 攻击、use-after-free 攻击等。

2.3　条件竞争漏洞及攻击方法

主要内容:TOCTOU 攻击、double-fetch 攻击等。

2.4　代码注入型攻击

2.5　代码重用型攻击

主要内容:return-to-libc、ROP、JOP 攻击。

2.6　控制流劫持攻击

2.7　数据流劫持攻击

2.8　内存泄露攻击

- 重点:主流软件漏洞类型的攻击模型。
- 难点:代码重用型攻击的构造。

第三章　软件漏洞挖掘与利用

3.1　软件漏洞挖掘面临的挑战

3.2　传统的静态、动态分析方法

3.3　主流的动静结合漏洞挖掘方法

3.4　软件漏洞利用技术

3.5　软件漏洞挖掘与利用前沿技术

- 重点:程序逆向分析方法、Fuzzing 技术、符号执行技术、从软件漏洞 PoC 构造漏洞利用样本。
- 难点:自动化、智能化的漏洞挖掘与利用新技术。

第四章　代码安全与代码完整性保护

4.1　代码安全面临的挑战

4.2　代码的安全编程

4.3　代码完整性保护

4.4　数据执行保护

- 重点:代码安全编程需要遵循的原则、代码完整性保护的主流方法及其架构。
- 难点:代码完整性保护的实施及其安全性分析、动态生成代码的完整性保护。

第五章　控制流完整性保护

5.1　控制流完整性保护的定义

5.2　控制流完整性保护面临的挑战

5.3　函数指针与返回地址保护

5.4　控制流图获取与指令转换

5.5　主流的控制流完整性保护方案

- 重点:间接函数调用目标函数(或地址)分析、间接函数调用指令和返回指令的转换、控制流完整性保护的主流方法及其架构。

■ 难点：基于中间代码的指针分析、细粒度控制流图获取技术、控制流完整性绕过技术。

第六章　数据流与数据完整性保护

6.1　数据流与数据完整性保护的定义与区别

6.2　数据流与数据完整性保护面临的挑战

6.3　数据流图获取与指令转换

6.4　主流的数据流与数据完整性保护方案

■ 重点：数据与指令的映射关系分析、数据流与数据完整性保护中关键指令的转换。

■ 难点：数据流与数据完整性保护技术的安全性分析和性能优化。

第七章　软件随机化保护技术

7.1　软件随机化保护技术的定义

7.2　软件随机化保护技术面临的挑战

7.3　软件中的代码/指令随机化

7.4　软件中的地址/布局随机化

7.5　软件中的数据随机化

7.6　主流的软件随机化保护技术方案

■ 重点：软件代码、数据及布局随机化保护技术的基本原理。

■ 难点：软件代码、数据及布局随机化保护技术的设计和实施。

第八章　污点分析技术

8.1　污点分析技术的定义与类型

8.2　静态污点分析技术

8.3　动态污点分析技术

8.4　典型的污点分析系统（Libdft、TaintDroid、FlowDroid 等）

■ 重点：静态和动态污点分析技术的对比、污点传播规则定义。

■ 难点：典型污点分析系统的设计和实施、过污染及欠污染分析、污点传播规则自动化推演。

第九章　软件安全形式化证明

9.1　软件安全形式化证明技术介绍

9.2　软件安全形式化证明面临的挑战

9.3　软件安全形式化证明的主流技术与典型系统

■ 重点：软件安全形式化证明的模型构建。

■ 难点：软件安全形式化证明典型系统的推演过程。

七、考核要求

考核成绩由期末考试成绩和课程作业成绩组成。

期末考试采用书面闭卷考试形式，主要考查学生对软件安全相关基础知识和高级技术的掌握程度。

课程作业由学生任选一个课程作业题目，实现该题目所要求的功能并提交报告，主要考查学生的软件安全设计、实现、分析能力，以及运用所学知识分析并解决具体问题的能力。

八、编写成员名单

马建峰(西安电子科技大学)、李金库(西安电子科技大学)、邹维(中国科学院信息工程研究所)、周亚金(浙江大学)、张超(清华大学)、姚青松(西安电子科技大学)、罗林波(西安电子科技大学)、杨力(西安电子科技大学)。

08 网络安全

一、课程概述

本课程以 APPDRR 模型为主线,主要介绍网络安全的基本概念、模型、机制以及关键技术,包括:网络风险评估(Assessment)、安全策略(Policy)、系统防护(Protection)、动态检测(Detection)、实时响应(Response)、灾难恢复(Recovery)。课程将理论与实践相结合,使研究生能够系统地掌握网络安全领域的关键技术,提升其科研能力、创新能力和工程实践能力,为其今后从事网络安全技术研究工作奠定坚实的基础。

二、先修课程

计算机网络、密码学、安全协议、密码应用与安全。

三、课程目标

本课程以 APPDRR 模型为主线,旨在系统地介绍网络安全的基本概念、模型、机制以及最新研究进展,使学生掌握网络安全的主要分析方法和核心技术,为学生从事网络安全的技术研究与工程实践提供理论和技术支撑。

