**中山大学研究生课程教学大纲**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 中文名称 | | 数据隐私保护与安全计算 | | | 课程编号 | | DCS5243 | |
| 英文名称 | | Data Privacy Protection and Secure Computing | | | | | | |
| 总学时 | | 36 其中实验课：0 | | | | | 学分 | 2 |
| 开课院系 | | 计算机学院 | 课程负责人 | 桑应朋 | 课程性质 | | □必修 ☑选修 | |
| 授课团队 | | 桑应朋、郑培嘉 | | | | | | |
| 课程类别 | | □公共课 □专业基础课 □专业方向课  □专业技术实践课 ☑选修课 | | | | | | |
| 授课方式 | | 面授 | | 授课语言 | | 中英双语 | | |
| 考核方式 | | 大作业 | | | | | | |
| 先修课程要求 | | 概率论、数理统计、密码学 | | | | | | |
| 教学目标（100字以内）  本课程围绕数据隐私保护和安全计算在先进计算和新型网络环境中的热点问题，在较为系统地介绍隐私数据保护与安全计算的工作机理基础上，着重介绍目前正在发展的一些新理论和新技术。通过该课程的学习，使学生掌握隐私保护和安全计算的基础理论和最新进展，为学生从事相关领域研究起到指导作用。 | | | | | | | | |
| 课程简介（教学内容及基本要求）  本课程主要介绍隐私数据的收集、存储与处理以及在部分信息隐匿下如何进行有效计算和分析。数据隐私保护是指数据的收集、存储及处理过程中保护其中敏感(涉及机密或隐私)的信息不外泄。安全计算则侧重于隐私保护下数据的使用和共享，即指在不泄漏数据隐私的前提下开展各种计算任务，如统计分析、数据挖掘等。  当前先进计算技术（如云计算、大数据分析等）和新型网络环境（如社交网络、无线传感器网/自组网/RFID网等）的出现与发展，不断为隐私保护带来新的挑战。本课程围绕数据隐私保护和安全计算在先进计算和新型网络环境中的热点问题，在较为系统地介绍隐私数据保护与安全计算的工作机理基础上，着重介绍目前正在发展的一些新理论和新技术。  本课程的主要内容如下  **一：**介绍课程领域的研究内容、方法、现状和研究意义  **重点掌握：**明确本领域的研究内容、方法和研究意义。  **教学时间分配：**课堂教学：1学时。  二：数据隐私保护基本方法1-匿名化方法  **重点掌握：**k-匿名化、l-diversity、t-closeness的概念和实现原理，去匿名化攻击，匿名化方法在图数据、时空数据等的隐私保护应用。  **教学时间分配：**课堂教学：5学时。  三：数据隐私保护基本方法2-随机化方法  **重点掌握：**加法噪声、乘法噪声及混合噪声的基本原理，随机化与匿名化的区别与联系。  **教学时间分配：**课堂教学：2学时。  四：数据隐私保护基本方法3-差分隐私方法  **重点掌握：**差分隐私的概念、基本原理、组合定理，非交互式差分隐私，差分隐私的应用  **教学时间分配：**课堂教学：4学时。  五：隐私保护下的数据挖掘与机器学习  **重点掌握：**隐私保护下分类、聚类、关联规则挖掘、深度学习等最新相关技术。  **教学时间分配：**课堂教学：4学时。  六: 高级网络环境中的隐私保护  **重点掌握：**无线传感器网络、社交网络、云计算、边缘计算等新型网络环境中隐私泄漏问题与保护技术。  **教学时间分配：**课堂教学：2学时。  七：安全多方计算理论基础  **重点掌握：** 攻击者模型、通信模型、同态加密技术、零知识证明协议的基本概念。  **教学时间分配：**课堂教学：6学时。  八：安全多方计算基本协议  **重点掌握：**百万富翁协议、不经意传输协议、电路赋值协议、恶意模型和通用组合模型。  **教学时间分配：**课堂教学：6学时。  九：安全多方计算应用问题  **重点掌握：**保护隐私的集合操作问题、向量比较问题、以及在数据挖掘和机器学习中的应用。  **教学时间分配：**课堂教学：6学时。  课程基本要求如下：   1. 掌握隐私保护和安全计算的基础理论，了解先进计算与新型网络环境中的隐私保护与安全计算的最新研究进展； 2. 能够初步进行数据隐私保护与安全计算领域的相关研究，完成课程小论文1篇。   教学环节安排：  本课程无指定教材，以教师课件讲授、论文阅读为主，教学语言为中英双语。课程材料包括课件及相关学术论文。  成绩评定方法：  考勤占比10%，大作业报告占比60%，大作业算法编程占比30%。大作业要求对隐私保护和安全计算相关领域的前沿研究进行综述，并实现和测评2～3个相关算法。 | | | | | | | | |
| 教材或主要参考书目、文献与资料 | 本课程无指定教材；主要参考书目如下：  [1] Privacy-Preserving Data Mining: Models and Algorithms, Aggarwal, Charu C.; Yu, Philip S. Springer, 2008. ISBN: 978-0-387-70991-8.  [2] Secure Multiparty Computation and Secret Sharing - An Information Theoretic Appoach, Ronald Cramer, Ivan Damgaard and Jesper Buus Nielsen. Cambridge Press. 2015. ISBN: 9781107043053. | | | | | | | |