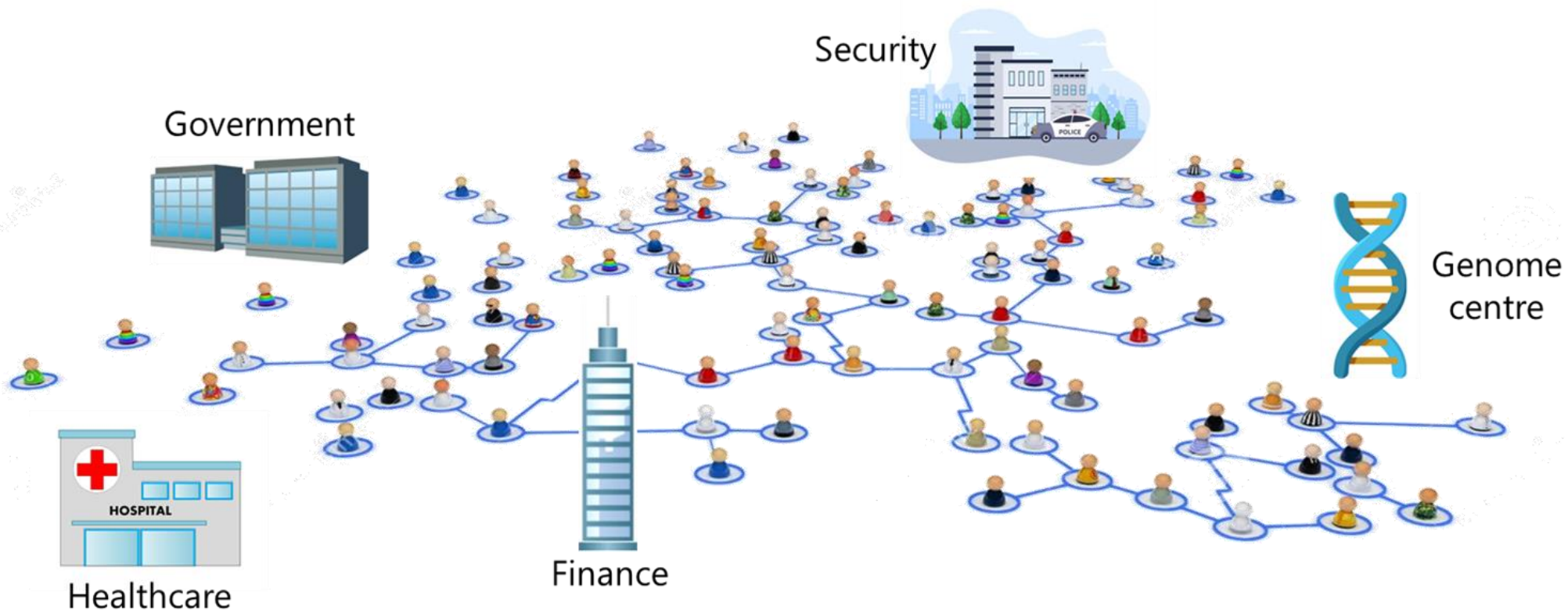
White Rabbit Time Synchronisation for Quantum Communications

Karolina Schatz

PhD Student (Supervisor: Prof Marco Lucamarini)
School of Physics, Engineering and Technology;
University of York & York Centre for Quantum Technologies

karolina.schatz@york.ac.uk

Why Quantum Communications?



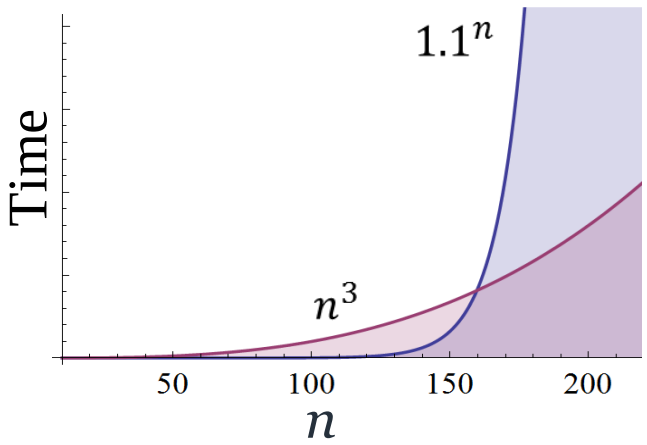
Future-proof cryptography is needed for
long-term information security

© 2024 University of York

Current cryptographic model

Exponential speed-up in factoring!

breaks

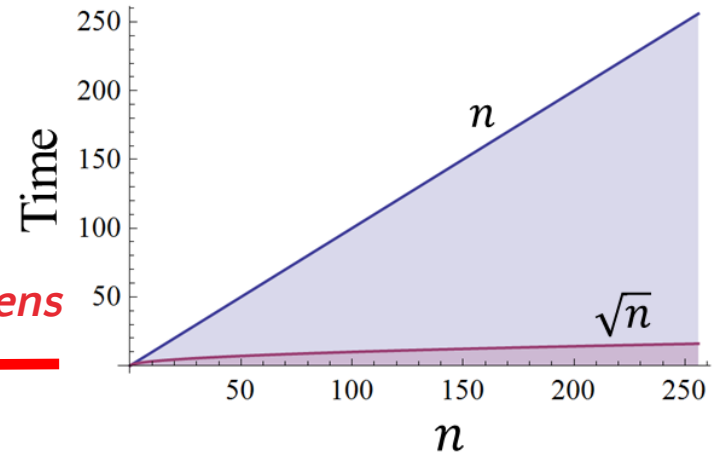


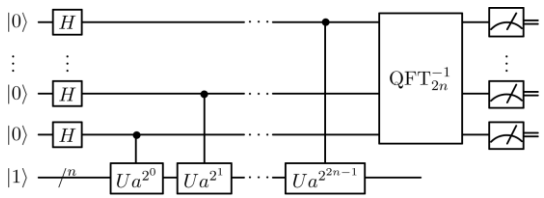
- Public Key Agreement
- Session Key Agreement
- Encryption

AES

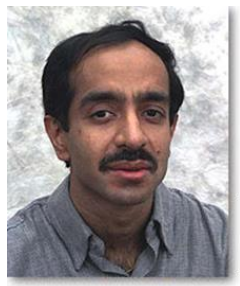
weakens

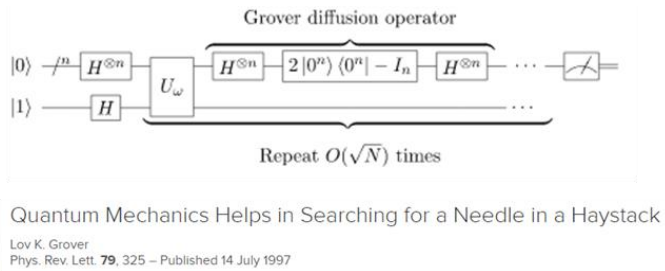
Quadratic speed-up in searching!





P. W. Shor, **Algorithms for quantum computation: Discrete logarithms and factoring,** *Proc. 35nd Annual Symposium on Foundations of Computer Science* (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.