四、适用对象

本课程适用于网络空间安全一级学科网络安全方向的博士研究生和硕士研究生。

五、授课方式

本课程内容丰富,涉及面较广,难度较大。课程的讲授应与课程实践环节相结合,选择若干专题安排课程实践。

六、课程内容

第一章 网络风险评估

1.1 网络脆弱性与安全威胁

1.2 网络攻击分类及其基本原理

1.3 网络安全体系结构与 APPDRR 模型

1.4 网络安全态势感知与评估

1.5 网络安全等级保护测评

■ 重点：网络安全体系结构与 APPDRR 模型。

■ 难点：网络攻击分类及其基本原理。

第二章 安全策略

2.1 安全策略的定义及内涵

2.2 基于身份的安全策略

2.3 基于规则的安全策略

2.4 基于角色的安全策略

2.5 基于属性的安全策略

2.6 多级安全策略

■ 重点：基于角色的安全策略、基于属性的安全策略。

■ 难点：多级安全策略。

第三章 系统防护

3.1 数据加密

3.2 访问控制

3.3 身份认证与 PKI/CA

3.4 恶意代码防护

3.5 主动防御与协同防护

3.6 隔离技术

3.7 防火墙与虚拟专用网

■ 重点：身份认证与 PKI/CA、主动防御与协同防护、防火墙与虚拟专用网。

■ 难点：主动防御与协同防护。

第四章 动态检测

4.1 入侵检测与入侵防御

4.2 深度包检测技术

4.3 密罐技术

4.4 模拟执行与沙箱技术

4.5 日志审计

4.6 漏洞扫描与渗透测试

4.7 高级持续性威胁(APT)检测

■ 重点：入侵检测与入侵防御、深度包检测技术、密罐技术、日志审计、漏洞扫描与渗透测试。

■ 难点：高级持续性威胁(APT)检测。

第五章 实时响应

5.1 应急响应策略与机制

5.2 事件关联分析

5.3 攻击链分析

5.4 安全状态评估
5.5 DDoS 流量过滤与阻断
5.6 网络攻击溯源与取证
5.7 反向扫描与渗透

- 重点:事件关联分析、攻击链分析、安全状态评估、网络攻击溯源与取证。
- 难点:网络攻击溯源与取证。

第六章 灾难恢复

6.1 灾难恢复能力等级及相关指标
6.2 灾难恢复计划
6.3 数据恢复
6.4 网络恢复
6.5 系统恢复
6.6 应用恢复

七、考核要求

考核成绩由期末考试成绩和实验成绩组成。

期末考试采用闭卷考试方式,主要考查学生对网络安全相关基础知识和关键技术的掌握程度。

实验由学生任选一个实验题目,实现该题目所要求的功能并提交实验报告,主要考查学生在网络安全领域的设计与实现能力,以及运用所学知识分析并解决具体问题的能力。

八、编写成员名单

李舟军(北京航空航天大学)、方滨兴(北京邮电大学)、祝跃飞(中国人民解放军战略支援部队信息工程大学)、李凤华(中国科学院信息工程研究所)、卢凯(国防科技大学)、张宏莉(哈尔滨工业大学)、段海新(清华大学)、王东滨(北京邮电大学)。

09 高级网络安全技术

一、课程概述

本课程在网络安全基础课程学习的基础上,进一步学习互联网体系结构的安全、网络基础设施的安全、安全通信协议以及前沿的安全技术。本课程将带领研究生探讨网络安全体系结构、互联网基础设施和协议设计中的安全漏洞、攻击和防御中的安全问题、攻击方法和防范措施,通过学习攻击、检测和防御的演进培养学生网络安全研究的对抗思维。

二、先修课程

计算机网络、密码学原理、网络安全基础课程。

三、课程目标

本课程旨在促进网络安全方向的研究生掌握网络安全方向的研究问题、研究方法和当前研究的现状和挑战，掌握网络安全的主要分析方法和核心技术，培养学生安全对抗方面的思维方式和技术能力。

四、适用对象

本课程适用于网络空间安全一级学科网络安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用讲授和研讨相结合的方式授课。

六、课程内容

第一章　课程概要

1.1　课程的主要内容和基本要求

1.2　课程必需的基本知识概要

第二章　互联网安全体系结构

2.1　互联网协议的层次结构、安全服务和安全机制

2.2　互联网编址、路由和域名系统中的安全威胁

2.3　网络安全风险分析模型

- 重点：安全服务和安全机制在互联网各层协议中的分配。
- 难点：理解端到端的安全设计、安全风险分析的思想。

第三章　路由系统安全

3.1　BGP 协议与域间路由策略模型

3.2　BGP 路由测量与分析

3.3　路由安全风险

3.4　路由安全机制 RPKI

- 重点：BGP 协议、针对 BGP 的攻击与防范。
- 难点：BGPsec 和 RPKI。

第四章　域名系统安全

4.1　DNS 原理与协议

4.2　DNS 安全风险分析

4.3　DNSSEC 原理与扩展应用

4.4　DNS 滥用的检测与分析

- 重点：DNS 各种攻击方法与防范措施。

■ 难点:DNSSEC。

第五章　安全通信协议与公钥基础设施

5.1　常用安全协议概要

5.2　SSL/TLS 发展历史及工作原理

5.3　TLS 协议的常见攻击方法

5.4　PKI/CA 的安全风险及常见攻击

■ 重点:TLS 协议工作原理和攻击方法。

■ 难点:TLS 协议的各种攻击方法。

第六章　应用协议安全

6.1　HTTP 协议

6.2　Web 浏览器安全

6.3　Web 服务端安全

6.4　电子邮件系统安全

6.5　SSH 协议

■ 重点:HTTP 协议安全问题、Web 的各种安全问题、方法机制。

■ 难点:Web 同源策略及各种攻击方法、防范机制。

第七章　分布式拒绝服务

7.1　分布式拒绝服务攻击原理与分类

7.2　僵尸网络原理、检测与分析

7.3　分布式拒绝服务攻击防御

■ 重点:分布式拒绝服务攻击的类别、放大攻击的放大倍数计算,针对分布式拒绝服务攻击的防范措施。

■ 难点:低速拒绝服务攻击、拒绝服务攻击的检测。

第八章　网络安全新进展

8.1　匿名通信

8.2　区块链与虚拟货币

8.3　典型的地下产业及检测

■ 重点:匿名通信网络及协议、Blockchain 工作原理。

■ 难点:匿名通信网络的构建、匿名度的计算。

七、考核要求

本课程采用考试的方式考核。

八、编写成员名单

段海新(清华大学)、张宏莉(哈尔滨工业大学)、李舟军(北京航空航天大学)、程光(东南大学)、郭山清(山东大学)、王东滨(北京邮电大学)。

10 信息内容安全原理

一、课程概述

信息内容安全旨在保护授权、合法的信息传播，限制非法和非授权信息的传输。本课程讲授舆情分析、隐私保护、多媒体安全等应用领域的共性理论与技术，主要涉及网络信息内容获取、检测、分析和管理的基本原理、方法和技术，包括网络信息的主动和被动获取技术，语言和语音等信息内容分析、信息安全管理等。

二、先修课程

计算机网络、模式识别、信息论。

三、课程目标

本课程旨在使学生了解信息内容安全问题面临的形势和技术挑战；掌握网络信息的主动获取和被动获取技术，音视频网络传输协议，主要的图像和音视频信息编码方式，文本内容识别、语音识别、语义理解和情感分析等基本原理和关键技术；了解信息内容安全响应和管理的相关技术方法，了解信息内容安全领域技术的新进展。

四、适用对象

本课程适用于网络空间安全一级学科信息内容安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用课堂讲授与研讨相结合的方式授课。一方面注重信息内容安全涉及的基本概念、基础理论、关键技术和典型模型的全貌讲解和深入剖析；另一方面注重联系信息内容安全的前沿问题，以实际案例出发，引导学生讨论分析解决问题的方法。

