Feasibility of satellite-to-ground continuous-variable quantum key distribution

Eleni Diamanti

LIP6, CNRS, Sorbonne University

with **Daniele Dequal**, ASI; **Luis Trigo Vidarte**, Sorbonne U. & IOGS; **Victor Roman Rodriguez**, Sorbonne U. & Thales Alenia Space; **Anthony Leverrier**, INRIA Paris; **Pino Vallone**, **Paolo Villoresi**, U. Padova

COAT Workshop, Châtillon, France

2-3 December 2019

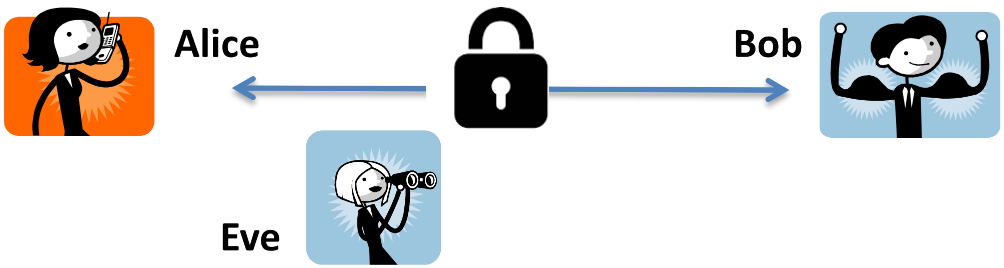
Quantum communication

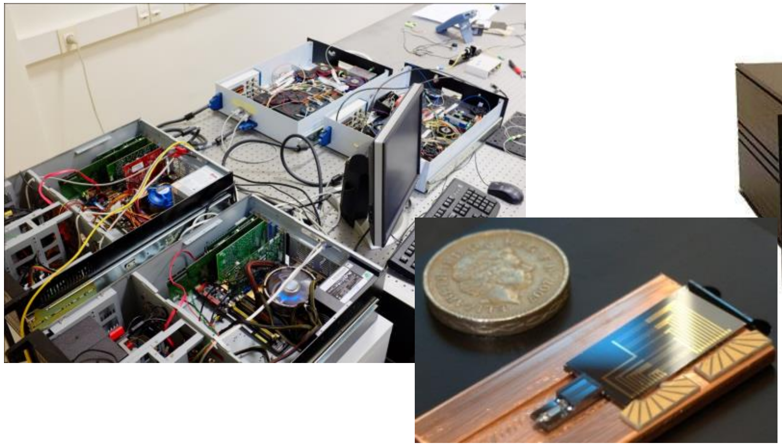
The art of transferring quantum information between distant nodes

Point-to-point secure communication: Quantum Key Distribution

Encoding in properties of quantum states of light

Provides a future-proof, unconditionally secure solution to the key distribution problem for secure message exchange between two trusted parties





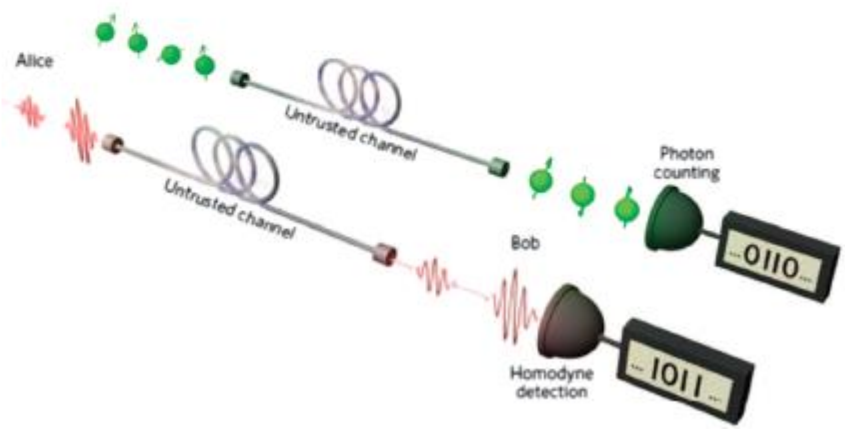
Discrete and continuous variable QKD

	Discrete variables	Continuous variables
Key encoding	Photon polarization, phase, time arrival	Electromagnetic field quadratures
Detection	Single-photon	Coherent (homodyne/heterodyne)
Post processing	Key readily available	Complex error correction
Security	General attacks, finite-size, side channels	General attacks, finite-size, side channels

