ETSI/IQC Quantum Safe Cryptography Event

Single-photon Metrology for testing the implementation security of QKD systems and components

Dr. Alice Meda

15/02/2023

WHY METROLOGY?

For QKD technology to become a viable real-world solution, end-users need confidence in it

QKD is theoretically secure but devices are far from theoretical models. Real systems are vulnerable to side channel attacks.

Table 1 – List of attacks against a typical QKD system and respective countermeasures. The acronyms in the table are listed at the end of the paper.

SECURITY ISSUE	DESCRIPTION	COUNTERMEASURES
Trojan-horse attack	Eve probes the QKD equipment with light to gain information about the device settings	privacy amplification (PA), isolators, filters
Multi-photon emission	When more than one photon is emitted in a pulse, information is redundantly encoded on multiple photons	PA, characterisation, decoy states, SARG04 and other protocols
Imperfect encoding	Initial states do not conform to the protocol	PA, characterisation
Phase correlation between signal pulses	Non-phase-randomised pulses leak more info to Eve, decoy states fail	phase randomisation, PA
Bright-light attack	Eve manipulates the photon detectors by sending bright-light to them	active monitoring, measurement device independent QKD (MDI-QKD)
Efficiency mismatch and time-shift attack	Eve can control, at least partially, which detector is to click, gaining information on the encoded bit	MDI-QKD, detector symmetrisation
Back-flash attack	Eve can learn which detector clicked and hence knows the bit	isolators, MDI-QKD, detector symmetrisation
Manipulation of Local Oscillator reference	In continuous variable QKD (CV-QKD), the local oscillator (LO) can be tampered with by Eve if it is sent on a communications channel	Generate LO at the receiver. Phase reloading, i.e. only synchronise the phase of LO

An Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has been installed from October 2008 to address standardization issues in QKD, to support the commercialization of QKD devices on various levels and stages.

www.etsi.org/technologies/quantum-key-distribution

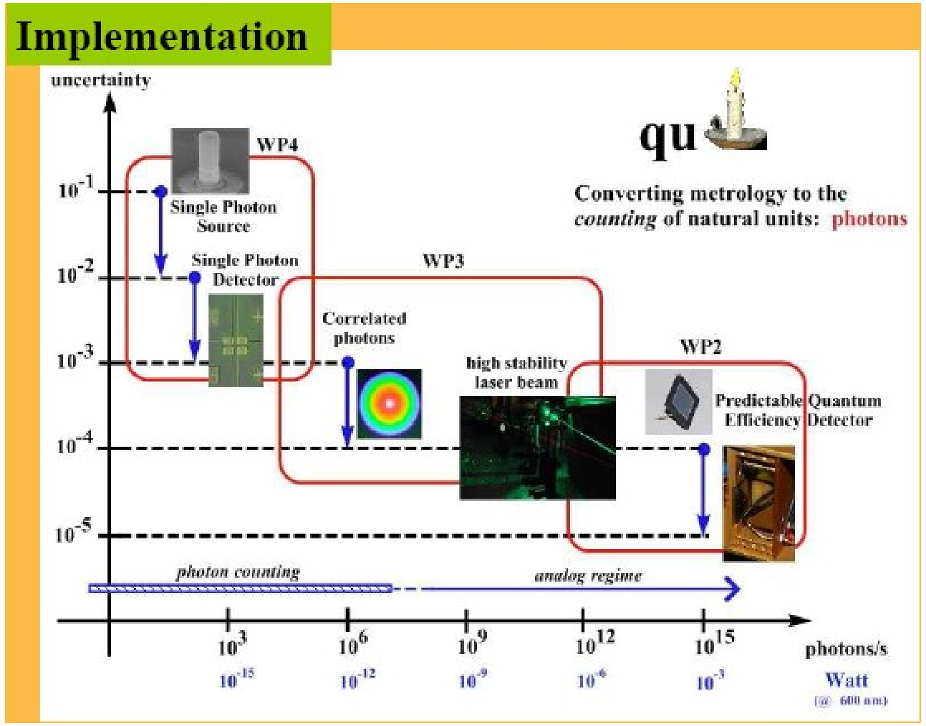
Implementation security: to test real equipment and to estimate how much information such equipment leaks to a potential adversary

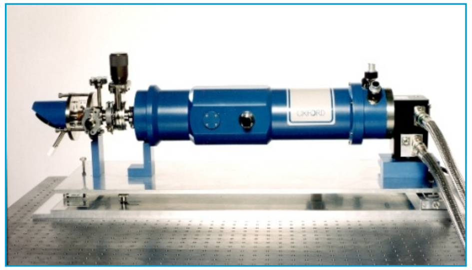
INRiM
ISTITUTO NAZIONALE DI RICERCA METROLOGICA

SI Traceablility in quantum photonics

Quantum Radiometry results necessary to the standardization framework for providing SI traceable characterization techniques at single-photon level.

