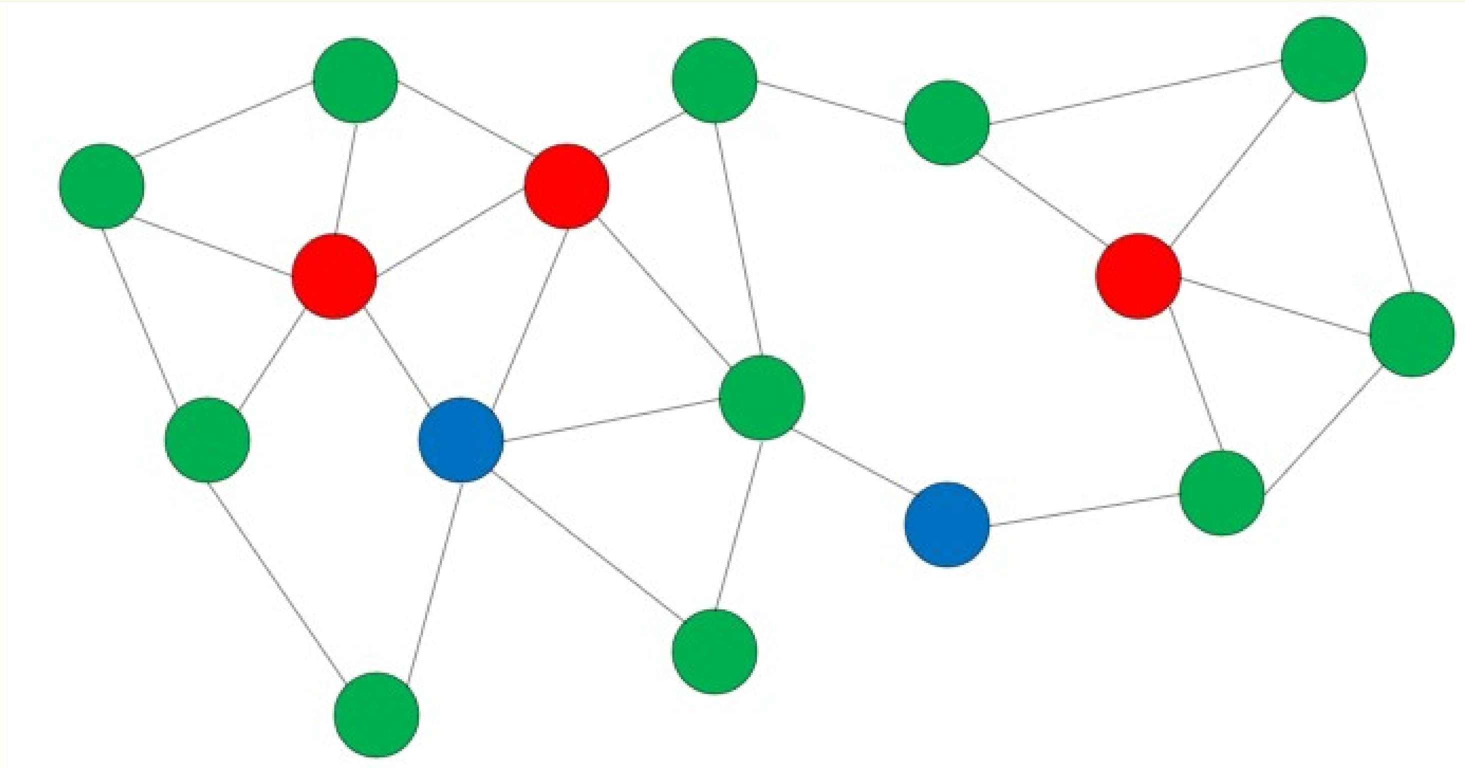
Reducing Network Cooling Cost using Twin-Field Quantum Key Distribution

Vasileios Karavias (1), Andrew Lord (2), Mike Payne (1)
vk330@cam.ac.uk
(1) University of Cambridge, Dept. of Physics, CB3 0HE, Cambridge, UK, (2) BT, Adastral Park, Martlesham Heath, IP5 3RE Ipswich, UK
UNIVERSITY OF CAMBRIDGE Cavendish Laboratory

Introduction

- Quantum Key Distribution (QKD) promises information theoretic security
- Distance achievable with such security limited by imperfect devices
- Decoy state BB84 [2] has become staple of point to point QKD
- Recently, Twin-Field QKD (TF-QKD) [3] has promised double the range and measurement device independent security in point to point connections

