隐私保护理论与实践

Differential Privacy: Theory and Practice

数据隐私的重要性逐渐引起大众重视。接二连三的隐私泄露事件激发了一连串数据发布和分析隐私概念的研究。本课程将介绍十几年来数据隐私保护方面的研究成果和现状。数据隐私非常有挑战性：一方面隐私和隐私保护是社会及法律的概念；另一方面我们需要给出精确的数学定义才能有效地使用技术手段保护数据隐私；同时，保护隐私和保存数据价值也有一定的冲突。

本课程主要介绍数据匿名处理和保护数据隐私的数据发布和分析技术。课程会先介绍如 k-匿名，L-多样性和 t-接近性等概念以及他们的弱点，接下来主要讲述差分隐私（differential privacy）相关概念和技术。差分隐私要求任意两个相邻的输入数据集给出的输出概率分布相近。如使用得当，差分隐私可以起到模拟“自主推出”的效果。

教学团队的三位老师都是数据和系统安全、隐私保护方面的专家。其中课程主讲李宁辉教授是最近两届国际顶级系统安全学术会议 ACM CCS 程序委员会主席，在国际安全研究领域享有崇高的学术地位，王晓阳教授和韩伟力副教授也对这方面有着深入的研究。

教师风采

李宁辉 教授 普渡大学
ninghui@cs.purdue.edu

2000 年于纽约大学获得博士学位，迄今在安全和隐私领域发表了 130 多篇论文。他担任过 IEEE Transactions on Dependable and Secure Computing, Journal of Computer Security, ACM Transactions on Internet Technology 和 Very Large Data Bases Journal 的编辑。为 ACM Special Interest Group on Security, Audit and Control (SIGSAC) 副主席，2014 和 2015 年 ACM 旗舰会议 ACM Conference on Computer and Communications Security (CCS) 程序委员会主席。

王晓阳 教授 复旦大学
xywangCS@fudan.edu.cn

复旦大学计算机学院与软件学院院长、教授、博导，国家千人。1992 年于南加州大学获得博士学位。主要从事时空移动数据分析，数据系统安全及私密，大数据并行式分析方面的研究工作。

韩伟力 副教授 复旦大学
wlhan@fudan.edu.cn

复旦大学软件学院副院长，中国电子学会信息安全专家委员会副主任委员，中国计算机学会上海秘书长，上海市计算机学会信息安全专委会秘书，CCF YOCSEF 上海副主席。2003 年于浙江大学计算机系获得博士学位。研究方向：访问控制；数字身份安全；分布式系统。为国家商用密码管理局 RFID 工作专项组专家成员，International Journal of Communication Systems 副编辑， Security and Communication Networks 客座编辑。曾参与组织多个国际重要学术会议及担任会议程序委员会委员 (SACMAT、ASIACCS、WWW、IEEE POLICY、ACM DIM 等)。

课程设置

学分：2 学分 **学时：**36 学时

上课时间：7 月 11 日 - 7 月 16 日

选课地址：

http://register.fudan.edu.cn/p/publish/show.html?queryType=set&searchName=paidInfo.search&projectId=37728

课程助管：王李霞 电子邮箱：wanglx@fudan.edu.cn

上课地点：张江校区 Z2107 教室

日期	星期	节次	上课内容	授课教师
7/11	一	2-4	什么是数据隐私，数据匿名处理，差分隐私介绍	李宁辉
7/11	一	5-8	隐私保护理论与实践研讨	韩伟力、王晓阳
7/12	二	2-4	差分隐私基本方法，属性，应用场景	李宁辉
7/13	三	2-4	直方图，列联表，频繁项集挖掘	李宁辉
7/13	三	5-8	隐私保护理论与实践研讨	韩伟力、王晓阳
7/14	四	2-4	差分隐私的意义，高级方法	李宁辉
7/15	五	1-4	聚类分析，学习分类器，发布图数据	李宁辉
7/15	五	5-8	隐私保护理论与实践研讨	韩伟力、王晓阳
7/16	六	1-4	差分隐私相关概念，研究课题	李宁辉
7/16	六	5-8	复习、撰写课程报告	韩伟力