Telecom quantum key distribution with a quantum dot

HERIOT WATT UNIVERSITY

Author: Frederik Brooke Barnes
Supervisors: Brian Geradot, Alessandro Fedrizzi
Date of registration: 1 September 2021
Institute: Institute of Photonics & Quantum Sciences

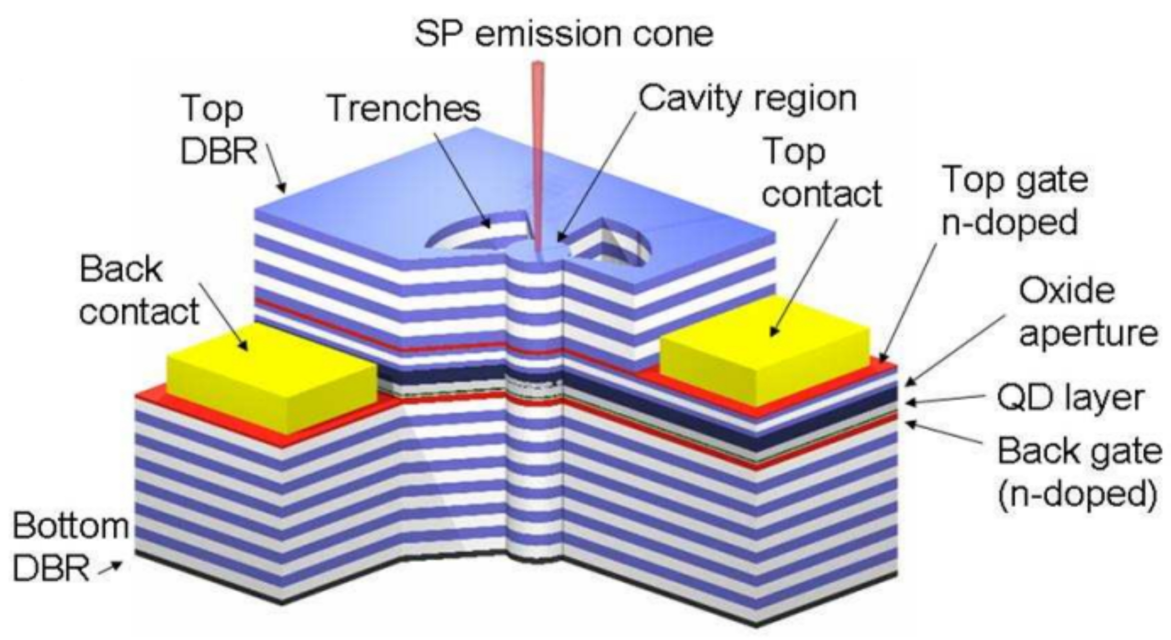
Overview

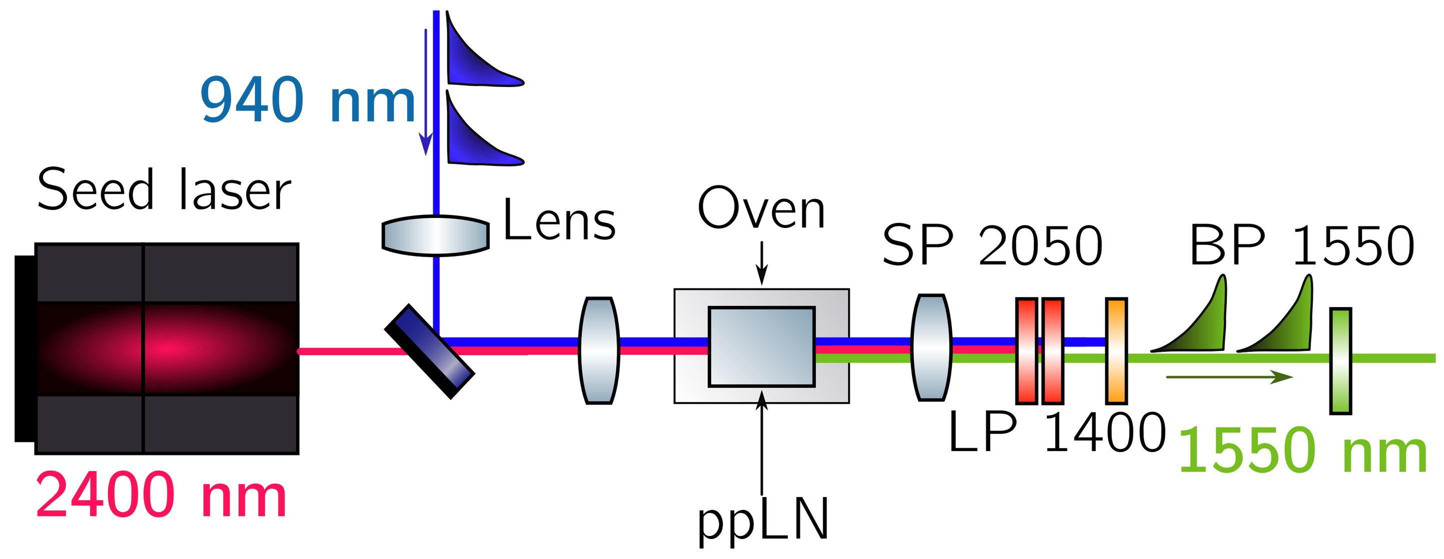
Quantum key distribution (QKD) promises information-theoretic secure communications [1]. This security relies on the impossibility of perfectly learning the quantum state of a single photon. We use a bright quantum dot (QD), frequency converted to telecom wavelength, as a single photon source. We achieve secure keys over 175 km of fibre, and high key rates, while considering the effect of finite key sizes.

Quantum dot

We use a self-assembled InGaAs/GaAs QD in a micropillar cavity [2] to produce low-noise, coherent 940 nm single photons. The QD is excited quasi-resonantly using a time-multiplexed, pulsed Ti:Sapphire laser at a repetition rate of 160 MHz. The single photons are filtered from the excitation laser using polarisation extinction.