Methods



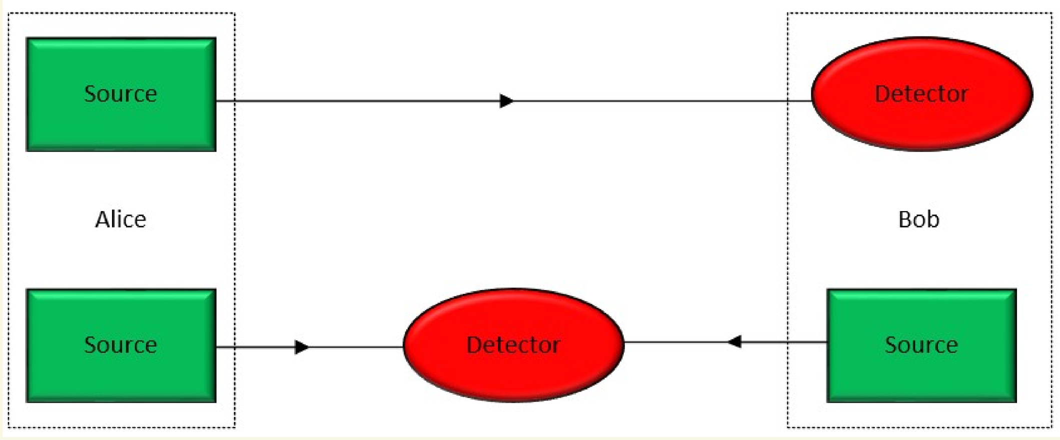
- Work on geometric graph with sets of nodes that wish to establish keys (Green) and potential detector locations that can be on (Blue) or off (Red). Average connectivity 3.5 connections per node
- Cooled TF-QKD method maximises

$$c_{net}^{B} = \sum_{i,j \in S} c_{i,j}^{max} \tag{1}$$

over all possible orientations, where S is set of Green nodes and $c_{i,j}^{max}$ is the max capacity connection between nodes i, j in the configuration
- Decoy BB84 and Uncooled TF-QKD finds minimum path between nodes and calculates rates using this distance. For Uncooled TF-QKD, detector placed at midpoint of minimum path