六、课程内容

第一章 信息内容安全概述

1.1 网络空间安全

主要内容：网络空间安全的定义、内涵、重要意义、技术体系等。

1.2 信息内容安全

主要内容：信息内容分类、信息编码格式（包括文本、音频、视频、图像）；信息内容安全的内涵、宗旨、面临的主要安全威胁。

1.3 信息内容安全技术体系

主要内容：信息内容的获取、识别和分析技术；信息内容的安全管理和保护技术。

1.4 信息内容安全技术现状与挑战

主要内容:信息内容安全的典型案例、挑战性问题、研究现状与发展趋势。

■ 重点:信息内容安全的内涵与意义、信息内容安全的技术体系。

■ 难点:信息内容安全的技术现状与挑战。

第二章　网络信息获取

2.1　音视频信息编码方式与传输协议

主要内容:H.264 与 MPEG-4 标准的音频编码、视频编码方法,音视频流媒体传输协议。

2.2　网络信息被动获取技术

主要内容:主要的网络协议、网络报文被动获取方法,协议还原方法(包括文本信息、图像信息和音视频信息),加密协议的数据获取方法,高性能捕包平台等。

2.3　网络信息主动获取技术

主要内容:主要的信息发布技术、分布式信息爬取技术、清洗技术、数据索引与查询技术等。

■ 重点:网络信息被动获取技术、网络信息主动获取技术。

■ 难点:大流量下的音视频信息获取与协议还原。

第三章　实体识别和关系抽取

3.1　网络实体识别技术

主要内容:基于文本语义的实体识别方法,基于统计机器学习的实体识别方法,实体消解方法。

3.2　实体属性与关系抽取技术

主要内容:基于规则的抽取方法,基于机器学习的抽取方法,基于深度学习的抽取方法,基于主题模型的抽取方法等;属性聚类方法。

■ 重点:基于机器学习的实体识别方法、基于机器学习的抽取方法。

■ 难点:面向应用领域的实体识别与关系抽取。

第四章　情感分析

4.1　文档级情感分类

主要内容:基于监督的情感分类,基于无监督的情感分类,跨领域情感分类,跨语言情感分类,文档的情绪分类。

4.2　句子级主客观和情感分类

主要内容:句子级主客观分类方法,句子级情感分类方法,句子级情绪分类方法。

4.3　属性级情感分类

主要内容:属性级情感分类方法,情感组合规则,规则表示,词义消歧和指代消解。

4.4　情感词典构建

主要内容:基于词典的方法,基于语料库的方法,隐含情感信息(期望或者不期望)的事实型描述。

■ 重点:多级情感分类方法、基于语料库的情感词典构建方法。

■ 难点:基于机器学习的文档级情感分类方法。

第五章　语音分析

5.1　典型的声学模型

主要内容:混合高斯与隐马尔可夫声学模型,深度神经元网络声学模型等。

5.2 语音识别方法

主要内容:基于隐马尔可夫模型的语音识别、基于矢量量化的语音识别、基于人工神经网络的语音识别等。

5.3 语音识别开源工具

主要内容:传统语音识别开源工具,深度学习开源框架。

- 重点:声学模型、语音识别系统架构。
- 难点:应用典型语音识别模型和开源工具解决实际问题。

第六章 话题聚类与事件分析

6.1 话题发现

主要内容:数据时效性分析技术,基于主题的话题发现,基于向量空间模型的话题发现等。

6.2 话题聚类分析

主要内容:常见的聚类算法,基于主题模型的聚类。

6.3 网络事件分析

主要内容:基于时间线的网络事件分析、基于空间位置的网络事件分析,事件影响力分析等。

- 重点:话题聚类方法、事件分析方法。
- 难点:网络事件影响力分析,信息传播趋势预测。

第七章 信息内容安全管理

7.1 信息内容安全政策法规

主要内容:相关各国的法律法规,执法与监督机构职责等。

7.2 信息内容安全管理体系

主要内容:法律保障、行政监管、行业自律、技术支撑、舆论监督、社会教育等。

7.3 信息内容安全管理技术

主要内容:舆情干预技术,包括角色建模、引导策略与引导效果评价等;网络信息内容安全应急响应技术等。

- 重点:信息内容安全管理体系、信息内容安全法律法规。
- 难点:信息内容安全应急响应技术。

七、考核要求

考核成绩由课程研讨和课程考试组成。

八、编写成员名单

张宏莉(哈尔滨工业大学)、李建华(上海交通大学)、杜瑞颖(武汉大学)、俞能海(中国科学技术大学)、王东滨(北京邮电大学)、韩伟红(广州大学)。

11 信息隐藏

一、课程概述

保护多媒体产品知识产权、使用密码技术受到限制而又必须进行隐蔽通信等需求,使信息隐藏中的数字水印技术和隐蔽通信技术得到了迅速发展。本课程主要讲授信息隐藏和信息隐藏分析的发展脉络和研究现状,以及数字水印、信息隐藏、多媒体内容取证、隐写分析等基本概念、理论和技术,当前的热点研究问题和挑战,使学生掌握信息隐藏和通信保密技术,具备分析和解决问题的综合素养和能力。

二、先修课程

信号与系统、数字图像处理、概率论与数理统计、密码学。

三、课程目标

通过本课程的学习,学生应掌握与信息隐藏有关的基本概念和原理,深度了解信息隐藏关键算法和技术,为从事信息隐藏和通信保密等科学研究和工程实践工作奠定基础。

四、适用对象

本课程适用于网络空间安全一级学科信息内容安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用讲授和研讨相结合的方式授课。

六、课程内容

第一章 概述

1.1 信息隐藏定义与特点

主要内容:信息隐藏应用背景、与其他安全通信技术的安全性与保密性对比。

1.2 信息隐藏基础知识

主要内容:常用的信号变换及检测方法,媒体信号处理技术,密码学、信号处理、图像处理等。

1.3 多媒体安全

主要内容:基本属性和安全威胁,信息机密性和完整性防护技术和方法等。

第二章 多媒体信息加密

2.1 图像加密

主要内容:图像加密方法的分类,包括加密操作所在的空间、像素位置和像素灰度值是否改变、解密图像与原图是否具有差异、加密算法结构、密钥种类、加密数据的百分比等。

2.2 混沌加密

主要内容:混沌加密的概念、混沌的稳定性理论和混沌图像加密的基本算法。

2.3 视频加密

主要内容:MPEG、H.264 等视频压缩格式的基本结构,基本视频加密算法。

第三章 数字水印

3.1 数字水印的概念与模型

主要内容:数字水印算法简介,数字水印在版权保护、窜改检测等媒体安全中的应用。

3.2 数字水印技术

主要内容:基本嵌入与提取算法、脆弱水印与鲁棒水印,有损水印与无损水印,3D 水印技术,数字水印算法攻击技术。

3.3 数字水印技术的评价指标与评价体系

第四章 数字隐写与分析

4.1 数字隐写概述

主要内容:数字隐写基本概念、数字隐写算法的分类、数字隐写在隐蔽通信领域的应用、数字隐写技术的评价指标。

4.2 图像隐写技术

主要内容:LSB 隐写算法、基于 BMP 格式的原始图像隐写技术,基于 JPEG 和 JPEG2000 的压缩图像隐写技术,调色板图像隐写技术,基于视觉特性的隐写技术,图像无损隐写技术。

