Theory of Quantum Cryptography

Claude Crépeau (crepeau@cs.mcgill.ca)
McGill University
School of Computer Science
McConnell Building
3480 University Street
Montréal, Québec
H3A 2A7, Canada

Abstract.

The basic notion of Quantum Key Distribution will first be discussed. Then, information theoretical notions of cryptography over quantum states such as encryption and authentication will be covered. Computational analogues will also be presented: quantum public key-cryptography, public-key authentication and the impossibility of quantum digital signatures. Two-party and multi-party computations over classical and quantum data will finally be described.