Fully Connected QKD Network on Time Shared Entanglement Distribution

A Ponasenko[1], V Rodimin[1], J Singh[1], V Revici[1], R Piera[1], A Pereszlenyi[1], J A Grieve[1], and Y Kurochkin[1]

[1] *Quantum communications, TII, Abu Dhabi, United Arab Emirates*
Contact Email: yury.kurochkin@tii.ae

Quantum networks are rapidly moving from research laboratories to the field applications. Most quantum networks are built on the trusted node approach because Quantum key distribution (QKD) distance is limited by photon loss and lower distance full mesh quantum networks will require N(N-1)/2 dark fiber lines where N is the number of participants. Telecom operators who are now the most active players in quantum networking become trusted node holders which can become an additional barrier for quantum networks adoption. An alternative solution is to use entanglement on the city scale quantum networks. In this case the Telecom operator combines a photon pair source with an optical switch. Network orchestrator software receives requests from users to have key pairs and configure optical networks with MEMS 2xN optical switch. In this case the network literally sells photon pairs to the clients which are making passive measurement of polarization encoded quantum states. Such a scheme has potential advantages - only receivers need to be certified while entanglement sources remain untrusted.

In our work we demonstrated it on the three node network. The Center of the network is the PPLN based source of polarization entangled states at 1310 and 1316 nm. Outputs of the source are connected to a 2×32 optical switch capable of connecting any two users in pairs. To make a receiver capable of both photon measurements we make 2 wavelength bragg filters allowing us to measure photons in both wavelengths with 2-nm bandwidth. Receivers are designed fully passive – fiber connected to the free space BBM92 polarization projection system followed by single photon detectors and time tagger. Polarization distortion is compensated with a fiber based polarization controller on the source side using publicly announced QBER. Key is followed by standard procedures of sifting, Cascade error correction and finite key privacy amplification. Derived keys are uploaded to 10G L2/L3 encryptors capable of building quantum-secure VPN tunnels between any participants. Here is the result of a fiber spool QKD test when one node is located at an entangled pair source location and two others are 10 km away.

A2 (10 km) - A1 (direct). QBER ∼2.8%, Secret key rate ∼125 b/s

A3 (10 km) - A2 (10 km). QBER ∼4.8%, Secret key rate ∼70 b/s

A3 (10 km) - A1 (direct). QBER ∼3.9%, Secret key rate ∼100 b/s

As soon as 10G encryptor consumes one 256 bit key per two minute, 2.2 bit per second is enough to maintain one connection. If one wants to feed all 32 node networks it should produce on average 70 bits per second what corresponds to the presented result.