ETSI/IQC Quantum Safe Cryptography Conference 2026

Traceable Calibration for QKD Security

Presented by: Luiz Couto

18/06/2026

DFM and the role of an NMI

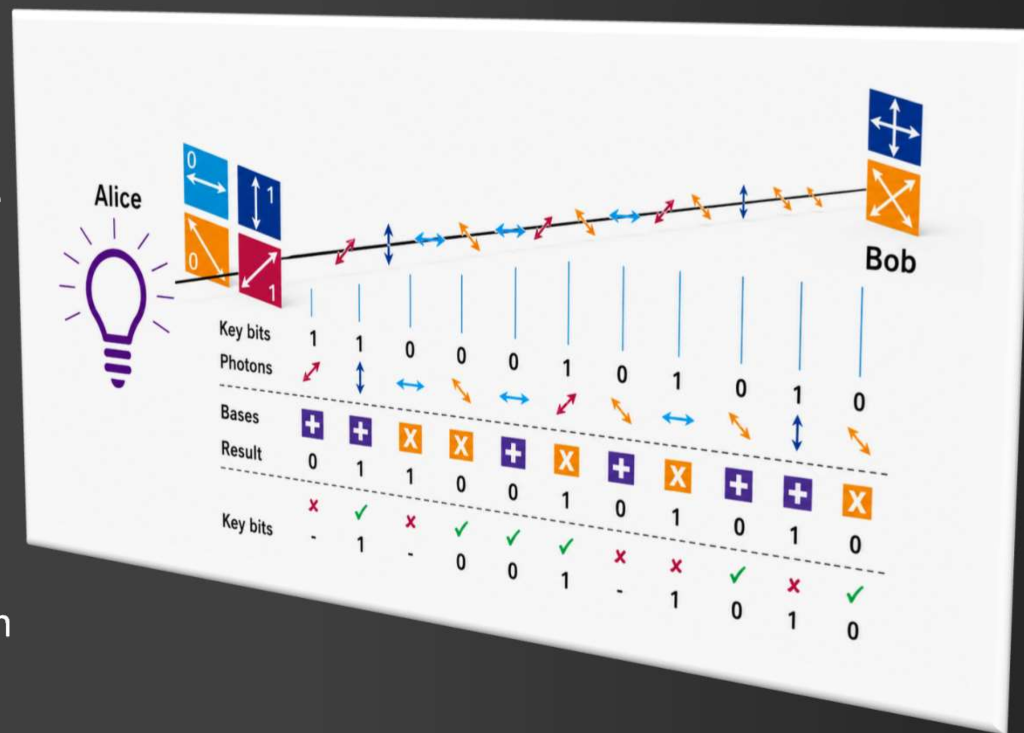
Why is a metrology institute involved in QKD?

- DFM is Denmark's National Metrology Institute
- NMIs provide traceability, uncertainty budgets and comparable measurements
- For QKD, this becomes part of building trust in deployed systems

QKD: secure in theory, calibrated in practice

The security proof relies on real measured parameters:

