Traceable characterisation of the optical components of faint-pulse QKD systems – results from the Metrology for Industrial Communications (MIQC) project

Christopher Chunnilall
christopher.chunnilall@npl.co.uk

ETSI/IQC Quantum-Safe-Crypto-Workshop
Ottawa, Canada
6 October 2014
Objective: to develop a pan-European measurement infrastructure to develop standards and characterisation facilities for commercial Quantum Key Distribution (QKD) devices.

Independent physical characterisation to demonstrate that the technology is working within specification

Focus on faint-pulse (weak coherent pulse) QKD over fibre at 1550 nm

3 year project

Sept 2011 – Aug 2014
Phase encoded, attenuated laser pulse QKD over fibre at 1550 nm
**Key Measurement Outputs of MIQC**

**Phase encoded, attenuated laser pulse QKD over fibre at 1550 nm**

**Photon emitters**
Traceable characterisation of commercial QKD sources:
- Attenuated laser pulses, phase encoding

**Quantum channel (optical fibre)**
- Traceable characterisation of single mode optical fibre
- Characterisation of propagation of photon state in single mode fibre

**Random number generator (idQuantique)**
- Open system true physical random number generator (TPRNG)
- Physically characterised and tested under different operating conditions

**Photon receivers**
Traceable calibration of commercial QKD receivers:
- Gated photon counting detectors
**Primary properties requiring characterisation**

- Mean photon number
- Probability distribution
- Temporal pulse jitter, duration
- Wavelength
- Spectral bandwidth
- Spectral indistinguishability

**Tree-topology photon number resolving detector**

- Spectral attenuation
- Chromatic dispersion
- Optical length
- Back-scatter
- Polarisation mode dispersion, dependent loss, decoherence
- Wavelength multiplexed fibre links

**High-resolution single-photon spectrometer**

- Detection efficiency
- Detection linearity
- Dark count probability
- After-pulse probability
- Deadtime and recovery time
- Temporal jitter
- Back-flash
- Detector indistinguishability (multi-detector receiver)

**Calculable, scalable light source (synchrotron)**

**Telecom wavelength attenuator**
Detector characterisation
(gated detector)
Traceable receiver metrics

1 % uncertainty \((k = 2)\)
1550 nm, 100 pW, fibre-coupled

0.005 % uncertainty \((k = 2)\)
visible wavelengths, 0.5 mW, collimated, free-space laser radiation

Pulsed laser
Calibrated variable attenuator
InGaAs SPADs

Synchronisation

Calibrated power meter
Primary Standard cryogenic radiometer
QKD receiver

2 % uncertainty \((k = 2)\)
Novel reference for calibrating single-photons receivers based on synchrotron radiation

Exploitation of strict proportionality of ring current and emitted radiation
Number of stored electrons changes spectral radiant power over 11 orders of magnitude without changes to the emitted spectrum

\[ QE^*_{SSPD} = \frac{\text{count rate}_{SSPD}}{\text{photon rate}_{InGaAs}} \times \frac{\text{number of stored electrons} (I_{low})}{\text{number of stored electrons} (I_{high})} \]
OTDR operating at single-photon level
Source characterisation
(pulsed sources)
a) Calibrated detector and commercial attenuator

3 % uncertainty
(k = 2)

2 % uncertainty
(k = 2)
Source photon number statistics

b) Calibrated detector and traceable attenuator based on InGaAs photodiodes

Attenuator based on transmission trap detector configuration

Current attenuation $\sim 6 \times 10^{-5}$ @ 1.55 µm
c) Reconstruction of probability distribution

"ON/OFF" Tomography

\[ \rho = \sum_{n,m=0}^{\infty} \rho_{nm} |n\rangle \langle m| \]

Photon number distribution

\[ \rho_n \equiv \rho_{nn} \]

For \textit{on/off} detectors like SPAD with quantum efficiency \( \eta \), the probability of no-clicks is:

\[ p_0(\eta) = \sum_{n=0}^{\infty} (1 - \eta)^n \rho_n = \sum_{n=0}^{\infty} A_n(\eta) \rho_n \]

- Truncating the p.d. to a certain \( N \)
- Changing the value of the quantum efficiency \( \eta_\mu \)

Diagram showing Poissonian and reconstructed probability distributions.
Source photon number statistics

d) PNR detector based on tree configuration

*Deconvolving the p.d. of incoming photons*

- Novel (entangled-assisted) quantum characterisation technique for PNR detector

- By measuring higher-order $g^{(n)}$, it is possible to deconvolve the underlying number and kind (poissonian, pseudo-thermal or single-photon) of occupied modes of a light field.

$$
 g^{(2)}, \ g^{(3)}, \ g^{(4)} \quad g^{(n)} = \frac{P(n)}{[P(1)]^{n}}
$$

Goldschmidt et al., PRA 88, 013822 (2013)

Brida et al., PRL 108, 253601 (2012)
Source Spectrum

Tunable single-photon spectrometer

- Operating range 1270 → 1630 nm
- FSR = 119 GHz, $\Delta \nu_{\text{cavity}} = 600$ MHz
- Low drift rate & single-photon sensitivity
- Tune to resonance and scan across QKD source spectrum
- Can be used to analyse different source encoding spectra
- Technically challenging to improve spectral resolution
Four on-demand web lectures discussing basic aspects of QKD

1. "Introduction to QKD"
   by Momchil Peev, AIT (Austria)

2. "Practical QKD systems"
   by Gregoire Ribordy, ID Quantique (Suisse)

3. "Security of QKD systems"
   by Norbert Lütkenhaus, Univ. of Waterloo (Canada)
   &
   Vadim Makarov, Univ. of Waterloo (Canada)

4. "Metrology for QKD"
   by Christopher Chunnilall, NPL (UK)
Summary

• Methods developed to address the measurement requirements required of QKD (benign environment)
• These include new, beyond state-of-the-art, methods and instruments

• Close interaction with ETSI QKD-ISG
• 14 peer-reviewed papers, plus 7 accepted for publication
• 55 presentations at meetings and conferences
• 4 on-line web-lectures
• Best practice guide
• Project website http://www.miqc.org
• Continue to take this work into future – MIQC2?
The MIQC-project: Metrology for Industrial Quantum Communications

M L Rastello, I P Degiovanni, G Brida

S Kück, I Muller, R Klein

A Vaigu, F Manoocheri, E Ikonen

D Stucki

K S Hong

A G Sinclair, C J Chunnilall, J Y Cheung

G Porrovecchio, M Smid

T Kubarsepp

A Tosi

A Al Natsheh
Further metrology ... MIQC2?

• MIQC is just the beginning ...
  – Metrology for side-channel and Trojan-horse attacks, and their countermeasures
  – Free-space QKD (visible wavelengths)
  – Other protocols, e.g. entanglement-based
  – ...

MIQC1 Consortium +
Thank you!

http://www.miqc.org