MAR14-2013-008939

Abstract for an Invited Paper
for the MAR14 Meeting of
the American Physical Society

Network-Centric Quantum Communications

RICHARD HUGHES, Los Alamos Natl Lab

Single-photon quantum communications (QC) offers "future-proof" cryptographic security rooted in the laws of physics. Today's quantum-secured communications cannot be compromised by unanticipated future technological advances. But to date, QC has only existed in point-to-point instantiations that have limited ability to address the cyber security challenges of our increasingly networked world. In my talk I will describe a fundamentally new paradigm of network-centric quantum communications (NQC) that leverages the network to bring scalable, QC-based security to user groups that may have no direct user-to-user QC connectivity. With QC links only between each of N users and a trusted network node, NQC brings quantum security to N^2 user pairs, and to multi-user groups. I will describe a novel integrated photonics quantum smartcard ("QKarD") and its operation in a multi-node NQC test bed. The QKarDs are used to implement the quantum cryptographic protocols of quantum identification, quantum key distribution and quantum secret splitting. I will explain how these cryptographic primitives are used to provide key management for encryption, authentication, and non-repudiation for user-to-user communications. My talk will conclude with a description of a recent demonstration that QC can meet both the security and quality-of-service (latency) requirements for electric grid control commands and data. These requirements cannot be met simultaneously with present-day cryptography.