Date: Friday, 31 July 2020

Time: 3:00pm – 4:00pm

Speaker: Professor Annabelle McIver (Macquarie University, Department of Computer Science)

Venue: Zoom

Title: The Category of Correlations

Abstract: Designing programs that do not leak confidential information continues to be a challenge. Part of the difficulty arises when partial information leaks are inevitable, implying that design interventions can only limit rather than eliminate their impact. We show, by example, how to gain a better understanding of the consequences of information leaks by modelling what adversaries might be able to do with any leaked information. The presentation is based on the theory of Quantitative Information Flow, and uses the well-known probability monad to provide an information-flow aware semantics for a small programming language. We will explore some properties of the language and demonstrate that "correlations" rather than the more familiar "prior/posterior" probabilities of Bayesian reasoning are fundamental to understanding how information leaks in programs.