Abstract Submitted
for the MAR12 Meeting of
The American Physical Society

Quantum network with trusted and untrusted relays XIONGFENG MA, University of Toronto, RAZIEH ANNABESTANI, University of Waterloo, CHI-HANG FRED FUNG, University of Hong Kong, HOI-KWONG LO, University of Toronto, NORBERT LÜTKENHAUS, DAVID PITKÄNEN, University of Waterloo, MOHSEN RAZAVI, University of Leeds — Quantum key distribution offers two distant users to establish a random secure key by exploiting properties of quantum mechanics, whose security has proven in theory. In practice, many lab and field demonstrations have been performed in the last 20 years. Nowadays, quantum network with quantum key distribution systems are tested around the world, such as in China, Europe, Japan and US. In this talk, I will give a brief introduction of recent development for quantum network. For the untrusted relay part, I will introduce the measurement-device-independent quantum key distribution scheme and a quantum relay with linear optics. The security of such scheme is proven without assumptions on the detection devices, where most of quantum hacking strategies are launched. This scheme can be realized with current technology. For the trusted relay part, I will introduce so-called delayed privacy amplification, with which no error correction and privacy amplification is necessarily to be performed between users and the relay. In this way, classical communications and computational power requirement on the relay site will be reduced.

Xiongfeng Ma
University of Toronto

Date submitted: 07 Dec 2011 Electronic form version 1.4