Quantum communication and quantum computing

Peter L. Knight, Imperial College London, United Kingdom

Quantum mechanics offers the information scientist a new rich resource, which is only recently being tapped to allow for secure communication in the form of quantum cryptography, and for tremendous parallelism in quantum information processing and computing. I will describe developments and prospects for each. Quantum cryptography has already advanced beyond the research laboratory to become a realizable technology with proven secret key distribution for encryption. Quantum computing, although at an earlier stage of development has been recognized as a major new development in physics, enables us (if a quantum computer is realizable) to attack problems previously thought to be too complex for normal computation in a reasonable time. Examples of quantum algorithms involving this kind of advantage are Shor’s for fast factorization (in itself a threat to secure communication) and Grover’s for data base searching. I will discuss the ways quantum mechanics allow such a speed-up, stressing how quantum entanglement is the key resource being exploited, and how quantum gates, networks, and the processors may be implemented in a realistically noisy environment. Simple demonstrators have already been built, and I will discuss prospects for future realization of large-scale processors.