Quantum Mechanics Helps in Searching for a Needle in a Haystack

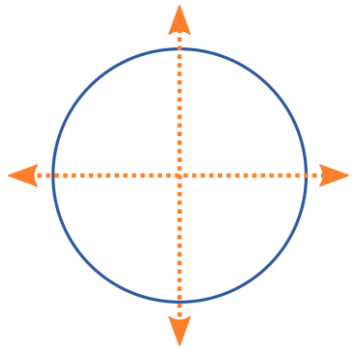
Lov K. Grover
Phys. Rev. Lett. **79**, 325 – Published 14 July 1997

© 2024 University of York

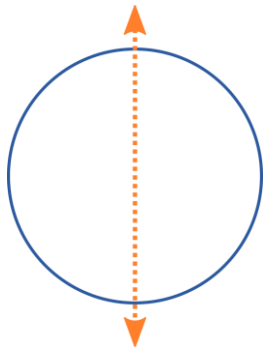
Quantum Superposition and Entanglement

Superposition

$$|\psi\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$$



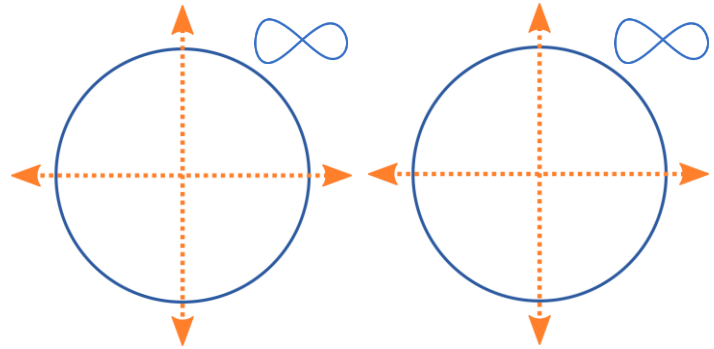
$$|\psi'\rangle = |V\rangle$$



A superposition collapses to a **random** single state upon observation

Entanglement

$$|\psi\rangle = \frac{|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2}{\sqrt{2}}$$

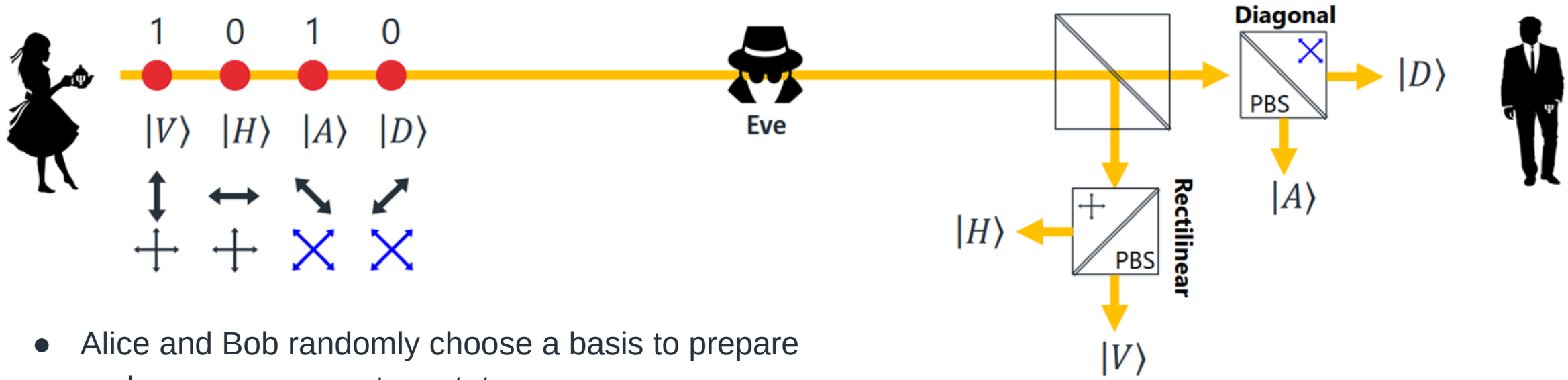


$$|\psi'\rangle = |V\rangle_1|V\rangle_2$$

An entangled state collapses **randomly & collectively** to constituent states, even when the individual particles are **physically distant**

© 2024 University of York

Quantum Key Distribution (BB84)



- Alice and Bob randomly choose a basis to prepare and measure a quantum state
- Only if they chose the same basis does the quantum state remain undisturbed
- Alice and Bob publicly communicate what bases they chose after they measure
- In the cases where their bases agree, they can extract a secret key bit

Eve sometimes will get the choice of basis wrong and find/collapse a superposition. She introduces errors!

Quantum Bit Error Rate (QBER)
BB84: QBER ≤ 11 %

G. Brassard, “Brief history of quantum cryptography: a personal perspective,” https://arxiv.org/abs/quant-ph/0604072

C. H. Bennett and G. Brassard, “Public key distribution and coin tossing” doi: 10.1016/j.tcs.2014.05.025.

© 2024 University of York

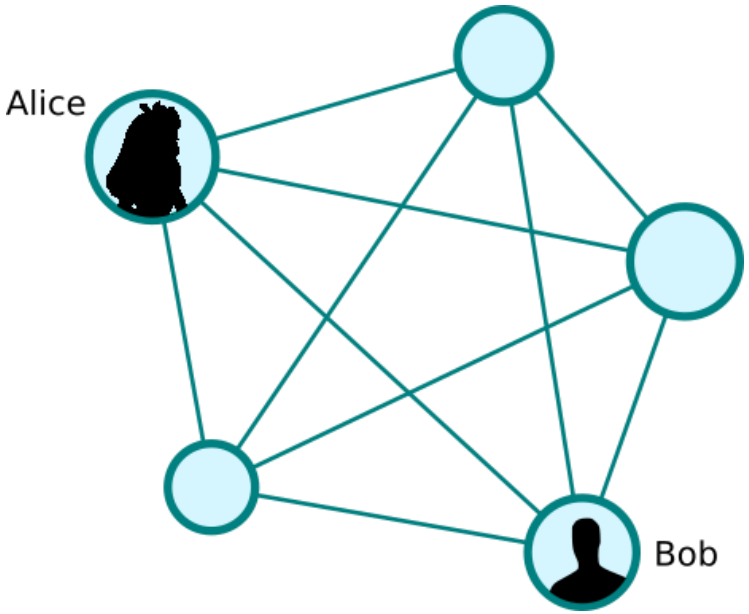
White Rabbit Time Synchronisation for QKD

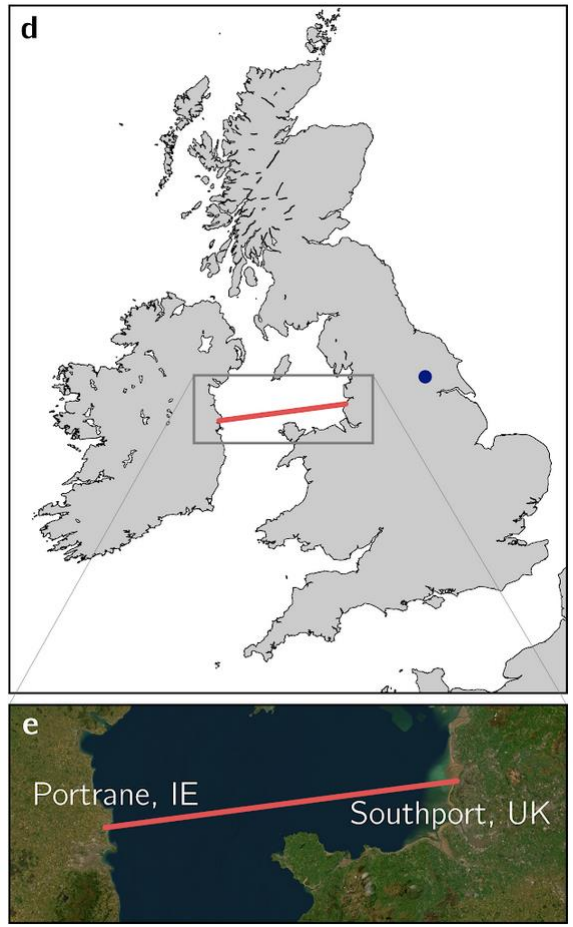
Temporal filtering is essential to achieve a low QBER

Specific QKD Timing Requirements:

- Precise synchronisation
- Low timing jitter
- High stability
- T_0 agreement
- Scalability
- Integrability with QKD

