TOSHIBA
Leading Innovation

CWTEC
TECHNOLOGY & ENGINEERING CONFERENCE

14 SEPTEMBER 2016
CAMBRIDGE COMPUTER LABS

Securing tomorrow's data using QKD

Zhiliang Yuan

Quantum Information Group

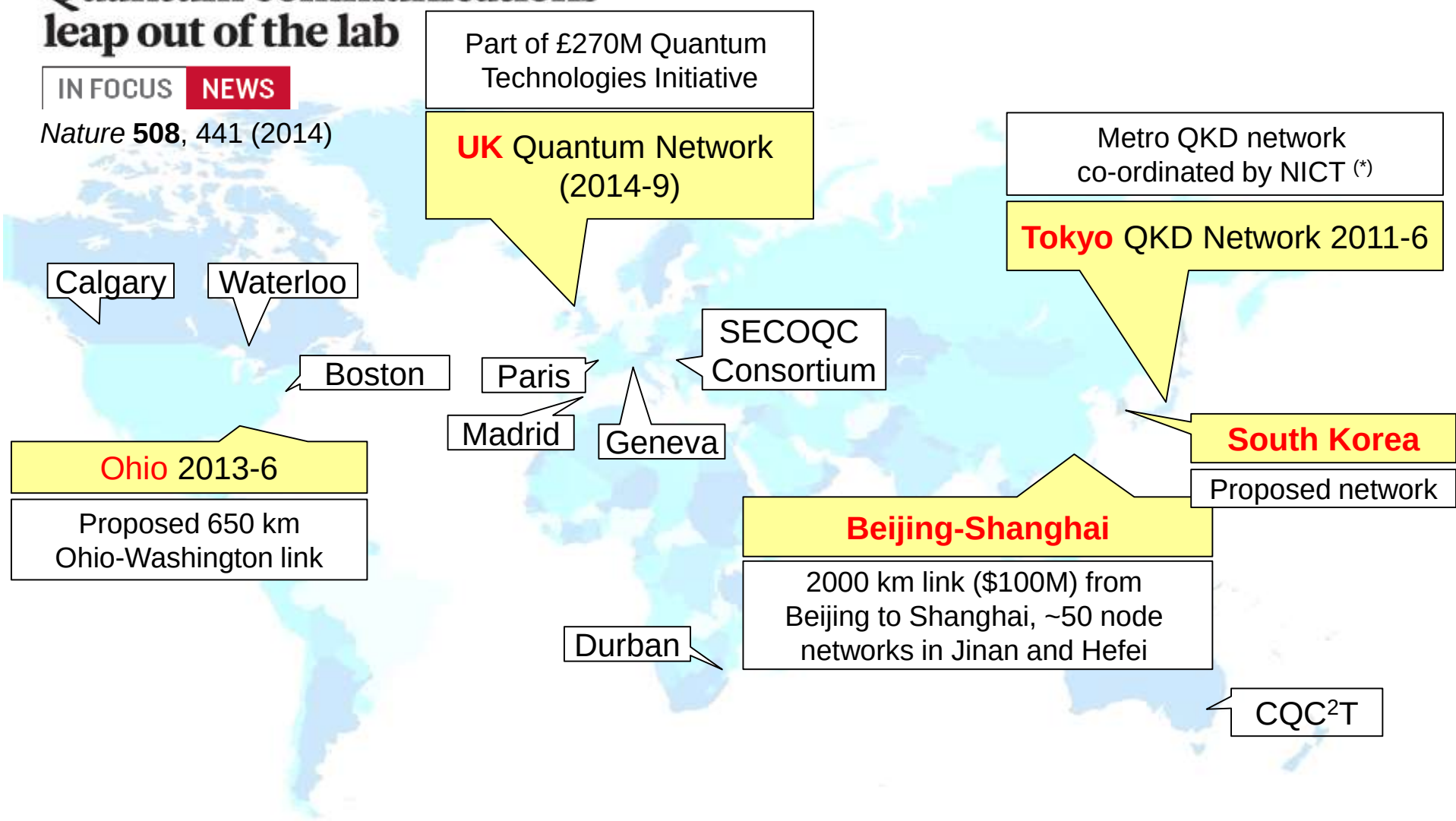
Toshiba Research Europe Ltd

208 Cambridge Science Park, Milton Road, Cambridge, UK

Quantum communications leap out of the lab

IN FOCUS NEWS

Nature **508**, 441 (2014)



(*) Talk by K. Tamaki @ http://tv.uvigo.es/es/serial/2302.html

European Commission - Press release

European Cloud Initiative to give Europe a global lead in the data-driven economy

Brussels, 19 April 2016

The Commission today presented its blueprint for cloud-based services and world-class data infrastructure to ensure science, business and public services reap benefits of big data revolution.

The Commission will progressively put in place the European Cloud Initiative through a series of actions, including:

- As of 2016: creating a **European Open Science Cloud** for European researchers and their global scientific collaborators by integrating and consolidating e-infrastructure platforms, federating existing scientific clouds and research infrastructures, and supporting the development of cloud-based services.
- 2017: **opening up by default all scientific data** produced by future projects under the €77 billion Horizon 2020 research and innovation programme, to ensure that the scientific community can re-use the enormous amount of data they generate.
- 2018: launching a flagship-type initiative to accelerate the nascent development of **quantum technology**, which is the basis for the next generation of supercomputers.
- By 2020: developing and deploying a large scale **European high performance computing, data storage and network infrastructure**, including by acquiring two prototype next-generation supercomputers of which one would rank among the top three in the world, establishing a European big data centre, and upgrading the backbone network for research and innovation (GEANT).

The public and private investment needed to implement the European Cloud Initiative is estimated at **€6.7 billion**. The Commission estimates that, overall, **€2 billion** in Horizon 2020 funding will be allocated to the European Cloud initiative. The estimation of the required additional public and private investment is **€4.7 billion** in the period of 5 years.

ETSI ISG-QKD Group

- ISG-QKD established in 2008
- Membership comprises large industry, telecom operators, SMEs, NMIs, government labs, universities
- Published Group Specification documents: Components and Internal Interfaces, Security Proofs, QKD Module specification, Application Interfaces, QKD Use Cases

Why?

- Interoperability of systems from different manufacturers
- Integration into ordinary telecom networks
- Stimulate application development on common interfaces
- Stimulate a component supply chain for Quantum Technologies
- Security assurance
  - Ensure that QKD is implemented securely

Work areas:

- Characterisation of quantum optical components and QKD modules
- Implementation security
- Deployment, interoperability etc.

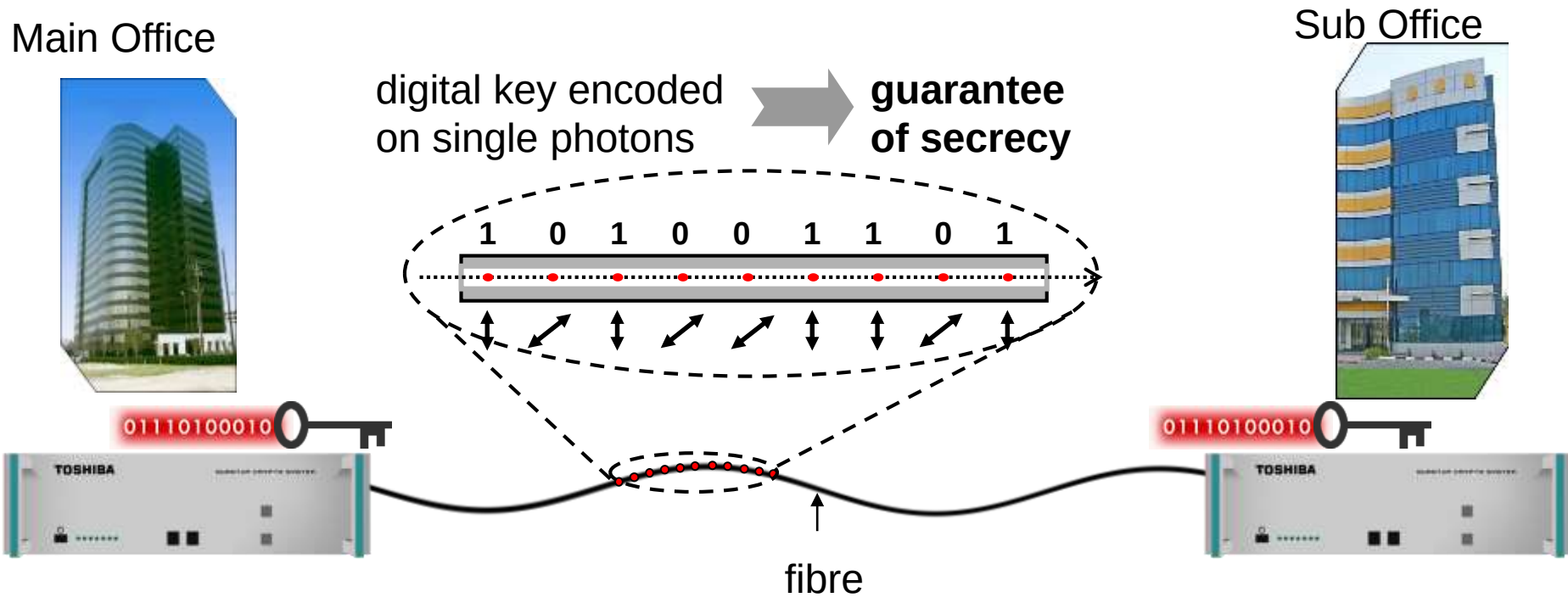
National Metrology Institutes:

