TEXAS A&M Institute of Data Science

TAMIDS Seminar Series

Center for Approximation and Mathematical Data Analytics (CAMDA)
Department of Mathematics

Mathematical Methods for Privacy-Preserving Machine Learning

In a world where artificial intelligence and data science become omnipresent, data sharing is increasingly locking horns with data-privacy concerns. Among the main data privacy concepts that have emerged are anonymization and differential privacy. Today, another solution is gaining traction—synthetic data. The goal of synthetic data is to create an as-realistic-as-possible dataset, one that not only maintains the nuances of the original data, but does so without risk of exposing sensitive information. The combination of differential privacy with synthetic data has been suggested as a best-of-both-worlds solution. However, the road to privacy is paved with NP-hard problems. The speaker will present three recent mathematical breakthroughs in the NP-hard challenge of creating synthetic data that come with provable privacy and utility guarantees and doing so computationally efficiently. These efforts draw from a wide range of mathematical concepts, including Boolean Fourier analysis, duality, empirical processes, and microaggregation. For instance, one will see some surprising connections between theoretical probability and anonymization. The speaker will also present the first noisefree method to achieve differential privacy. This is joint work with March Boedihardjo and Roman Vershynin.

Thomas Strohmer, Ph.D.

Professor, Department of Mathematics
Director, Center of Data Science and Artificial Intelligence Research
University of California, Davis

Date: Monday, Oct 11, 2021
Time: 1:50 – 2:40 p.m. US Central Time
Zoom Meeting ID: 998 4499 3279
Passcode: 724615
Faculty host: Simon Foucart, MATH

Biography

Dr. Thomas Strohmer is Professor of Mathematics and Director of the Center of Data Science and Artificial Intelligence Research at the University of California, Davis. He got his M.S. and Ph.D. in Mathematics in 1991 and 1994 respectively from the University of Vienna, Austria. He spent one year as Erwin-Schroedinger fellow at the Department of Statistics at Stanford University. His research interests are in data science, machine learning, applied harmonic analysis, numerical analysis, digital signal processing, and information theory. He received several Best Paper awards for his research. He also serves as consultant to industry in the areas of artificial intelligence, medicine, image processing, and telecommunications.

You can also click this link to join the seminar https://tamu.zoom.us/j/99844993279?pwd=TkJodWFVRURyMmkwakI4SWZGeVJTQT09

TEXAS A&M UNIVERSITY | TEXAS A&M AGRILIFE | TEES Texas A&M Engineering Experiment Station

For more information about TAMIDS seminar series, please contact Ms. Jennifer South at jsouth@tamu.edu