Quantum Radiometry: Effort to create a linkage between the typical optical power measurement regime of conventional radiometry and the single-photon counting regime

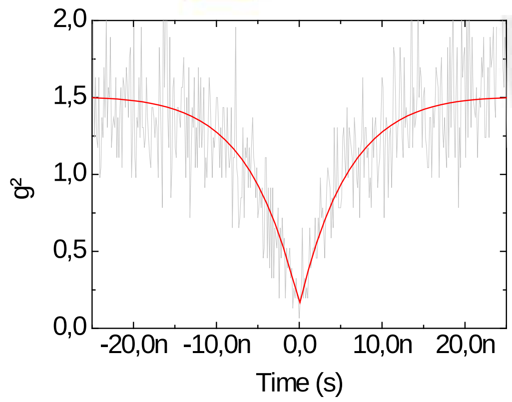




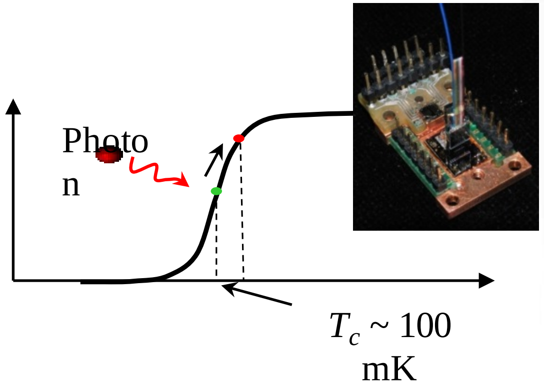
Quantum Metrology for Quantum Communication

QUANTUM RADIOMETRY TARGETS

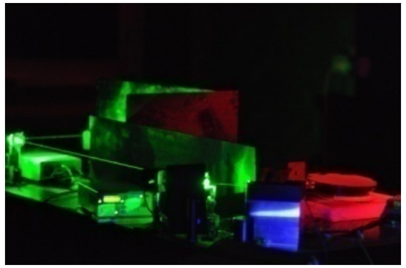
- Develop suitable metrics for:
  - Single Photon Sources
  - photon counting detectors



- Develop methods and measurement facilities for characterising non-classical properties of light:
  - anti-bunching
  - indistinguishability
  - entanglement
  - quantumness



- Develop measurement techniques:
  - to identify QKD systems security vulnerability
  - to assess attacks countermeasures



Opt. Engineering 53(8), 081910 (2014)

Examples: Single Photon Detectors (SPD)

A device that probabilistically transforms the impinging single-photon into a macroscopically detectable electrical signal.

The detector provides the number of detection events within certain time duration, from which the detection count rate can be determined.

D1 - Detector gate repetition rate f_{gate}

D2 - Dark count probability p_{dark}

D3 - After-pulse probability $p_{after\_first}(\Delta T)$ or $p_{after\_all}(\Delta T)$ or p_{after_total}

D4 - Photon detection probability (Detection efficiency) $\eta(\nu)$ or $\eta(\lambda)$

D5 - Linearity factor (for detection efficiency) F_L

D6 - Detection efficiency range due to polarization variation of input pulses $\Delta\eta$

D7 - Dead time t_{dead}

D8 - Recovery time $t_{recovery}$

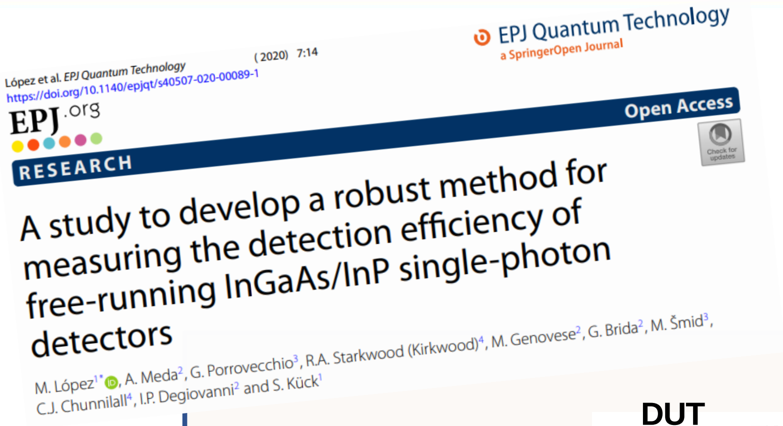
D9 - Detector signal jitter $\eta(t,T)$, where T denotes photon arrival time