- Counts: 5 MHz
- $g^2(0)$: 2.0 %
- V_{HOM}: 88 %





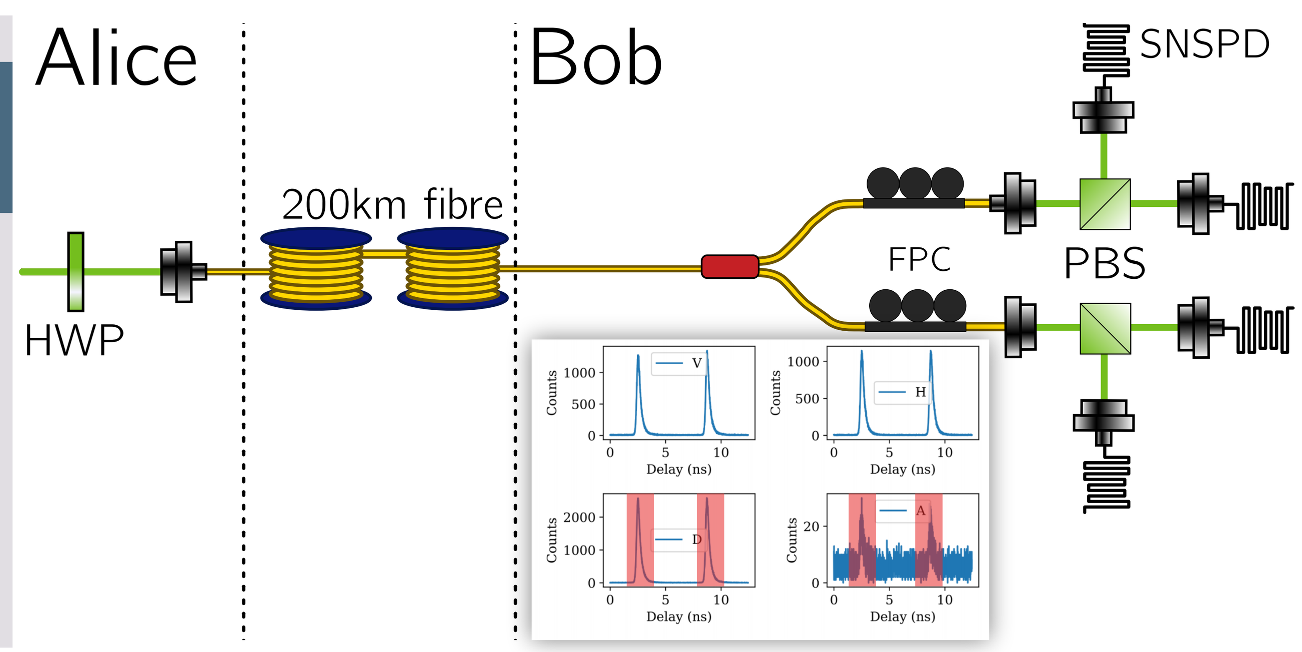
Quantum frequency conversion

The best performing QDs emit near 900 nm [3]. For transmission over long distances of optical fibre, 1550 nm is required. Type 0 difference frequency generation is used to convert 940 nm photons to 1550 nm through three-wave mixing with a home-built 2400 nm seed laser in a periodically-poled lithium-niobate crystal (ppLN) [4].

- Counts: 1.7 MHz
- $g^2(0)$: 3.6 %
- Coherent

Quantum key distribution

The BB84 protocol [1] is used to share keys between Alice and Bob over telecom fibre. Alice prepares polarisation states (H,V,A,D) and Bob performs measurements in the Z- and X-basis. Measurements are made using superconducting nanowire single photon detectors (SNSPDs) and time-gated to optimise quantum bit error rate (QBER). An improved analysis of the finite key rate (FKR) for single photon sources is used [5], demonstrating a significant improvement when acquiring secret keys in practical time scales - in contrast to asymptotic key rates (AKR) [1] which require an infinite key length and measurement time.



Results

$$\mathrm{FKR} = \frac{1}{N_S}\left[\underline{\mathrm{N}}^X_{R,nmp}\left(1 - H\left(\bar{\phi}^X\right)\right) - \lambda_{EC} - 2\log_2\frac{1}{2\varepsilon_{PA}} - \log_2\frac{2}{\varepsilon_{cor}}\right]$$

$$\mathrm{AKR} = p_{\mathrm{click}}\left[A\left(1 - H\left(\frac{e_X}{A}\right)\right) - f_{\mathrm{EC}}(e_Z)H(e_Z)\right]$$

Practical impact

Want a 1 kbit key in 1 second?