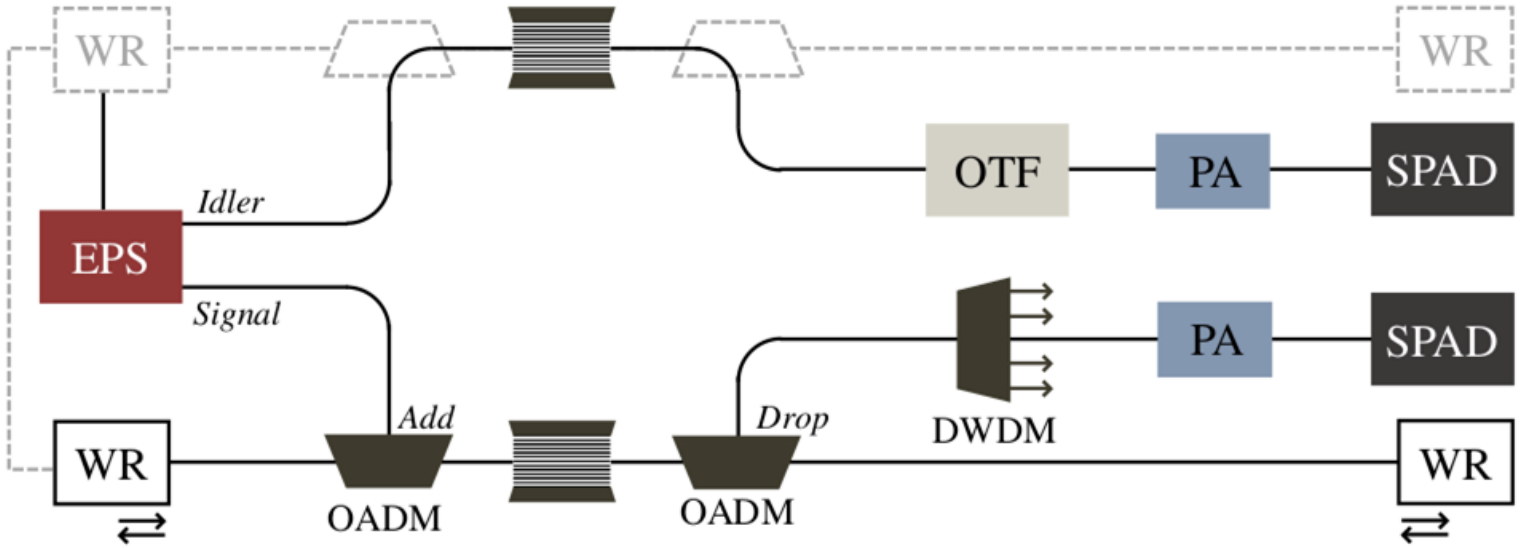
Two regimes of interest at York:



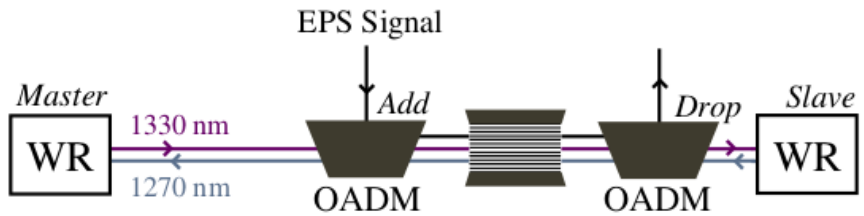


© 2024 University of York

White Rabbit and Entanglement Coexistence



- Quantum signal is added to and dropped from an active WR communication line
- Co-propagation of WR and entangled photons for 1km of SMF
- DWDM passively splits to different end users (Bob, Charlie…)
- Tunable filter allows Alice to address specific DWDM channels

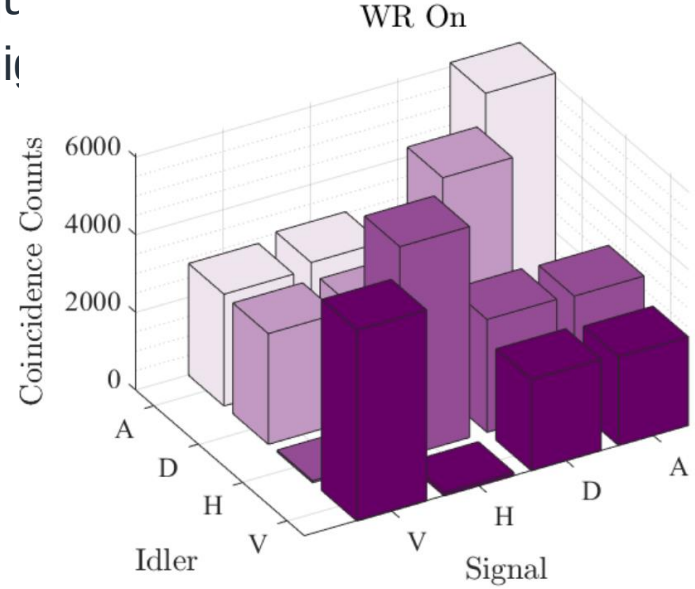


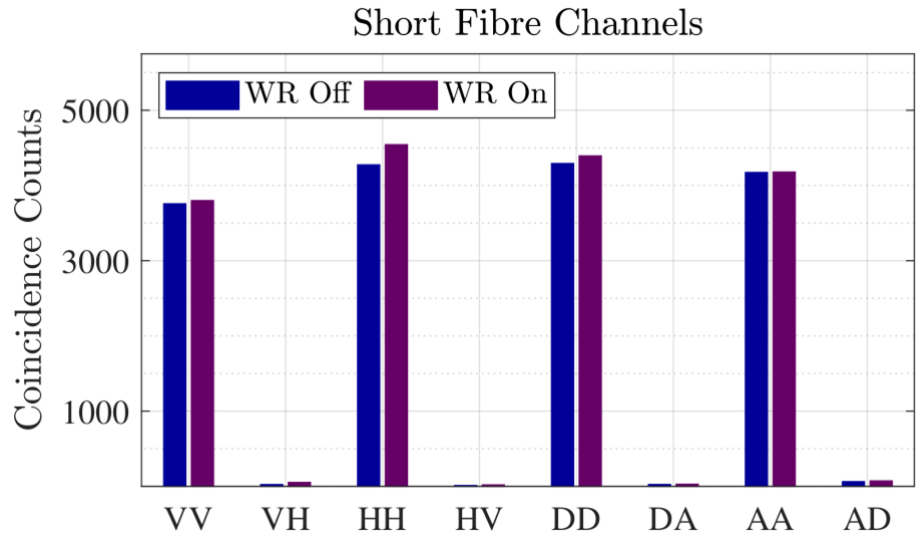
Schatz, K. et al. in [Proceedings Volume Quantum Technology: Driving Commercialisation of an Enabling Science III], 123350F (2023), https://doi.org/10.1117/12.2647691

© 2024 University of York

WR/Entanglement – Results

- High entanglement visibility (>96%) in two orthogonal bases → suitable for BBM92
- Visibility is maintained with WR ON in the same fibre
- For ~1 km length, WR scatters into the quantum signal, but visibility remains hi