D10 - Photon detection probability (detection efficiency) profile $\eta(t)$

D11 - Spectral Responsivity $\eta(\nu)$ or $\eta(\lambda)$

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Pilot study on the quantum efficiency measurements


López et al. EPJ Quantum Technology (2020) 7:14
https://doi.org/10.1140/epjqt/s40507-020-00089-1

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH

Open Access

A study to develop a robust method for measuring the detection efficiency of free-running InGaAs/InP single-photon detectors

M. López[1*], A. Meda[2], G. Porrovecchio[3], R.A. Starkwood (Kirkwood)[4], M. Genovese[2], G. Brida[2], M. Šmid[3], C.J. Chunnilall[4], I.P. Degiovanni[2] and S. Kück[1]

DUT

Fiber-coupled ID Quantique type ID-220

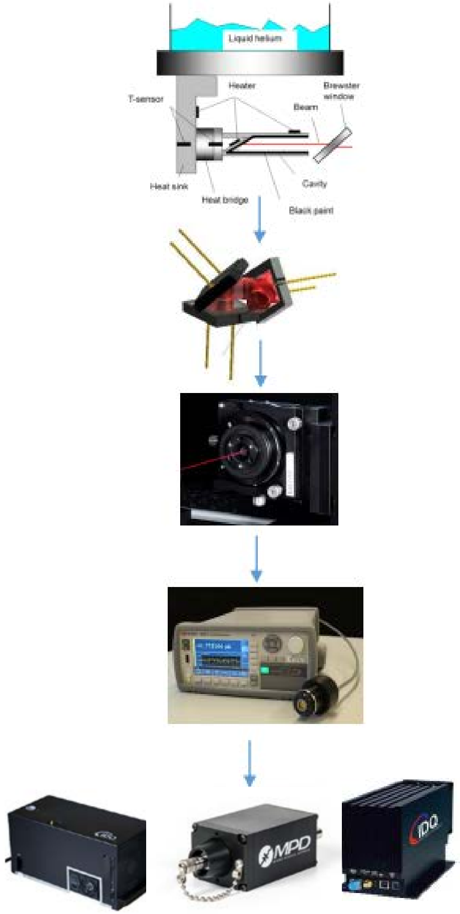
Configuration:
$\eta = 10$ % and D = 10 μs

Photon Source: ID Quantique, id300

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA · PTB Messen • Forschen • Wissen · CMI CZECH METROLOGY INSTITUTE · NPL National Physical Laboratory

Traceability chain:

InGaAs-SPAD



Cryogenic Radiometer (primary standard)
λ_i = 406.7 nm,..., 1010 nm, Φ = 400 μW
$u(\Phi) \leq 0.008$ %

λ_i = 406.7 nm,..., 1010 nm, Φ = 600 μW

Si trap detector (transfer standard)
406.7 nm ≤ λ ≤ 1010 nm, Φ = 10 μW ≤ Φ ≤ 5 mW
$u(\Phi) \leq$ 0.02 %,...,0.05 %

λ = 632.8 nm; Φ = 300 μW

Thermopile detector (14BT)
632.8 nm ≤ λ ≤ 1640 nm, 30 μW ≤ Φ ≤ 3 mW
$u(\Phi) \leq 0.15$ %

λ = 1550 nm; Φ = 100 μW

Si Photodiode	**InGaAs photodiode**
λ = 850 nm , Φ = 100 μW	λ =1550 nm, Φ = 100 μW

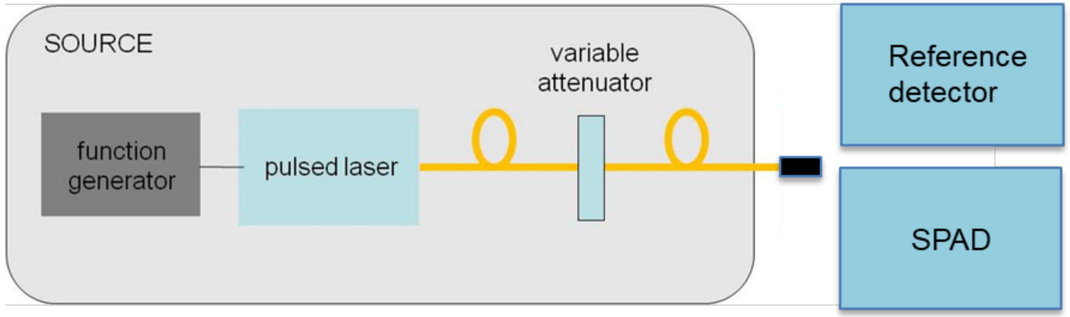
$u(\Phi) \leq 0.20$ %

Nonlinearity of the photodiode
Attenuator transmission

Si SPAD	**InGaAs/InP SPAD**
λ = 850 nm	λ = 1550 nm
Phot. rate ≈ 10000 photons/s	Phot. rate ≈ 600 photons/s