- Optical metrology for quantum-enhanced secure telecommunication
- Characterising side-channel attacks and counter-measures
- Metrology of components

Overview

- Introduction to QKD
- GHz QKD Cryptosystem
- QKD in Telecom Networks
- Novel Phase Modulation Technology

Quantum Key Distribution (QKD)



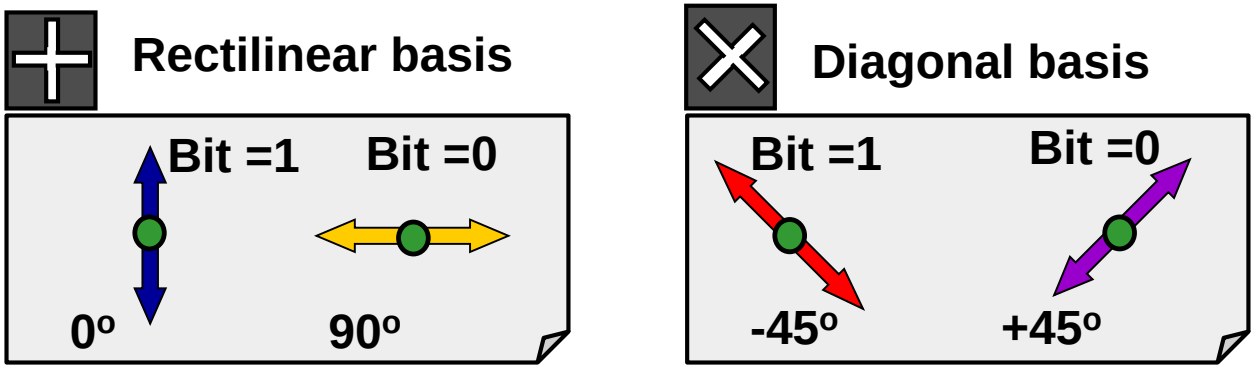
Features

- **Encryption keys formed with transmission of single photons**
- **Each individual key can be guaranteed secret (without any assumptions about Eve's resources)**
- **Not vulnerable to future advances in Computing, Maths or Engineering**
- **Frequent key refresh & simplified key management**

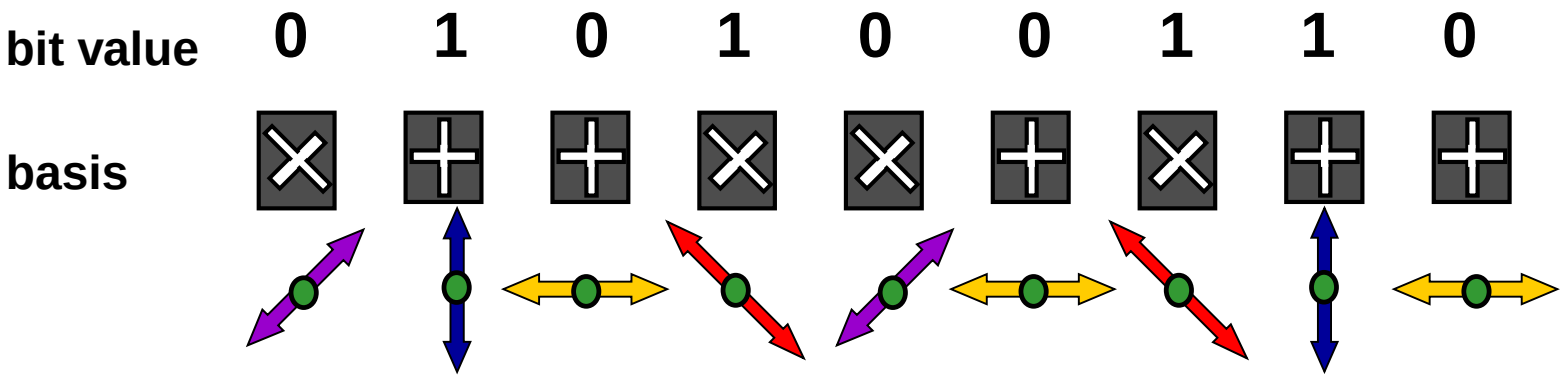
Encoding Quantum Bits

'Four state protocol', Bennett and Brassard, 1984

- **Alice encodes each bit in one of two non-orthogonal bases**
  - **choice is random for each bit**



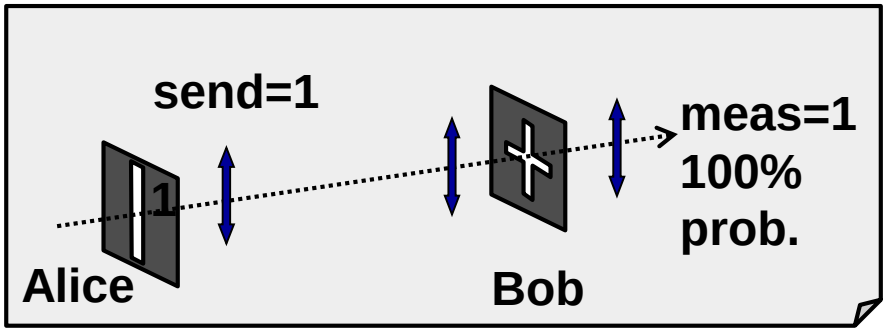
- **for each clock cycle Alice sets both bit value and basis**



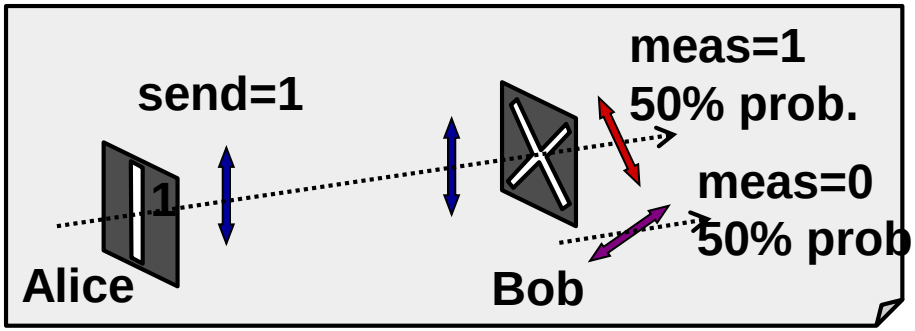
Quantum Bit Measurement

- Bob makes random choice of measurement basis for each bit

If A&B use **same** bases → **deterministic** result



If A&B use **different** bases → **probabilistic** result



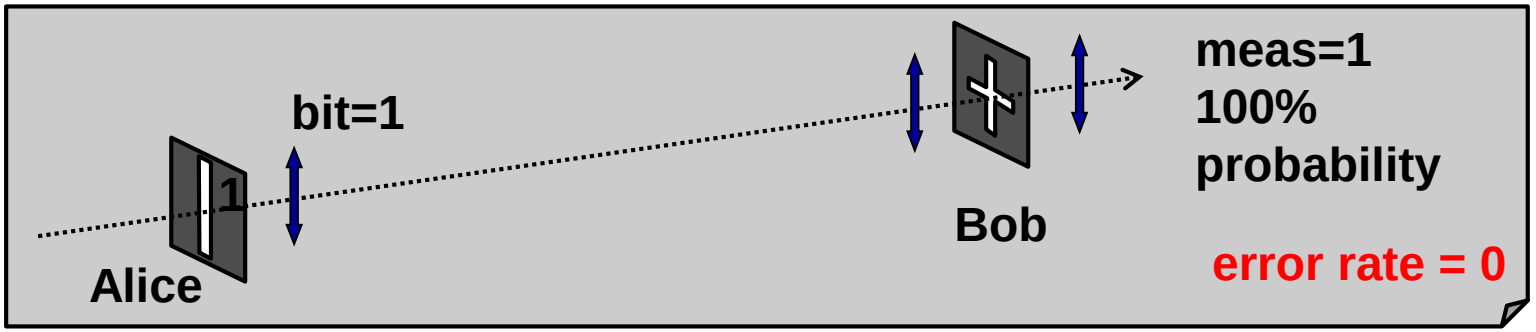
- After measurements, Alice and Bob compare bases (not bit values!)

