



## 计算机科学与技术学院智汇论坛第四期

时间: 2021-11-19 作者: 文章来源: 计算机科学与技术学院 浏览: 520

报告题目: Private Data Analysis with Local Differential Privacy

报告摘要: With the prevalence of big data analytics, service providers are increasing enthusiastic in collecting and analyzing usage data of users to improve their services. However, this comes at the price of privacy risks, not only for users but also for service providers who are vulnerable to internal and external data breaches. Local Differential Privacy (LDP), where each user perturbs her data locally before sending to an untrusted party, is a new and promising privacy-preserving model for individual data collection and analysis. LDP has been deployed in many real products recently by several major software and Internet companies, including Google, Apple and Microsoft. This seminar talk first introduces the rationale of LDP model behind these deployed systems, then surveys the current research landscape in LDP, and finally identifies several open problems and research directions in this community.

主讲人: 叶青青

时 间: 2021年11月22日 上午10:00~11:00

会议ID: 571 841 948



主讲人简介:

Dr. Qingqing Ye is a research assistant professor in the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University. She received her PhD degree in Computer Science from Renmin University of China in 2020. She has received several prestigious awards, including China National Scholarship, Outstanding Doctoral Dissertation Award, and IEEE S&P Student Travel Award. Her research interests include data privacy and security, and adversarial machine learning.

报告题目: 物联网和人工智能中的隐私保护

报告摘要：报告首先介绍物联网和人工智能这两个新兴领域中出现的各类隐私问题，包括个人信息和媒体资料的盗取、人工智能模型和数据被逆向工程等。随后报告目前可以解决这些问题的技术方案，包括差分隐私和联邦学习等。最后将展望这一领域的研究前景和技术趋势。

主讲人：胡海波

时间：2021年11月22日 上午11:00~12:00



主讲人简介：

胡海波博士现为香港理工大学电子及资讯工程学系副教授，信息安全学位课程主任，IEEE和中国计算机学会高级会员，中国计算机学会数据库专委会委员、中国保密协会隐私保护专委会委员。2005年于香港科技大学计算机科学及工程学系获得哲学博士学位。毕业后在香港科技大学和香港浸会大学历任博士后，研究助理教授等职务，2015年起历任香港理工大学资讯工程学系助理教授、副教授。主要研究领域为信息安全、隐私保护、时空数据管理等。作为项目负责人主持多项国家自然科学基金、香港研究资助局及香港创新科技署创新及科技基金项目，总额折合超过2000万港币，并作为主要参与者协同主持参与了国家自然科学基金联合基金重点支持项目、香港研究资助局协作研究基金等大型研究项目，拥有4项美国专利。在国际数据库领域顶级会议和期刊，包括ACM SIGMOD, TODS, IEEE TKDE, TPDS, TIFS, TDSC, TMC, ICDE, S&P, VLDB等发表90余篇学术论文及专著章节，谷歌学术引用数超过3200，H因子31。曾任国际会议DASFAA 2011专题讨论共同主席，CloudDB 2011、DaMEN 2011, 2013程序委员会共同主席，并担任三十余次国际会议如ICDE, VLDB等程序委员会委员，是IEEE TKDE, TPDS, TDSC, TMC, VLDBJ等顶级期刊的长期审稿人。胡海波博士曾获得ACM香港最佳博士论文奖、IEEE MDM 2019等3项国际会议最佳论文奖、IEEE ICDE 2020和VLDB 2018最佳评审奖、微软Imagine Cup、GSI IoT Award及WAIM Distinguished Young Lecturer等多项奖励及荣誉。