Title: Quantum Key Distribution Over Active Telecom Fibres

Date: Jul 20, 2011 01:10 PM

URL: http://pirsa.org/11070069

Abstract: Quantum Key Distribution is a form of public-key cryptography where the security comes from the unique properties of quantum mechanical systems: entanglement and the no-cloning theorem, rather than computational complexity. With increased adoption of fibre optic networks, it may be possible to implement QKD in parallel with classical data traffic. Many research projects have demonstrated QKD over fibre optic networks at the same wavelengths as existing network traffic. These projects require sophisticated noise cancellation due to wave mixing between quantum and classical signals, as well as having to use complex non-silicon based photodiodes. Our research uses lower wavelengths for QKD over active telecom fibres to avoid these problems. Entangled lower-wavelength photons are combined with telecom wavelength laser signals carrying a large amount of traffic, and passed through single mode telecom fibres. We show that data bandwidth usage has a negligible effect on the quantum bit error rate (QBER) and visibility for distances up to 6km. We find key rates of 61 bits per second with QBER rates of 10% at 6km. This research demonstrates the simplicity and applicability of QKD to existing fibre optic infrastructure in corporate, government, and academic campuses.

Entanglement Distribution and QKD on active 1550 nm telecommunications Fibres

Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

July 20, 2011

Cryptography

One-Time Pad

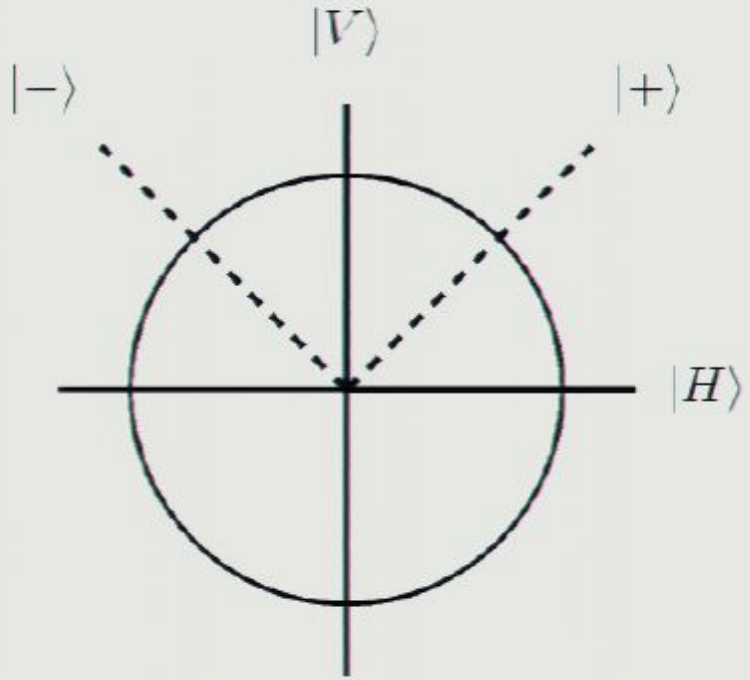
Encryption:

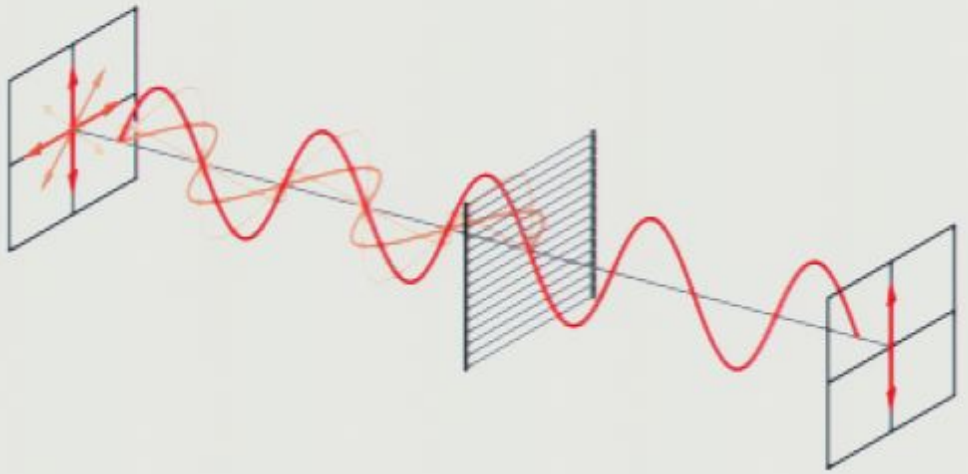
1001001 1000110	plaintext
1010110 0110001	key
0011111 1110110	ciphertext

