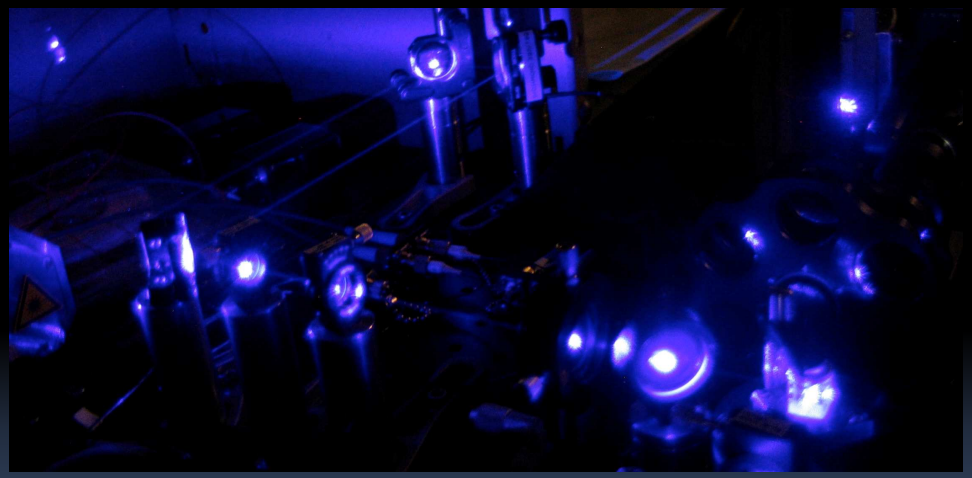
# Quantum key distribution at 810 nm through installed fibre optics



Evan Meyer-Scott*, Hannes Huebel, Chris Erven, Thomas Jennewein
Institute for Quantum Computing, University of Waterloo
* emeyersc@iqc.ca

# Overview

- Quantum Key Distribution
  - Premise
  - Protocols
- Free-Space Implementation
  - Free-space link
  - Source
  - Detector
- QKD at 810 nm through telecom fibre
  - Purpose
  - Simulation
  - Experiment
  - Results
  - Future work

# Motivation for QKD

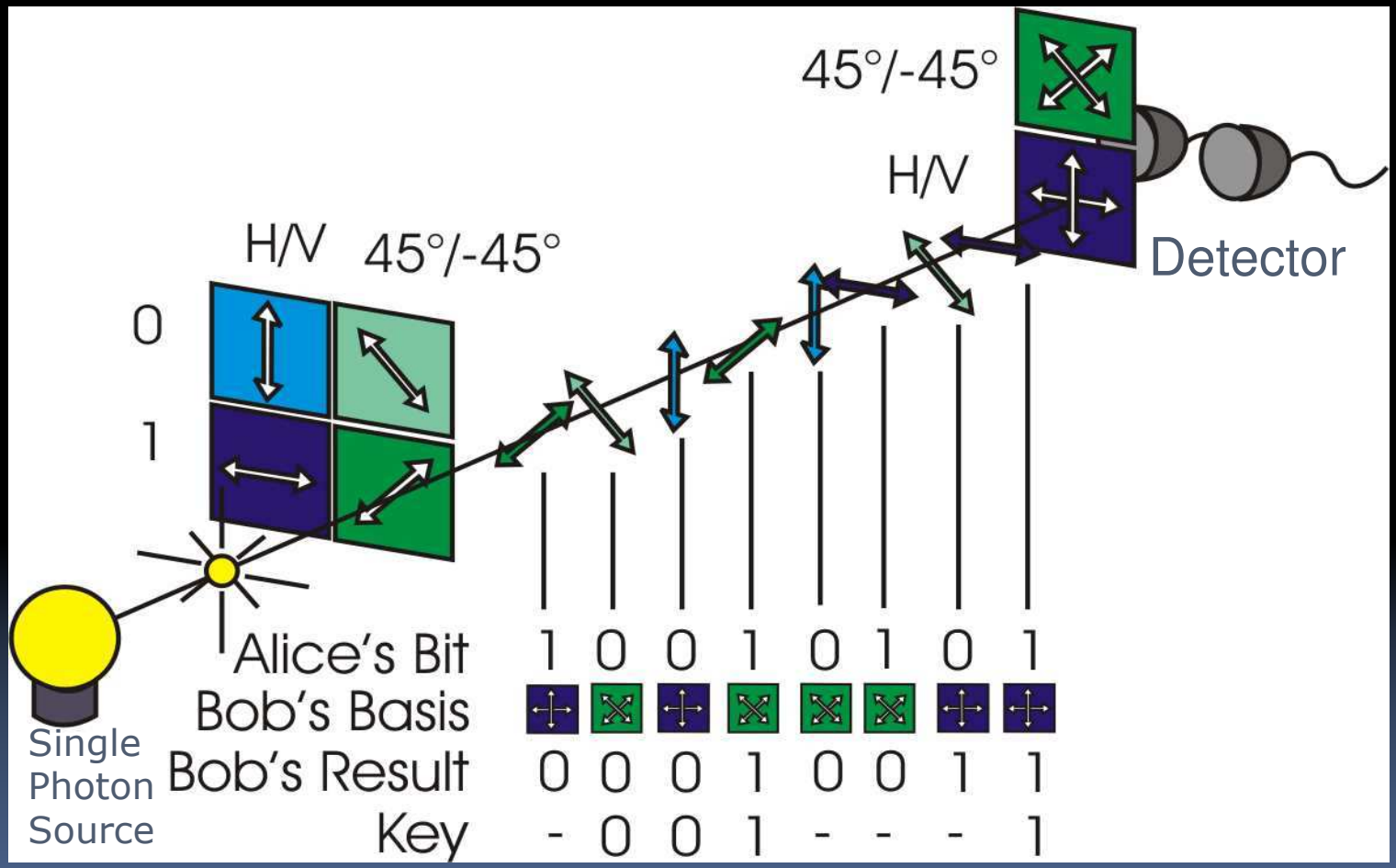
## Classical Cryptography

- Public key
  - Relies on mathematical complexity
- Private Key
  - One time pad is provably secure, but key must be physically distributed to both parties