$u(\Phi) \leq 1.00$ % ($U_{exp} \approx 2$ %)

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA



$$\eta_{\mathrm{DUT}} = \frac{P_{\mathrm{c}}}{\alpha \cdot P_0}$$

- P_C : average optical power of the effective photons measured by the DUT

- P_C is calculated from the photon rate absorbed by the DUT corrected for dead time and dark counts (ρ_{corr}) , at λ = 1550.05 nm

$$\mathrm{P}_c = \frac{\rho_{corr} hc}{\lambda} \qquad \rho_{corr} = f_{laser}\,\mu\eta_{DUT}$$

with f_{laser} = repetition rate of the laser ,
μ mean number of photons per pulse

- In the absence of dark counts and dead times, the probability of having a “*click*” per laser pulse is $q = 1 - e^{-\mu\eta_{DUT}}$

The number of the corrected count rate is therefore: $\rho_{corr} = -f_{laser} \ln(1-q)$

$$\alpha P_0 = \frac{h \cdot c}{\lambda} f_{laser}\mu = -\frac{h \cdot c}{\lambda} f_{laser} \frac{1}{\eta_{\mathrm{DUT}}} \ln(1-q)$$

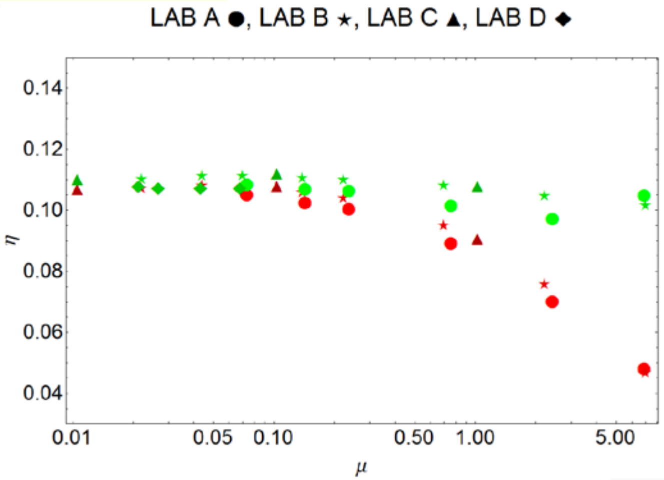
The probability of having a click q must be inferred considering how dark counts and dead time D affect the counting process in a free running single-photon detector (Model)

Model for pilot study :

$$q = \frac{\rho_{click}}{f_{laser} - \rho_{click}} + \frac{f_{laser} \cdot (\rho_{click} - \rho_{click}^2 D + f_{laser} \cdot (\rho_{click} D + \rho_{click}^2 \cdot D^2 - 1))}{D \cdot (f_{laser} - \rho_{click})^2 (f_{laser} - \rho_{click} + \rho_{click} \cdot f_{laser} D)} \cdot \rho_{dark} \cdot D$$

Regime:

- Free running
- Pulsed laser with fixed f_{laser}
- up to 2.4 photons per pulse



Applied Physics Letters | ARTICLE | scitation.org/journal/apl

Detection of ultra-weak laser pulses by free-running single-photon detectors: Modeling dead time and dark counts effects

Cite as: Appl. Phys. Lett. 118, 174002 (2021); doi: 10.1063/5.0046014
Submitted: 31 January 2021 · Accepted: 6 April 2021 · Published Online: 26 April 2021

Hristina Georgieva,[1] Alice Meda,[2] Sebastian M. F. Raupach,[1] Helmuth Hofer,[1] Marco Gramegna,[2] Ivo Pietro Degiovanni,[2,3] Marco Genovese,[2,3] Marco López,[1] and Stefan Kück[1,a)]

