

Securing Genome Data with Quantum Key Distribution

Alex Dixon, James Dynes, Marco Lucamarini,
Simon Tam, Alan Plews, Martin Brice, Zhiliang Yuan,
Yoshimichi Tanizawa, Shinichi Kawamura, Hideaki Sato,
Andrew Shields

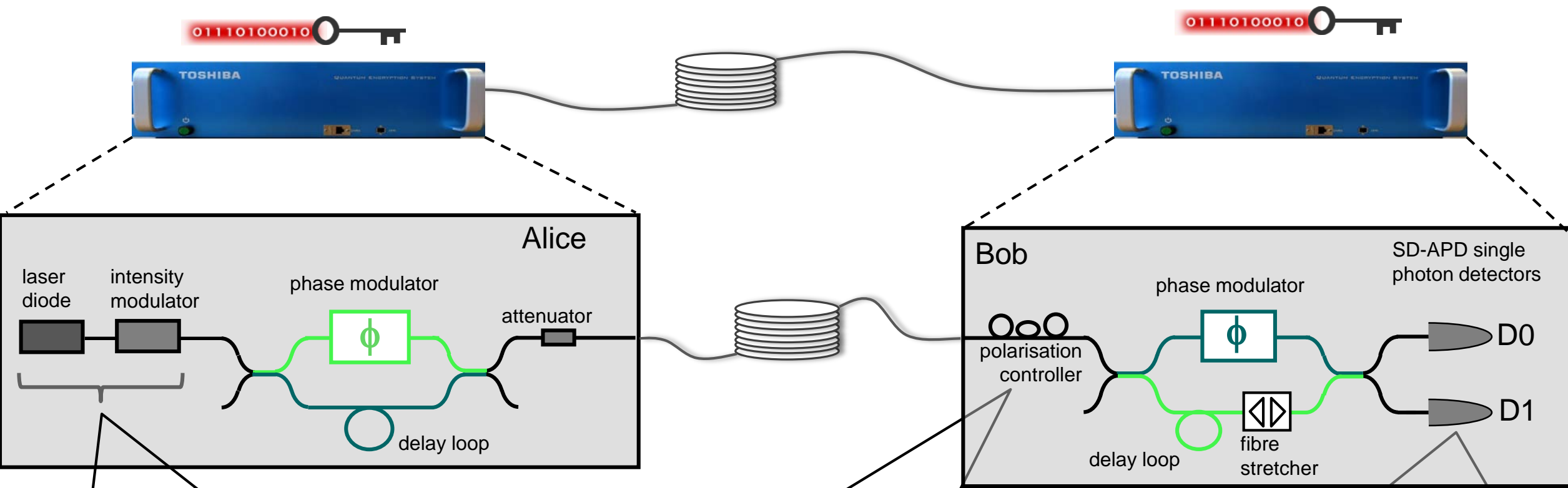
Toshiba Research Europe Limited, Cambridge, UK &
Toshiba Corporate Research and Development Center
Tokyo, Japan

Outline

- 1 Toshiba R&D System in Tokyo QKD Network
- 2 Toshiba Business Development (Video)



Quantum Key Distribution - Technology



T12 Decoy BB84 QKD Protocol

Modulate source intensity to prevent pulse splitting attack
Allows very high security
(failure probability $\epsilon < 10^{-10}$) [1]

Active Stabilisation

Continuous monitoring and adjustment of photon polarisation and phase.
Allows stable continuous operation
(0.8 Tbit of key / per month) [2]

Self-Differencing Avalanche PhotoDiode

Record photon detection rates (10^9 /s).
Allows very high key rates
(2.38 Mb/s for 35km fibre) [3]

Gen III QKD System

➤ Major advance in real-world security and usability

Security Countermeasures

➤ Protect against proposed QKD attacks, eg Trojan horse attack, APD blinding attack, time shift attack etc

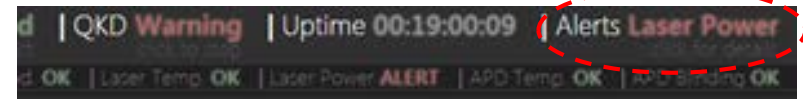


Creative commons/John Mosbaugh

see poster by Marco Lucamarini at QCrypt

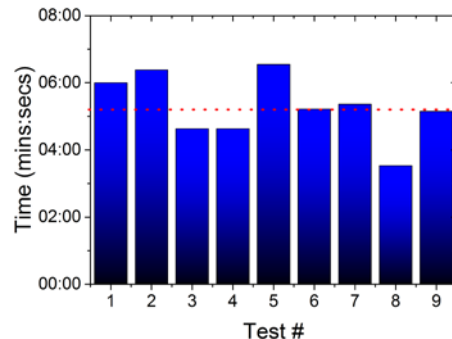
Component Monitoring

➤ Monitor status of critical components (eg laser, modulators, detectors) for failure



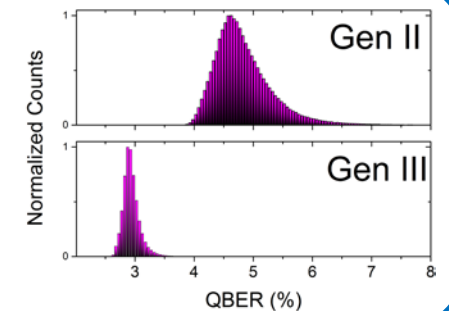
System Auto-start

➤ Auto-alignment allows use by non-expert
➤ Average time from cold start to operation ~5mins



Active Stabilisation

➤ Improved active stabilisation for variable ambient conditions.
➤ Increase in phase stability is > x2

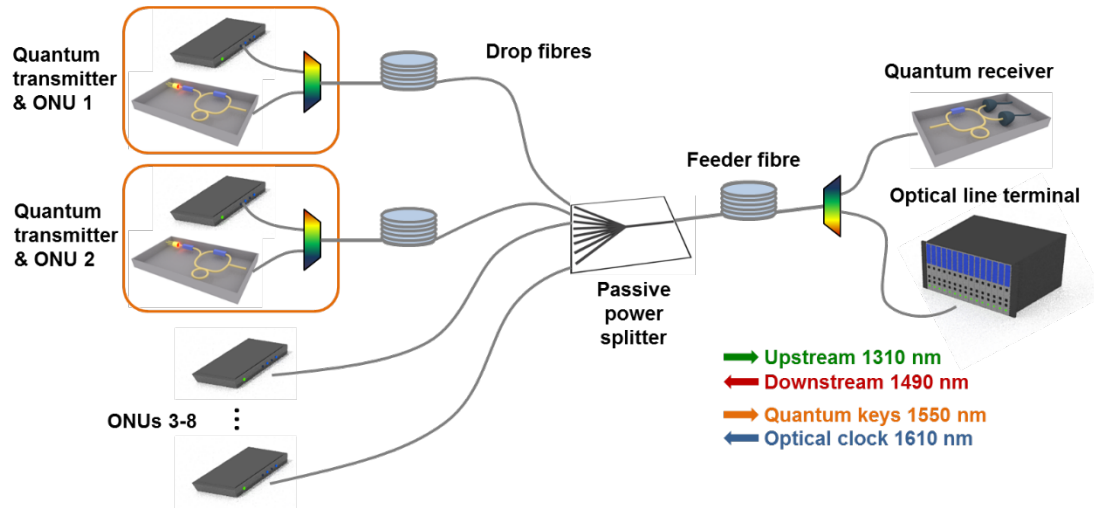


see poster by Alex Dixon at QCrypt

Unpublished

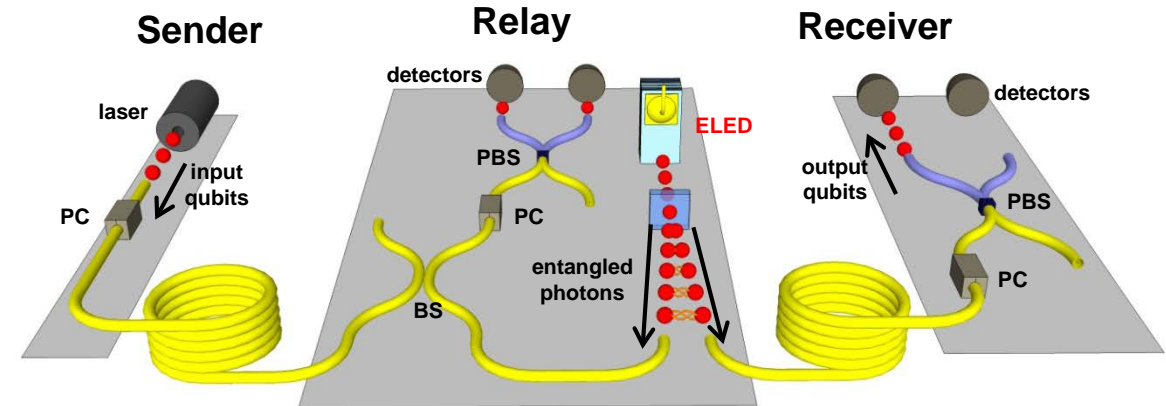
Next Generation QKD

QKD in GPON Access Networks



See talk by Bernd Frohlich at QCrypt (Mon)

Semiconductor-LED-based Quantum Relay



See talk by Christiana Varnava at QCrypt (Thurs)

TOSHIBA

Leading Innovation >>>