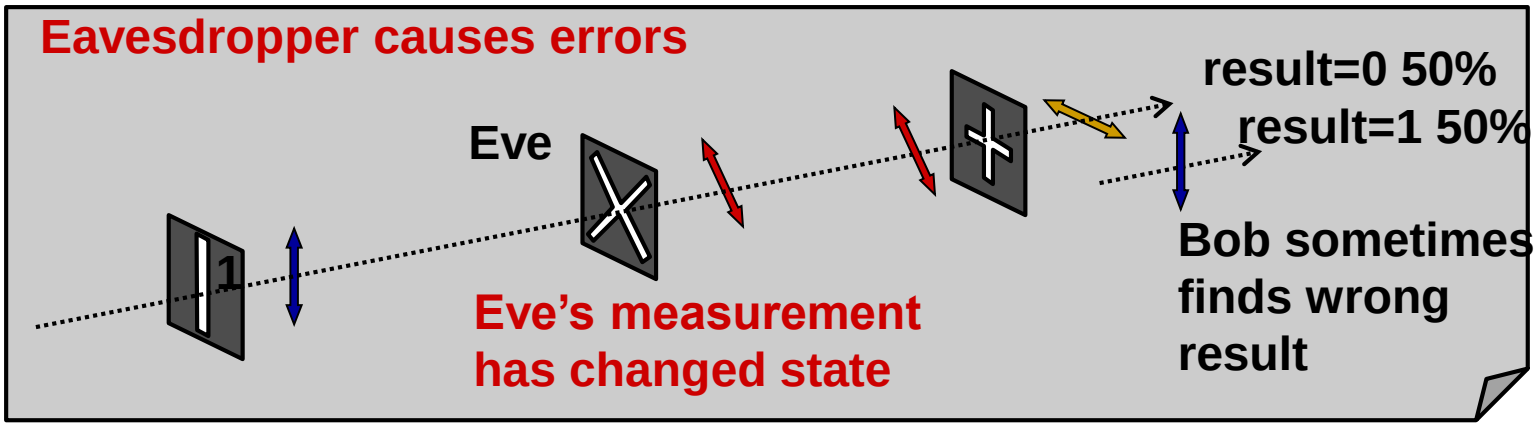
  They keep bit only if :-
  - they have used the same basis
  - Bob has detected photon

→ A&B form shared bit sequence

Detection of Eavesdropping

Alice and Bob compare bases after Bob's measurement and post-select only those results for which they use same basis





High error rate indicates presence of eavesdropper

Bob and Alice compare a small part of their key
(errors in key = Eve may be present)

Error Processing

excluding any info. (potentially) known to Eve

Imperfections (noise etc) of a real system also cause errors, which are indistinguishable from those due to Eve

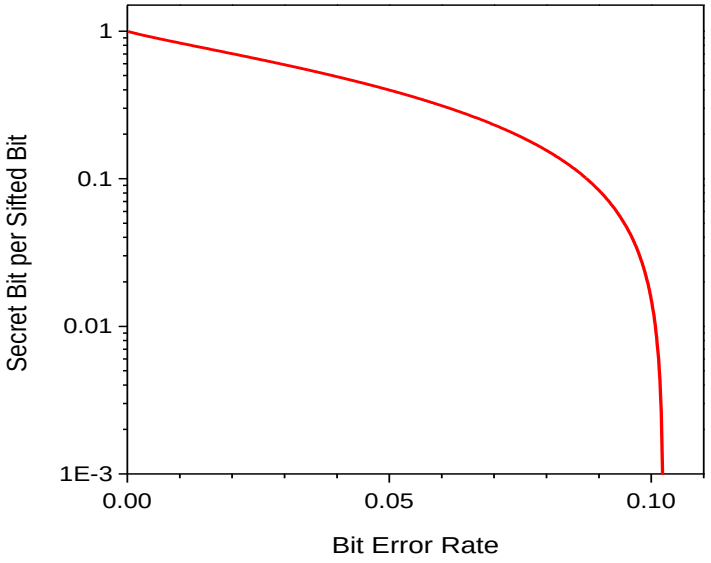
'Privacy amplification' can be used to exclude any information *potentially* known to Eve due to finite error rate

(Bennet, Brassard, Crepeau, Maurer, IEEE Trans Inf Theory 41, 1915 (95))

Final key rate after error correction and privacy amplification:

$$R_{Secure}=qR_{Raw}\{1-[1+f(e)]h(e)\}$$

q*: protocol efficiency, *h(e): Shannon entropy, f(e) error correction efficiency



Bit error rate must be smaller than a threshold for secret distillation!

GHz QKD Cryptosystem

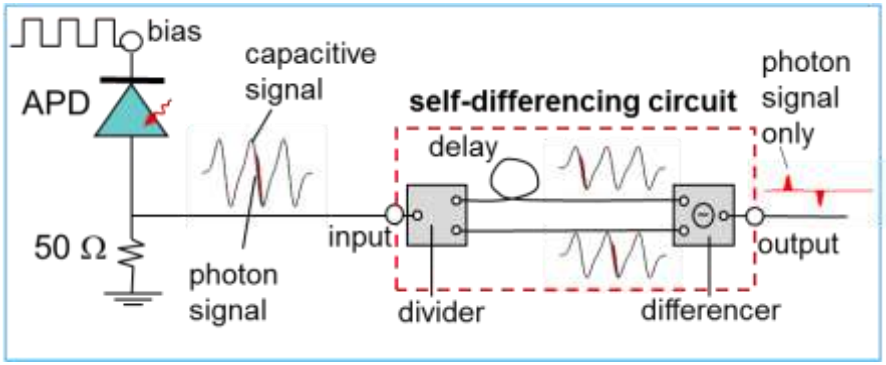
Features

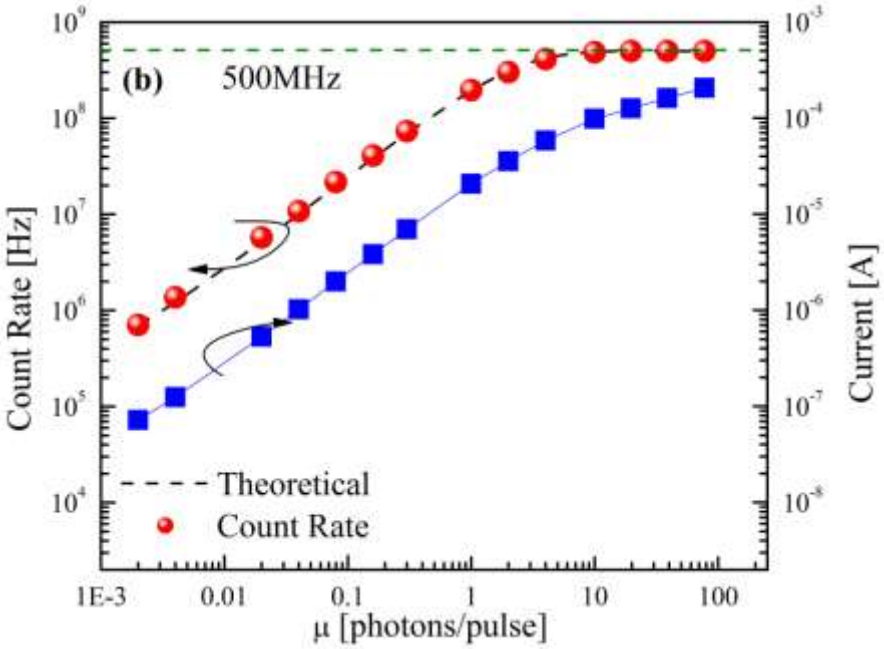
- ✓ 1GHz clock rate
- ✓ Key exchange rate (**>1Mb/s@50km**)
- ✓ Over 150 km (30 dB)
- ✓ Rigorous security proof
- ✓ Operable over single fibre
- ✓ Room-temperature operation

Underlying technologies

- ✓ **Fast self-differencing detectors**
- ✓ **Active stabilization technology**
- ✓ **Detector noise resilient**
- ✓ Efficient decoy-state BB84 protocol
- ✓ Fast privacy amplification routine
- ✓ **Phase modulation technology**

Self-differencing Detectors

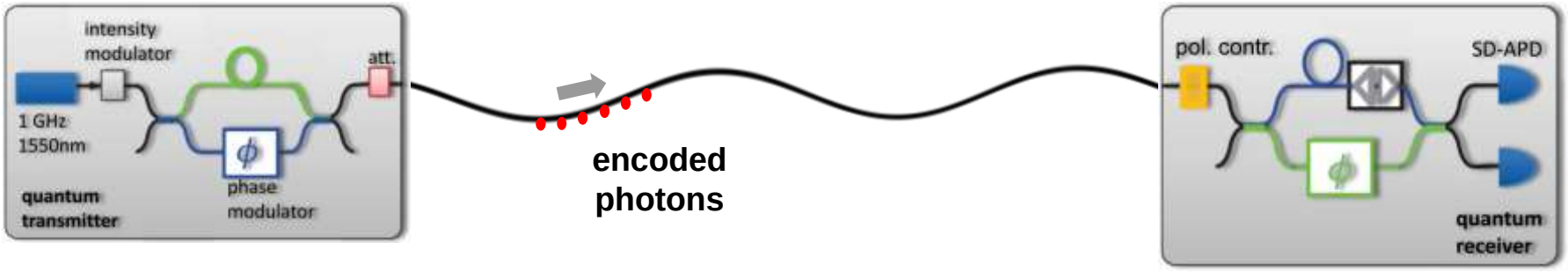




- ✓ Compact semiconductor avalanche photodiodes (APDs)
- ✓ High count rate (500Mcounts/s) and efficiency (up to 55%) enable highest secure key rate
- ✓ Operable at room-temperature
- ✓ Intrinsic noise rejection (10 dB) by fast gating

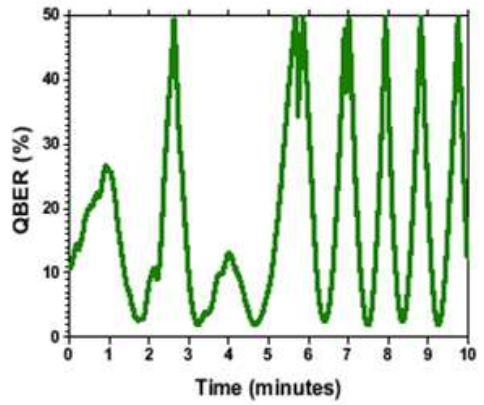
Comandar et al, J. Appl. Phys. **117**, 083109 (2015)