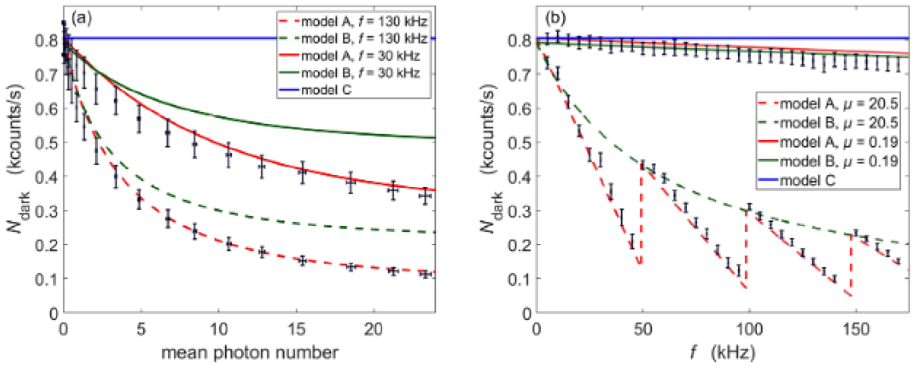
AFFILIATIONS
[1]Physikalisch-Technische Bundesanstalt (PTB), Bundesallee 100, 38116 Braunschweig, Germany
[2]Istituto Nazionale di Ricerca Metrologica (INRIM), Strada delle Cacce 91, I-10135 Torino, Italy
[3]Istituto Nazionale di Fisica Nucleare (INFN), Sezione Torino, Via Giuria 1, I-10125 Torino, Italy

PHYSICAL REVIEW A **105**, 042615 (2022)

Detection rate dependence of the inherent detection efficiency in single-photon detectors based on avalanche diodes

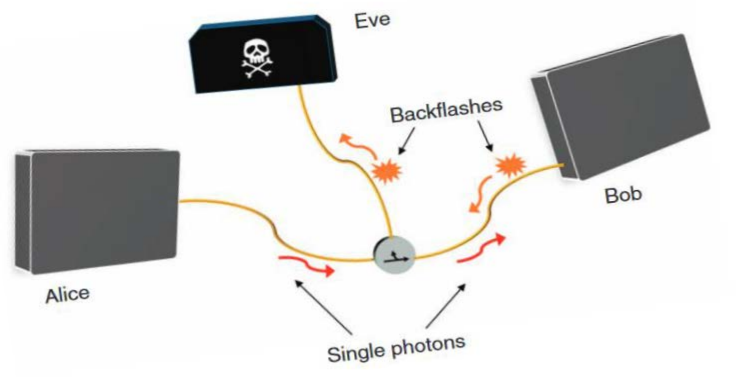
Sebastian M. F. Raupach,[1,*] Ivo Pietro Degiovanni,[2,3] Hristina Georgieva,[1] Alice Meda,[2] Helmuth Hofer,[1] Marco Gramegna,[2] Marco Genovese,[2,3] Stefan Kück,[1] and Marco López[1]
[1]*Physikalisch-Technische Bundesanstalt, Bundesallee 100, 38116 Braunschweig, Germany*
[2]*Istituto Nazionale di Ricerca Metrologica, Strada delle Cacce 91, 10135 Torino, Italy*
[3]*Istituto Nazionale di Fisica Nucleare, Sezione Torino, Via Giuria 1, 10125 Torino, Italy*