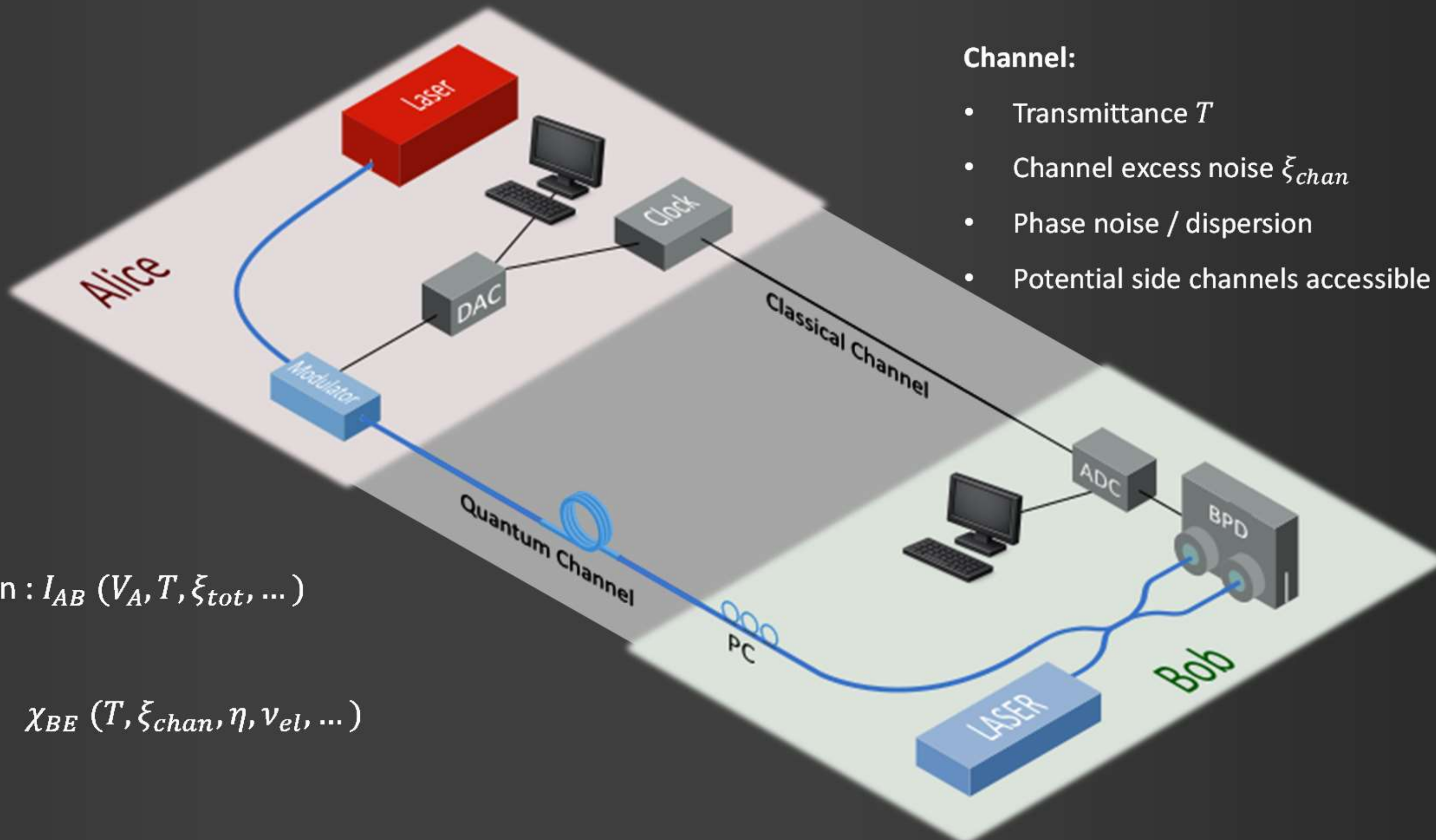
- QKD security depends on assumptions about the implemented system
- Loss, receiver efficiency and noise are not just performance numbers
- If these parameters are biased, the security claim can also be biased



Where calibration enters the secure key rate (CV-QKD)

Transmitter (Alice):

- Modulation variance V_A
- Laser phase/frequency stability
- Modulator calibration & linearity
- Prepared-state excess noise



Channel:

- Transmittance T
- Channel excess noise ξ_{chan}
- Phase noise / dispersion
- Potential side channels accessible to Eve

Composable key-rate:

- Alice–Bob mutual information : $I_{AB}\ (V_A, T, \xi_{tot}, \dots)$
- Eve's accessible information: $\chi_{BE}\ (T, \xi_{chan}, \eta, \nu_{el}, \dots)$
- Secret key rate:

$$K \geq \frac{n}{N}\left[\beta\, I_{AB} - \chi_{BE} - \Delta(n)\right]$$

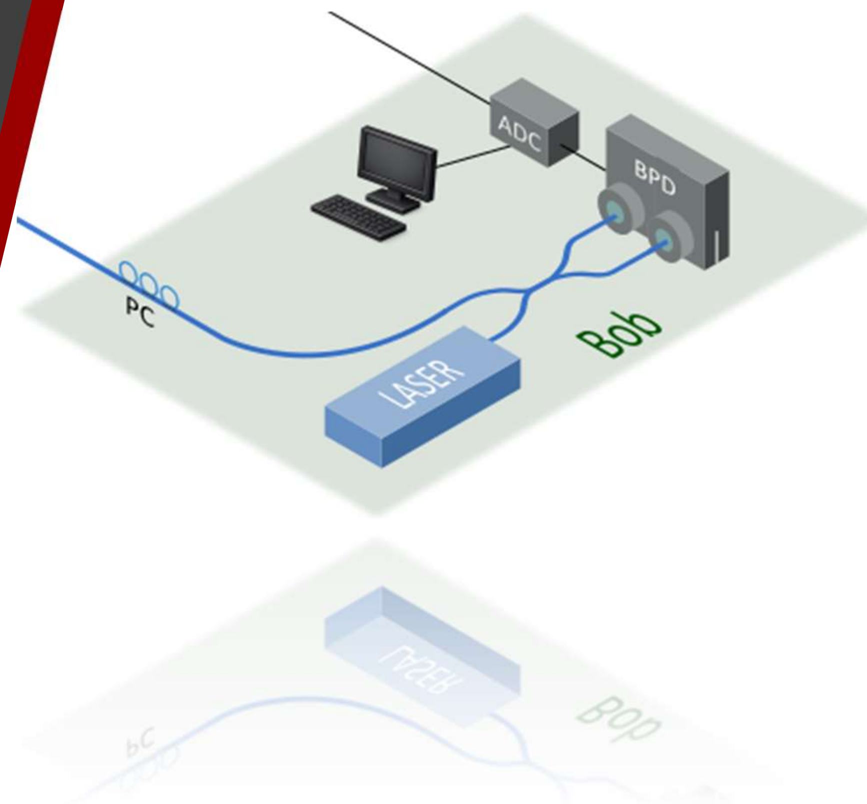
Receiver (Bob):

- Detection efficiency η
- Electronic noise ν_{el}
- Shot-noise calibration
- Reconciliation efficiency β

Worked example: receiver efficiency

Zooming in on Bob:

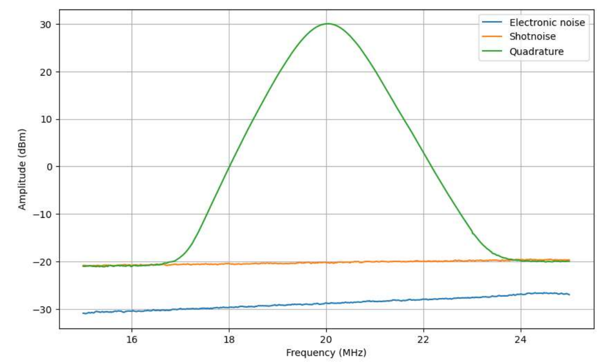
- Detection efficiency η
- Electronic noise v_{el}
- Shot-noise calibration
- These affect both performance estimates and security bounds

