CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, Edificio Norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

AGCO Seminar

Speakers: Victor Sanches Portella, IME-USP.

***Title*:** Fingerprinting Techniques for Lower Bounds in Differential Privacy and a New Fingerprinting Lemm

Abstract:

Analyzing sensitive data presents a fundamental dilemma: how can we extract population-level insights while protecting individual privacy? Differential Privacy (DP) provides a rigorous mathematical framework to address this challenge, offering formal guarantees against sensitive data exposure. Beyond its widespread adoption in practice, DP has revealed surprising connections to various fields like online learning, machine learning generalization, and robust statistics.

In this talk, I'll provide a brief introduction to the core ideas of differential privacy. I will then give an overview of fingerprinting techniques, a powerful tool for proving lower bounds for DP problems. Finally, I'll present a recent work of mine with Professor Nick Harvey from the University of British Columbia, where we expand upon these techniques to establish tight lower bounds for privately estimating Gaussian covariance matrices. A key technical challenge is handling the dependencies between the parameters being estimated. I will show how we leverage the Stein-Haff identity to overcome this issue, and how this work suggests a way to use Stokes' theorem as a more general tool to circumvent this kind of obstacle.

***When*:** October 01, **3:00 pm - 4:00 pm.**

***Where*:** Sala 1, Edificio Felipe Villanueva, Campus San Joaquín, UC.