Decryption:

0011111 1110110	ciphertext
1010110 0110001	key
1001001 1000110	plaintext

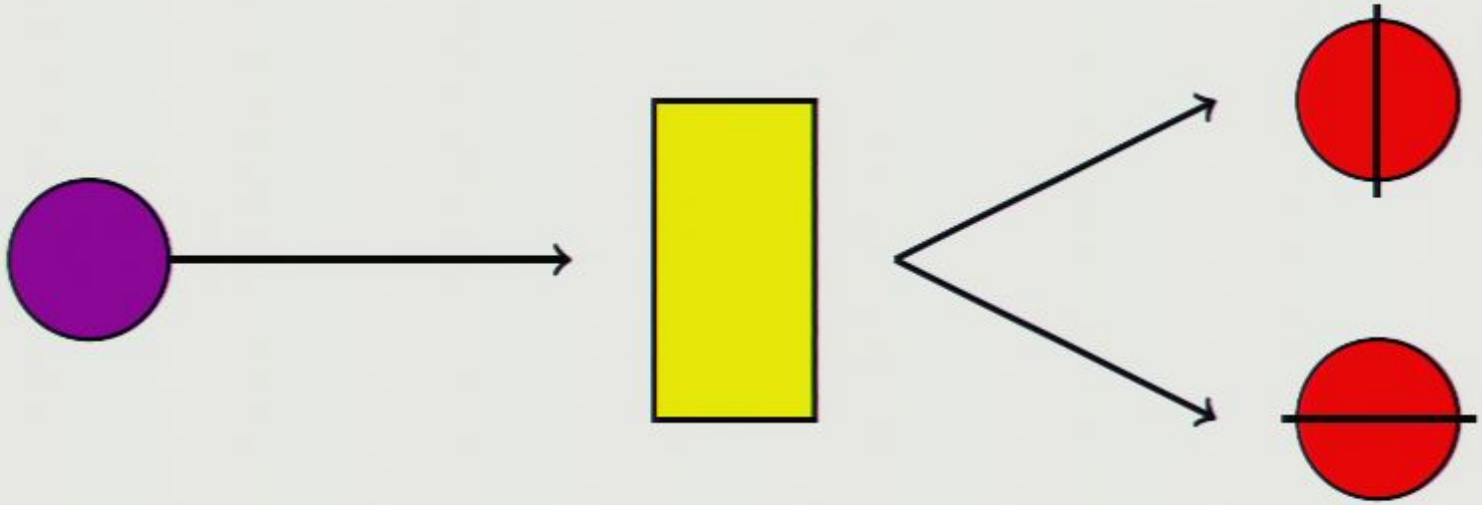
Quantum Bits



