Memory-assisted quantum key distribution

Mohsen Razavi
University of Leeds, UK

Abstract

Conventional quantum key distribution (QKD) links are often limited in reach to a few hundreds of kilometres at which point their secret key generation rates approach zero. One solution to long-distance QKD relies on using *trusted* intermediate nodes to break the distance into shorter segments. If the trust requirement cannot be met, one then needs to use the quantum repeater approach by which entangled states can be distributed over long distances. Quantum repeaters, however, require quantum memory modules and/or advanced quantum gates with specifications not attainable with today's technology. Here I describe a memory-assisted QKD system where by using *imperfect* quantum memories, with specifications very close to what we can achieve today, we can beat in distance and rate existing conventional QKD links that do not use quantum memories. This offers an intermediary solution to moderately long-distance QKD until quantum repeaters become operational.