## Quantum Cryptography

- Private key
  - QKD takes care of physical distribution
  - Any eavesdropping will disturb the system

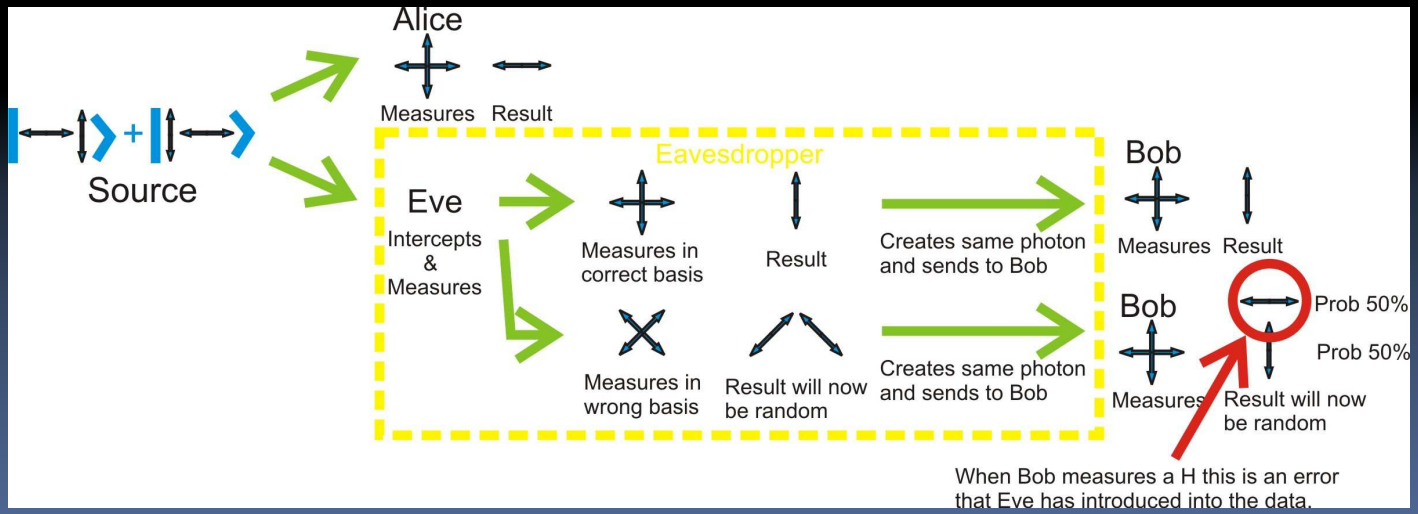
# BB84 Protocol




Bennet and Brassard Proc of. Int.Conf. Computers, Systems & Signal Processing, Bangalore India 175 (1984)

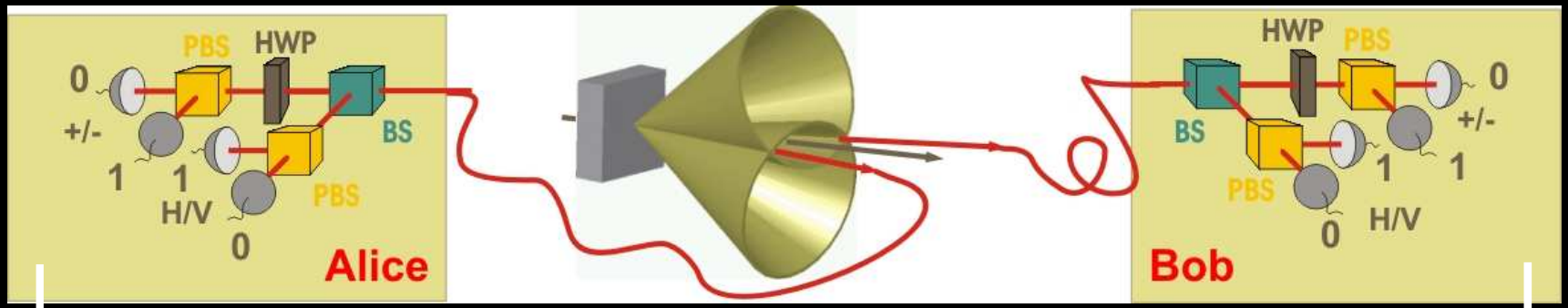
# BBM92 Protocol

- An anti-correlated Bell State is generated in polarization-entangled photons and one qubit is sent to each Alice and Bob
- Alice and Bob each measure randomly in one of two bases (H/V or +45/-45) and discard bits measured in different bases
- This results in a (not error-free) anti-correlated, random shared key
- Equivalent in guaranteed security to BB84 protocol




C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” Physical Review Letters, vol. 68, 1992.