4.3 隐写分析算法

主要内容:数字隐写的嵌入与提取、基于图像像素统计特性的隐写分析技术、基于图像格式的隐写分析技术、基于机器学习分类器的批量隐写检测技术。

第五章 数字图像取证

5.1 基础知识

主要内容:主动取证与被动取证的概念及应用,图像取证的原理、算法以及应用背景。

5.2 同幅图像与异幅图像的取证机理

5.3 数字图像取证

主要内容:基于遗留痕迹的数字图像取证技术,基于成像设备一致性的数字图像取证技术,基于自然图像统计规律的图像取证技术。

5.4 图像反取证技术

主要内容:基于图像统计特性一致化的图像反取证技术,基于成像过程控制的图像反取证技术。

七、考核要求

考核成绩由期末考试和课程作业组成。

八、编写成员名单

张宏莉(哈尔滨工业大学)、俞能海(中国科学技术大学)、陆哲明(哈尔滨工业大学)、李琼

(哈尔滨工业大学)、王丽娜(武汉大学)、刘粉林(中国人民解放军战略支援部队信息工程大学)。

12 社交网络分析

一、课程概述

本课程主要介绍社交网络分析的现状、发展以及面临的挑战,从结构与演化、群体与互动、信息与传播三个方面展开,围绕社交网络的结构特性与演化机理分析社交网络群体行为的形成与互动规律、社交网络的信息传播模型及演化规律等,系统讲授社交网络分析中的基本理论、关键技术和方法。

二、先修课程

计算机网络、机器学习。

三、课程目标

通过本课程的学习,学生应从结构与演化、群体与互动、信息与传播三个方面掌握社交网络分析的基本概念、基本理论和关键技术,了解其发展历程、典型算法与应用,培养应用社交网络分析的理论和技术解决实际问题的能力。

四、适用对象

本课程适用于网络空间安全一级学科信息内容安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用讲授和研讨相结合的方式授课。

六、课程内容

第一章 社交网络分析概述

1.1 社交网络的起源

1.2 在线社交网络的发展

1.3 在线社交网络的概念、特点以及在线社交网络分析所面临的挑战

- 重点:社交网络概念,在线社交网络的特点及其影响。
- 难点:在线社交网络分析面临的挑战。

第二章 社交网络结构特征分析及建模

2.1 社交网络结构统计特性

2.2 小世界现象、分散搜索模型

2.3 社交网络结构建模方法与演化机制

■ 重点:社交网络统计特性,流行度的成因,小世界分散搜索模型。

■ 难点:形成社交网络结构统计规律的理论模型分析。

第三章 虚拟社区发现

3.1 虚拟社区的定义及其应用

3.2 虚拟社区的静态发现算法

3.3 虚拟社区的动态发现算法

3.4 算法的评价指标

■ 重点:模块度最优化算法,派系过滤算法,局部扩展优化算法。

■ 难点:从发展角度理解在不同应用背景下提出的社区发现算法。

第四章 用户行为分析

4.1 在线社交网络用户使用行为分析

4.2 影响在线社交网络用户采纳行为的因素,基于技术接受模型的用户采纳模型,基于计划行为理论的用户采纳模型

4.3 影响用户忠诚的因素,基于期望确认的用户忠诚模型,基于心流体验理论的用户忠诚模型

4.4 社交网络中用户的行为规律

4.5 群体互动规律

■ 重点:社交网络用户的采纳特性分析与建模,社交网络用户的忠诚分析与建模。

■ 难点:影响用户采纳行为和忠诚的心理因素及量化,心理变化及量化。

第五章 影响力分析及应用

5.1 社交网络用户间影响强度的分析

5.2 社交网络用户间影响强度计算方法,基于网络结构的影响强度计算、基于行为的影响强度计算、基于话题的影响强度计算

5.3 影响力个体发现的应用,影响力个体发现算法

5.4 影响力最大化应用,影响力最大化分析算法(贪心算法、启发式算法等)

■ 重点:社交网络用户间影响强度的计算,个体影响力分析。

■ 难点:大网络规模下的影响力最大化分析。

第六章 社交网络信息传播规律

6.1 社交网络中信息传播的影响因素

6.2 社交网信息传播模型

主要内容:基于网络结构、群体状态和信息特征的传播模型和应用。

6.3 信息热度预测方法

主要内容:基于历史热度、网络结构、用户行为、时间序列法的预测。

6.4 信息溯源技术

■ 重点:社交网信息传播的影响因素分析和传播建模,信息溯源技术。

■ 难点:信息缺失、网络结构不确定性对信息溯源精度的影响。

第七章　话题发现与话题演化分析

7.1　话题发现的研究、发展及应用

7.2　话题发现分析

主要内容:基于主题模型的话题发现、基于向量空间模型的话题发现,基于网络结构的影响强度计算、记忆效应、基于行为的影响强度计算、基于话题的影响强度计算,预测的方法和应用实例。

7.3　话题演化分析

主要内容:基于主题的话题演化分析,基于近邻时间片关联的演化分析。

- 重点:话题的发现方法,话题的演化分析方法,话题分析的应用。
- 难点:社交网络中的话题发现与演化分析,传统媒体中的话题发现与演化分析。

七、考核要求

考核成绩由课堂研讨、课程作业和期末考试组成。

八、编写成员名单

张宏莉(哈尔滨工业大学)、郭莉(中国科学院信息工程研究所)、李爱平(国防科技大学)、齐佳音(上海对外经贸大学)、田志宏(广州大学)。

13　隐私保护

一、课程概述

隐私保护是个人信息广泛共享与充分利用的重要基础。针对万物泛在互联、数据广域共享、动态差异保护所面临的新挑战,本课程主要讲授隐私信息在单一信任域、多信任域、不可预测的信息传播途径等场景下保护的基本方法、基本理论及关键技术。本课程为研究生开展在隐私保护领域的科学研究提供基础理论和方法指导。

二、先修课程

概率论、信息论。

三、课程目标

本课程系统介绍隐私保护的基础知识和最新研究进展,使研究生全面了解隐私保护的基本概念、原理和方法,掌握隐私保护研究的常用方法,具备针对不同应用场景开展隐私动态度量、保护方案设计、保护效果评估、泄露风险分析、隐私侵犯溯源与取证等方面研究的能力。本课程为研究生从事隐私信息保护系统研发工作提供理论与技术指导。