Active Stablisation

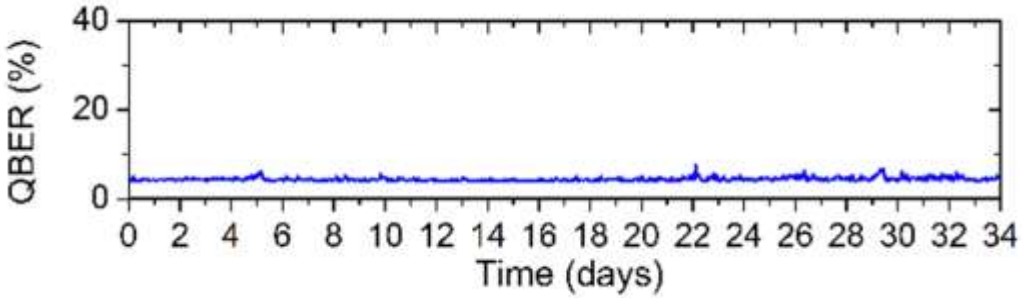


- Fibre based Mach-Zehnder interferometer for phase encoding
- Drift in interferometer length and polarisaton ➔ Instability
- Introduce active feedback system

Free-drifting



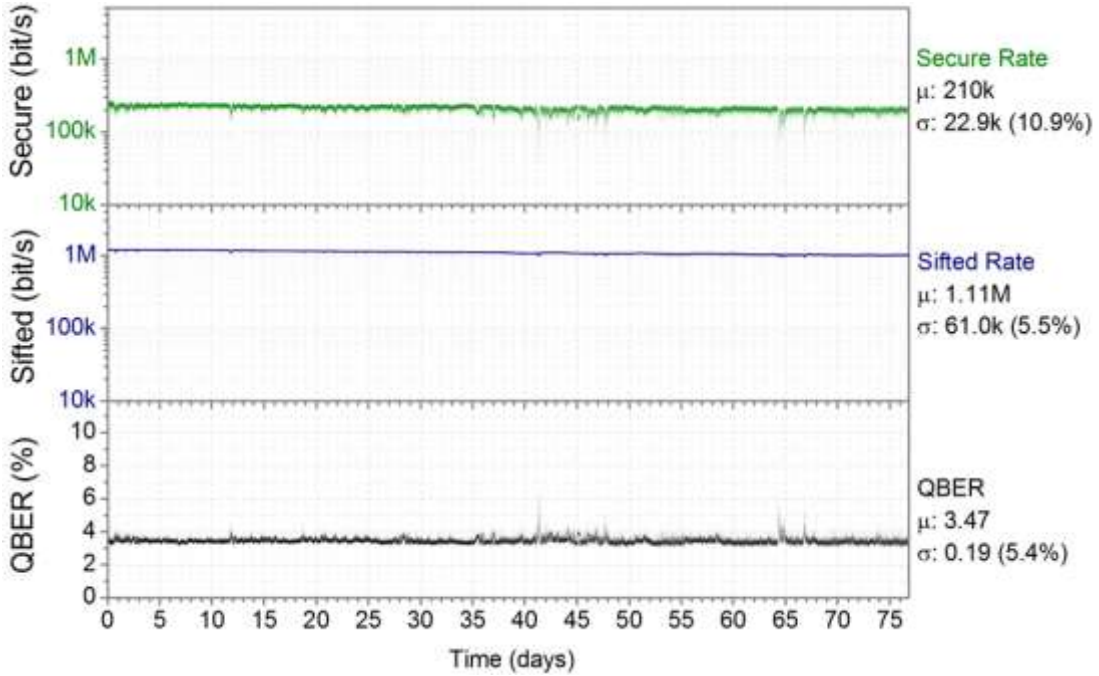
Actively Stabilised



Dixon *et al*, Opt. Express **23**, 7583 (2015)

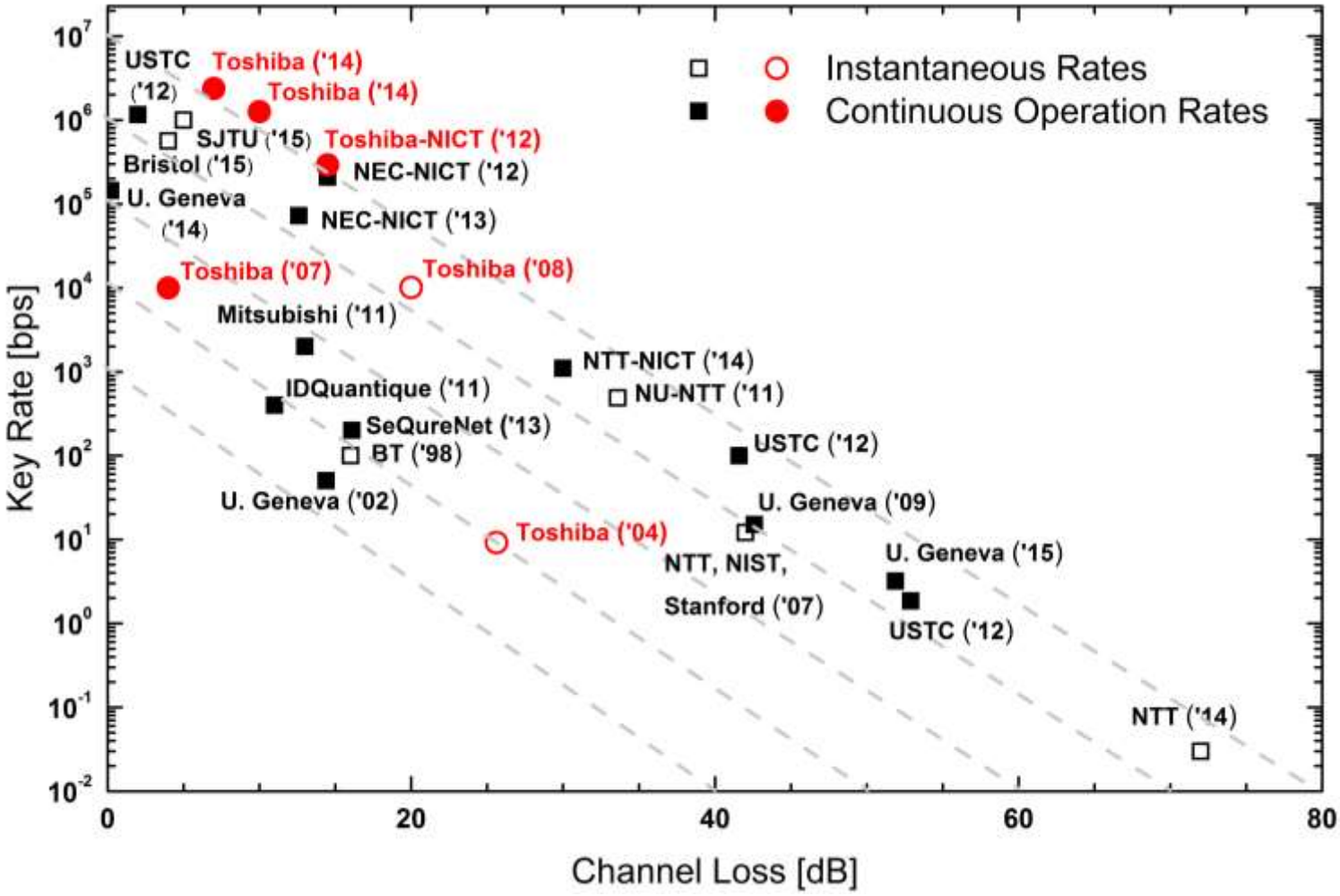
Field Trials

Map Imagery ©2014 TerraMetrics, Map data ©2014 Google, ZENRIN



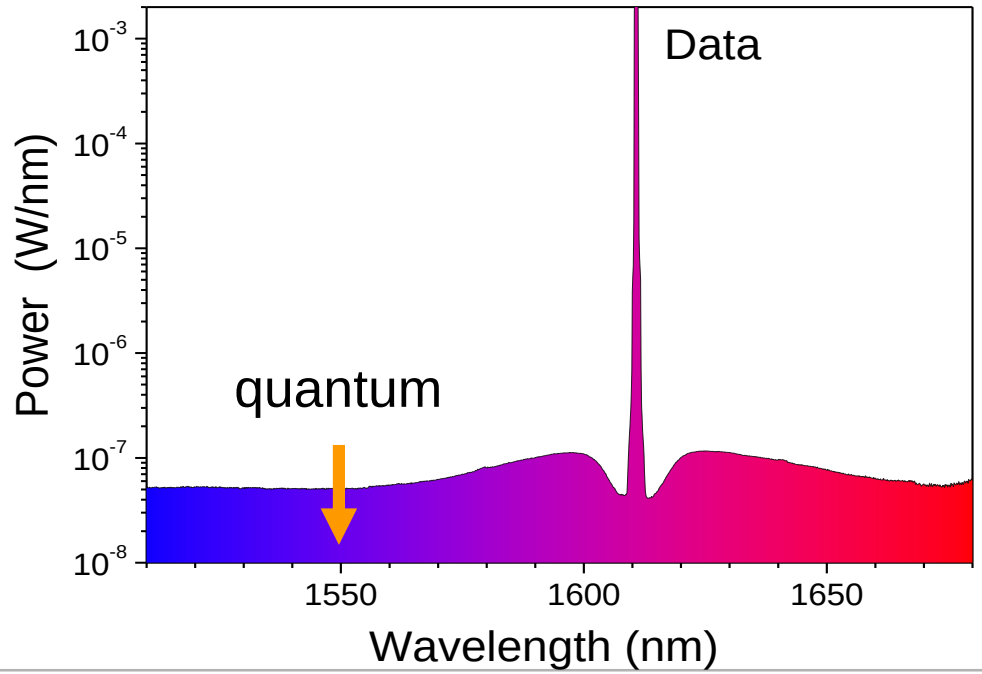
- Installed QKD system in JGN-X fibre network
- Fibre link 45km with attenuation = 0.32 dB/km
  - 50% of the fibre are aerial lines → subjected to weather conditions
- Continuous operation > 67 days, a total of 1.33 Terabits exchanged
- System kept operating despite a series of weather depressions
- Secure bit rate ~ 210kbps