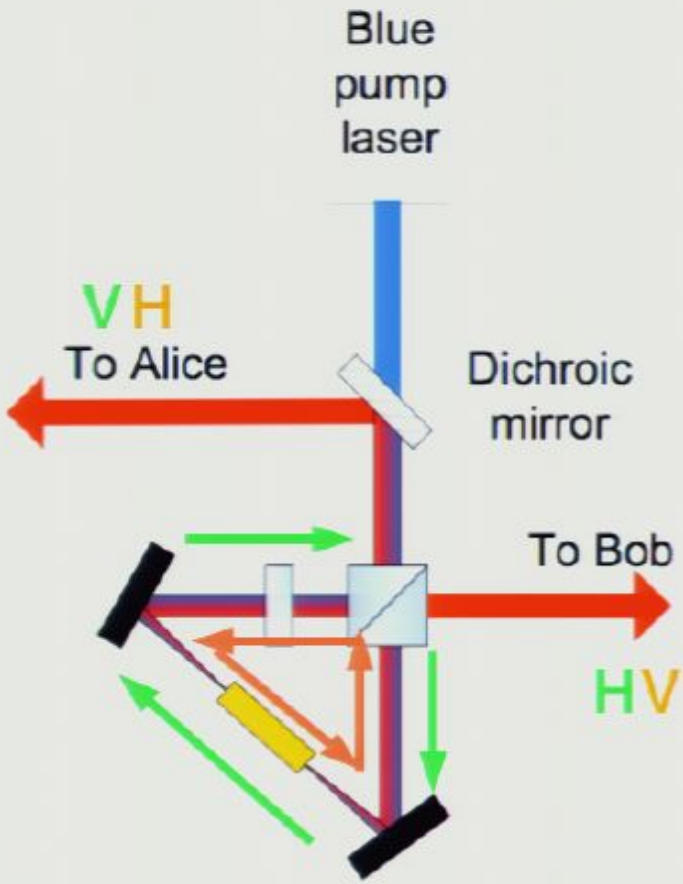


Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

Downconversion

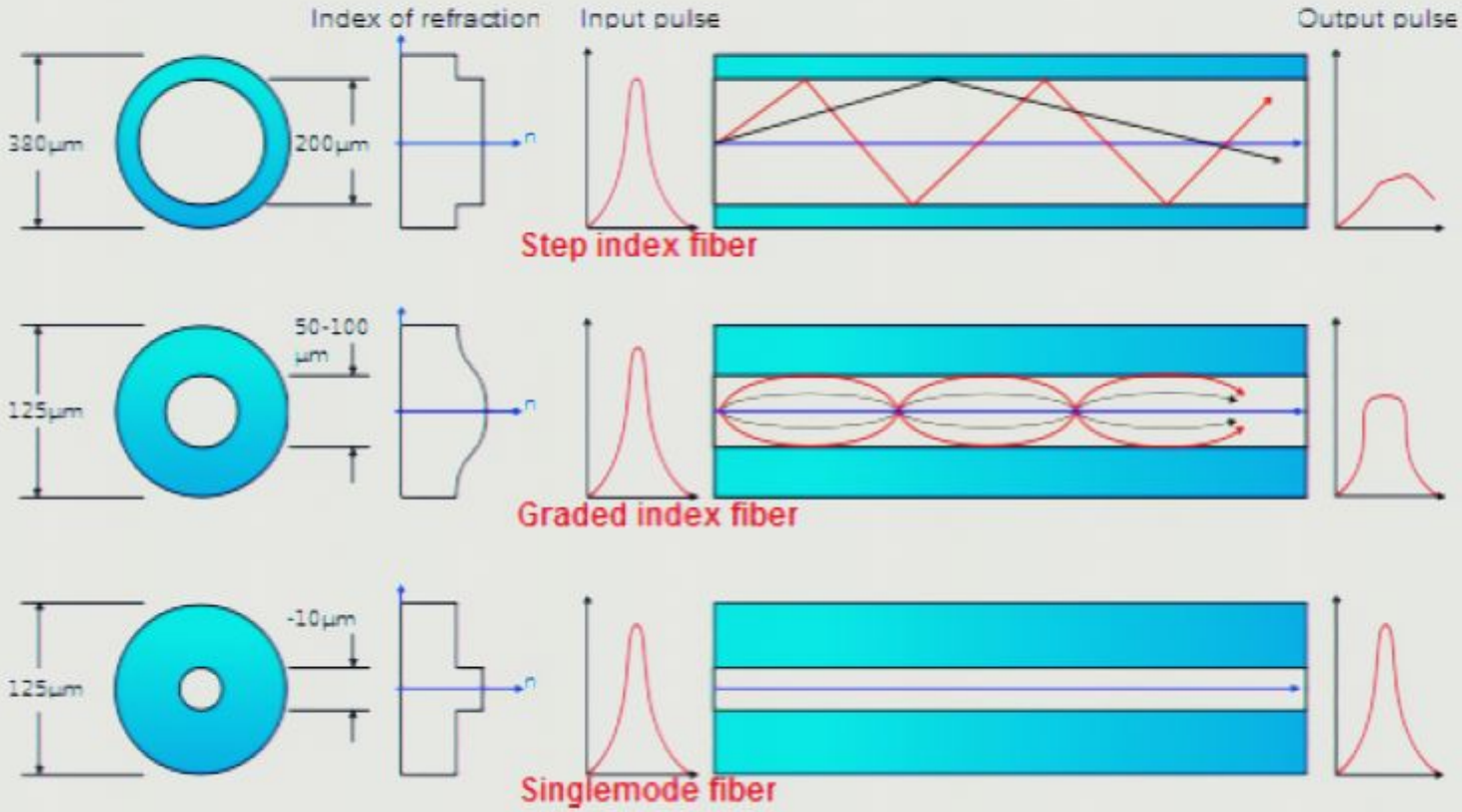