四、适用对象

本课程适用于网络空间安全一级学科应用安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用讲授和实践相结合的方式授课。一方面注重隐私保护基本概念、基础理论和典型保护方案的全貌讲解和深入剖析；另一方面从新业态、产业生态圈和信息传播模式等角度，重点讲授隐私保护的需求分析、关键问题提炼、新型保护方案设计等方面的研究思维；此外，选取实际案例，将理论与技术应用于具体场景，分析和解决实际问题，如隐私信息脱敏、保护效果评估、隐私延伸控制等。

六、课程内容

第一章　隐私保护概述

1.1　隐私的定义与保护需求

主要内容：隐私在法律法规、行业、学术界的定义；隐私数据在采集、传输、存储和使用等环节的具体保护需求。

1.2　隐私泄露的实例分析

主要内容：在信息系统内部、跨信息系统等场景下的隐私泄露实例；终端用户、服务提供商等的隐私保护目标。

1.3　隐私保护常用技术

主要内容：基于匿名技术、密码学、访问控制等的隐私保护技术。

1.4　大数据分析技术对隐私保护的影响

主要内容：基于机器学习、深度学习等大数据分析技术的隐私信息挖掘；抗大数据分析的隐私信息脱敏。

■ 重点：隐私信息的组织管理、应用场景与保护需求分析的关联性；隐私保护常用技术的理论基础、分类方法及其适用场景。

■ 难点：大数据集的规模、保护方案的效果和人对隐私的感悟度之间动态平衡的思维方法。

第二章　隐私计算概论

2.1　隐私计算理论与技术体系

主要内容：隐私计算的基本定义、基础理论、计算框架、信息系统框架、延伸控制机理、关键技术体系。

2.2　隐私信息的形式化定义

主要内容：隐私信息向量、隐私属性向量、广义定位信息集合、审计控制信息集合、约束条件集合、传播控制操作集合。

2.3　隐私计算的刻画要素

主要内容：隐私信息、隐私运算操作集合、隐私保护代价、隐私保护效果。

2.4　隐私保护算法的设计准则

主要内容：预处理、算法框架、算法参数设计、算法组合、算法复杂性与效能分析。

2.5 隐私保护效果评估

主要内容:可逆性、延伸控制性、偏差性、复杂性、信息损失性。

2.6 隐私计算语言

主要内容:隐私定义语言、隐私操作语言、隐私控制语言。

2.7 隐私侵犯的溯源取证

主要内容:隐私信息界定、侵犯行为判定、轨迹信息提取、侵犯取证与溯源。

2.8 隐私计算的应用示例

主要内容:在系统内部不同域间、封闭系统间、开放系统间信息交互时的应用示例。

■重点:隐私计算框架、隐私信息系统框架、隐私保护算法的通用设计准则、动态跨系统传播中的隐私侵犯取证与溯源。

■难点:隐私信息的形式化描述、传播途径不可控的隐私信息延伸控制、算法设计准则的基础数学理论。

第三章 基于访问控制的隐私保护

3.1 访问控制基础

主要内容:隐私保护实体及其关系、隐私信息全生命周期控制模型、访问控制策略。

3.2 隐私信息访问安全模型

主要内容:隐私信息访问安全模型的定义原则、原子操作、安全原语、设计准则、基本组成。

3.3 隐私信息访问控制策略生成、冲突检测与消解

主要内容:策略描述语言、策略非一致性冲突检测与消解、多级安全策略冲突检测与消解模型、基于 XACML/属性/状态/逻辑的冲突检测与消解方法。

3.4 基于访问控制的隐私保护机制发展趋势

主要内容:细粒度多级安全的访问控制模型及其策略、访问权限的可伸缩性动态调整方法、访问授权的过程追踪与回溯方法。

■重点:面向网络空间的访问控制模型及资源传播链、网络传播链;隐私信息访问的原子操作抽象、安全模型机理;跨系统隐私信息交换的访问控制策略冲突检测与消解。

■难点:隐私信息传播路径的泛在网络拓扑描述;场景变化的感知、访问控制策略的抽象定义、场景适应的权限动态伸缩。

第四章 基于密码学技术的隐私保护

4.1 隐私计算中常用的密码学技术

主要内容:同态加密、安全多方计算、性质保持加密、零知识证明、秘密分享。

4.2 基于密文计算的隐私保护

主要内容:密文搜索、私有信息检索;保护隐私的深度学习、密文数据聚合。

4.3 安全多方计算与隐私保护

主要内容:安全多方计算的形式化定义、功能、应用场景;基于零知识/乱码电路/不经意传输的安全多方计算隐私保护技术。

■重点:同态加密、性质保持加密在隐私保护中的具体应用;公开可验证的安全两方/多方计算。

■难点:在多方参与的隐私保护场景中密码学相关知识的具体应用;基于同态性质的密文计

算方法设计。

第五章　基于概率论/信息论的隐私保护

5.1　基于概率论/信息论的隐私度量

主要内容：信息熵、条件熵、互信息、相对熵、率失真函数在隐私度量及隐私保护效果评估中的应用。

5.2　匿名技术

主要内容：k-匿名、l-多样性、t-贴近性、置信度边界模型、(a,k)-匿名模型、(k,e)-匿名模型。

5.3　随机化技术

主要内容：随机扰动、随机化应答。

5.4　差分隐私保护

主要内容：隐私预算、敏感度、拉普拉斯/高斯/指数等加噪机制、组合性质。

- 重点：隐私保护效果量化评估、复杂数据的差分隐私保护。
- 难点：匿名、随机化隐私保护的效果量化分析；差分隐私保护机制和参数的遴选原则。

第六章　面向应用场景的隐私保护技术

6.1　生物信息服务隐私保护

主要内容：指纹隐私、人脸隐私、虹膜隐私、基因数据隐私保护。

6.2　社交网络隐私保护

主要内容：社交网络隐私定义；基于 k-匿名、随机化等技术的社交信息隐私保护方案；图数据的隐私保护方案。

6.3　医疗数据隐私保护

主要内容：基于数据加密技术、差分隐私技术、匿名技术的数据安全查询和发布。

6.4　云计算中的隐私保护

主要内容：基于同态加密、可搜索加密、差分隐私技术的数据安全外包计算；隐私保护的完整性验证。

6.5　位置信息服务

主要内容：位置服务隐私保护概述、基于语义的位置信息隐私保护；查询隐私和轨迹隐私保护。

- 重点：不同类型数据查询与发布的隐私保护；多方协同的位置隐私保护。
- 难点：面对特定场景的隐私保护机制优化组合与效果评估；场景适应的抗大数据分析的隐私保护。

第七章　隐私信息流转管控

7.1　隐私信息流转描述方法

主要内容：CIPSO 选项格式、报文级标签、版式文件细粒度描述。

7.2　隐私信息流转管控技术

主要内容：隐私信息分片与重组；传输路径发现与管控；应用协议代理还原、隐私信息细粒度过滤、异常行为检测。

7.3　信任模型、信任链、信誉系统

主要内容:主观/客观信任、授权模型、动态/静态信任链、分布式信誉系统。

7.4 信任度评估模型和动态信任评估

主要内容:直接、间接、总体信任度评估模型。

- 重点:融合声誉/策略/行为等因素的信任动态度量模型、隐私保护的实体信任动态评估。
- 难点:信任关系动态管理维护与可信保持、基于机器学习的动态信任评估。

七、考核要求

考核成绩由课程作业成绩和期末考试成绩组成。

课程作业主要考核对隐私保护相关理论、方法及模型的理解和使用上述理论、方法及模型解决实际问题的能力。

期末考试采用闭卷考试形式,主要考核对隐私保护技术、隐私计算理论、信任管理、隐私信息流转管控等方面重点难点问题的掌握程度。

八、编写成员名单

李凤华(中国科学院信息工程研究所)、李晖(西安电子科技大学)、牛犇(中国科学院信息工程研究所)、翁健(暨南大学)、任奎(浙江大学)、李洪伟(电子科技大学)、俞能海(中国科学技术大学)。

14 新技术安全

一、课程概述

物联网、移动互联网、工业互联网、云计算、大数据、人工智能、区块链等新技术在发展过程中,不仅自身面临严峻的安全挑战,在应用过程当中也带来了衍生的安全问题。本课程主要讲授新技术自身安全防护和新技术应用安全的基础理论和关键技术,将为研究生开展应用安全方向的科学研究提供基础理论和方法指导。

二、先修课程

密码学原理、系统安全。

三、课程目标

本课程系统介绍新技术安全的基础理论和最新安全技术,使研究生全面了解新技术安全的基本概念、原理和方法,掌握新技术应用安全保障的常用技术与方法,具备发现新技术及其应用的安全问题并提出解决方案的能力,为研究生从事与新技术安全相关的理论研究、技术创新和系统开发等工作打下坚实的基础。

四、适用对象

课程适用于网络空间安全一级学科应用安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用讲授、研讨和实践相结合的方式授课。一方面注重物联网、移动互联网、工业互联网、云计算、大数据、人工智能和区块链等新技术安全基本原理、常用技术、安全体系的全貌讲解和深入剖析;另一方面注重通过研讨激发和培养学生发现问题和分析问题的能力,并且通过具体实例,培养学生解决新技术安全问题的能力。