# QKD with BBM 92




| H/V | +/- | H/V | +/- | +/- | +/- | H/V | H/V | +/- | H/V | +/- |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |

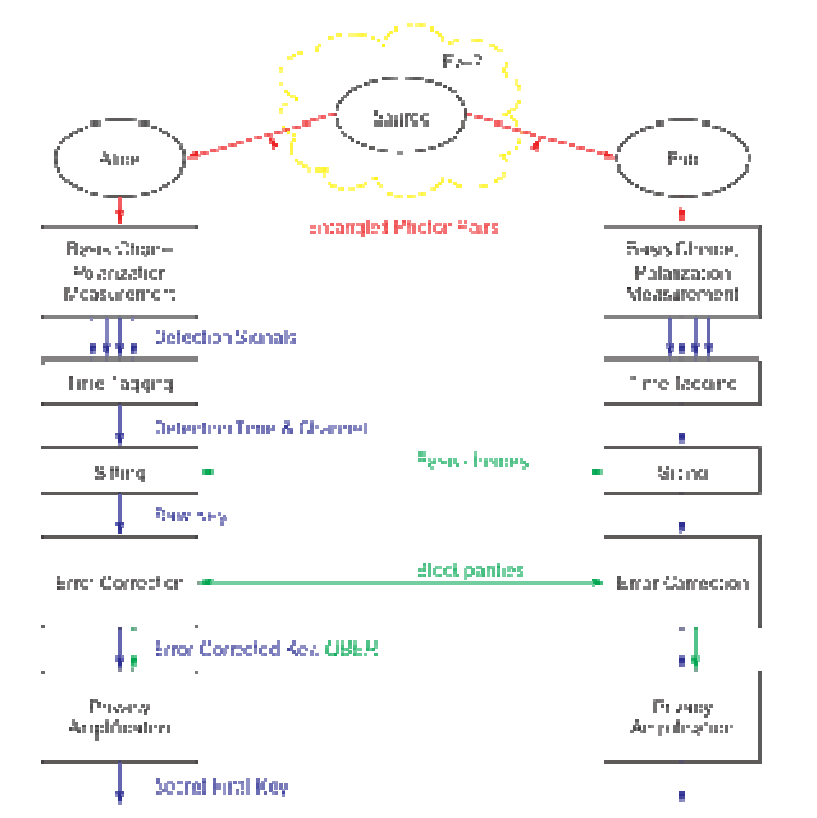
| H/V | H/V | +/- | +/- | H/V | +/- | H/V | +/- | +/- | H/V | H/V |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |

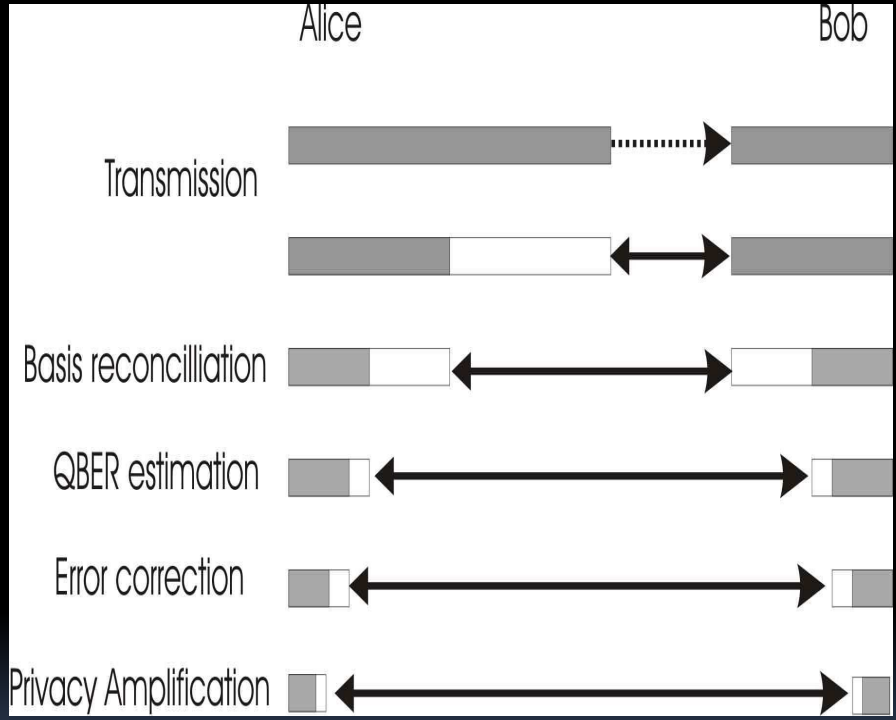
Polarization-Entangled Photons are created, coupled into optical fibres and sent to Alice and Bob

Alice and Bob announce their measurement bases. Events measured in different bases are discarded -> **Sifted Key**.

Alice and Bob measure the polarization of the photons randomly in one of two bases (H/V, +/-) -> Raw Key

