MAR11-2010-002892

Abstract for an Invited Paper
for the MAR11 Meeting of
the American Physical Society

Twenty Seven Years of Quantum Cryptography!

RICHARD HUGHES, Los Alamos National Laboratory

One of the fundamental goals of cryptographic research is to minimize the assumptions underlying the protocols that enable secure communications between pairs or groups of users. In 1984, building on earlier research by Stephen Wiesner, Charles Bennett and Gilles Brassard showed how quantum physics could be harnessed to provide information-theoretic security for protocols such as the distribution of cryptographic keys, which enables two parties to secure their conventional communications. Bennett and Brassard and colleagues performed a proof-of-principle quantum key distribution (QKD) experiment with single-photon quantum state transmission over a 32-cm air path in 1991. This seminal experiment led other researchers to explore QKD in optical fibers and over line-of-sight outdoor atmospheric paths ("free-space"), resulting in dramatic increases in range, bit rate and security. These advances have been enabled by improvements in sources and single-photon detectors. Also in 1991 Artur Ekert showed how the security of QKD could be related to quantum entanglement. This insight led to a deeper understanding and proof of QKD security with practical sources and detectors in the presence of transmission loss and channel noise. Today, QKD has been implemented over ranges much greater than 100km in both fiber and free-space, multi-node network testbeds have been demonstrated, and satellite-based QKD is under study in several countries. "Quantum hacking" researchers have shown the importance of extending security considerations to the classical devices that produce and detect the photon quantum states. New quantum cryptographic protocols such as secure identification have been proposed, and others such as quantum secret splitting have been demonstrated. It is now possible to envision quantum cryptography providing a more secure alternative to present-day cryptographic methods for many secure communications functions. My talk will survey these remarkable developments.