六、课程内容

第一章　物联网安全

1.1　物联网安全体系架构

主要内容:ISO 物联网参考架构;异构物联网接入认证体系、物联网跨域数据交换与受控共享。

1.2　物联网通信协议及安全

主要内容:物联网物理层、网络层、应用层协议及安全。

1.3　物联网终端可信计算环境

主要内容:智能终端可信体系架构、物联网可信计算环境、终端网络一体化安全设计、可信根融合与迁移。

1.4　设备身份管理

主要内容:海量设备身份管理与标识、轻量级身份认证、设备跨域快速安全漫游切换。

1.5　轻量级密码技术

主要内容:轻量级数据加密算法、轻量级密钥管理、低功耗密码芯片与系统。

1.6　漏洞检测与渗透测试技术

主要内容:物联网智能终端、协议及应用的漏洞检测;物联网系统的渗透测试;物联网设备测绘。

- 重点:物联网通信协议及安全;海量设备身份管理与标识;物联网智能终端的漏洞检测。
- 难点:异构物联网安全互联互通协议设计;物联网 APT 攻击检测。

第二章　移动互联网安全

2.1　4G/5G 网络安全

主要内容:4G/5G 安全架构;5G 接入安全、网络切片安全;网络功能虚拟化安全。

2.2　天地一体化网络安全

主要内容:天地一体化网络服务架构、全球卫星互联网及其安全架构、天地一体化认证与鉴权。

2.3　开放平台及应用安全

主要内容:移动互联网能力开放的平台架构、层次安全服务模型。

2.4　智能终端操作系统安全

主要内容:Android 系统安全机制和权限管理;iOS 系统安全机制和权限管理。

■ 重点:5G 网络和天地一体化安全体系结构;移动互联网能力开放的层次安全服务模型。

■ 难点:天地一体化网络统一认证框架与协议设计;5G 网络的鉴权、空口安全、海量用户的高并发/高吞吐率的安全服务。

第三章　工业互联网安全

3.1　工业互联网概述

主要内容:工业互联网技术演化;工业互联网网络体系、平台体系、安全体系。

3.2　工业互联网网络体系

主要内容:工控网现场总线协议、TSN 网络协议;SCADA/DCS/PLC/HMI 等工控系统架构;工业互联网标识解析技术。

3.3　工业互联网平台体系

主要内容:工业互联网边缘层、工业 PaaS 层、应用层;工业微服务组件;工业数据建模与分析、平台资源部署与管理。

3.4　工业互联网安全体系

主要内容:工业互联网分层分域隔离;工业互联网统一身份认证和数据安全;威胁态势感知和入侵检测。

■ 重点:工业互联网的标识解析及安全;工业互联网的安全防护。

■ 难点:分层分域双向安全隔离与受控交换;工控系统脆弱性分析和威胁态势实时感知。

第四章　云计算安全

4.1　虚拟化与安全

主要内容:虚拟化安全架构;虚拟机管理与监控;CPU、内存、设备、网络虚拟化;虚拟机的安全隔离、迁移、回滚;恶意行为检测。

4.2　容器与微服务的安全架构

主要内容:容器镜像、运行时安全;容器与微服务安全隔离;容器云网络安全;微服务架构入侵检测、访问控制。

4.3　SDN 安全

主要内容:恶意数据流检测;交换机行为监控、流表资源可控管理;控制通道安全防护、控制层业务安全;策略冲突检测与消除。

4.4　云数据安全

主要内容:云数据加密存储,加密云数据去重、共享、检索、编辑,云数据完整性验证等。

4.5　云计算安全标准

主要内容:ISO/IEC JTC1/SC27 云计算标准、NIST 云计算安全标准、中国云计算安全标准。

■ 重点:虚拟化的安全架构与虚拟机安全隔离;云存储数据的安全机制。

■ 难点:虚拟机恶意行为的实时监控与快速处置;加密云数据的高效检索。

第五章　大数据安全

5.1　大数据全生命周期的高效可信保障

主要内容:数据汇集完整性保护;可信融合与清洗;大数据可用性感知;数据源跟踪与追溯。

5.2　大数据存储安全

主要内容：分布式文件系统安全、时空数据库安全；大数据访问审计。

5.3 大数据安全处理

主要内容：明文封闭计算；高性能密码按需服务、高并发的随机加解密、海量密钥管理。

5.4 大数据流转的安全测评与审查

主要内容：跨域/跨系统/跨国境流转的取证与监管；跨数据中心流动多环节安全。

5.5 大数据安全管理框架

主要内容：大数据应用系统访问控制；大数据确权与交易跟踪；大数据交换与开放安全；数据采集合规性和使用。

■ 重点：大数据存储系统安全与数据存储加密技术；差异化应用的可定制可重构大数据安全管理体系框架。

■ 难点：场景适应的大数据访问控制；大数据频繁隐性流转的取证与溯源。

第六章 人工智能安全

6.1 人工智能安全概述

主要内容：人工智能的自身安全；人工智能的衍生安全；人工智能的主动控制与被动控制安全。