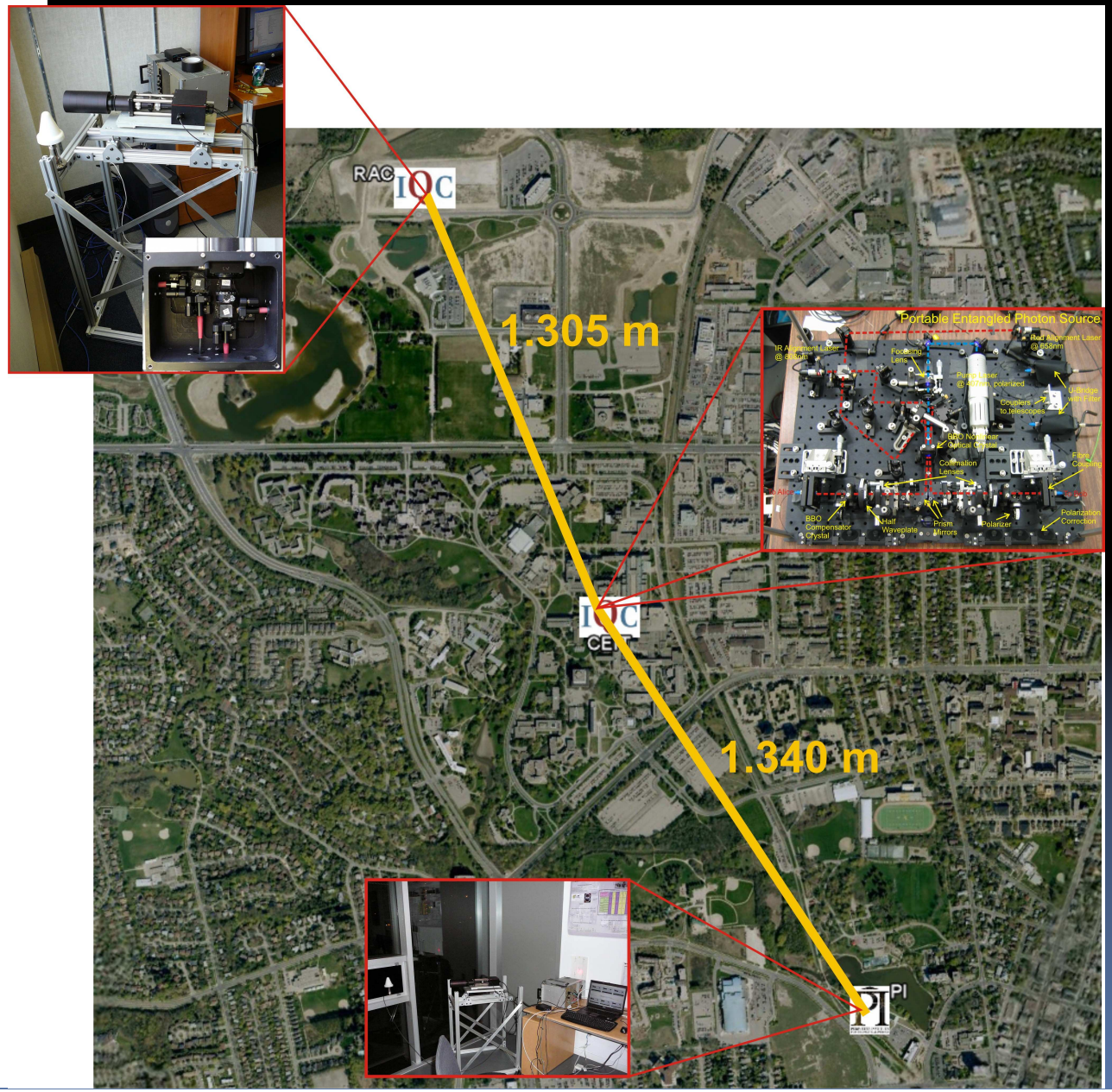
# Implementation




G. Weihs and C. Erven, “Entangled free-space quantum key distribution,” vol. 6780, p. 13, SPIE, 2007

# Free Space Link

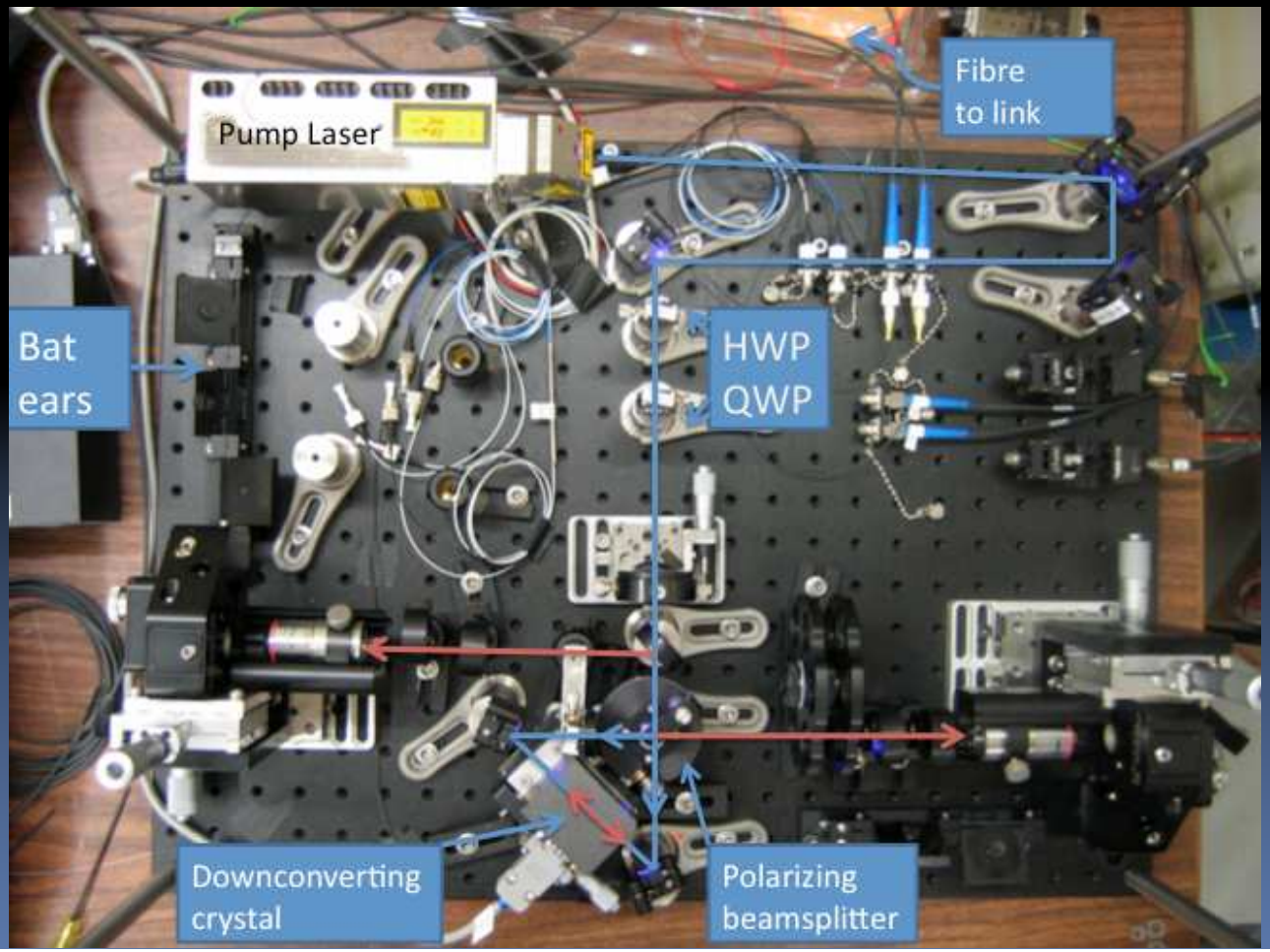



Sender telescopes and source remotely controlled by Alice or Bob (after initial alignment)