QKD on Dark Fibre



Integration into telecom networks

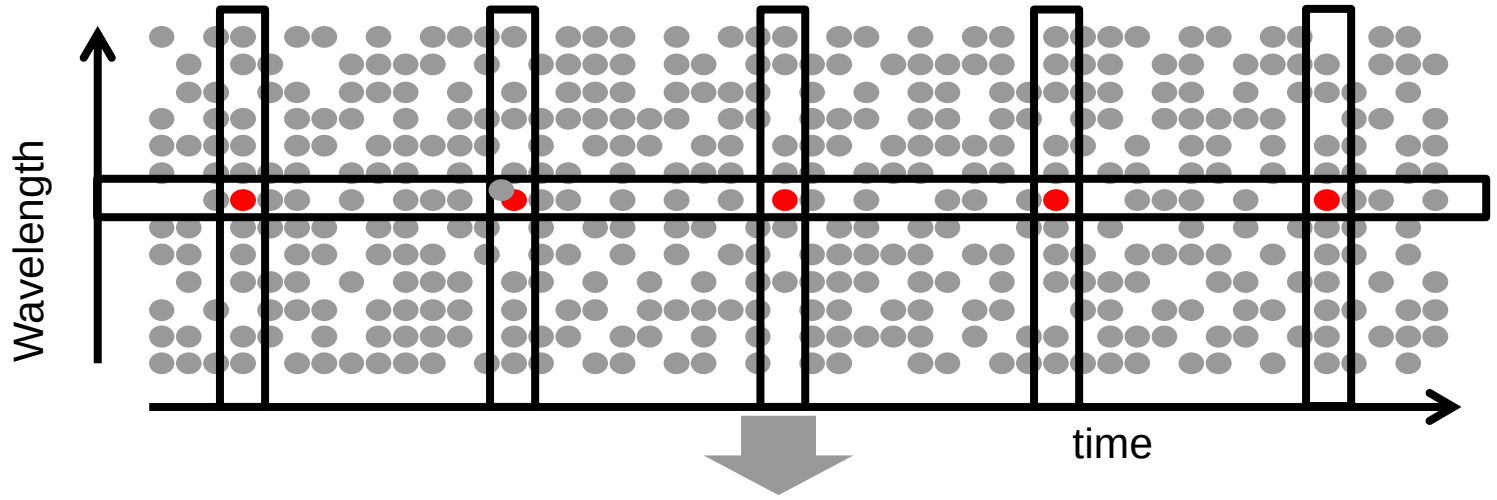
- Dark fibre is expensive and not always available
- Telecom networks already populated with intense data signal, typically 10^7 - 10^8 times stronger than QKD signal
- Inelastic scattering of data signals (Raman scattering) may swamp quantum signals



Raman noise suppression

1 Filter in wavelength

2 Filter in time



Time-bandwidth limit: $$\Delta\nu \times \Delta t \geq \frac{2\ln 2}{\pi} \cong 0.44$$

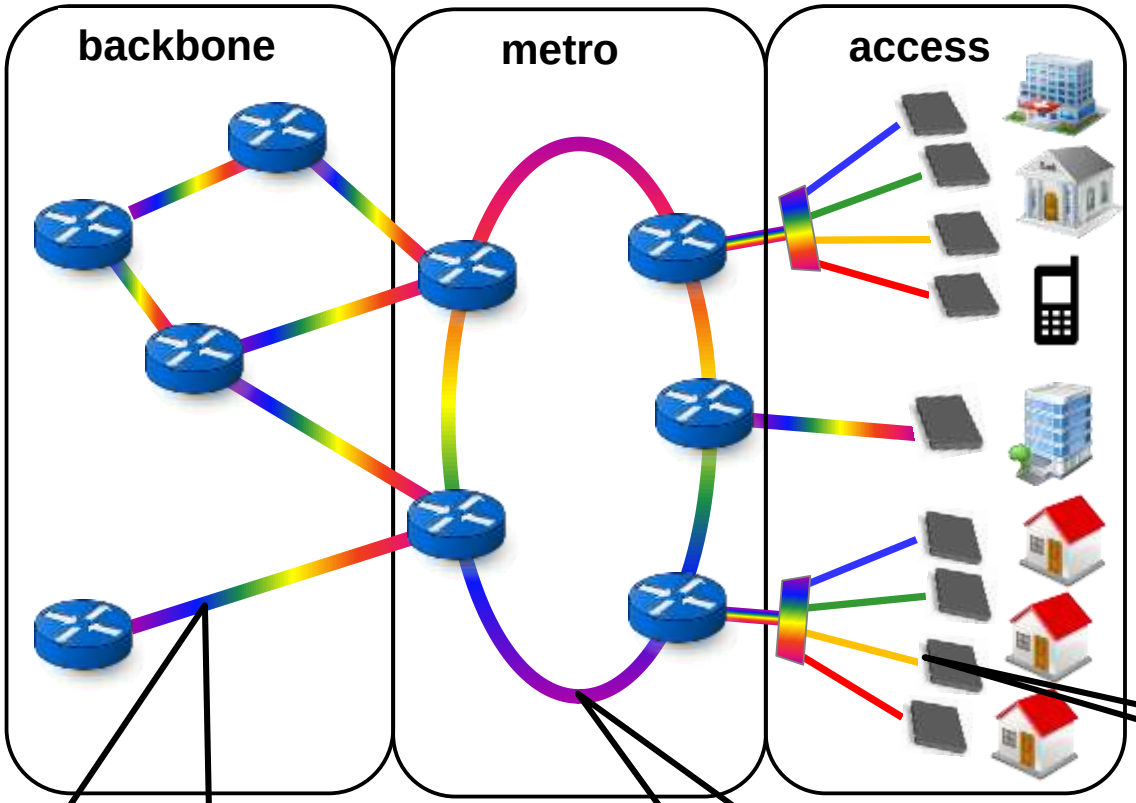
3 Reducing data laser power

- reduces scattered light by factor of 10000!
- QKD is possible after wavelength/temporal filtering.

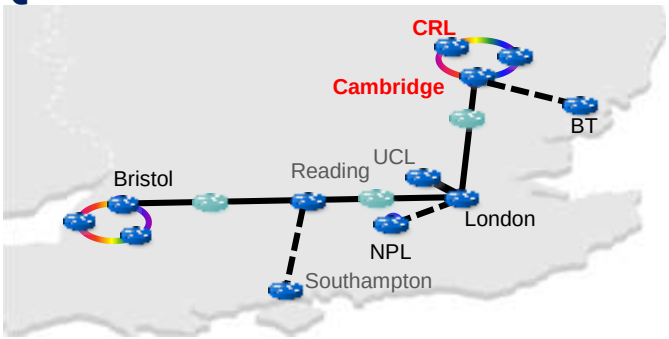
Patel *et al*, PRX **2**, 041010 (2012); APL 104, 051123 (2014)

UK Quantum Network

Develop QKD technology for different network segments (backbone, metro, access)



Long-Term Test in UK Quantum Network



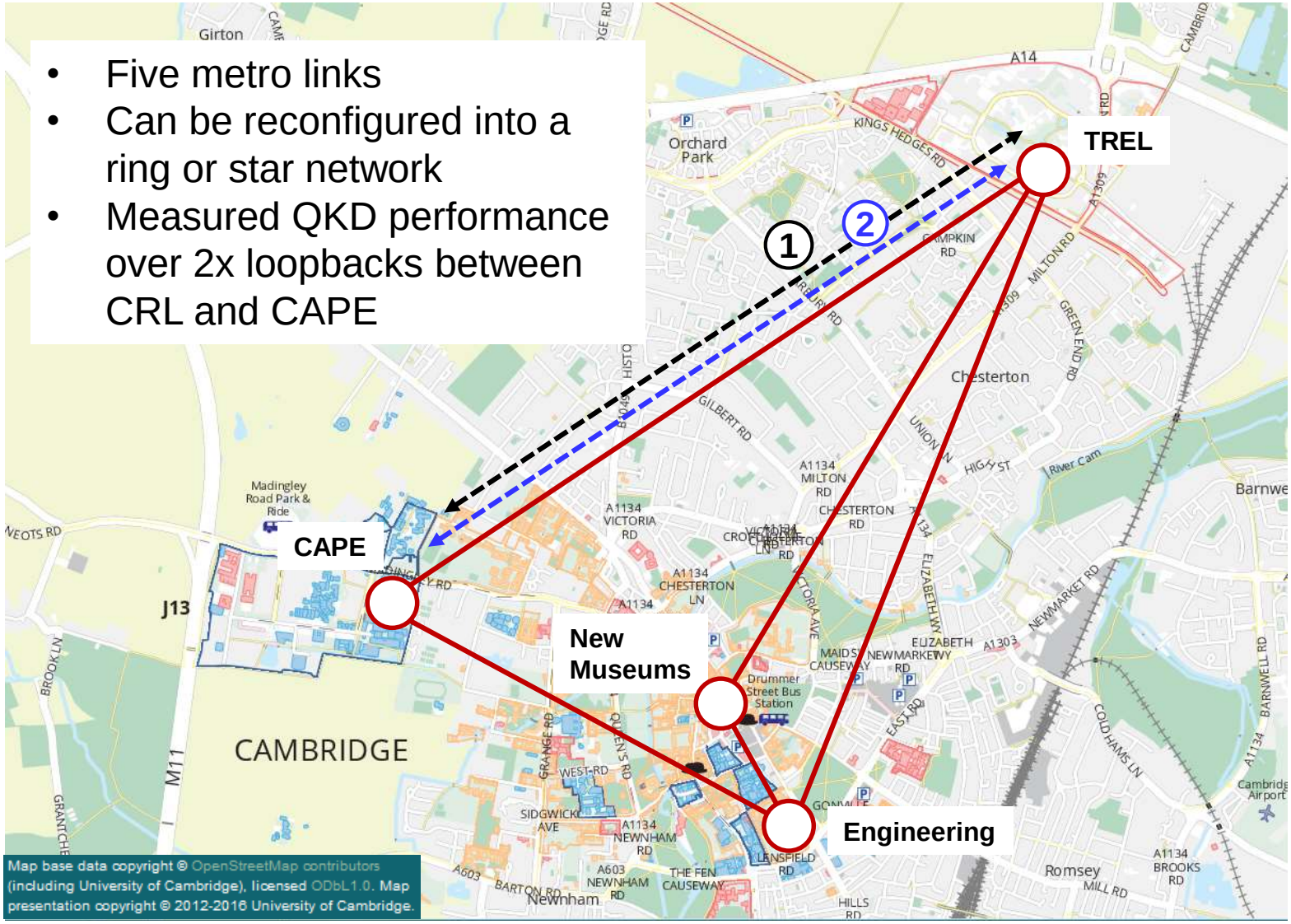
Extend single link to > 200km (x2 current) sufficient for nearly all links in UK and develop trusted relay technology for arbitrary distance technology.