Sagnac Source of Entangled Photons

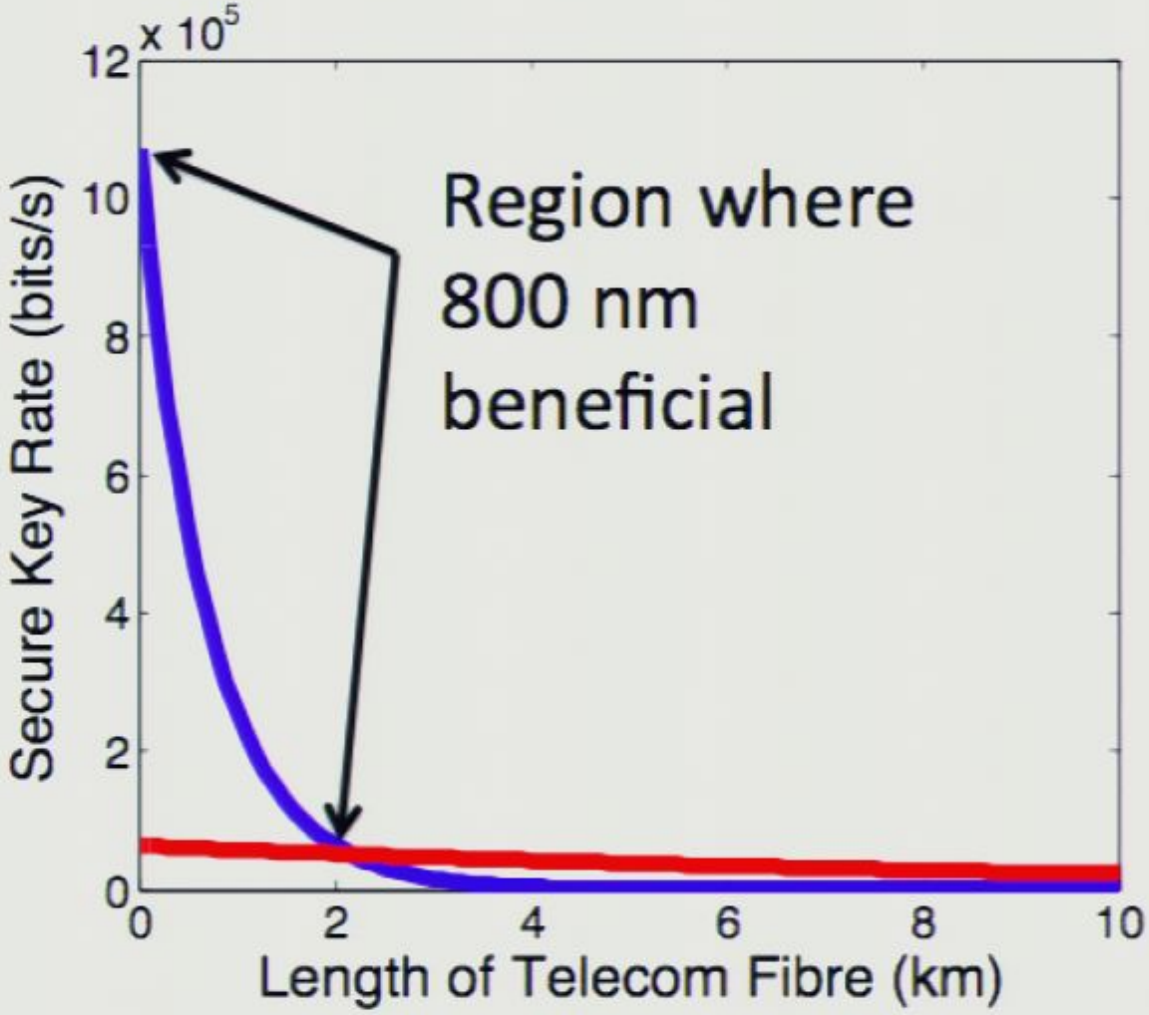


Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