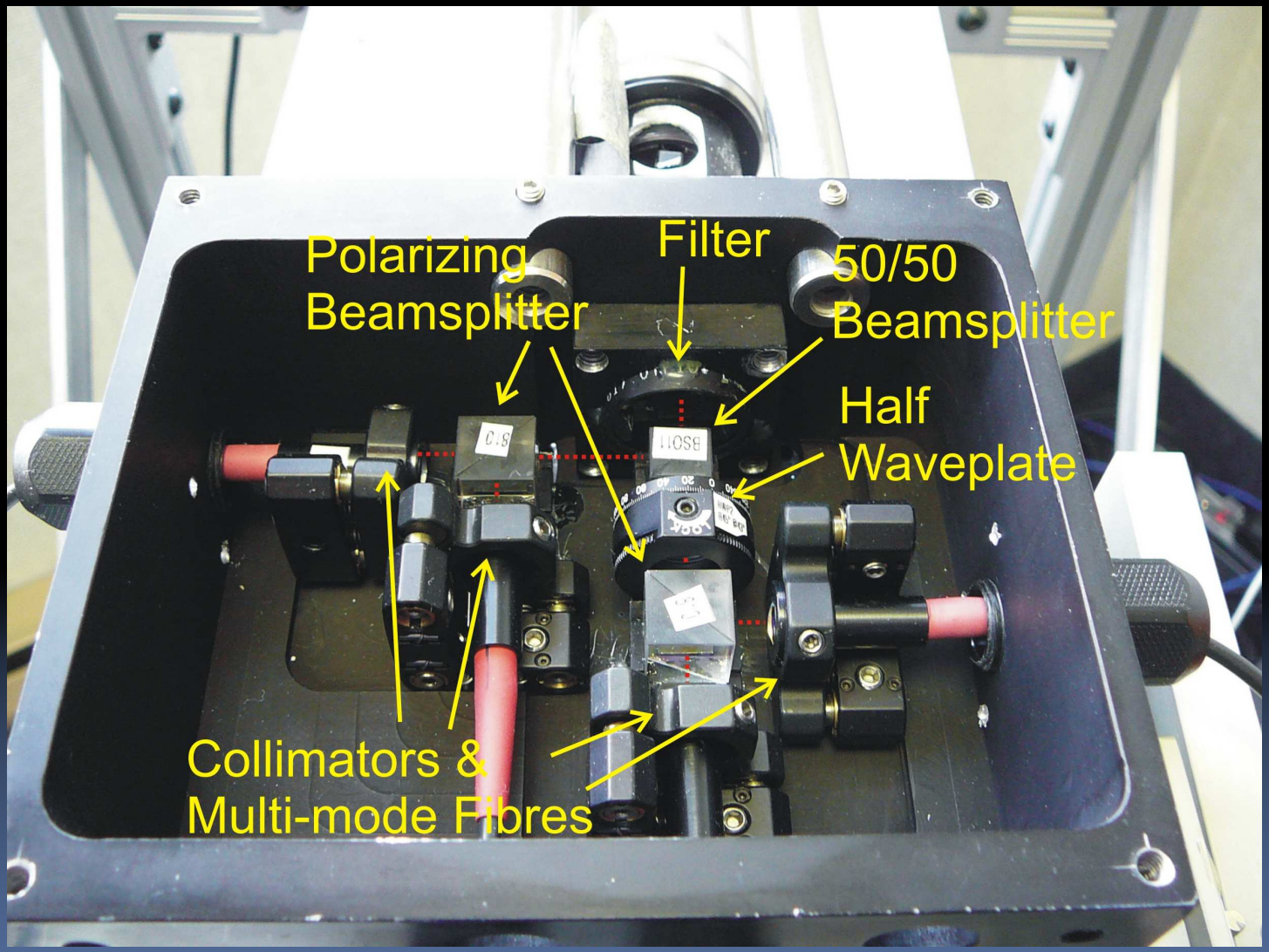
- Raw Key Rate: 565 bits/s
- Secure Key Rate: 85 bits/s
- Quantum Bit Error Rate: 4.92%, due to transverse walk-off in BBO crystals, imperfect polarizing beam splitters, birefringence in fibres to telescope