6.2 人工智能技术的脆弱性

主要内容：数据导致的人工智能脆弱性；人工智能算法、执行过程脆弱性，人工智能评估过程脆弱性。

6.3 人工智能与网络安全

主要内容：基于人工智能的网络防御、自动化攻防方法和框架；人工智能行为体与风险管控。

6.4 人工智能与信息安全

主要内容：匿名化措施失效等大数据安全；推荐算法加速不良信息传播；人工智能衍生信息的真伪审查。

6.5 人工智能的伦理道德

主要内容：人工智能技术的伦理道德；人工智能行为体的道德约束、责任归属。

■ 重点：基于人工智能的网络攻防技术、人工智能对信息安全的影响。

■ 难点：自动化攻击方法与主被动控制；服务模式、商业利益与不良信息传播的自我约束。

第七章 区块链安全

7.1 区块链概述

主要内容：区块链密码基础，区块链的技术本质、共识机制，区块链的服务模式与社会治理的关系。

7.2 与链相关的数据安全与隐私保护

主要内容：混币；恶意信息攻击、密钥泄露/丢失、监管。

7.3 区块链的网络层安全

主要内容：网络劫持攻击；节点泄露漏洞、日食攻击。

7.4 区块链的共识层安全

主要内容：治理机制；51%算力攻击、贿选攻击、女巫攻击、无利害关系问题、硬分叉。

7.5 区块链的合约层安全

主要内容:重入攻击、数据类型漏洞、逻辑漏洞、时间戳依赖攻击。

7.6 区块链的生态安全

主要内容:勒索软件、恶意矿机病毒、加密货币、钱包、交易对联动攻击。

- 重点:共识机制的设计思想;智能合约的安全设计方法。
- 难点:区块链的理论基础、技术架构与社会治理的辩证关系;安全高效的共识机制设计。

七、考核要求

考核成绩由课程实验成绩和课程研究论文成绩组成。

课程实验主要考查学生对新技术领域中关键技术和方法的理解程度和编程实践能力,要求学生选择一个新技术方向复现已有的技术方法及其效果,并形成实验文档。

课程研究论文主要考查学生对新技术本身及应用的安全问题的发现能力和解决方案的创新研究能力,要求学生能够针对具体复杂的新技术应用场景的特点提出新方法,解决新问题,形成研究论文。

八、编写成员名单

李凤华(中国科学院信息工程研究所)、李晖(西安电子科技大学)、张小松(电子科技大学)、邹德清(华中科技大学)、阚海斌(复旦大学)、王东滨(北京邮电大学)、沈玉龙(西安电子科技大学)。

15 应用系统安全

一、课程概述

应用系统安全是保障应用系统稳定可靠运行的重要基础。针对系统跨域互联、数据海量异构、信息受控共享所面临的新挑战和安全需求,本课程主要讲授应用系统在跨管理域、跨安全域、跨系统数据流动等服务模式下安全运行的基础理论、关键技术及其在典型应用场景下的安全实践,为研究生开展应用安全方向的科学研究提供基础理论和方法指导。

二、先修课程

密码学原理、数据库原理、网络安全。

三、课程目标

本课程系统介绍应用系统安全的基础知识和最新研究进展,使研究生全面了解应用系统安全的基本概念、原理和方法,掌握应用系统安全保障的常用技术与方法,具备针对电子政务、电

子商务、电子支付等典型信息系统独立设计安全解决方案的能力和应用系统安全评估等方面的研究能力，为研究生从事与应用系统安全相关的规划、设计等工作打下坚实的基础。

四、适用对象

本课程适用于网络空间安全一级学科应用安全方向的博士研究生和硕士研究生。

五、授课方式

本课程采用理论教学和应用实践相结合的教学方法，一方面注重对应用系统安全的原理、常用技术、安全体系进行全貌讲解和深入剖析；另一方面从信息泛在服务模式出发，重点讲授应用系统安全的需求分析、关键问题提炼、安全体系架构设计、新型安全保护方案设计等方面的思维方法；此外，选取智慧城市安全等实际案例，将理论与技术应用于具体场景，分析和解决实际问题。

六、课程内容

第一章　应用系统安全概论

1.1　信息化与应用系统的发展趋势

主要内容：信息化与应用系统的概念、关键要素、变迁过程与未来趋势。

1.2　大型应用系统的安全挑战

主要内容：大型应用系统的应用案例、在采集/传输/处理/存储/销毁等环节面临的安全挑战。

1.3　应用系统安全技术体系

主要内容：应用系统的安全需求，包含可信性、机密性、完整性、可用性、可生存性等融合的保障技术体系。

1.4　应用系统安全管理体系

主要内容：应用系统安全的管理范围、策略、关键要素，以及组织架构、运行维护管理、教育培训。

1.5　应用系统安全标准体系

主要内容：TCSEC 标准、BS7799 标准、信息安全等级保护。

- 重点：应用系统安全技术体系、管理体系、标准体系的关联性；融合保障技术体系。
- 难点：应用系统安全技术体系、关键技术、管理手段的演化思维；网络安全等级保护的技术内涵。

