NJIT

Department of Computer Science & NJIT Cybersecurity Research Center

IEEE Fellow Distinguished Lecture

Differential Privacy in Practice

Rebecca Wright

Department of Computer Science, Barnard College

Hosts: Shantanu Sharma and Vincent Oria

Date: Wednesday, September 24, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Zoom Link: https://njit-edu.zoom.us/j/95903616720?pwd=UrsFtzLWaZFP0ePgVmqLxAOES8ECNn.1

Abstract:
Introduced by Dwork et al. in 2006, differential privacy (DP) can provide rigorous mathematical guarantees of user privacy. Differential privacy has been a research success and has been adopted by a number of large organizations, including companies like Apple, Google, and Microsoft, as well as the US Census Bureau and the Israeli Ministry of Health. Nonetheless, there are socio-technical challenges that have limited its broad adoption.

In this talk, we will describe some of our work on differential privacy, including a recent our interview-based research study seeking specifically to address the question: for technical individuals newly introduced to differential privacy, which concepts are most challenging to grasp, and what factors contribute to these challenges? We will also discuss the use of differential privacy for generating synthetic location data.

Bio:
Dr. Rebecca Wright is the Druckenmiller Professor of Computer Science and Director of the Vagelos Computational Science Center at Barnard College. Prior to joining Barnard, she was a professor in the Computer Science Department and Director of DIMACS at Rutgers, a professor in the Computer Science Department at Stevens Institute of Technology in Hoboken, New Jersey, and a researcher in the Secure Systems Research Department at AT&T Labs and AT&T Bell Labs. Her research is primarily in the area of information security, including cryptography, privacy, foundations of computer security, and fault-tolerant distributed computing. Recent work includes accountability, differential privacy, privacy-preserving data mining, and secure multiparty approximations. Her ongoing research goals are the design of protocols, systems, and services that perform their specified computational or communication functions even if some of the participants or underlying components behave maliciously, and that balance individual needs such as privacy with collective needs such as network survivability and public safety.

Dr. Wright serves as an editor of the International Journal of Information and Computer Security and the Transactions on Data Privacy. She is a member of the board of the Computing Research Association's Committee on Widening Participation in Computing Research (CRA-WP). She was a member of the board of directors of the International Association for Cryptologic Research from 2001 to 2005 and the steering committee of the Information Security Conference from 2006 to 2010, and an editor of the Journal of Computer Security from 2001 to 2011. She was Program Chair of Financial Cryptography 2003 and the 2006 ACM Conference on Computer and Communications Security (CCS) and General Chair of Crypto 2002. She has served on numerous program committees, including Crypto, the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, and the Usenix Security Symposium. She received a Ph.D. in Computer Science from Yale University in 1994 and a B.A. from Columbia University in 1988. She received an honorary M.E. from Stevens Institute of Technology in 2006. She is a Fellow of the IEEE and a Distinguished Member of the ACM.