DOUG STINSON, University of Waterloo

Block designs and protocols for local differential privacy

There has been considerable recent interest in using block designs in the design of protocols for local differential privacy. The goal is to provide privacy for people reporting possibly sensitive data while still enabling an underlying probability distribution to be accurately estimated. The basic idea goes back to the "randomized response" method proposed by Warner in 1965, where each participant reports a correct yes-no response with some prespecified probability $\theta > 1/2$ and an incorrect response with probability $1 - \theta$. In this talk, I will review recent research by a variety of authors that employs BIBDs as a randomization mechanism when data having multiple possible values is being aggregated. This research is joint work with Maura Paterson.