Secure quantum communication with nanowire quantum dots

Michael E. Reimer

Quantum key distribution (QKD) utilizes the fundamental laws of quantum mechanics to share a key between remote parties for secure communication. Secure communication over long distances can be made possible by using satellite QKD. Even more impressively, this holds the potential to take secure communication over long distances to a level never seen before, allowing communication to remain secure from one side of the globe to the other. Up to now, attenuated lasers were used as the main source to generate the secure key by using weak coherent pulses and a decoy-state protocol. However, such sources add cost on signal processing and channel noise due to multi-photon emission events. Problematically, this constrains the secure key length under high channel losses and limited key exchange duration. In this talk, I will show that these limitations can be overcome by using a semiconductor quantum dot that generates single photon pulses with high efficiency and low multiphoton emission.

In our work we utilize a semiconductor quantum dot within a nanowire waveguide to enhance the extraction efficiency as compared to a bare quantum dot in the bulk and minimize the multiphoton emission to below 10^{-6}. Using this quantum dot single-photon source we show that it is possible to generate a key length per satellite pass that is up to one order of magnitude higher than that of a weak coherent pulse QKD link with the same laser repetition rate. This shows that under the same channel conditions and pulse frequency, a BB84 QKD protocol using a quantum dot single-photon source impressively outperforms a decoy-state QKD protocol using a faint laser source. Additionally, in some instances the quantum dot could enable key generation where an attenuated source would simply fail [1].

I will also discuss how these nanowire quantum dots can be used to generate pairs of entangled photons, another important resource for secure quantum communication. I will present our recent progress for integrating such sources with quantum memories for fiber-based quantum networks and our recent work towards achieving entangled photons with near-unity efficiency and fidelity [2]. In quantum dots, the entanglement fidelity is generally degraded by an asymmetric quantum dot confining potential caused by the dot shape and composition. Two approaches will be presented to remove the effect of the asymmetric confining potential on the entanglement fidelity. First, we demonstrate a novel optical approach based on emulating fast rotating waveplates with on-chip electroabsorption modulators to remove the effect of the confining potential on the entanglement fidelity after the photons have been emitted [3] and second, we show that electrostatic gates precisely positioned around the dot can be utilized to apply a quadrupole field to it, thus ensuring the entanglement fidelity is enhanced towards unity [4].

References

[1] P. Chaiwongkhot *et al.*, Enhancing secure key rates of satellite QKD using a quantum dot single-photon source, arXiv:2009.11818 (2020).

[2] A. Fognini, A. Ahmadi, M. Zeeshan, J.T. Fokkens, S.J. Gibson, N. Sherlekar, S.J. Daley, D. Dalacu, P.J. Poole, K.D. Jöns, V. Zwiller, and M.E. Reimer, Dephasing free photon entanglement with a quantum dot, *ACS Photonics* **6** (7), 1656-1663 (2019).

[3] A. Fognini, A. Ahmadi, S.J. Daley, M.E. Reimer, and V. Zwiller, Universal fine-structure eraser for quantum dots, *Optics express* **26** (19), 24487-24496 (2018).

[4] M. Zeeshan, N. Sherlekar, A. Ahmadi, R.L. Williams, and M.E. Reimer, Proposed scheme to generate bright entangled photon pairs by application of a quadrupole field to a single quantum dot, *Phys. Rev. Lett.* **122** (22), 227401 (2019).