第二章　关系数据库安全

2.1　关系数据库安全概述

主要内容：关系数据库的概念、安全目标、安全风险、主要挑战和安全关键技术（安全性控制、完整性控制、并发性控制、数据恢复）。

2.2　访问控制机制

主要内容：访问控制概念、访问控制模型、访问控制策略、实现实例。

2.3　SQL 注入攻击

主要内容:SQL 注入攻击的原理、检测方法与防护手段。

2.4 关系数据库加密技术

主要内容:关系数据库的加密基本准则、加解密参考框架、列加密的密钥管理、支持高并发的高性能实现机制。

2.5 推理分析与隐通道分析

主要内容:推理分析与隐通道分析的概念、隐通道原理与机制、隐通道审计与度量、隐通道消除。

2.6 关系数据库审计

主要内容:关系数据库的审计需求、审计策略与审计系统。

2.7 异构数据库安全融合

主要内容:异构数据库的安全融合准则、融合方法(包括异构访问控制策略翻译、数据非一致性检测与消除等)。

■ 重点:机密性模型和完整性模型;高并发、多算法、多密钥的透明列加密;隐通道快速审计与准确度量。

■ 难点:数据访问安全模型的安全性证明;基于信息流的隐通道审计与度量。

第三章 非关系数据库安全

3.1 非关系数据库概述

主要内容:非关系数据库的应用特性、发展历程和主要安全挑战。

3.2 非关系数据库安全架构

主要内容:非关系数据库的安全风险与安全体系架构。

3.3 一致性确保与容错技术

主要内容:数据的一致性确保、完整性验证、容错与纠错等技术。

3.4 NoSQL 注入

主要内容:NoSQL 注入攻击的原理、检测方法与防护手段。

3.5 数据导入安全

主要内容:数据导入的方法、面临的风险、安全机制。

3.6 数据库容灾与恢复技术

主要内容:数据失效检测、业务无缝迁移、灾难快速恢复等机制。

3.7 图数据库

主要内容:图数据库概念与模型、典型图数据库、图数据库优化、图数据库典型应用。

■ 重点:数据一致性校验机制;图数据库高效查询。

■ 难点:图数据库中的高效索引与推理。

第四章 身份管理与认证

4.1 身份管理

主要内容:实体身份分类、定义及形式化抽象描述,多元身份的关联特征,域内身份管理方法,域间身份管理方法。

4.2 授权管理

主要内容:授权模型、权限分配、更新与撤销机制。

4.3 多因素身份认证

主要内容:多因素身份认证的定义、常用方法、多因素组合认证。

4.4 FIDO 认证协议

主要内容:FIDO 认证协议、应用及实现技术。

- 重点:访问权限自适应调整;多要素跨域交叉认证。
- 难点:跨域多元身份管理模型、关联协同授权;多因素组合认证的安全性分析。

第五章 电子政务系统安全

5.1 电子政务系统概述

主要内容:电子政务的主要特征、服务模式演进、IT 技术演化、新的安全挑战。

5.2 办公自动化系统

主要内容:办公自动化系统概述与设计原则、典型办公自动化业务系统数据流抽象。

5.3 政务信息资源管理

主要内容:政务信息资源的管理原则与目标、控制模式、数据治理技术(包括数据标签描述与绑定、数据流转机制)。

5.4 电子政务安全技术保障体系

主要内容:电子政务系统的安全风险、安全评估,电子政务安全技术保障体系(包括跨域安全协同防护、跨域身份认证、数字证书服务、移动接入、数据加密存储与传输、数据延伸控制等)。

5.5 电子政务内外网隔离技术

主要内容:电子政务内外网隔离需求、内外网隔离技术(包括物理/逻辑安全隔离、信息摆渡、单向隔离交换、双向隔离交换)。

- 重点:双向隔离交换原理与机制;面向规模化互联网络的电子政务一体化安全防护。
- 难点:抗隐蔽通信的双向隔离;电子政务系统安全态势感知与安全性评估。

第六章 电子商务系统安全

6.1 电子商务安全概述

主要内容:电子商务的主要特征、多系统联动的交易威胁、用户隐私威胁、安全需求、安全要素、安全标准规范和安全挑战。

6.2 电子商务安全信用管理

主要内容:信用管理概论、社会信用体系、信用风险评估指标与计算。

6.3 移动电子商务安全

主要内容:移动电子商务安全隐患、安全体系架构、安全技术。

6.4 跨境电子商务安全

主要内容:跨境电子商务的数据中心安全防护、多信息系统联动的安全体系架构、数据安全合规性自动检测、数据隐性流动监测与控制。

6.5 电子商务系统中的用户隐私保护

主要内容:用户消费行为画像、企业信息保护、个人信息隐私保护、敏感信息泄露风险、敏感信息交互的延伸控制。

- 重点:生态圈多信息系统联动的安全体系架构;业务服务模式驱动的数据流动监测、跨境安全合规性检测。

■难点:征信计量准确性;电子商务系统中的按需隐私保护。

第七章　电子支付安全

7.1　国内和国际电子支付体系概论

主要内容:国内和国际电子支付的主要特点、电子支付系统的基本功能、多要素关联的强审计与取证。

7.2　电子支付系统安全架构

主要内容:服务模式驱动的电子支付安全需求分析、信息系统安全体系架构、安全支付协议、业务数据异动检测。

7.3　支付认证技术

主要内容:传统认证、指纹认证、人脸认证、声纹认证。

7.4　互联网电子支付

主要内容:互联网电子支付形式及其对应的实现原理、安全风险,与金融机构关联支付、自管账户体系支付、主动/被动扫码支付、免密代理支付等典型安全解决方案。

■重点:不同支付模式的安全体系架构、设计原理异同点;组合支付协议设计与安全性分析。

■难点:支付协议的形式化描述与安全性证明;场景适应的多因素身份认证机制。

第八章　智慧城市安全

8.1　智慧城市技术体系

主要内容:智慧城市的信息服务模型、技术体系及关键技术(包括数据精准采集与高并发汇集、数据高效组织与跨域共享等)。

8.2　智慧城市大数据安全技术

主要内容:智慧城市大数据安全需求、海量异构数据可信认证与动态授权、跨系统的数据共享监测、数据共享过程审计与溯源。

8.3　智慧城市信息安全保障体系

主要内容:智慧城市的信息安全风险挑战、柔性重构一体化安全保障模型、防护机制重构策略、全网纵横联动防护控制。

8.4　智慧城市安全实践

主要内容:智慧交通、智慧停车、智慧物流、城市信息港等的安全解决方案。

■重点:与物联网互动的数据多源高效采集、数据广域受控共享;信息多因素融合决策的动态授权。

■难点:全网安全态势感知、纵横联动的协同防护、基于目标驱动的差异化控制;万物互联的数据广域受控共享。

七、考核要求

考核成绩由课程作业成绩和课程论文成绩组成。

课程作业由学生从提交的若干作业专题报告中任选一个主题进行课堂报告,根据报告内容、报告效果评定成绩。

课程论文由学生针对特定业务系统的安全需求撰写论文,考查其综合分析与解决问题的

能力。

八、编写成员名单

李凤华(中国科学院信息工程研究所)、邱卫东(上海交通大学)、郭云川(中国科学院信息工程研究所)、李晖(西安电子科技大学)、王东滨(北京邮电大学)。