Extended regime to 23 photons per pulse



Backflash emission

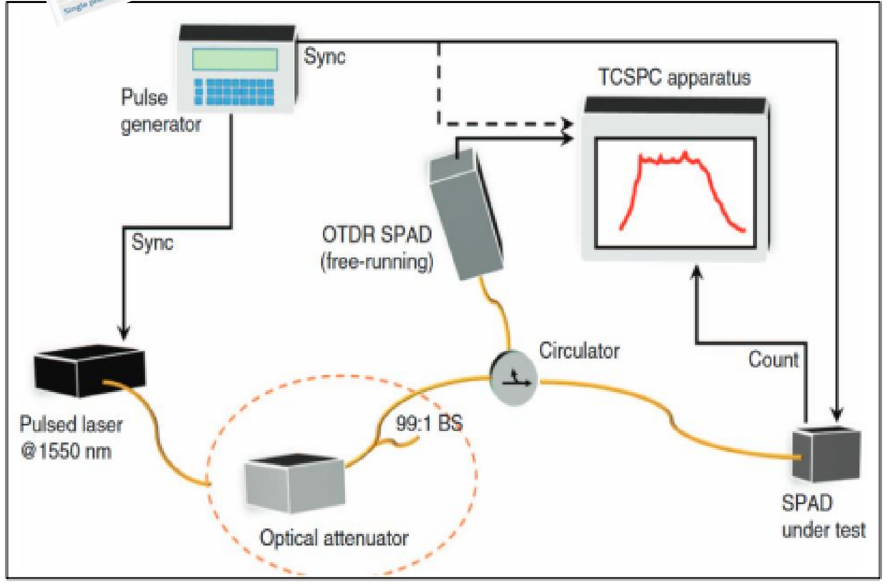
14IND05

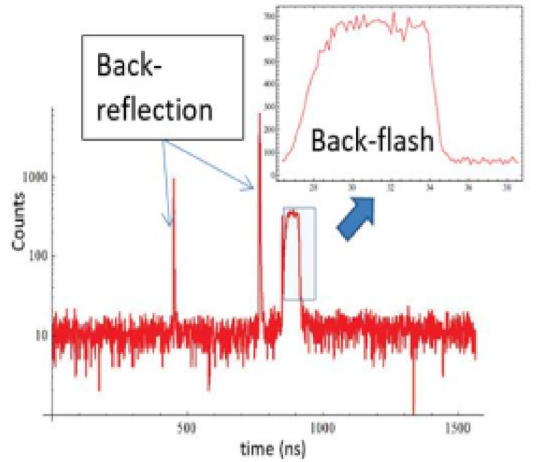


INRIM SINGLE PHOTON OTDR

- The source is an attenuated pulsed laser
- Temporal trace: histogram of counts/time
- Temporal resolution: 130 ps (jitter of the detector), spatial resolution: 13 mm
- Back-Reflected light is detected by a free running InGaAs/InP detector; significant light leakage (8%) and identifiable temporal profile

Quantifying backflash radiation to prevent zero-error attacks in QKD





2 Commercial Detector tested QE=10%, 100ns (same BF distribution)

A. Meda, et al. Light: Science & Applications 6, E16261 (2017)

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Quantum Metrology for Quantum Communication

Project Coordinator: **INRIM**
Quantum Candela: radiometric measurements in the natural units, the number of photons

EMRP
European Metrology Research Programme
Programme of EURAMET
The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

SIQUTE

Project Coordinator: **PTB**
Deterministic and efficient single-photon sources for quantum metrology

EMRP
European Metrology Research Programme
Programme of EURAMET
The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

Project Coordinator: **INRIM**
Metrology for Quantum Key Distribution (QKD) in fiber

EMPIR
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

Project Coordinator: **INRIM**
Metrology for free-space QKD and Anti-"Quantum-Hacking"

Project Coordinator: **PTB**

EMPIR
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

SIQUST

Efficient single-photon sources for quantum technologies and quantum metrology

SEQUME

Project Coordinator: **PTB**
Single- and entangled photon sources for quantum metrology

INRiM
ISTITUTO NAZIONALE DI RICERCA METROLOGICA

19NRM06 MeTISQ

Project Coordinator: INRIM

The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

Metrology for Testing the Implementation Security of Quantum Key Distribution Hardware

Project Consortium

NMI & DI: INRIM, PTB, NPL, A*, DFM, METROSERT, CMI

Industries: TOSHIBA, IDQ, MPD

Academia: POLITECNICO MILANO 1863

Chief Stakeholder

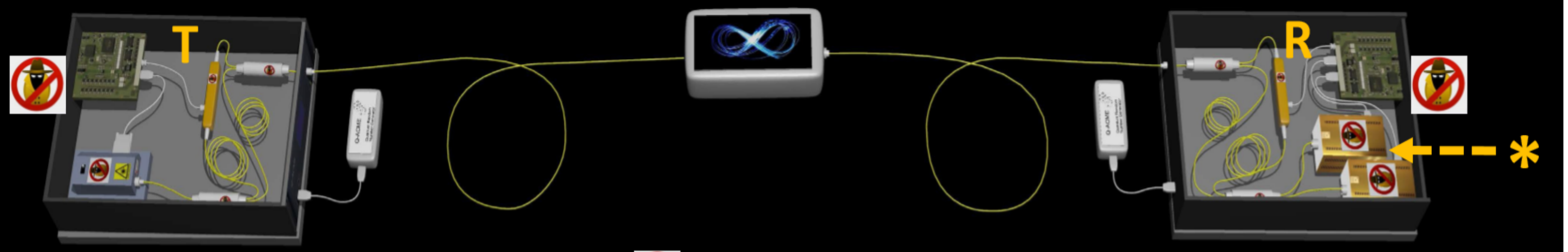
ETSI World Class Standards

Stakeholder Advisory Board

Quantum Communications Hub, Bureau International des Poids et Mesures, Universidad Politécnica de Madrid, AIRBUS, University of York, Demokritos National Centre for Scientific Research, Single Quantum, NIST National Institute of Standards and Technology, QuIC Quantum Industry Consortium, OPEN QKD, ITU, Quantum Technologies, CEN CENELEC Focus Group on Quantum Technologies, CiViQ, ISO

http://empir.npl.co.uk/metisq/

MeTISQ aims to **develop and standardise robust, SI-traceable measurements, at the single-photon level**, to characterise:



- **complete QKD modules:** Transmitter and Receiver **T & R**
- **new kinds of single-photon detector:** active components of a QKD module *
- **vulnerabilities to hacking attacks/effectiveness of counter-measures** to such attacks: **implementation security**

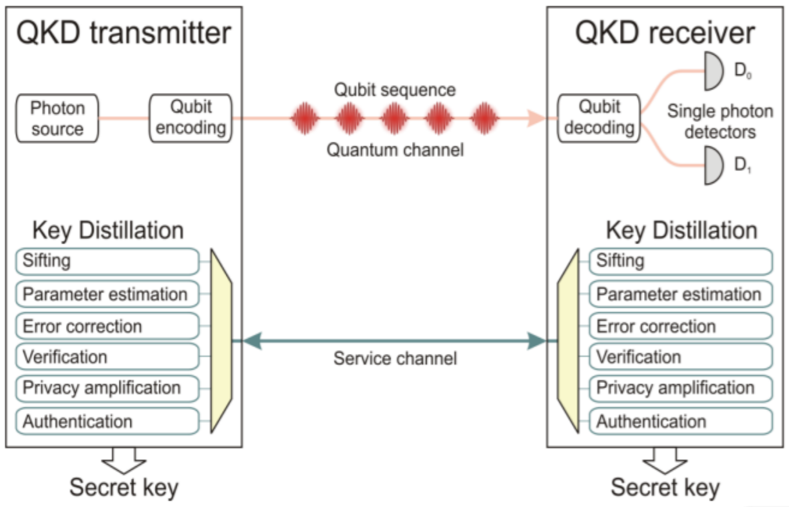
Start date: 01 September 2020
Duration: 36 + 6 months

Standardised methods will support the commercialisation of novel QKD devices

Point-to-point (P2P) DV QKD are the most documented protocols by standardization bodies.

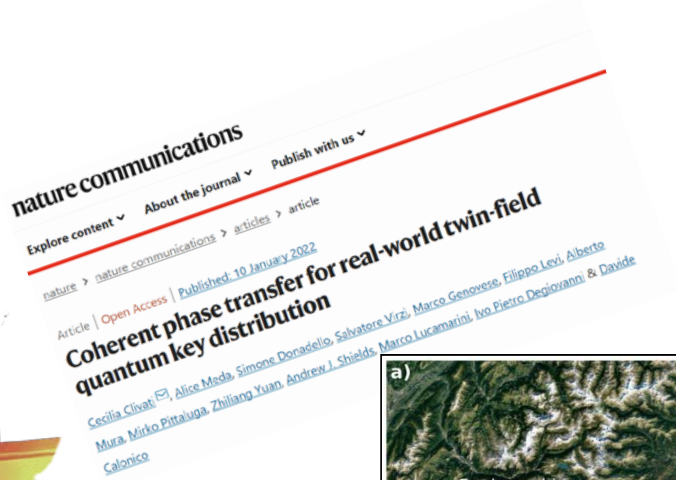
Twin field:

- weaker dependence on channel losses
- no need of trusted nodes or repeaters



[ETSI-WP8] ETSI White Paper No. 8 Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges

Italian TF-QKD-ready field trial Quantum Backbone for QKD


nature communications

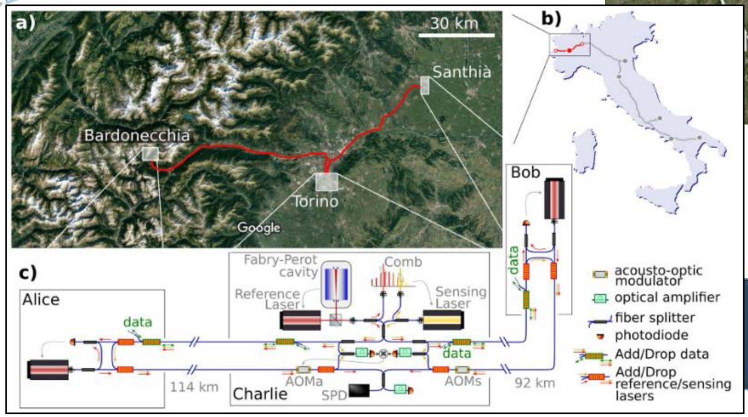
Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature > nature communications > articles > article

