Pacific Institute *for the* Mathematical Sciences

Thursday, August 25, 2022
Talk @ 3:30 pm
Followed by reception @ 4:30 pm

Bob Wright Centre – BWC A104
University of Victoria

Gautam Kamath
Cheriton School of Computer Science
University of Waterloo

Statistical Estimation with Differential Privacy

Naively implemented, statistical procedures are prone to leaking information about their training data, which can be problematic if the data is sensitive. Differential privacy, a rigorous notion of data privacy, offers a principled framework to dealing with these issues. I will survey recent results in differential private statistical estimation, presenting a few vignettes which highlight novel challenges for even the most fundamental problems, and suggesting solutions to address them. Along the way, I'll mention connections to tools and techniques in a number of fields, including information theory and robust statistics.