BB84, Decoy state, Coherent One Way, Differential Phase Shift, Measurement Device Independent

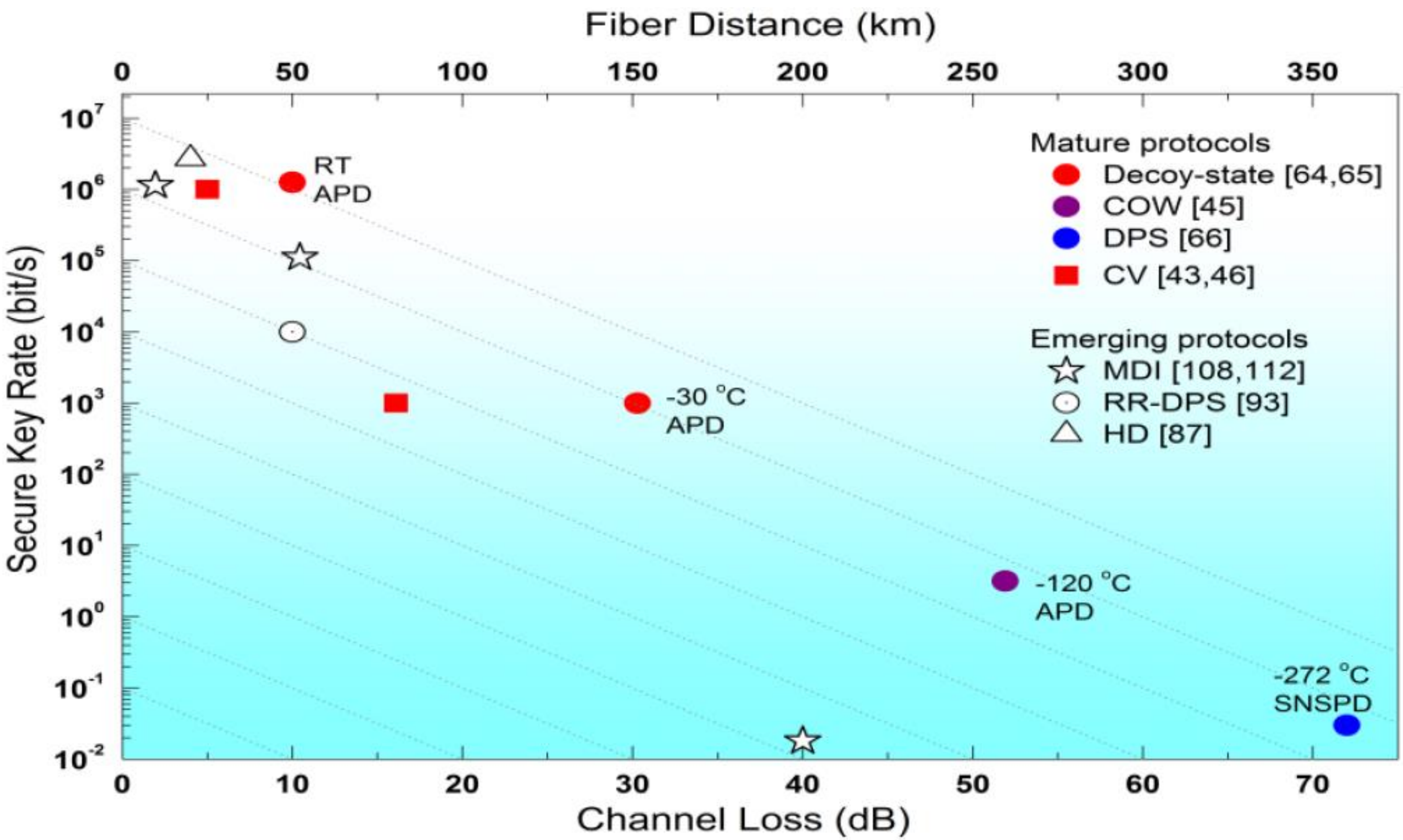
CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection)

