MICHELE MOSCA, University of Waterloo/Perimeter Institute, Waterloo
Quantum Key Agreement in a Classical World

Quantum key distribution (QKD) promises secure key agreement by using quantum mechanical systems. Assuming practical and affordable QKD systems become widely available, what role will QKD play in future cryptographic infrastructures?

QKD can provide long-term confidentiality for encrypted information without reliance on computational assumptions. Will anyone really care?

Like classical key establishment protocols, QKD requires authentication to prevent man-in-the-middle attacks. If authentication is achieved using a short shared secret key, one can regard QKD as a form of key expansion. If one is willing to accept some conservative computational assumptions, does QKD still add any value?

I will discuss these and related questions and present situations where QKD can add practical value. I will ask the audience some questions too.