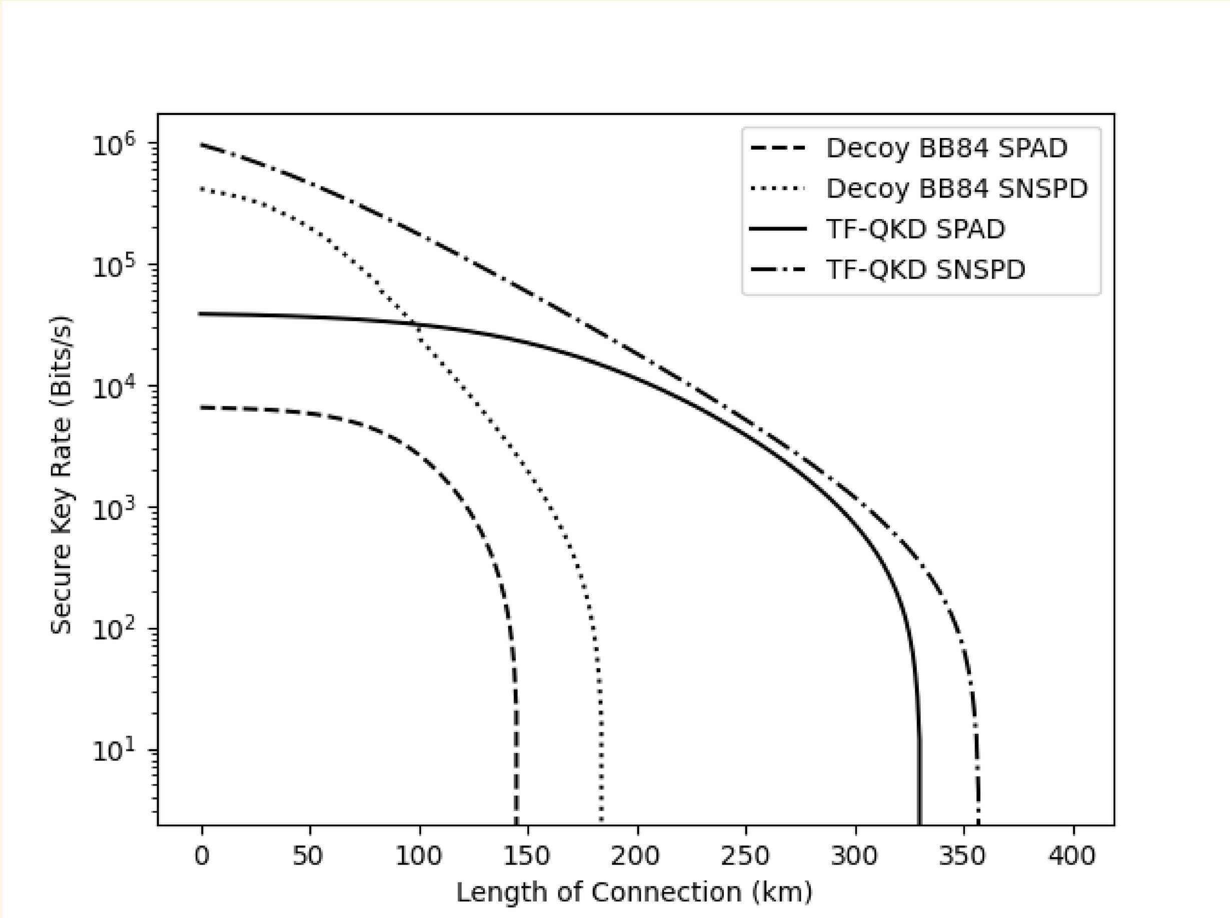
Our Work

- Devices such as Superconducting Nanowire Single Photon Detectors (SNSPDs) offer improved key distribution rates and distances but need to be cooled
- TF-QKD topology allows for detector collocation in network. Leads to cheaper cooling which could make the use of SNSPDs viable
- We compare this cooled detector collocation network to Decoy BB84 network solutions



Secret Key Rates

- Decoy BB84 and TF-QKD rates calculated using methods from [2] and [4] respectively for SNSPDs and Single Photon Avalanche Diodes (SPADs) which do not require cooling



TF-QKD rates given for symmetric system. For full details see [1]

Results

- Cooled Localised TF-QKD gives similar overall key rates to Cooled Decoy BB84 and increases the possible range of a fully connected network to similar distances as unlocalised uncooled TF-QKD. Cooling offsets the effect of localisation
- Uncooled solution improvement offset by difficulty in scalability. Localisation of detectors decreases range of network by only small amount while allowing for easily scalable solution
- Improvement per node decreases only slightly with increasing number of nodes in graph, $|S|$

Solution	0 Capacity Size/Km	Total Capacity Ratio: TF-QKD Cooled / Current Solution		
No. of Graph Nodes	$\|S\| = 40$	$\|S\| = 20$	$\|S\| = 30$	$\|S\| = 40$
Decoy BB84 Uncooled	50	34 ± 3	33 ± 3	32 ± 3
Decoy BB84 Cooled	80	0.92 ± 0.08	0.90 ± 0.08	0.87 ± 0.07
TF-QKD Uncooled	120	3.7 ± 0.6	3.4 ± 0.5	3.1 ± 0.3
TF-QKD Cooled	110	-	-	-

- Most untrusted node networks use switches, these have a loss of $1 - 2dB$
- Adding the switch losses to the model, it is evident that TF-QKD with localisation is a significant improvement over Decoy BB84, despite the localisation
- The overall key distribution rate of localised TF-QKD decreases more compared to other solutions, but is still a significant improvement over Decoy BB84 without cooling. The possible range of the fully connected network is much improved compared to Decoy BB84

Solution	0 Capacity Size/Km			Total Capacity Ratio: TF-QKD Cooled / Current Solution		
Switch Loss (dB)	1	1.5	2	1	1.5	2
Decoy BB84 Uncooled	< 10	< 10	< 10	28 ± 4	26 ± 4	27 ± 4
Decoy BB84 Cooled	20	< 10	< 10	0.76 ± 0.13	0.70 ± 0.12	0.73 ± 0.12
TF-QKD Uncooled	80	70	40	2.3 ± 0.4	2.1 ± 0.4	2.1 ± 0.4
TF-QKD Cooled	70	60	30	-	-	-

Conclusion

- We showed that a localised cooled detector node solution using TF-QKD can achieve key rates similar to a cooled Decoy BB84 solution and increases the area with just 4 cooled locations
- Allows for realistic cost-effective cooled solution to QKD networks
- For full details see [1]

Acknowledgements

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) EP/V519662/1 and by BT.

References

[1] V. Karavias, A. Lord, and M. Payne. Reducing network cooling cost using twin-field quantum key distribution. *arXiv:2107.02665*, 2021.

[2] H.-K. Lo et al. Decoy state quantum key distribution. *Physical Review Letters*, 94, 6 2005.

[3] M. Lucamarini et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557, 5 2018.

[4] W. Wang et al. Simple method for asymmetric twin-field quantum key distribution. *New Journal of Physics*, 22, 1 2020.