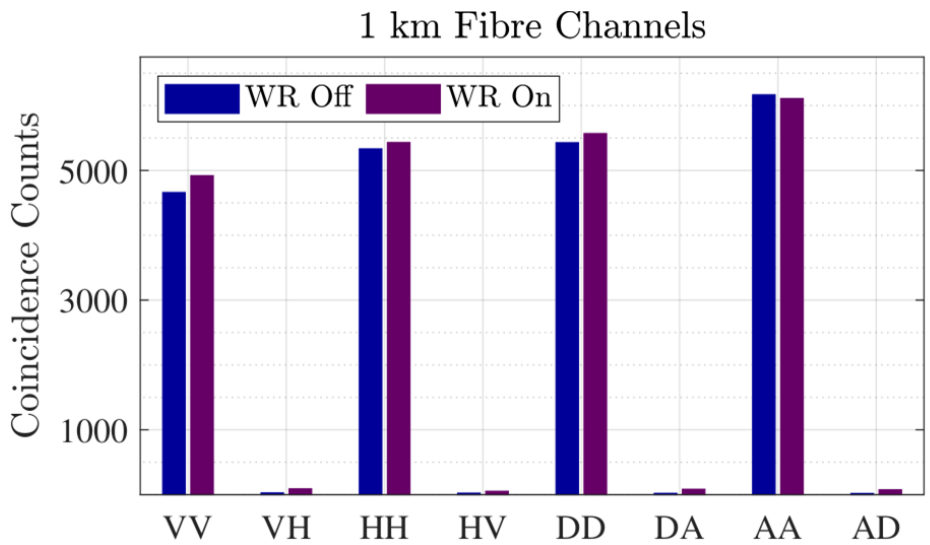




⌀ Visibility

WR Off: 98.6%

WR On: 98.0%

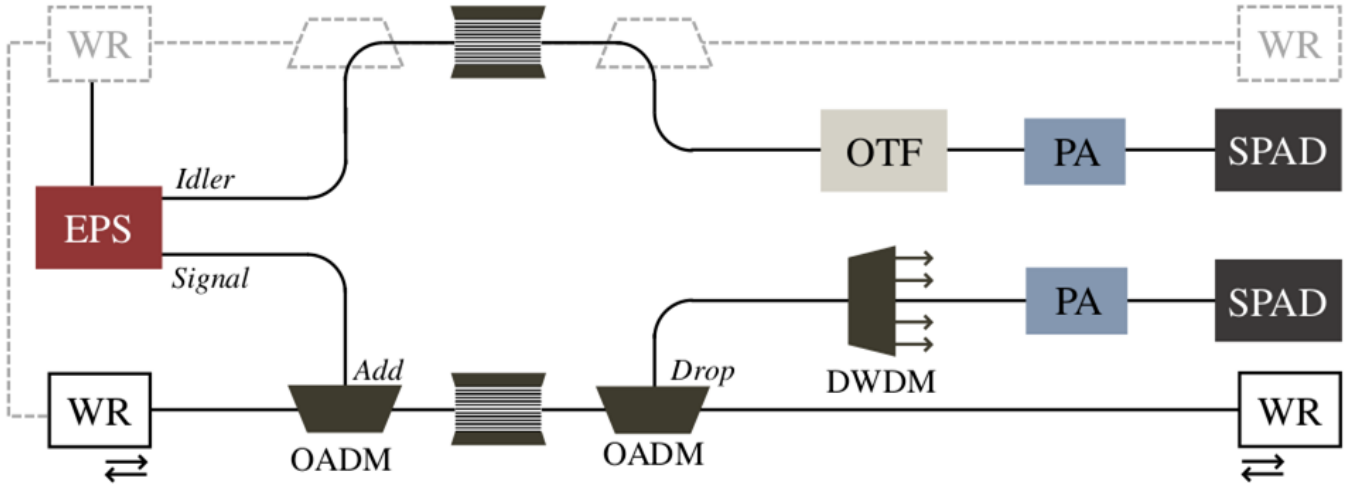


WR Off: 99.2%

WR On: 97.3%

© 2024 University of York

What next?

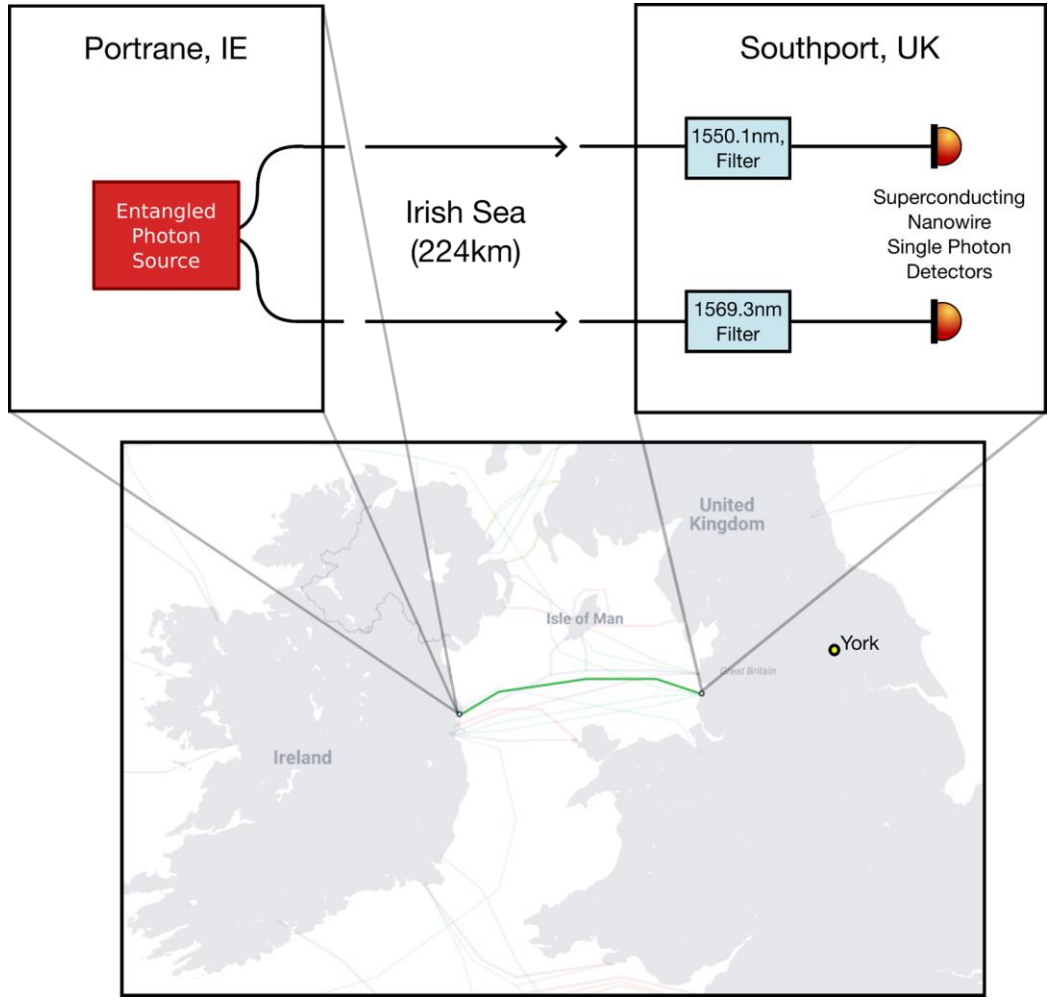


- Leverage WR for synchronisation
- Field demonstration: move Alice and Bob to separate locations
- Increase the WR and entanglement co-propagation fibre length
- Implement a full QKD protocol