Demonstrate Cambridge Quantum Network with four nodes.

Develop portable endpoint QAN for large scale network.

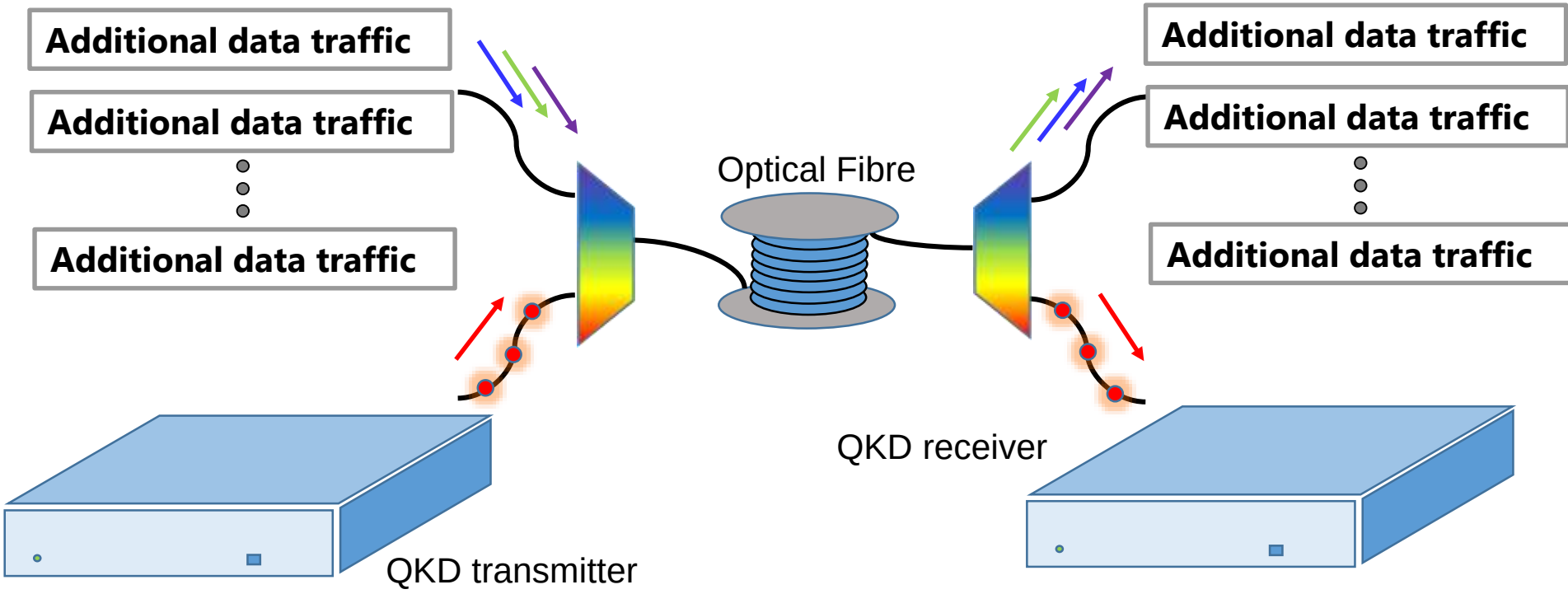
Cambridge Metro Network

- Five metro links
- Can be reconfigured into a ring or star network
- Measured QKD performance over 2x loopbacks between CRL and CAPE



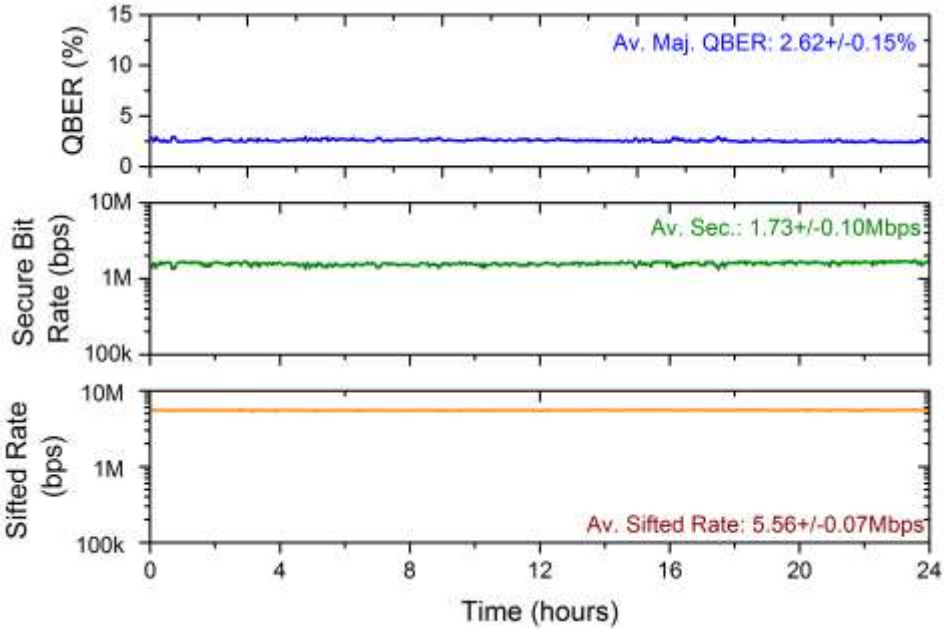
Single fibre QKD systems

- Five single fibre QKD systems for Cambridge Metro Network
- 1Gb/s clock rates with > Mbps secure bit rates over 10dB loss
- Key failure probability < 10^{-10}
- Single fibre operation allows other data traffic to be seamlessly integrated onto the same fibre



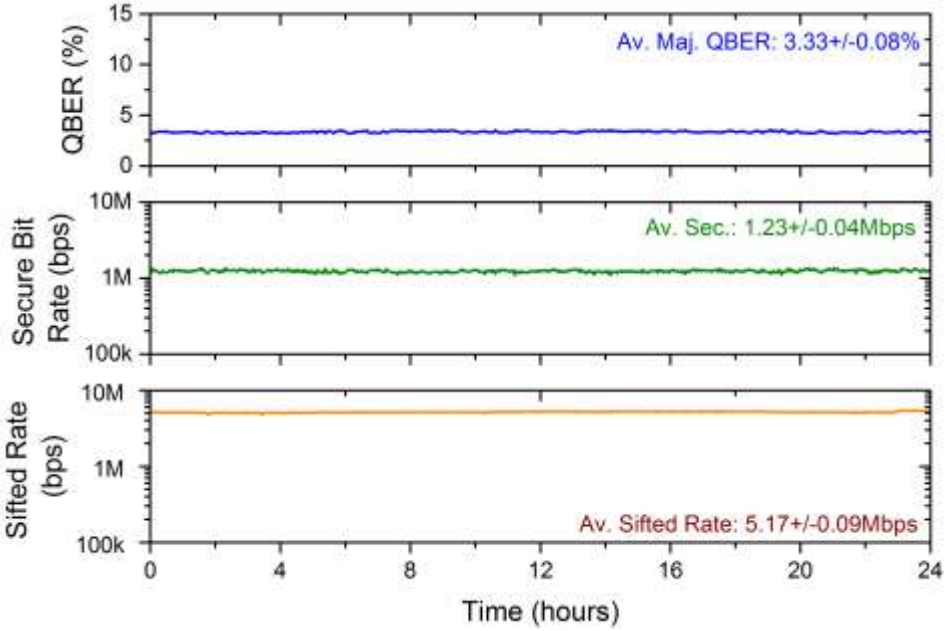
Current Cambridge Metro Network QKD Performance

- CRL-CAPE-CRL link ①



- Fibre distance = 21km (loss ≡ 8.3dB)
- Secure bit rate = 1.73Mbps
- QBER = 2.62%

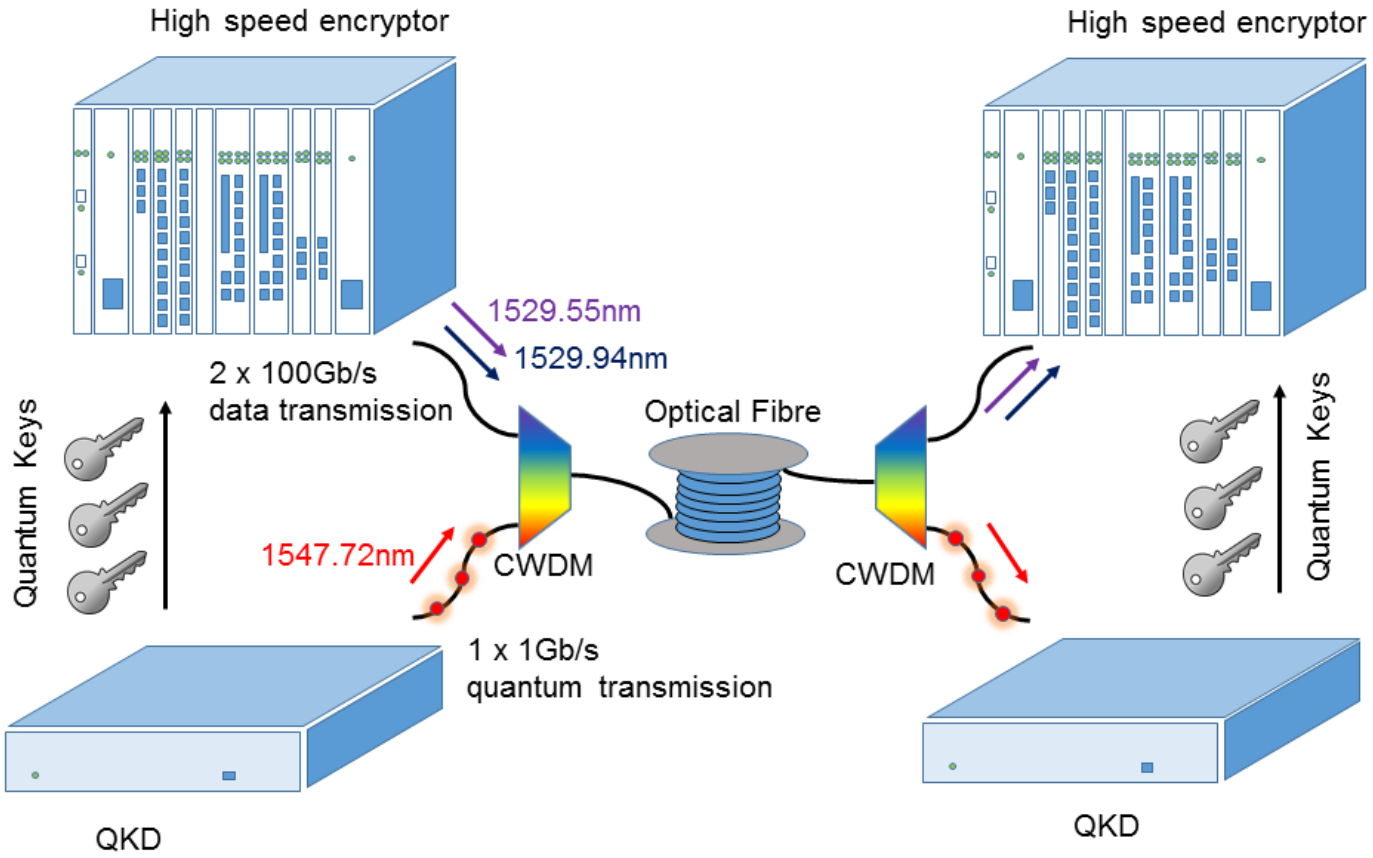
- CRL-CAPE-CRL link ②



- Fibre distance = 31km (loss ≡ 9.3dB).
- Secure bit rate = 1.23Mbps
- QBER = 3.33%

- **Indicates promising network QKD performance with > Mbps rates**

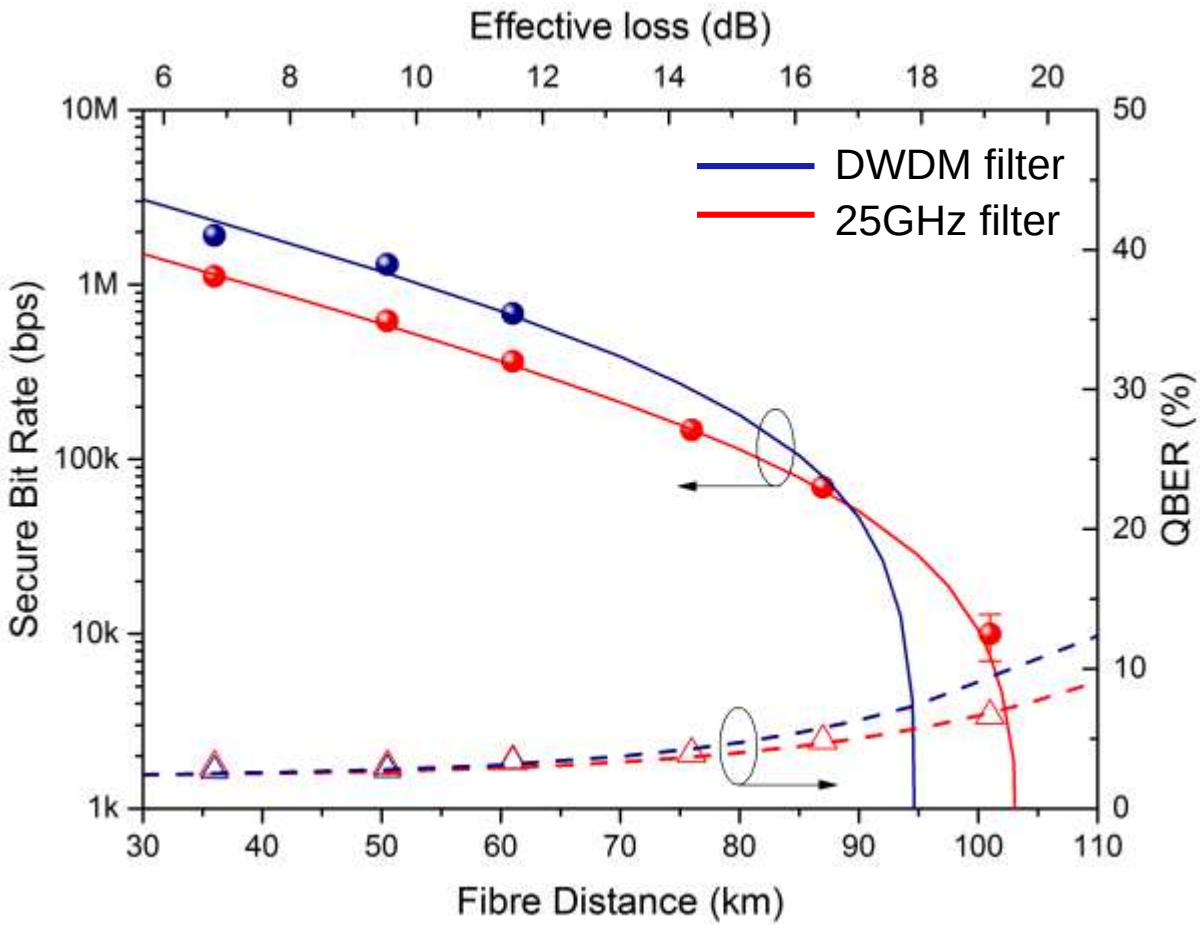
Network Quantum Link Encryption



- Experiments to test QKD multiplexed with ultra high (> 100Gb/s) data transmission
- Use a DP-QPSK coherent transport solution with enhanced error correction
- Transmit QKD and data using different wavelengths
- Use QKD to refresh high speed encryption key

J. F. Dynes *et al*, submitted (2016)

Single fibre quantum comms. – Distance dependence



- QKD & 200Gb/s data for fibres up to 100km
- Secure bit rate at short distances: 1.9 Mb/s with data = 200 Gb/s @ 36km

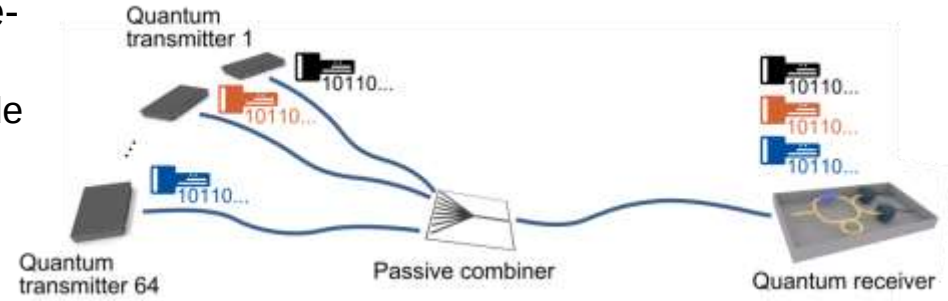
J. F. Dynes *et al*, submitted (2016)

Quantum Access Network

Quantum **A**ccess **N**etwork (QAN) to create large-scale QKD networks.

- Multiple users share connect to common network node
- Share cost of fibre and QKD hardware

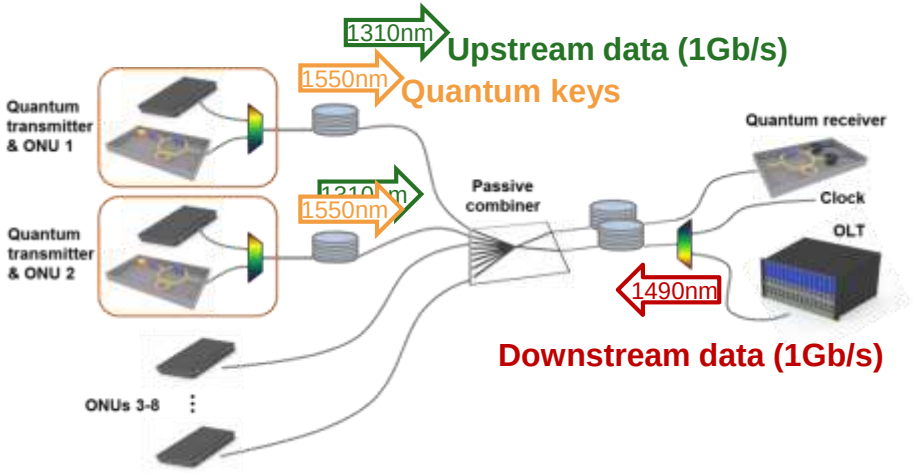
Nature **501**, 69 (2013)



Combine 128-user QAN with Gigabit Data Network

Experimental Set-Up

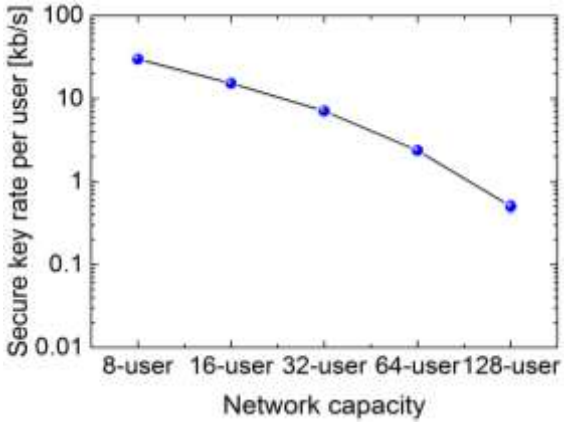
- Combine QKD with Gb/s Access Network signals.



- best results using dual feeder fibre.

Results

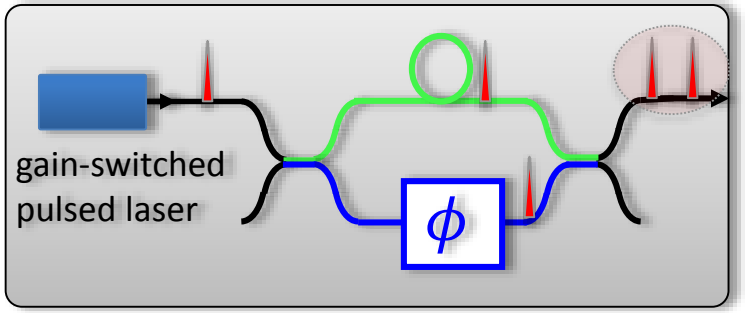
- QKD operating with fully functional Gb/s network.
- Connect up to 128 users to single network node.



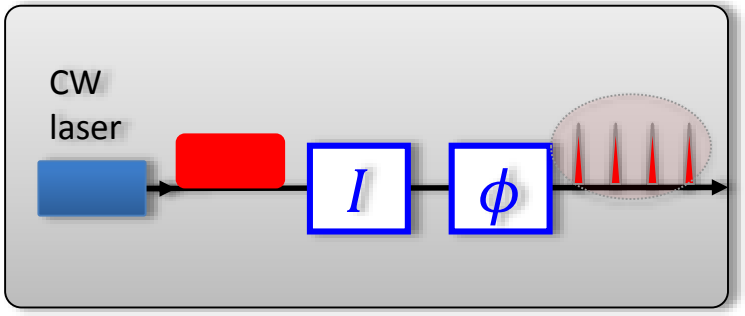
Sci. Rep. **5**, 18121 (2015)

Current Phase Modulation Technology

Discrete Phase

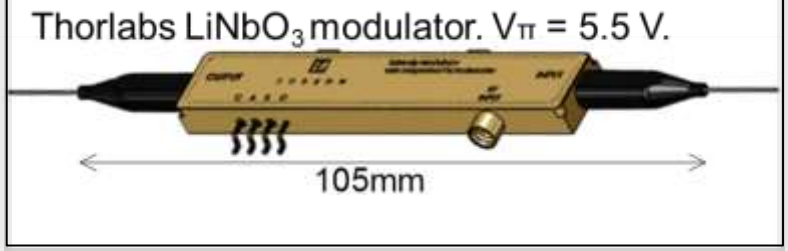


Distributed Phase



- Incompatibility between protocols
- Cumbersome structure
- Require external $LiNbO_3$ modulator(s)
- Require RF amplifier(s) to drive

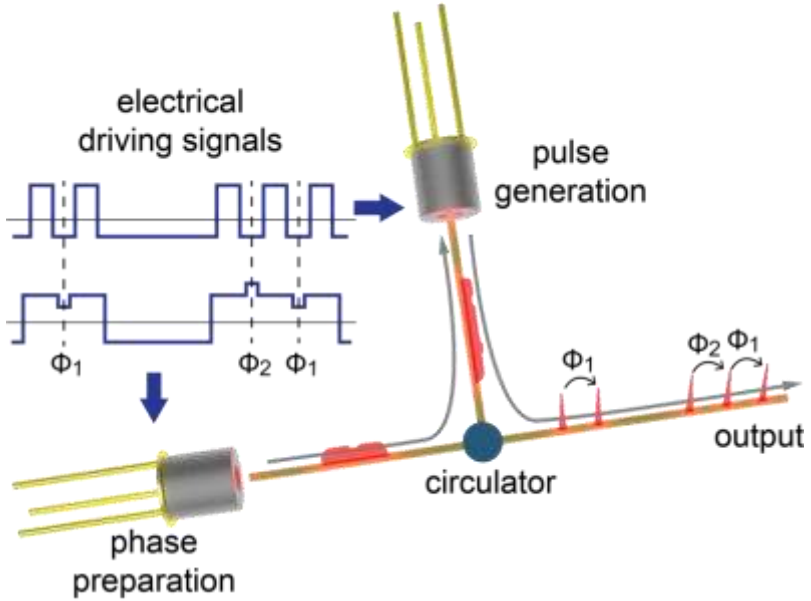
$LiNbO_3$ Modulator
$V\pi$: 5.5V (Thorlabs)

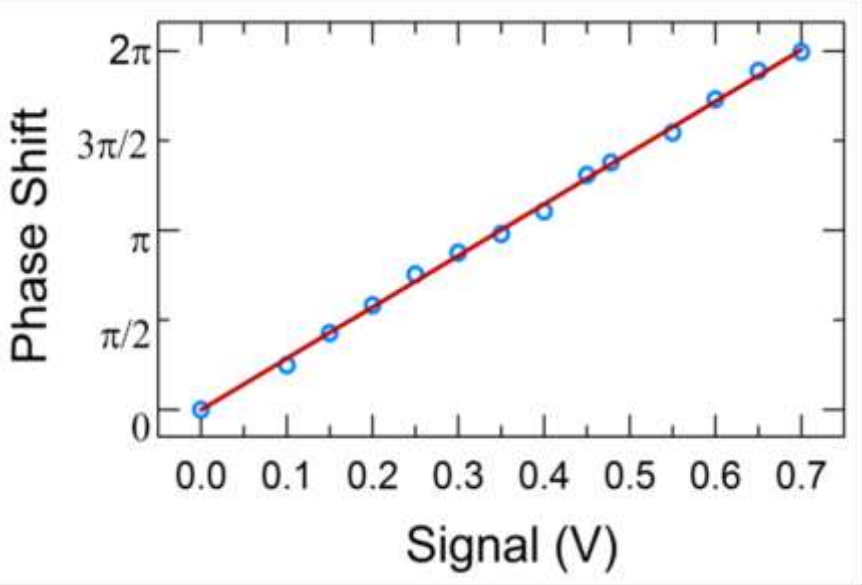


- Photonic integration helps shrink the optics size ***but it alone cannot reduce RF driving voltages***
- Innovation is required to remove the need for RF amplifiers

Direct phase modulation technology

- Direct modulation of laser diodes (DML) is attractive
  - ✓ Simplicity
  - ✓ low drive voltage
- Primarily used for intensity modulation
- Unable to produce pure phases
- **Solution: coherence injection**





- Halfwave voltage: 0.35V.
  - Compatible with CMOS
  - Removes the need for RF amplifiers

Yuan et al, Phys. Rev. X 6, 031044 (2016)

Conclusion

- **GHz QKD System**
  - Self-differencing detectors
  - Active stabilisation technology
  - Coexistence of QKD and data over same fibre
  - 1 Mbit/s key rate @ 50 km
- **UK QKD Network**
  - QKD for different network segments
  - Cambridge Metro Network
  - 128-user Access Network demonstrated in Lab
- **Direct Phase Modulation Technology**
  - Remove the need for external phase modulators
  - Low halfwave voltage (0.35V) – CMOS compatible
  - Compatible with all major QKD protocols


TOSHIBA
Leading Innovation