# Sagnac Source

- Visibiility: 97% H/V and 95% +/-



# Detector Module



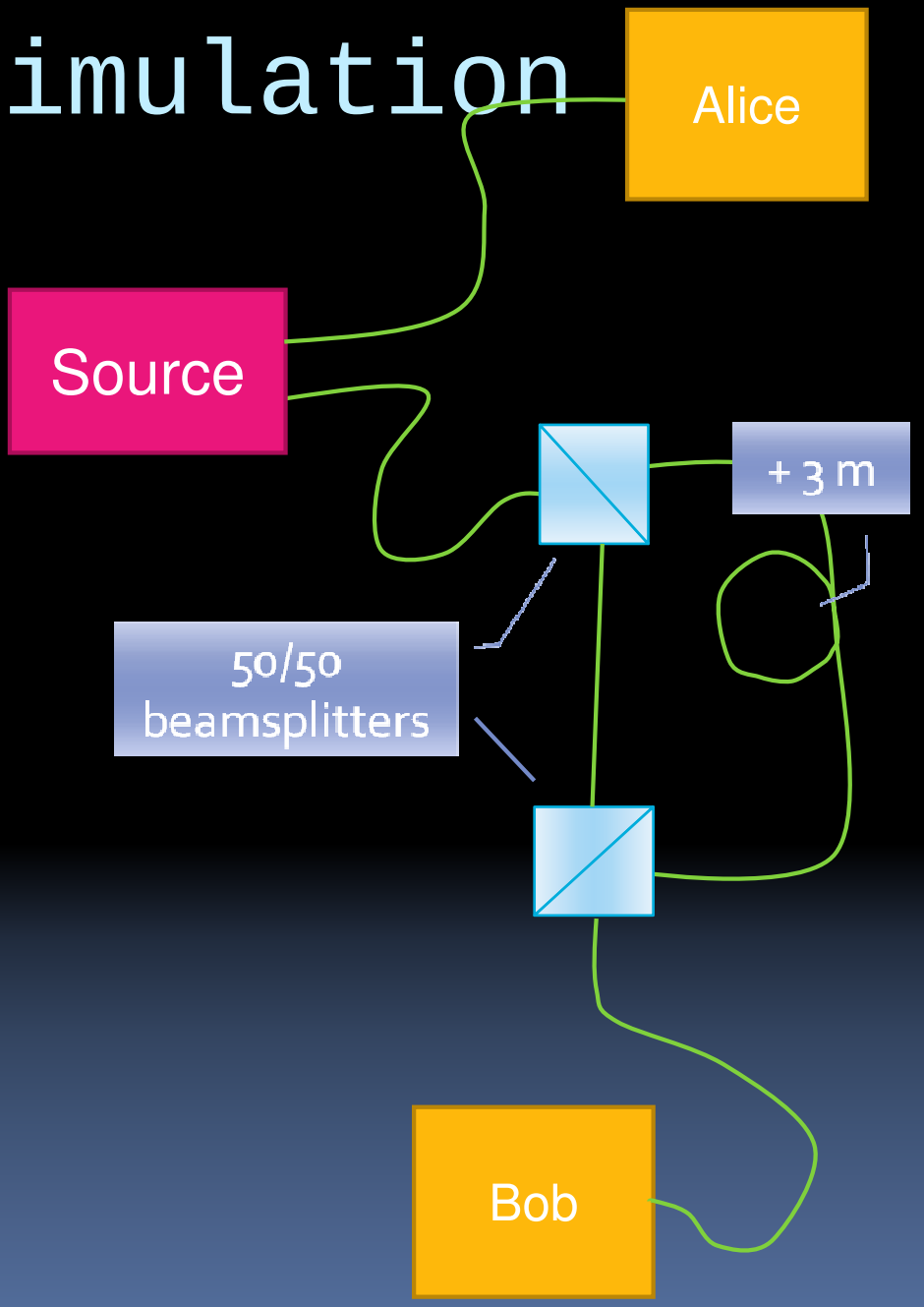
# QKD at 810 nm through telecom fibre

- Telecom industry uses 1550 nm photons
- But good, cheap and small single-photon detectors and sources do not exist at this wavelength
- So use 810 nm photons in existing fibre – expect 6 dB losses in short (2 km) link
- Since the fibre core of 1550 nm fibre is too large for 810 nm photons, two spatial modes travelling at two different speeds are expected