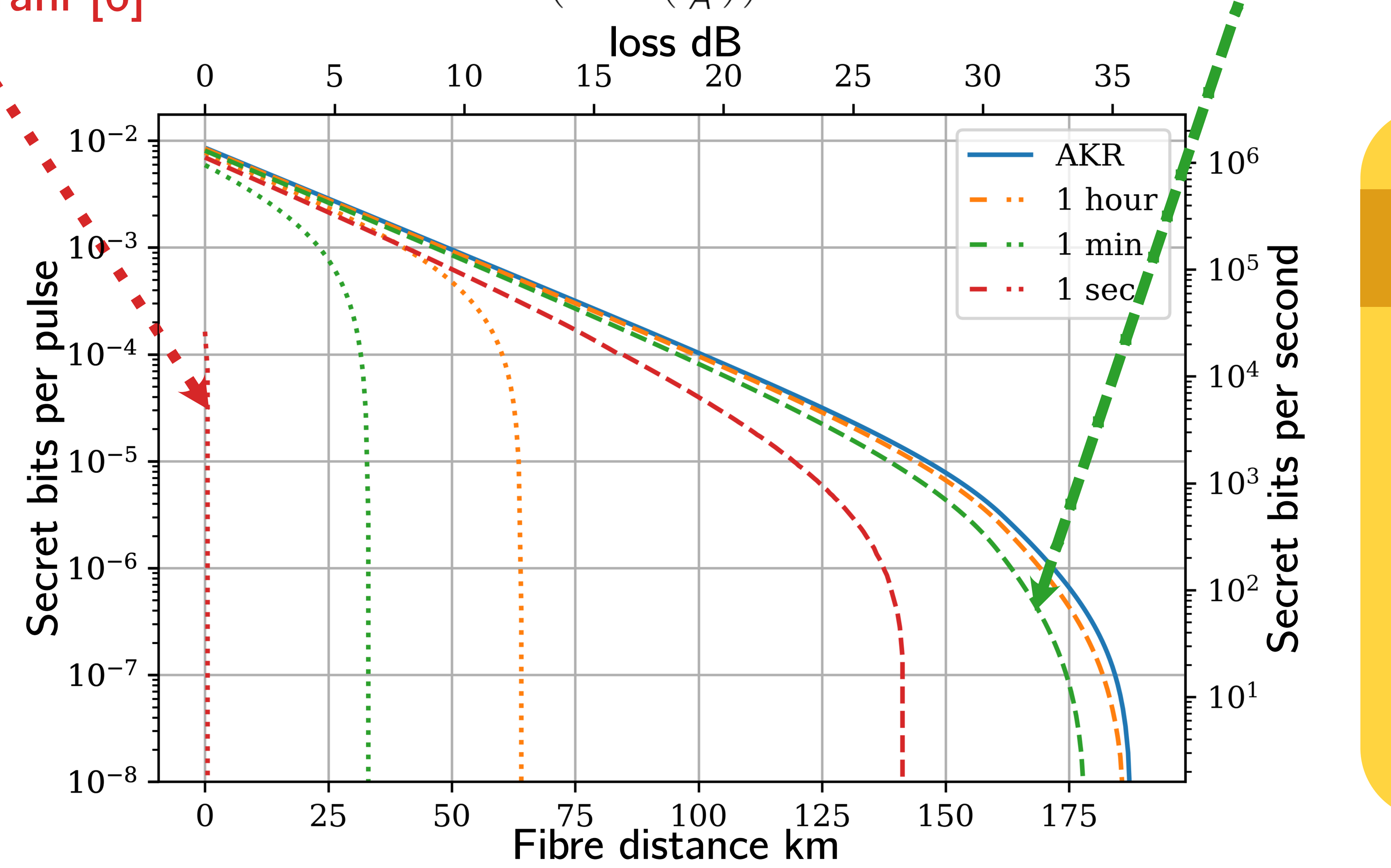
1 km → 125 km

Want 100 kbit/s over 50km?

1 hour → 1 second

Time required to reach 90% AKR at 125 km?

10,000 years → 1 hour



Next steps?

Decoy state protocols

Measurement device independent protocols

Inhomogeneous networks

References

[1] Quant. Inf. Comput. 5, 325 (2004). [2] Nature Photonics 1, 704 (2007). [3] Nature Nanotech 12, 1026–1039 (2017) [4] Appl. Phys. Lett. 118, 174003 (2021), [5] Pre-print available, [6] NJP, 11, 045024 (2009)

Acknowledgements

University of California at Santa Barbara: Nick G. Stoltz, Dirk Bouwmeester
University of Strathclyde, Glasgow: Roberto G. Pousa, John Jeffers, Daniel K. L.Oi
Heriot-Watt University: Christopher L. Morrison, Francesco Graffiti, Zhe Xian Koong, Peter Barrow, Brian Geradot, Alessandro Fedrizzi