4CF07-2007-000021

Abstract for an Invited Paper
for the 4CF07 Meeting of
the American Physical Society

Twenty two years of quantum key distribution

RICHARD HUGHES, Los Alamos National Laboratory

Following their 1984 invention of quantum key distribution (QKD), Bennett and Brassard and colleagues performed a proof-of-principle QKD transmission over a 32-cm air path in 1991. This seminal experiment led other researchers to explore implementations of QKD in optical fibers and over line-of-sight outdoor atmospheric paths ("free-space"), resulting in dramatic increases in range, secret bit rate, security and availability. These advances have led to, and been enabled by, improvements in sources, single-photon detectors and the deeper understanding of QKD security with practical sources and detectors in the presence of transmission loss and channel noise. Today, QKD has been implemented with unconditional security over ranges greater than 100km, over multi-kilometer distances in high background environments in both fiber and free-space, and at high (GHz) clock rates over shorter distances. In my talk I will review the key enabling advances underlying these developments of experimental QKD over the past 16 years, describe the present status of the field, and compare and contrast different approaches to implementing security against photon number splitting attacks. I will describe some recent results from QKD in dedicated ("dark") optical fiber using ultra-high efficiency, low-noise transition edge sensor (TES) photo-detectors, achieving ultra-long transmission distances, and unconditional security over 107km through the use of a decoy-state protocol. I will also describe progress in making QKD compatible with all-optical fiber networks, including the co-existence of QKD signals with conventional optical data on the same fiber. I will conclude my talk with a survey of the prospects for QKD transmission distances exceeding 200km, which will include a comparison of the various single-photon detector technologies now becoming available for quantum communications.