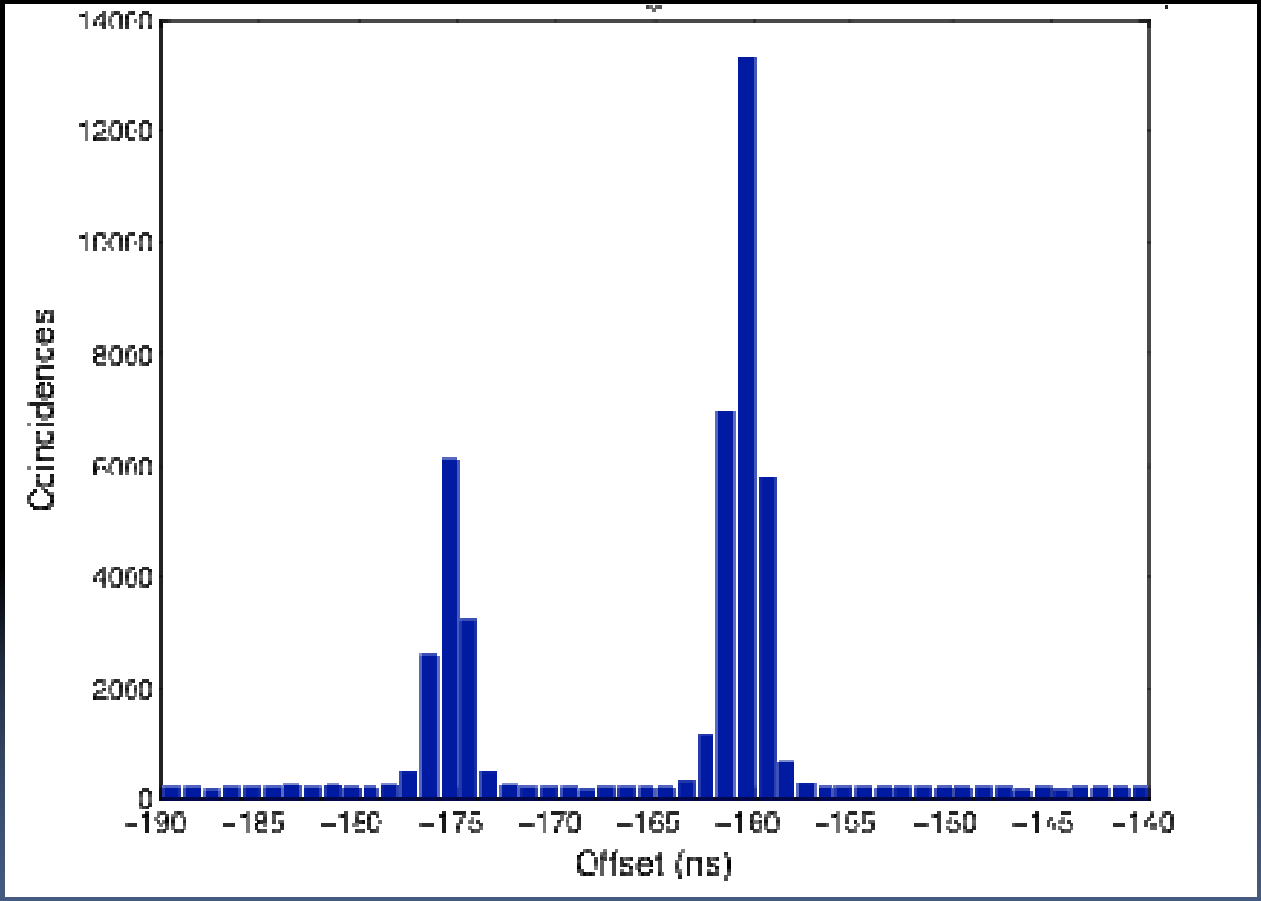
| | **810 nm** | **1550 nm** |
|---|---|---|
| Attenuation in Fibre | 3 dB/km | 0.22 dB/km |
| Detector Quantum Efficiency | 40% | 10% |
| Total loss for 2km link | 90% | 91% |

# Preliminary Simulation

- A 3 m fibre was introduced in one channel to simulate delay of the second spatial mode
- Coincidence analysis software was used to ensure good visibility in both H/V and +/- bases was possible



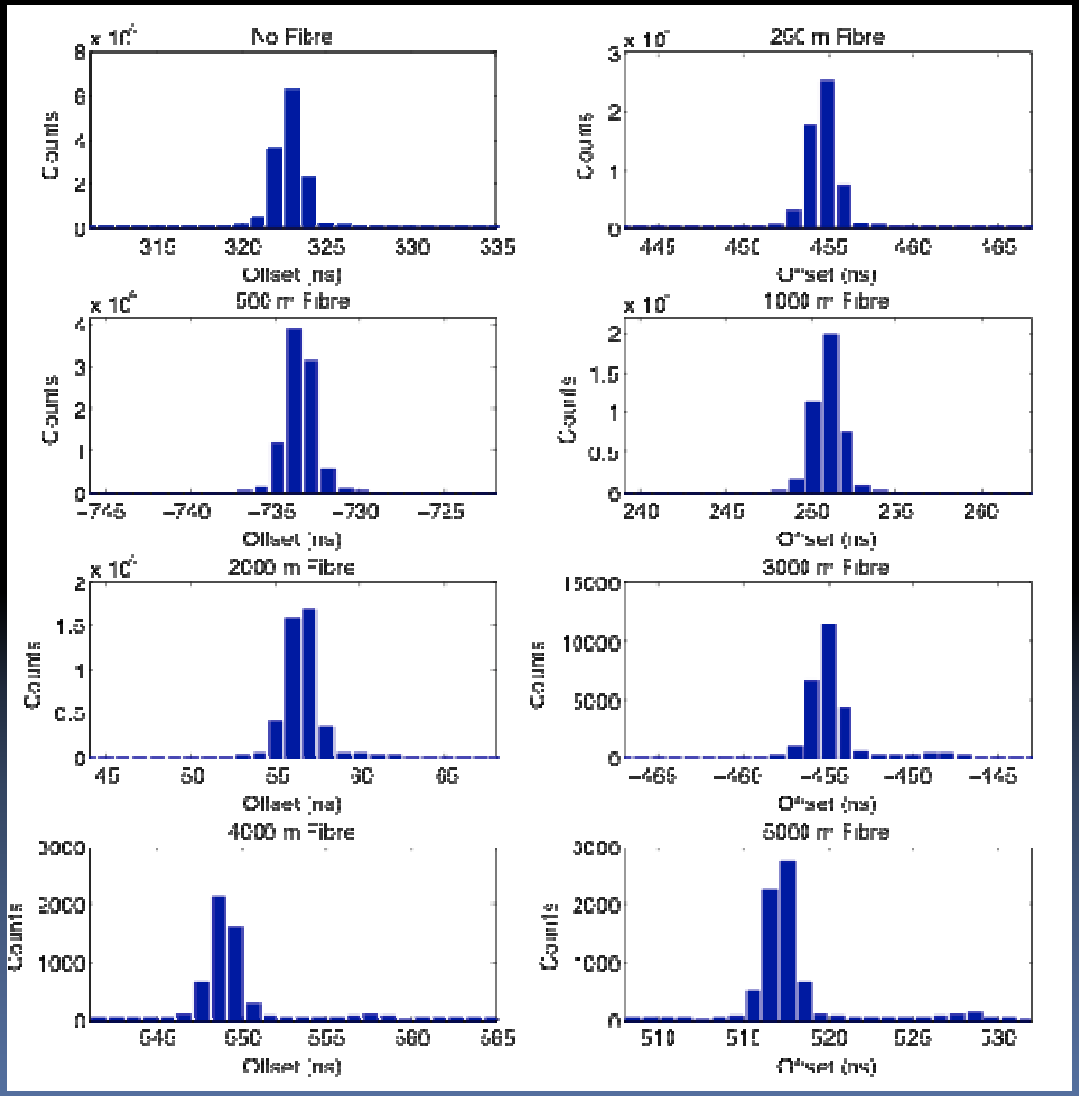
# Simulation of two spatial modes in fibre