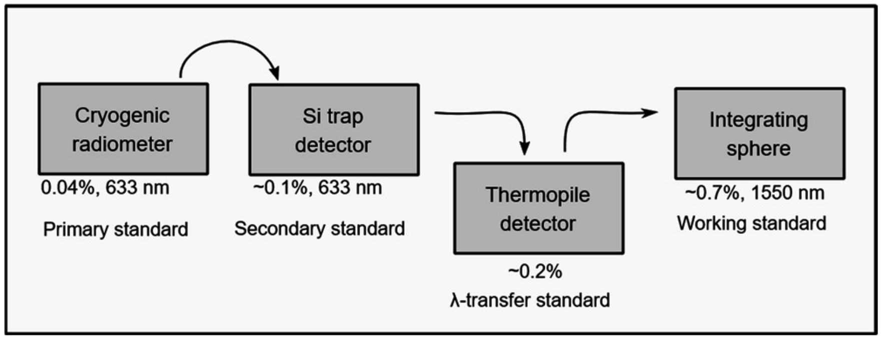


SI-traceable calibration protocol

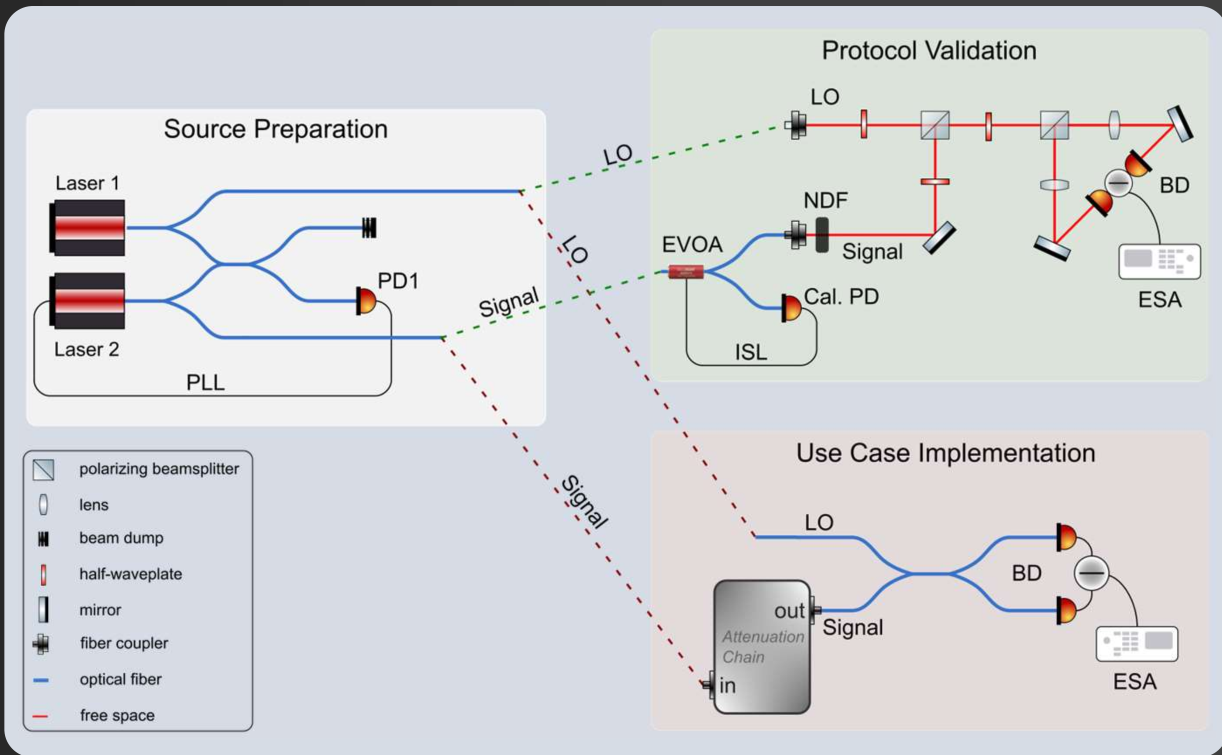
From ESA observables to calibrated receiver efficiency:

- Shot-noise-referenced measurements
- Heterodyne beat-note power
- LO shot-noise variance
- Optical power traceable to SI units
- Full uncertainty budget



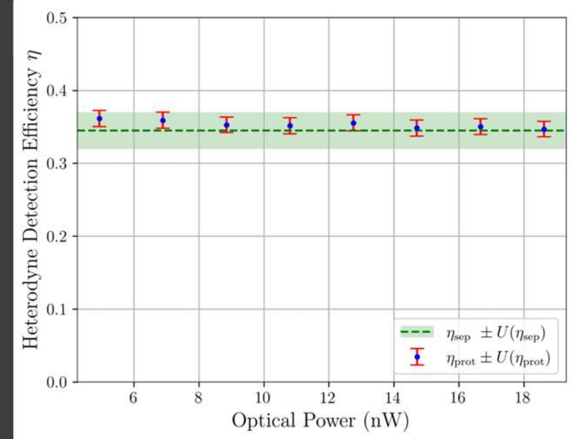


Results

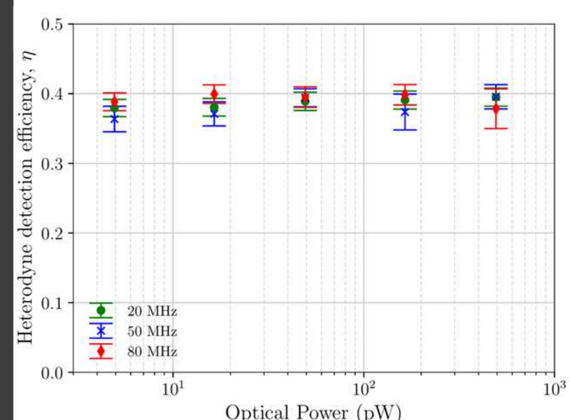


https://doi.org/10.48550/arXiv.2602.20301

$\eta = 0.352 \pm 0.011\ (k = 2)$



$\eta = 0.386 \pm 0.011\ (k = 2)$



From calibration to standardisation

DFM and CEN/CLC/JTC 22:

- CV-QKD needs standardised test conditions, measurement conventions and uncertainty reporting
- This supports conformity assessment, benchmarking and deployment monitoring
- DFM is contributing to JTC 22 work on coherent optical detectors, including homodyne and heterodyne receivers
- Focus: SI-traceable calibration procedures, reference setups and harmonized reporting for future standards/specifications

Thank you!

Ministry of Higher Education and Science Denmark
Innovationsfonden
eureka network projects
METROLOGY PARTNERSHIP
EURAMET