Article | Open Access | Published: 10 January 2022

Coherent phase transfer for real-world twin-field quantum key distribution

Cecilia Clivati, Alice Meda, Simone Donadello, Salvatore Virzì, Marco Genovese, Filippo Levi, Alberto Mura, Mirko Pittaluga, Zhiliang Yuan, Andrew J. Shields, Marco Lucamarini, Ivo Pietro Degiovanni & Davide Calonico



Dr. Salvatore Virzì poster

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

EMN-Q | European Metrology Network for Quantum Technologies

EMN for Quantum Technologies: EMN-Q

From: Strategic Agenda (V1.0, 22 Oct. 2020)

Rationale

- **To align with industrial requirements, those of the EC Quantum Technologies Flagship** and national and inter-governmental QT programmes, as well as those of any **relevant stakeholder**
- **To contribute to QT developments through NMI's and DI's research** and innovation activities
- **To give input into the standardisation & certification** of QT
- **To promote of the benefits of metrology** to the stakeholder community.

Vision

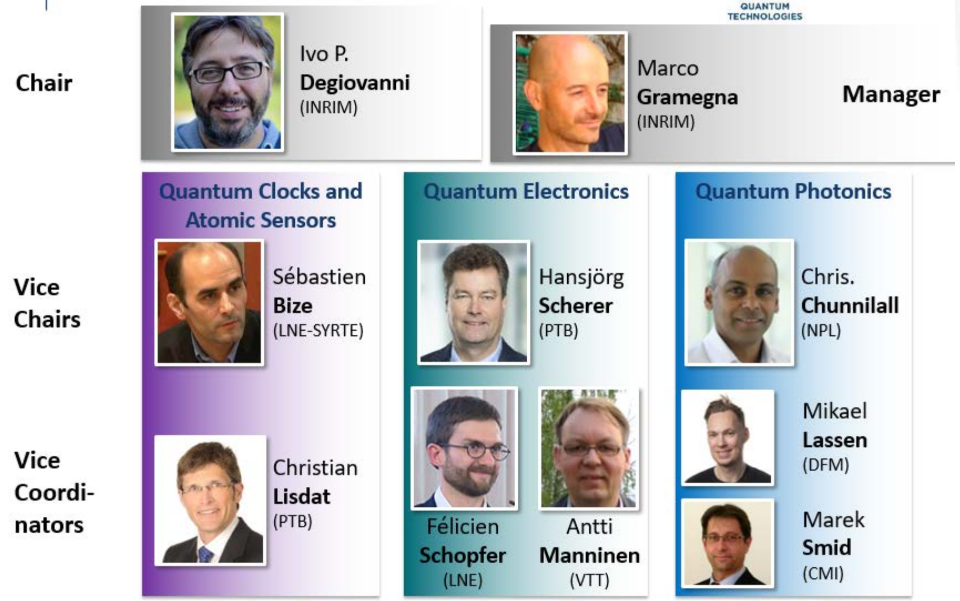
EMN-Q aims at being the recognised European unique reference point representing European metrology for Quantum Technologies.

www.euramet.org/quantum-technologies

quantum@euramet.org

Today, EMN-Q has **18 EURAMET Members and Partners** from 15 countries.

EMN-Q Structure and Organisation



Aalto	FI	LNE	FR
Metrosert	EE	LNE-LCM/CNAM	FR
CEM	SP	LNE-SYRTE	FR
CMI	CZ	METAS	CH
DFM	DK	VTT-MIKES	FI
GUM	PL	NPL	UK
INRIM	IT	PTB	DE
IPQ	PT	RISE	SE
JV	NO	UME	TR

INRIM – Quantum Optics Labs

Contacts:

m.genovese@inrim.it

a.meda@inrim.it

INRiM - Quantum Metrology and Nanotechnologies Division

https://quantum-optics.inrim.it/research

QUANTUM OPTICS RESEARCH PROGRAM

"CARLO NOVERO" LABS

EMN-Q

contacts: quantum@euramet.org

www.euramet.org/quantum-technologies

i.degiovanni@inrim.it

m.gramegna@inrim.it

QUANTUM TECHNOLOGIES

Thanks for your attention!

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA