Actively-Stabilised Variable-Asymmetry Mach-Zehnder Interferometer for QKD Device Characterisation

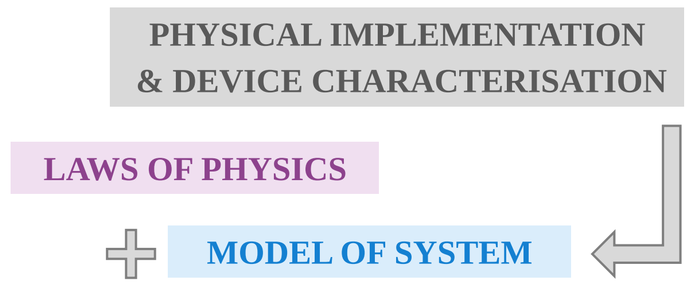
S. Albosh[1,2], T.P. Spiller[1] and C.J. Chunnilall[2]

[1]*University of York, York, YO10 5DD, UK* [2]*National Physical Laboratory, Hampton Road, Teddington, Middlesex, TW11 0LW, UK*

Email: sophie.albosh@npl.co.uk

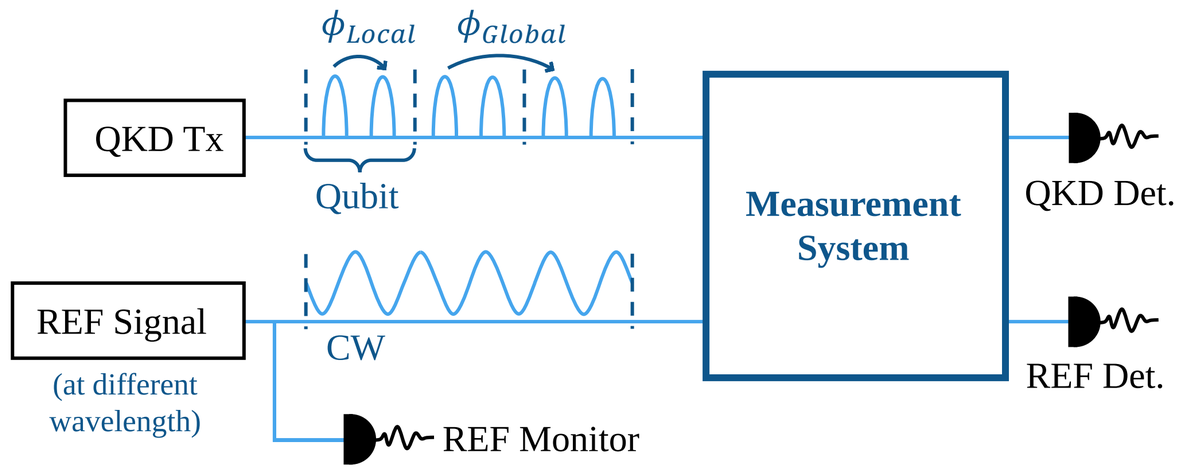
QKD Device Characterisation

- Security of QKD protocols requires that the hardware be characterised to quantify the information leakage to an eavesdropper and assess the system implementation security [1-5]
- Prevalence of phase-encoding (ϕ_{Local}) and phase-based security conditions (ϕ_{Global}) requires characterisation of phase relationships in the QKD signal
- A measurement system to characterise the phase properties of QKD hardware modules has been constructed



Measurement System

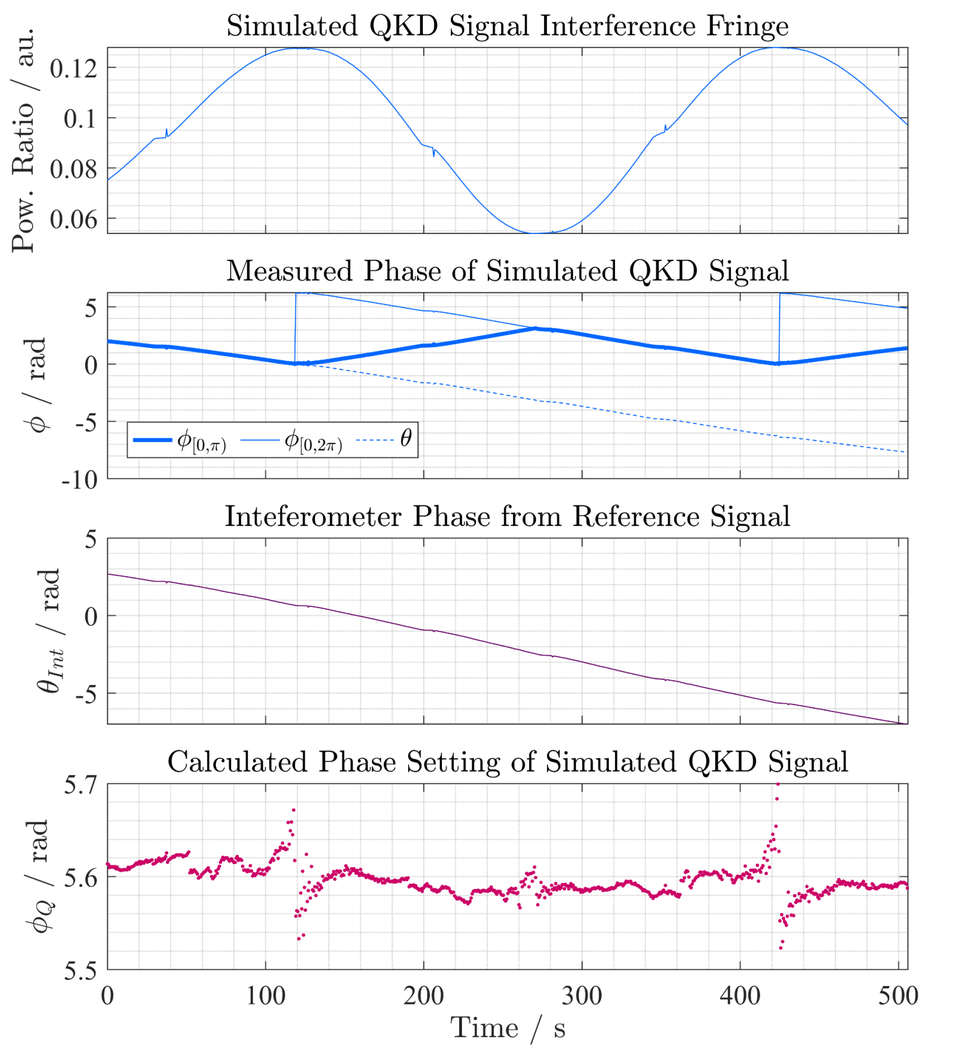
- Asymmetric Mach-Zehnder interferometer; actively stabilised using feedback from a reference laser; interferometer can be locked at any phase setting
- Interferometer asymmetry can be extended arbitrarily and varied on the submicron and wavelength-scale
- The device is designed for operation in the C-band, is transportable and can be used to characterise devices in situ



Preliminary Testing: Bright Simulated QKD Signal

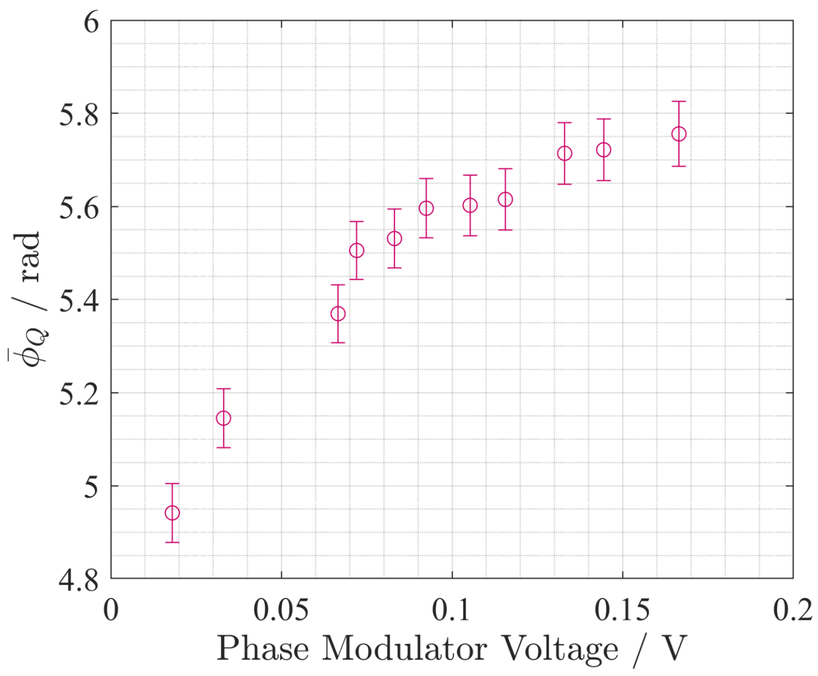
- Simulate bright phase-modulated QKD signal pulses
- Send pulses into measurement system and perform a phase sweep of the interferometer for each phase setting
- Calculate the phase difference between the pulse pairs

Phase Unwrap (One Modulator Setting)



Mean value of ϕ_Q: $\bar{\phi}_Q = 5.60 \pm 0.02$ rad

QKD Signal Phase (Many Modulator Settings)



$\bar{\phi}_Q$ for many phase modulator settings. Error bars result from uncertainties in reference signal.

References

[1] Lucamarini M. et al., *Implementation Security of Quantum Cryptography Introduction, challenges, solutions,* ETSI White Paper No. 27, 2018, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

[2] ETSI, *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems*, ETSI Group Specification, 2016, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf

[3] Loeffler M. et al., *Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution*, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/29227

[4] ISO/IEC, *ISO/IEC CD 23837-2.2*, (under development), https://www.iso.org/standard/77309.html

[5] ETSI, ISG QKD Activity Report 2020, https://www.etsi.org/committee-activity/activity-report-qkd

QUANTUM COMMUNICATIONS HUB
AQuaSeC
UK Research and Innovation
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
MeTISQ
19NRM06 MeTISQ
EURAMET