© 2024 University of York

The UK–IE QKD Feasibility Study

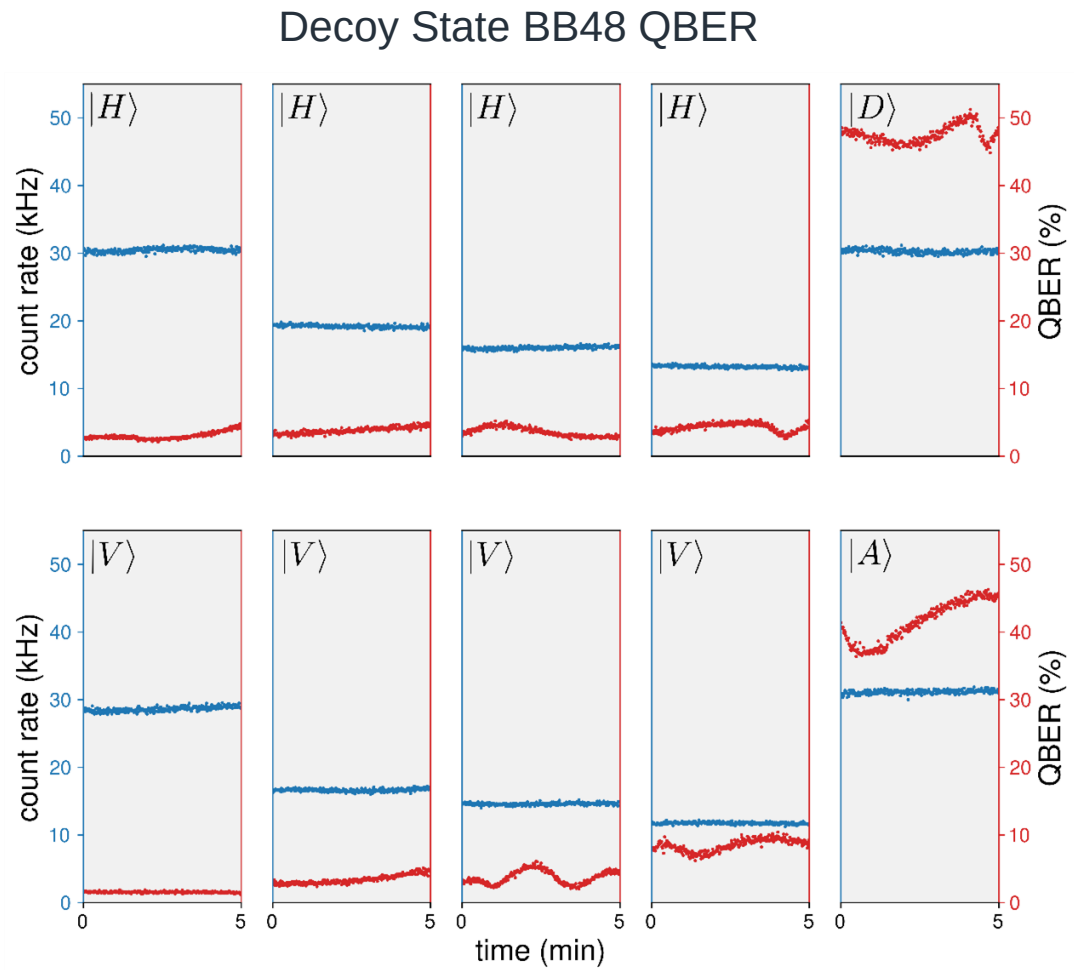
- Field trial to determine feasibility of QKD on a deployed fibre link
- 224 km of submarine, ultra-low loss fibre between the UK and the RoI
- Approximately 38 dB loss per fibre
- Our fibres are ‘dark’, but the link also contains active fibres
- Goal: assess viability of supporting quantum communications using a variety of techniques

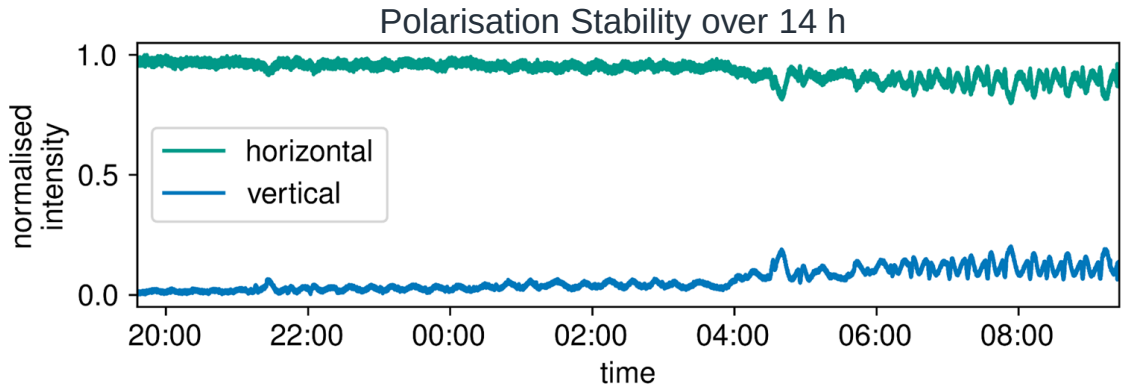


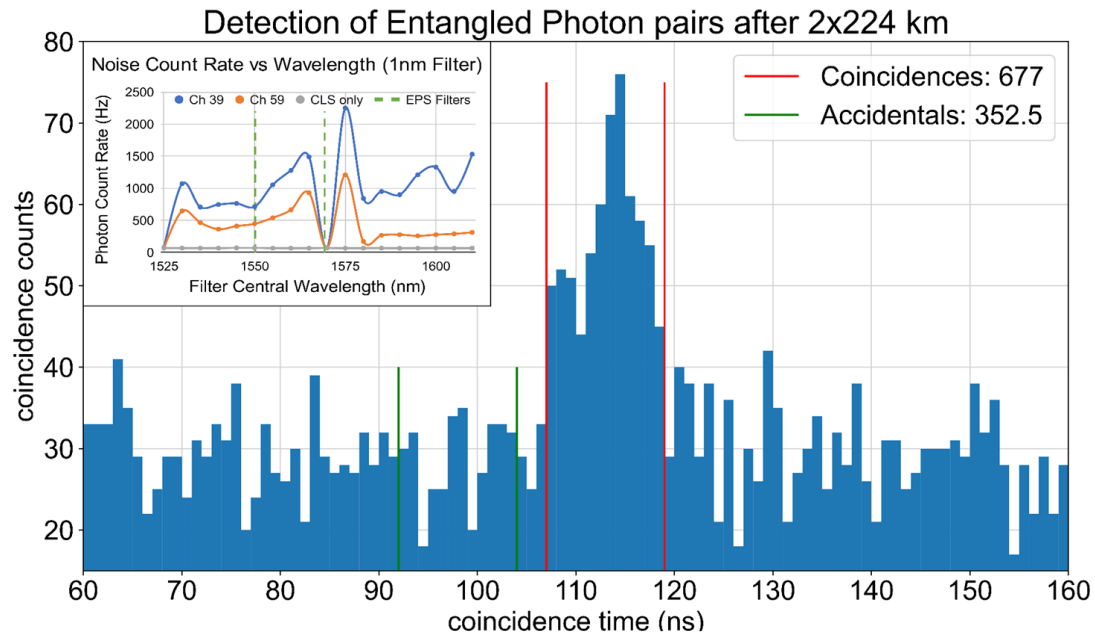
B. Amies-King, K.P. Schatz et al., “Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link.” doi: 10.3390/e25121572.