Software selects one peak only, leading to good visibilities:
H/V 95%
+/- 95%

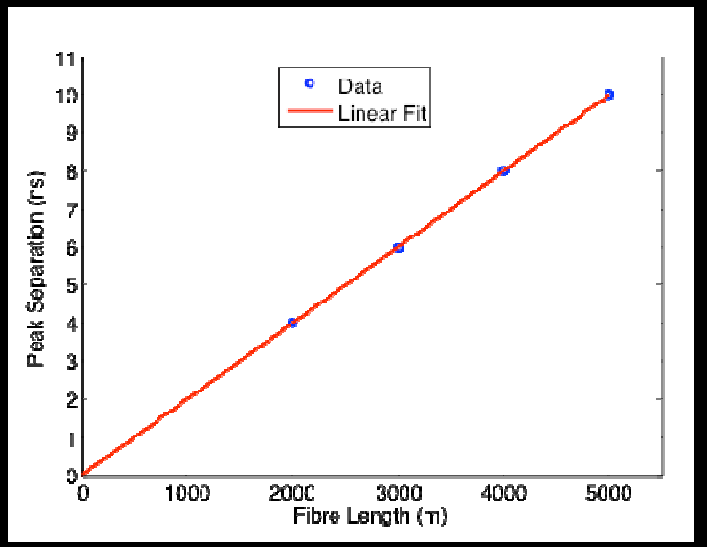
# Test with fibre on spools

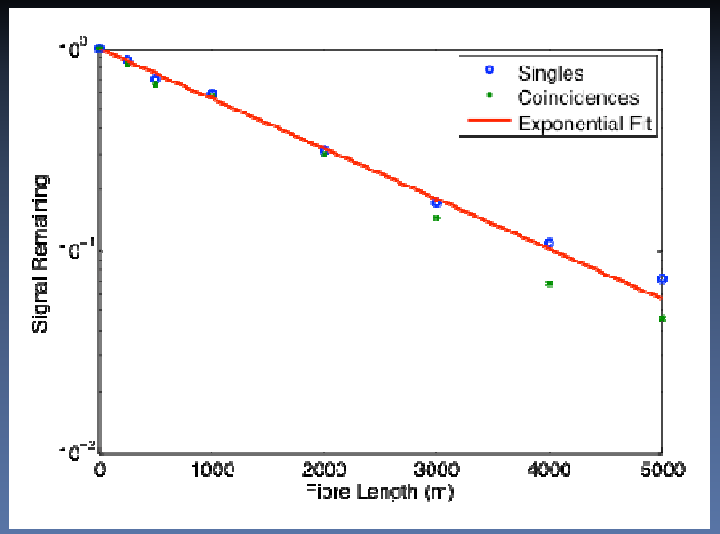
- Various lengths of fibre on spools were used to transmit between the source and Alice
- 2nd peak very small, visible for longer fibres
- Visibility at 2 km:
  - 95% H/V
  - 91% +/-



# 2nd Peak Location and Attenuation vs. Fibre Length

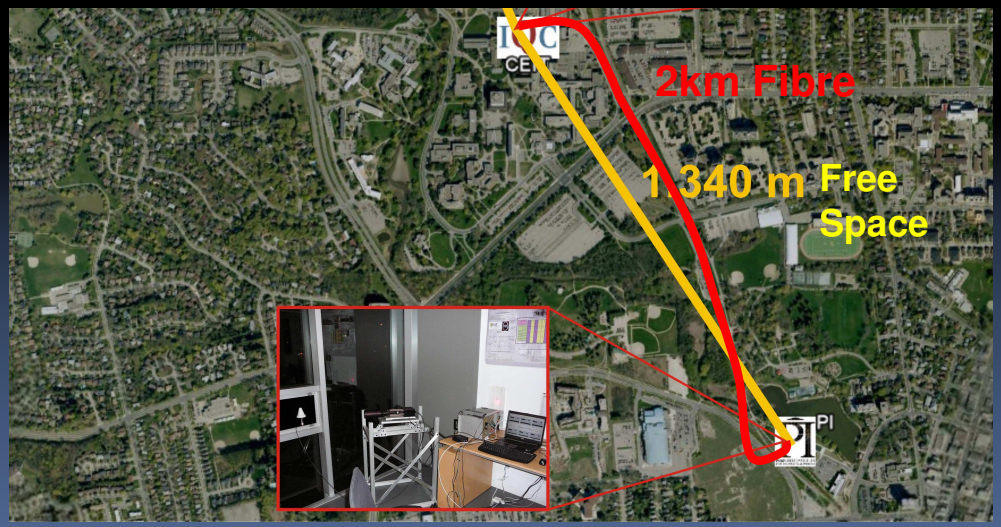
- 2nd peak moves away linearly with fibre length
- 68% attenuation at 2km gives:
- 87% total loss (compare with 91% predicted loss for 1550 nm)



# Future Work

- Existing fibre links in Waterloo will be used to demonstrate economy of 810 nm QKD over short distances



# Acknowledgements

Thanks to Chris Erven and Hannes Huebel for images.