Optical Fibre

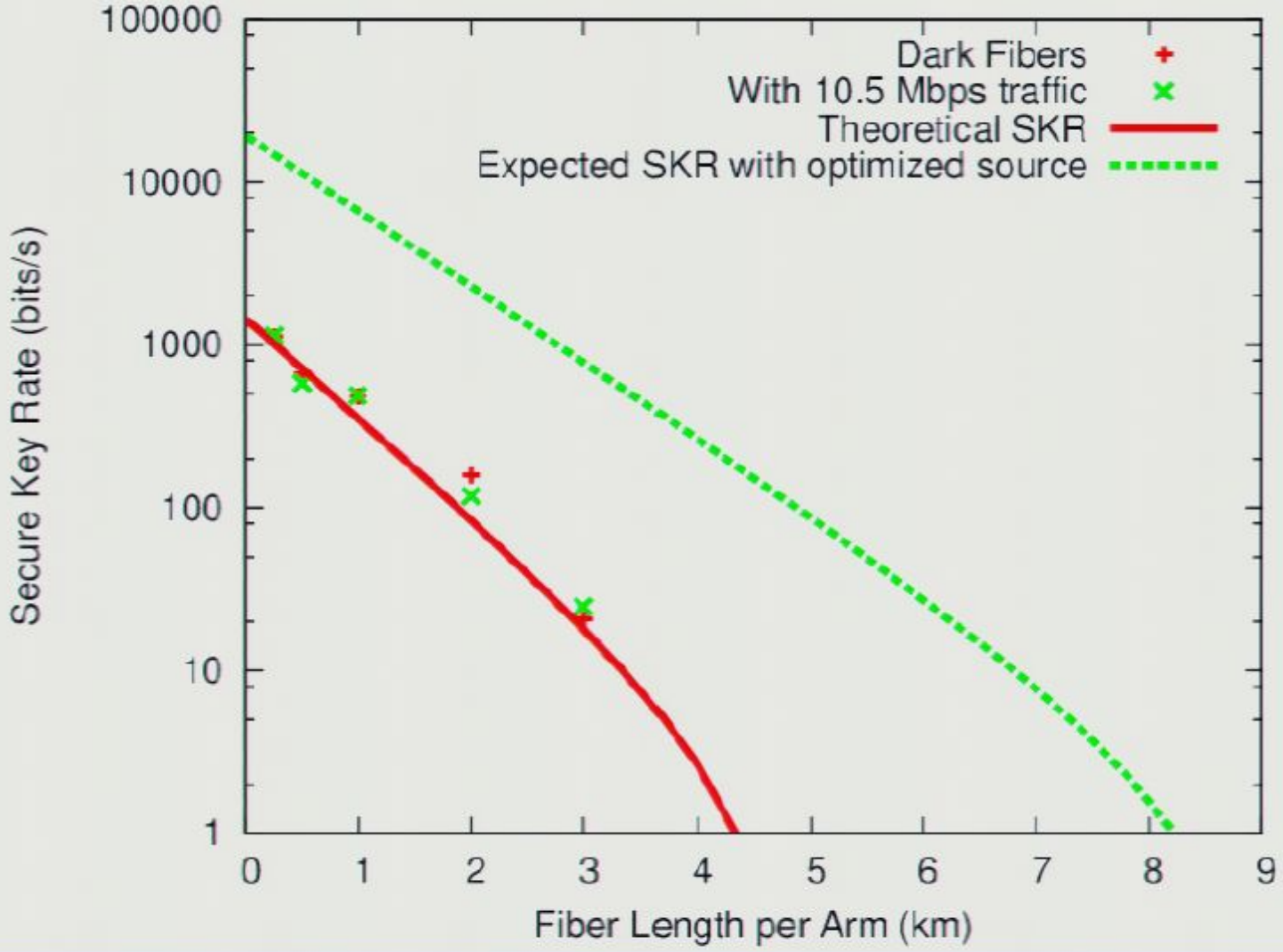


Optical Fibre



Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