© 2024 University of York

UK–IE Feasibility Study – Results



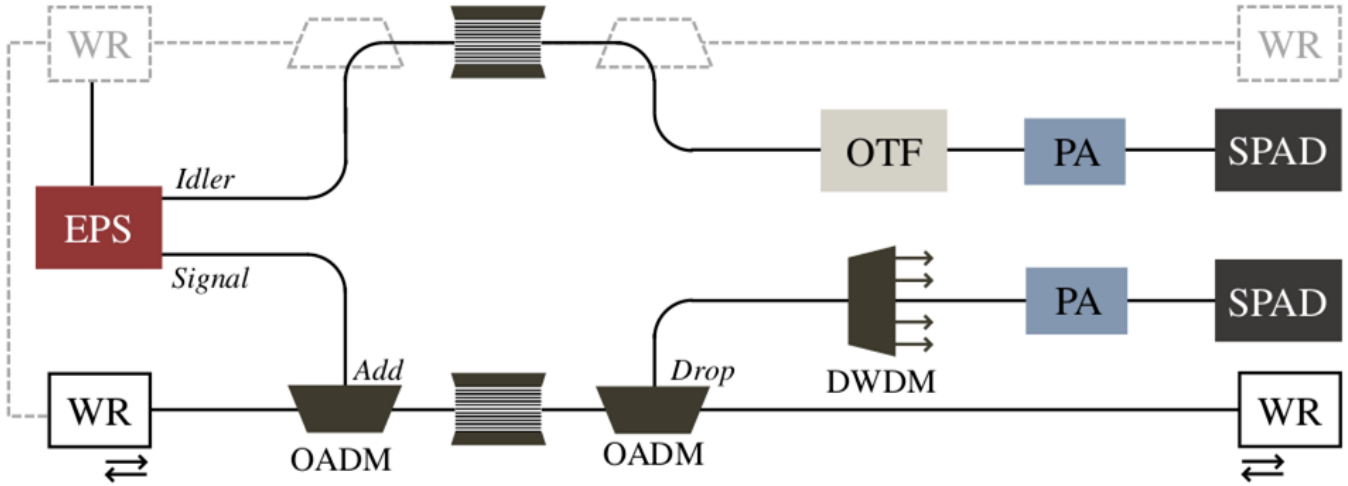




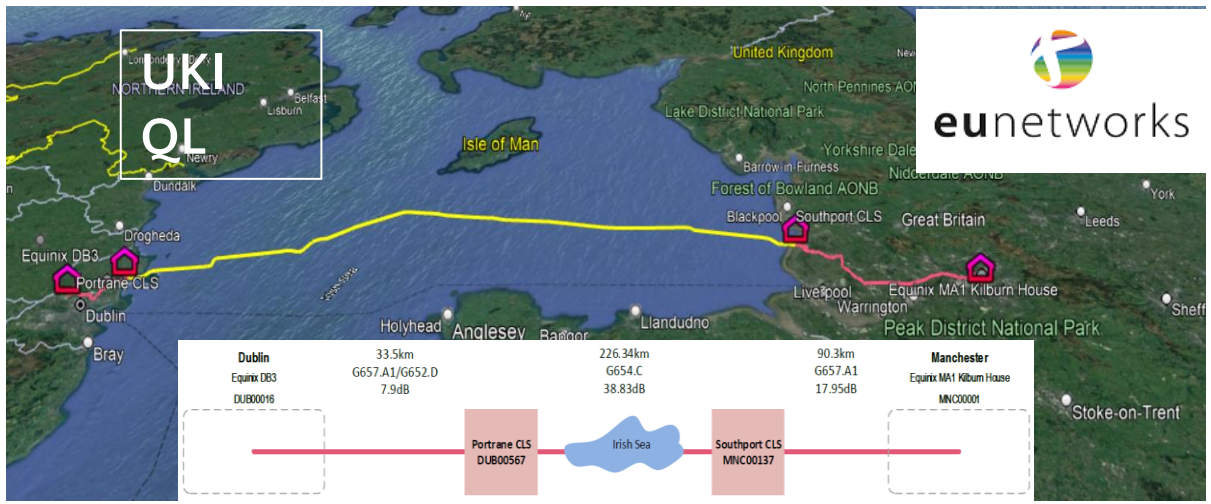
B. Amies-King, K.P. Schatz et al., “Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link.” doi: 10.3390/e25121572.

© 2024 University of York

What next?



- Leverage WR for synchronisation
- Field demonstration: move Alice and Bob to separate locations
- Increase the WR and entanglement co-propagation fibre length
- Implement a full QKD protocol



- Many more experiments planned!
- Move from feasibility test to QKD demonstrations
- New records for entanglement, and maybe also White Rabbit?

© 2024 University of York

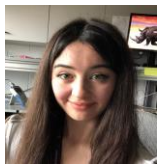
The York Experimental Quantum Communications Group


Rupesh Kumar


Tim Spiller


ML


Vinod Rao


Jennifer Bartlett

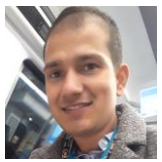

Emma Medlock


Juan Vieira


Karolina Schatz


Ry Render

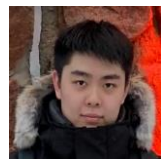

Ben Amies-King


Nischal Gajurel


Zhe-Hui Kong (w/ RAL)


Nur Sena Yerebasmaz (w/ NPL)


Luke Arabskyj (w/ NPL)


Haofan Duan

Ormond Taylor

Group activities started in September 2022. New additions expected soon.

© 2024 University of York

Current Quantum Key Distribution (QKD) Topics

Different protocols for different challenges:

- Eavesdropper Attacks
  - Decoy states, entanglement QKD
- Optical losses & distance limit
  - Twin-Field QKD, quantum repeaters
- Device imperfections
  - Measurement-device-independent QKD

Commercial Technological Level

Typical Distance in fibre (Loss)

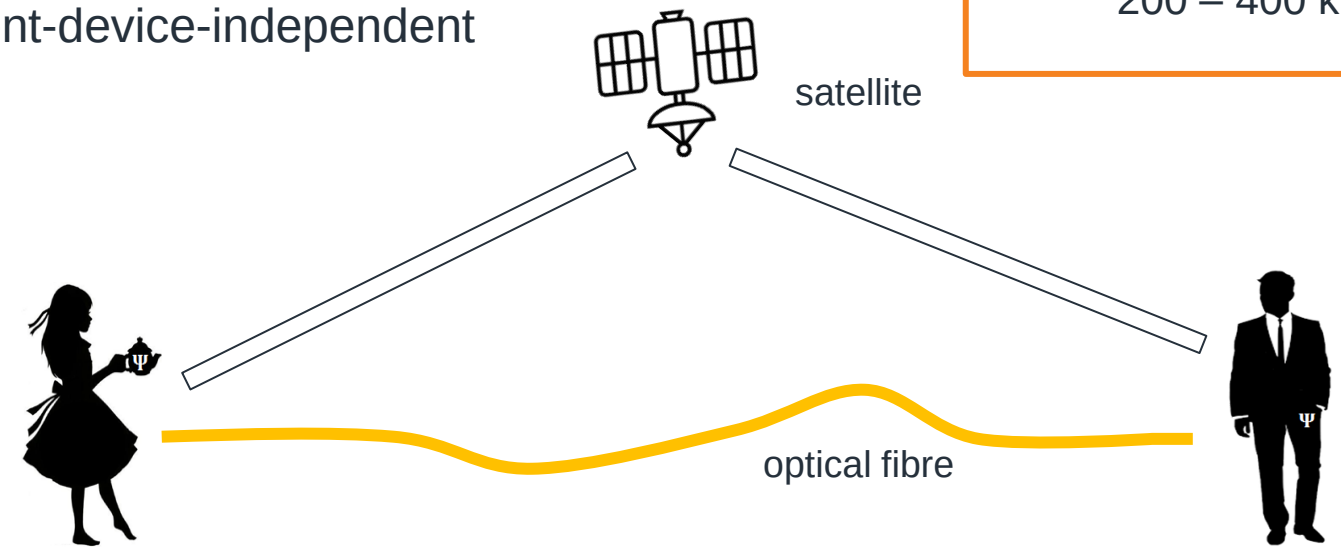
~100 km (20 dB)

Secret Key Rate @50km

1 Mbps [*]

Maximum Distance in fibre (Loss)

200 – 400 km (40 – 80 dB) [**]

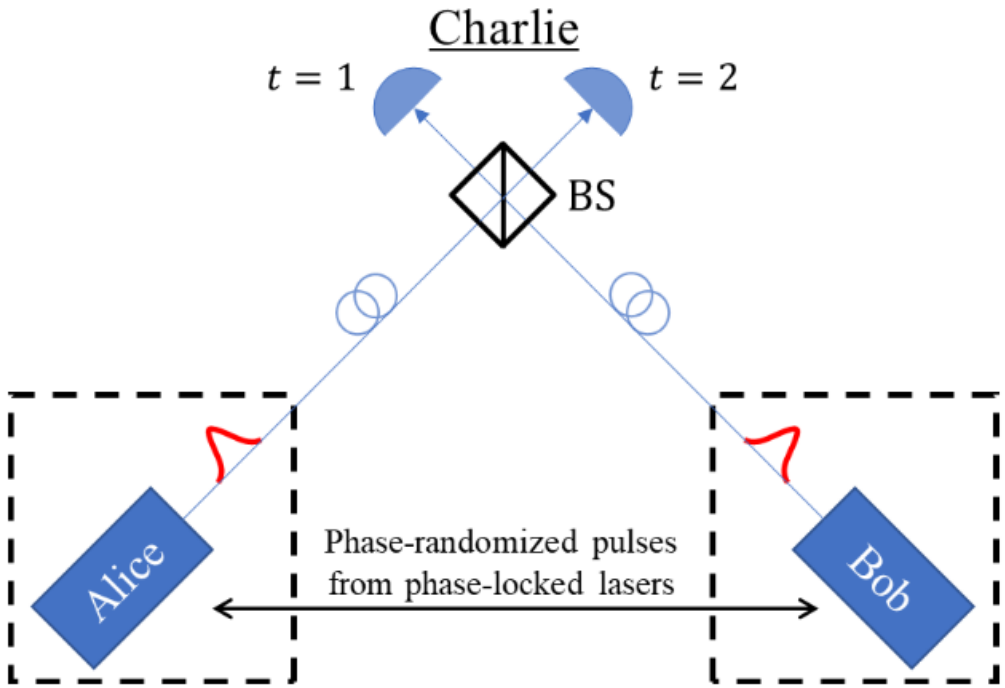


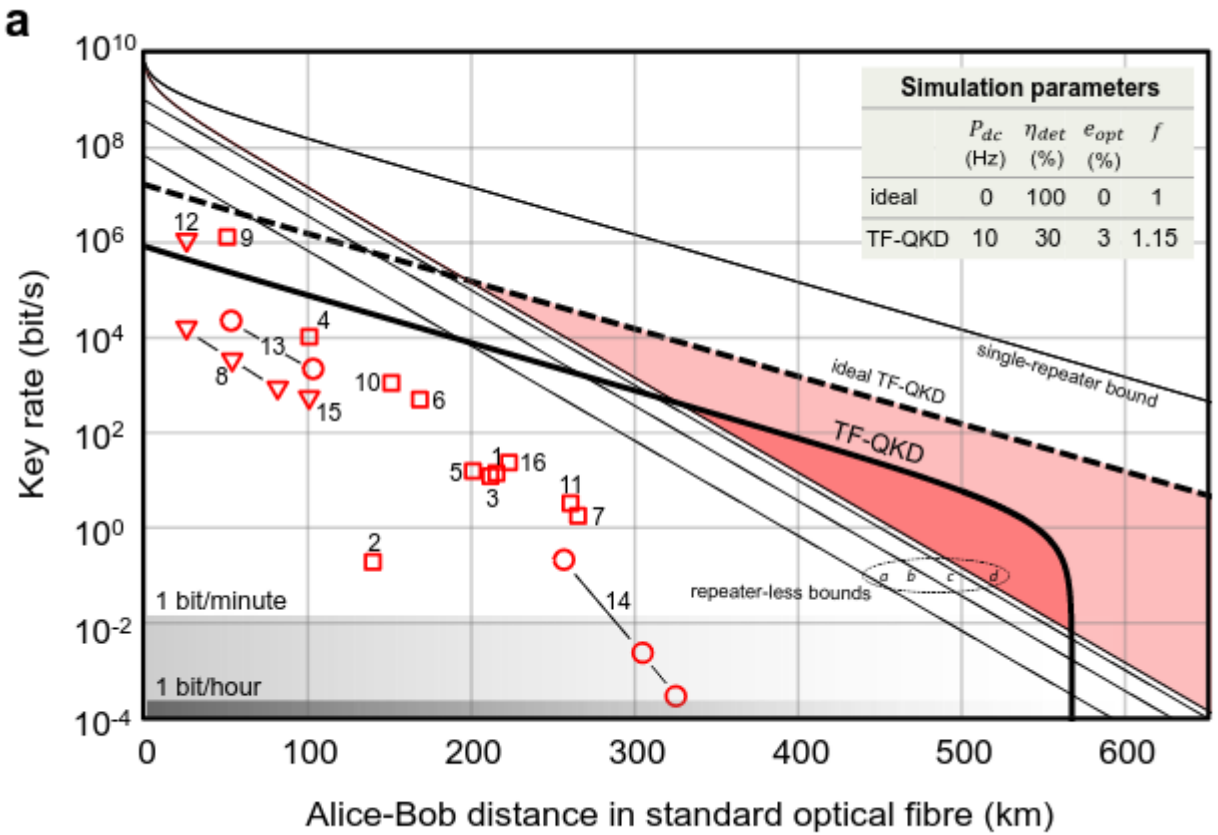
[*] ML *et al*., Opt. Express 21, 24550 (2013)

[**] B. Fröhlich *et al*., Optica 4, 163 (2017); A. Boaron *et al*., Phys. Rev. Lett. 121, 190502 (2018)

© 2024 University of York

Twin-Field QKD



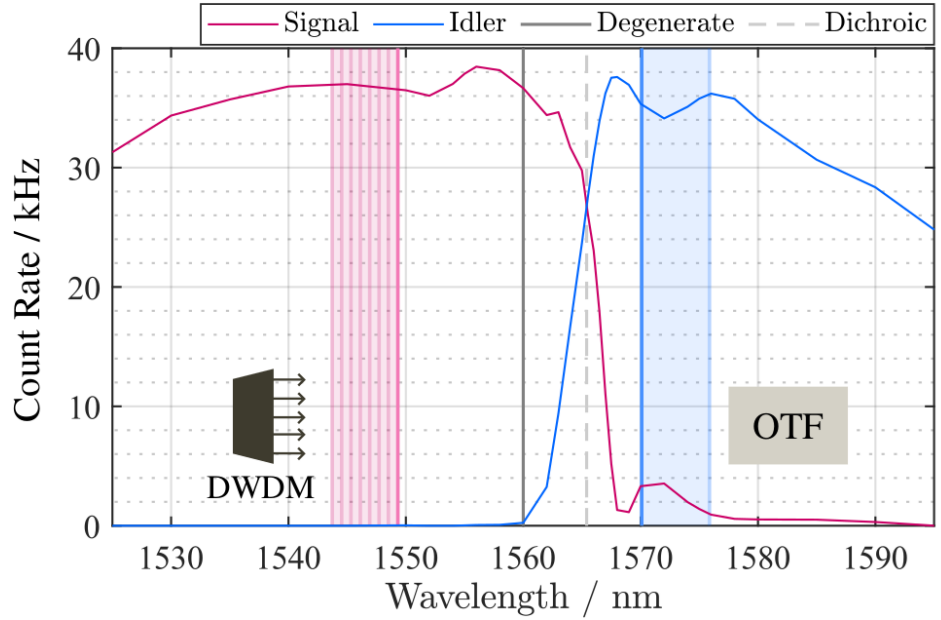


M. Lucamarini et al., “Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters” doi: arXiv:1811.06826.

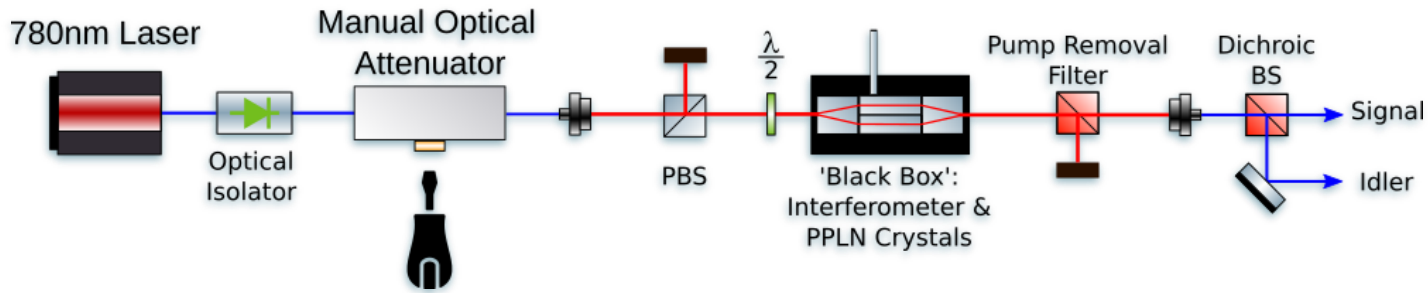
© 2024 University of York

Source of Entangled Photons

- Polarisation entangled photons produced via Spontaneous Parametric Down Conversion
- State: $|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$
- Compact and robust due to auto-balanced displacement interferometer

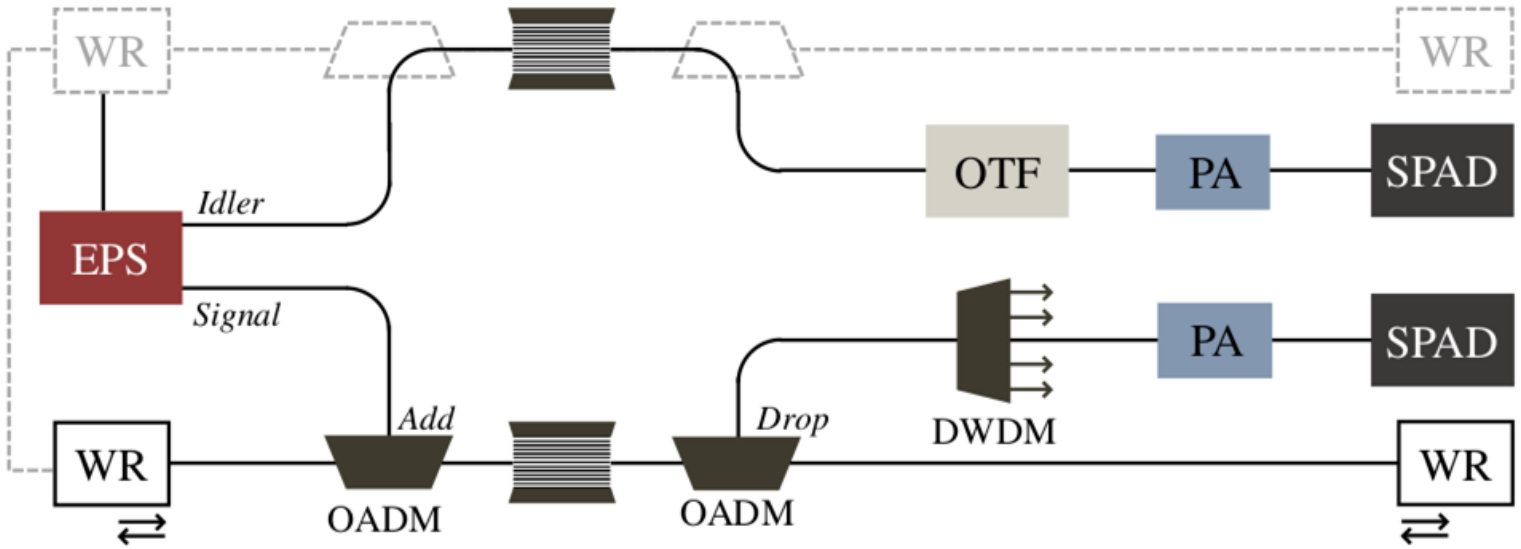


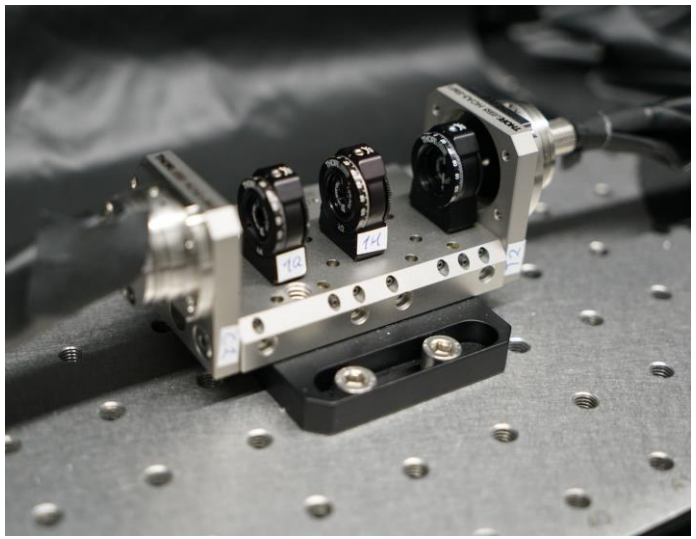
Ruby - Schematic



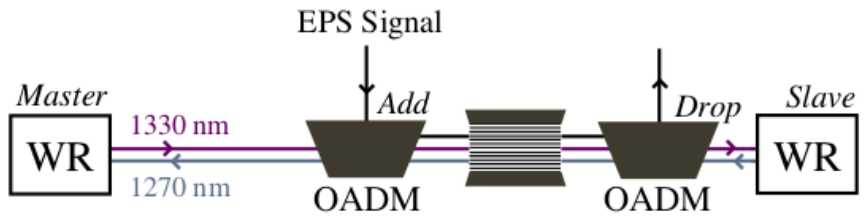
© 2024 University of York

White Rabbit and Entanglement Coexistence



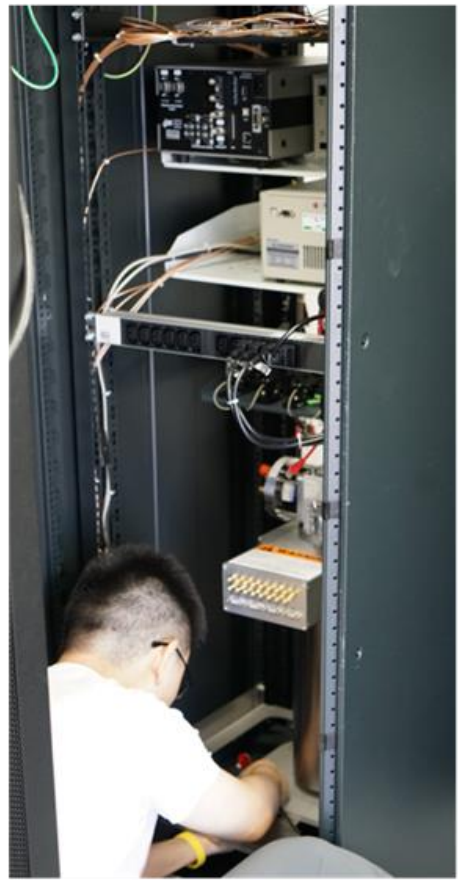


- Quantum signal is added to and dropped from an active WR communication line
- Copropagation of WR and entangled photons for 1km of SMF
- DWDM passively splits to different end users (Bob, Charlie…)
- Tunable filter allows Alice to address specific DWDM channels



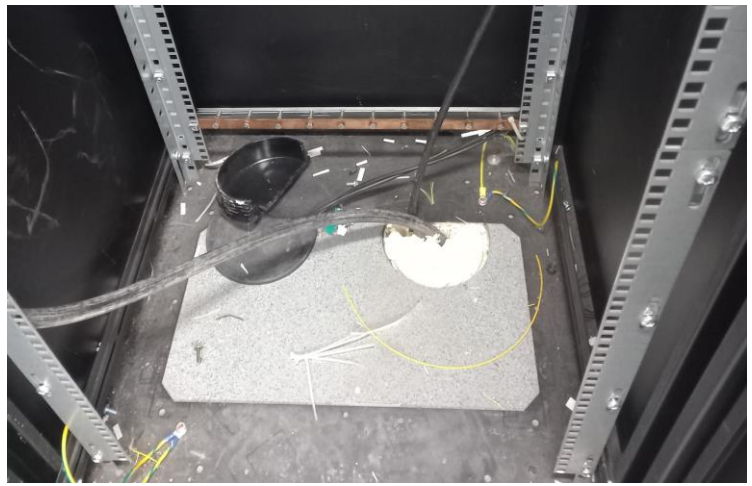
© 2024 University of York

UK-IE Feasibility Study



© 2024 University of York

UK-IE Feasibility Study



© 2024 University of York