Metrology for QKD – an industrial quantum optical communication technology

Christopher Chunnilall
christopher.chunnilall@npl.co.uk

1st ETSI Quantum-Safe-Crypto-Workshop
Sophia-Antipolis, France
26-27 September 2013
Objective: to develop a pan-European measurement infrastructure to develop standards and characterisation facilities for commercial Quantum Key Distribution (QKD) devices.

QKD devices require independent physical characterisation in order to convince end-users that the technology is working within specification.

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

3 year project

Start Sept 2011; now 2 years into project
QKD

- physical (as opposed to algorithmic) process
- security depends on physical performance of system at time of key creation (as well as algorithmic post-processing)

IS IT PERFORMING AS IT SHOULD?

Security from hacking (Side-channels)
Basis and bit indistinguishability (pulses, detectors)

Customer assurance ✓
Market confidence ✓
No catastrophe ✓

System optimisation
- Expected QBER, ΔQBER
- Bit rate and distance
- Privacy amplification

System stability
‘Natural’ change;
Performance-changing attacks

Measurement of the physical parameters of the system
Standards and characterisation facilities – interaction with ETSI QKD-ISG

- Three MIQC partners (INRIM, NPL, PTB) are members of the ETSI QKD-ISG, and facilitate information exchange between the ISG and MIQC

- The MIQC project has collaborated closely with the ISG to identify and document the physical parameters of faint-pulse QKD systems which require measurement

- The MIQC project is developing the necessary capability to measure these parameters in a way that is traceable to the SI with a quantified uncertainty

- This expertise will be fed back to the ISG in order to draft appropriate standards which define the relevant measurement processes for universal implementation
traceable measurements

m  A  mol  cd  kg  K  s

Environment  Communications  Healthcare  Food

Industry  Science  Doctors  Regulators  Health & safety  Transport

Geographical & temporal consistency
Universal acceptance

http://www.bipm.org/en/si/
Key Measurement Outputs of MIQC

**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
- Development of in-line calibration devices

**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

**QKD testbeds**
- Development of testbeds
Primary properties requiring characterisation

- Mean photon number
- Probability distribution
- Temporal pulse jitter, duration
- Wavelength
- Spectral bandwidth
- Spectral indistinguishability
- Tree-topology photon number resolving detector
- High-resolution single-photon spectrometer

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

- 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 efficiency
(gated detector)

[Established technique, adapted for QKD]
Optical power traceability chain (SI)

Primary standard
Cryogenic radiometry

NMI reference detectors

Low power reference detector

0.005 % uncertainty
visible wavelengths,  
0.5 mW,  
collimated,  
free-space laser radiation

1 % uncertainty ($k = 2$)
1550 nm,  
100 pW,  
output from optical fibre
Pulsed laser
5 kHz – 100 MHz

Variable attenuator (uncalibrated)
Variable attenuator (calibrated)

Cryogenic radiometer

Dark count probability
Detection efficiency
After-pulse probability (ETSI draft document)

<table>
<thead>
<tr>
<th>Pulse frequency</th>
<th>Power ($\mu = 1$)</th>
<th>dB (wrt 128 pW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GHz</td>
<td>128 pW</td>
<td>0</td>
</tr>
<tr>
<td>50 MHz</td>
<td>6.4 pW</td>
<td>-13</td>
</tr>
<tr>
<td>1 MHz</td>
<td>128 fW</td>
<td>-30</td>
</tr>
<tr>
<td>50 kHz</td>
<td>6.4 fW</td>
<td>-43</td>
</tr>
</tbody>
</table>

Low jitter variable delay (Synchronisation)

Frequency divider

Synchronisation (dark count subtracted)

Normalised counts

Delay (ps)

51500 52000 52500 53000 53500 54000 54500

1.0E+00 1.0E+01 1.0E+02 1.0E+03 1.0E+04
Dark counts, after-pulses, detection efficiency
(Illustrative data)

262144 ($2^{18}$) sweeps of 131072 ($2^{17}$) timebins of width 0.1 ns

\[ f_{\text{det}} = 4 \text{ MHz} \]
\[ \text{freq. division} = 16 \]

Dark counts
\[ P_{\text{dc}} = 2.46 \times 10^{-6} \text{ per gate} \]

‘True counts’
+ after-pulses
+ dark counts;
( blanking = 0)
\[ P_{\text{ap}} = 0.0109, \text{ DE} = 0.28 \]

‘True counts’
+ after-pulses
+ dark counts;
( blanking = 7)
\[ P_{\text{ap}} = 0.0025, \text{ DE} = 0.28 \]

Counts per timebin

Uncertainty: < (2% combined with count uncertainty) ($k=2$)
Probability distribution

Tree-topology
photon number resolving detector

[Beyond state-of-the-art method]
PNR detector tree structure

Detector Tree:

- Four click/no-click detectors (commercial SPADs);
- three pigtailed 50:50 beam splitters (commercial).
Dead-time effects in “smart” configuration

Gating

SPADs

D1

D2

D3

D4

FPGA-validated gates
“Smart” vs. passive gating

Passive gating photodetections:
[Images of photodetections]

“Smart” gating photodetections:
[Images of photodetections]

Passive gating valid events:
[Diagram of events]

“Smart” gating valid events:
[Diagram of events]

✓ Less detection events.
✓ Much more reliable counts, specially at high rates.

Free from saturation effects!
Experimental setup

Sources

- Rotating ground glass disk
- Laser
- Laser
- SPDC source
- Laser
- Heralding detector

Pseudo-thermal state
Coherent (poissonian) state
Heralded single photon state

«Noiseless» Heralded Single Photon Source

Data collection and post-processing device
Poissonian + thermal states

Contact: i.degiovanni@inrim.it

Goldschmidt et al., PRA 88, 013822 (2013)
Three other beyond state-of-the-art methods

(1 slide overviews)
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

Contact: alastair.sinclair@npl.co.uk
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

\[ QE_{SSPD}^* = \frac{countrate_{SSPD}/number of stored electrons(I_{low})}{photonrate_{InGaAs}/number of stored electrons(I_{high})} \]

Contact: Ingmar Müller, Lutz Werner, PTB division Detector radiometry and radiation thermometry, ingmar.mueller@ptb.de, lutz.werner@ptb.de
Shuttered Heralded Single Photon Source

Contact: i.degiovanni@inrim.it
Summary

- Methods are being developed to address the measurement requirements required of QKD
- These include new, beyond state-of-the-art, methods and instruments

- Close interaction with ETSI QKD-ISG
- 9 peer-reviewed papers, 43 presentations at meetings and conferences
- Workshop on quantum optical technologies, with a Symposium on QKD measurements planned for summer 2014
- Best practice guide & training package to be developed
- Project website [http://www.miqc.org](http://www.miqc.org)
- Continue to take this work into future
Thank you!

http://www.miqc.org