Secure Key Rate vs. Distance

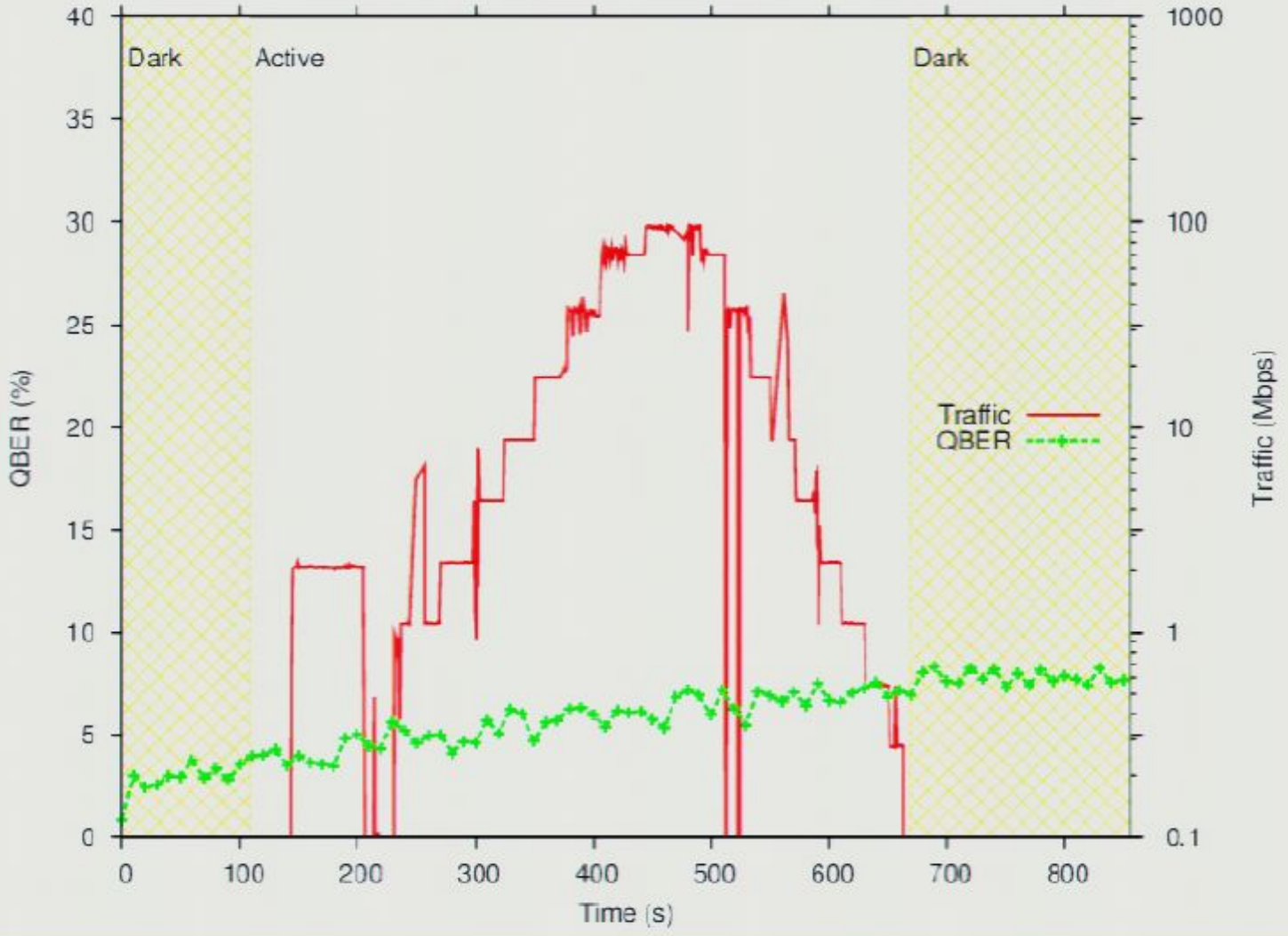


Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

Quantum Bit Error Rate (QBER)

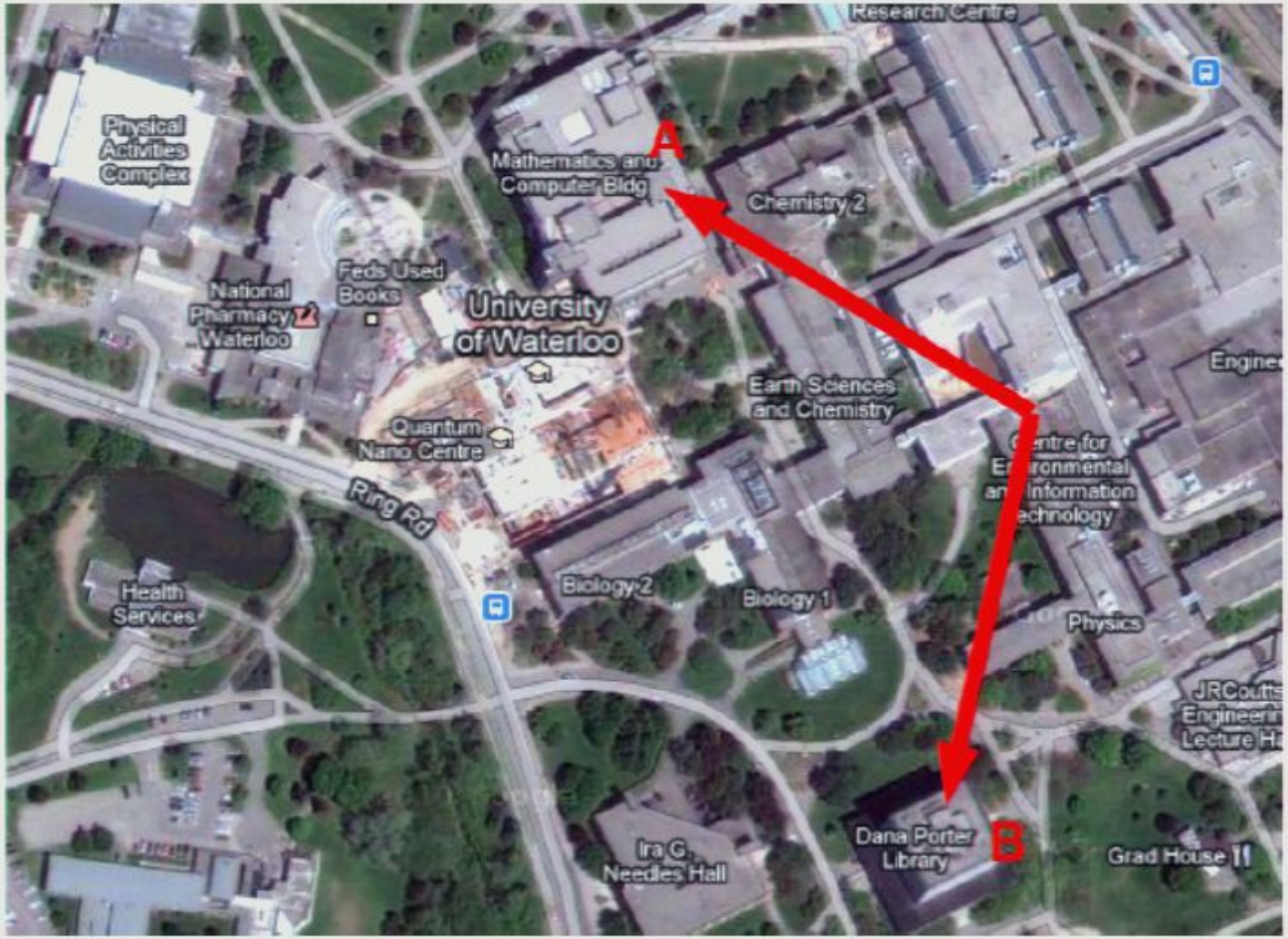
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

QBER with Traffic



Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

QKD Network



Catherine Holloway, Evan Meyer-Scott, Chris Erven, Thomas Jennewein

Conclusions

- Entanglement successfully distributed over short stretches (up to 6km) of telecom fibre
- Wavelength-specific fibre is not required for short wavelength quantum entanglement experiments
- Classical traffic can be introduced in the optical fibres using fibre splitters without affecting the QBER.