Exploits standard telecom technology



V. Scarani et al, Rev. Mod. Phys. 2009
ED and A. Leverrier, Entropy 2015

State of the art of point-to-point fibre-optic QKD



ED, H.-K. Lo, B. Qi, Z. Yuan, npj Quantum Information 2016

Overcoming channel losses

Inherent range limitation due to optical fiber loss

Quantum networks and Satellite communications

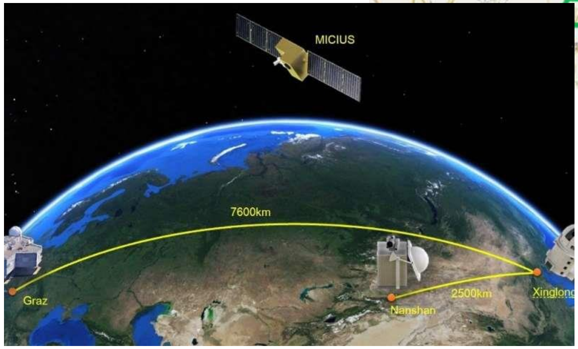
Trusted node networks

SECOQC QKD network, 2008

South Africa, Swiss, Tokyo, UK QC Hub networks

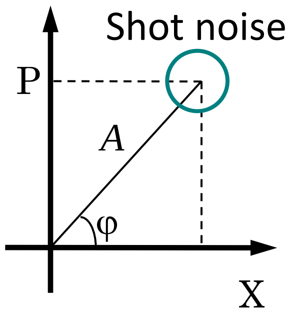
China 2000 km, 32-node network

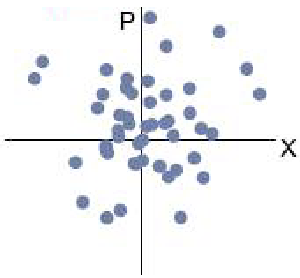
OpenQKD – EU Quantum Communication Infrastructure with terrestrial and space segments



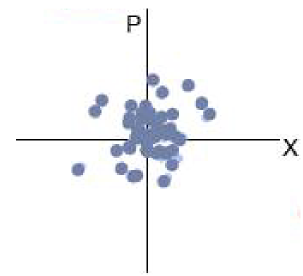
LEO Micius: downlink DV-QKD, uplink quantum teleportation, entanglement distribution, videoconferencing across the globe in trusted node-satellite model

Coherent state CV-QKD and model assumptions



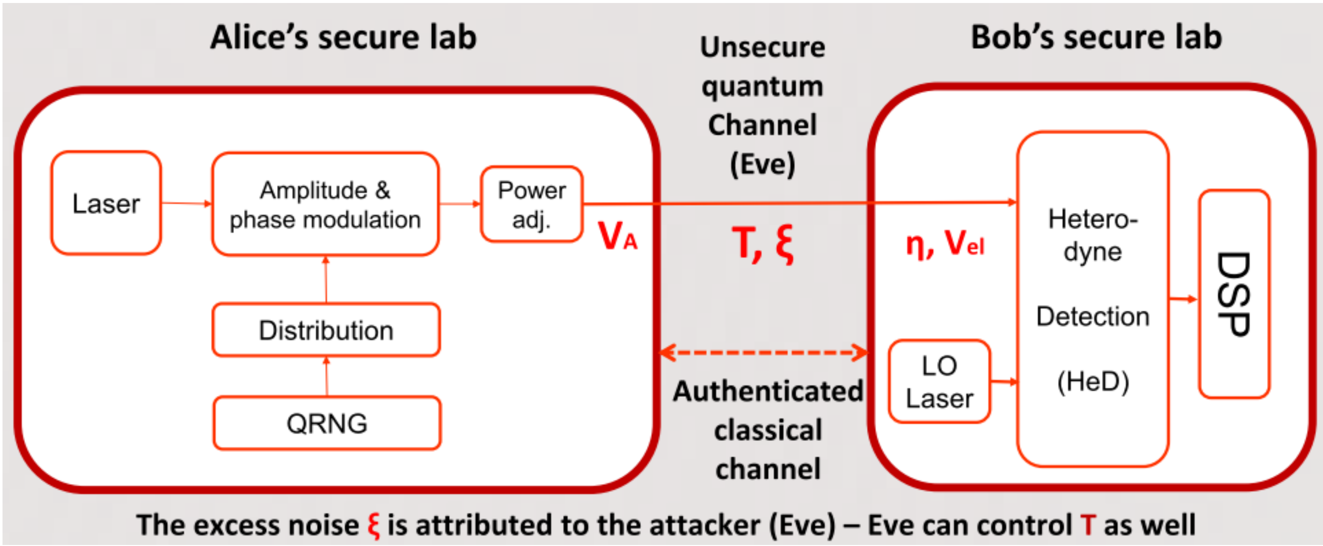


Gaussian modulation, QPSK, QAM,…



Heterodyne detection, trusted noise

Shot noise limited, low noise, high bandwidth



Pilots for phase recovery, narrow linewidth lasers

Classical post-processing steps

Additional model assumptions:

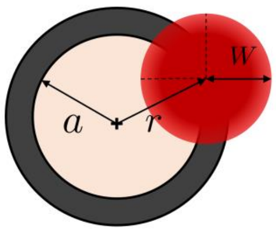
Downlink, ground station with 1.5 telescope aperture

Circular orbit passing at station zenith

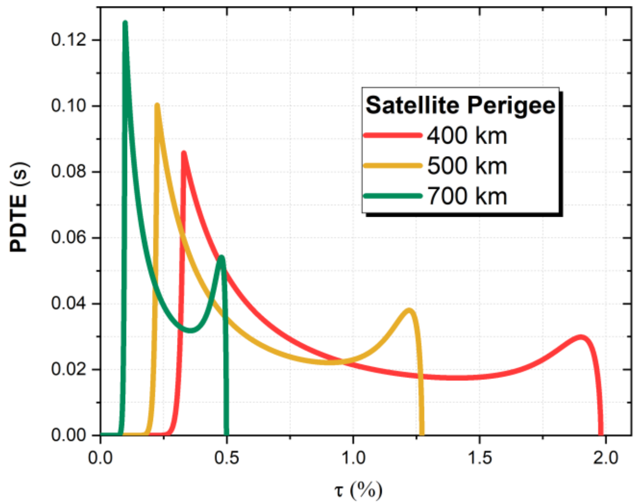
Micius performance for pointing and tracking, 3 dB fibre coupling losses

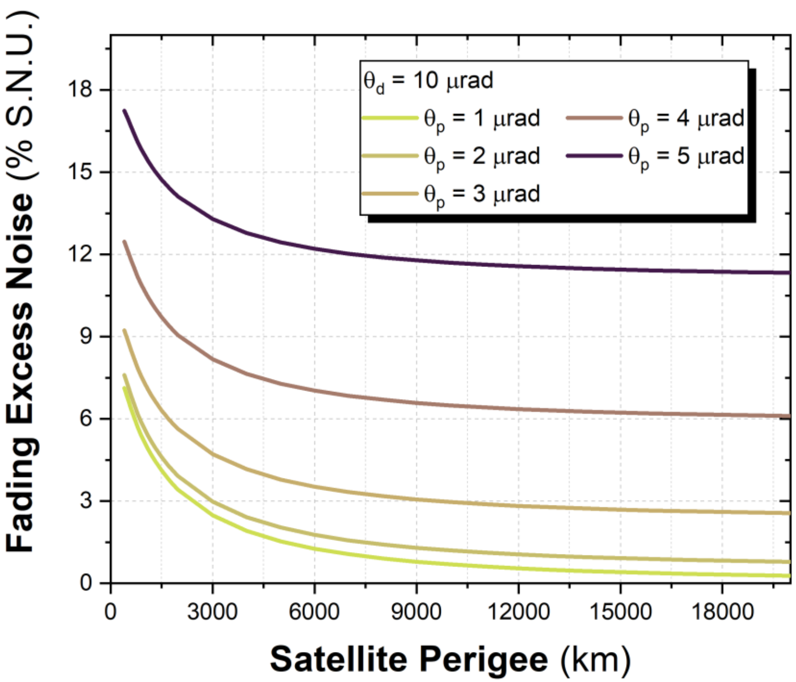
Channel model and effect of fading

Ref: D. Vasylev et al, Phys. Rev. Lett. 2012



r: Pointing error + beam wandering
W: Divergence + beam spreading





Main challenge:
Security analysis for a fluctuating channel
Fading introduces an additional noise source

$$\langle K \rangle = \beta \langle I_{AB} \rangle - f(\langle \Gamma \rangle)$$

$$\xi_{\text{fading}} = \mathrm{Var}\left(\sqrt{\tau}\right) V_A$$

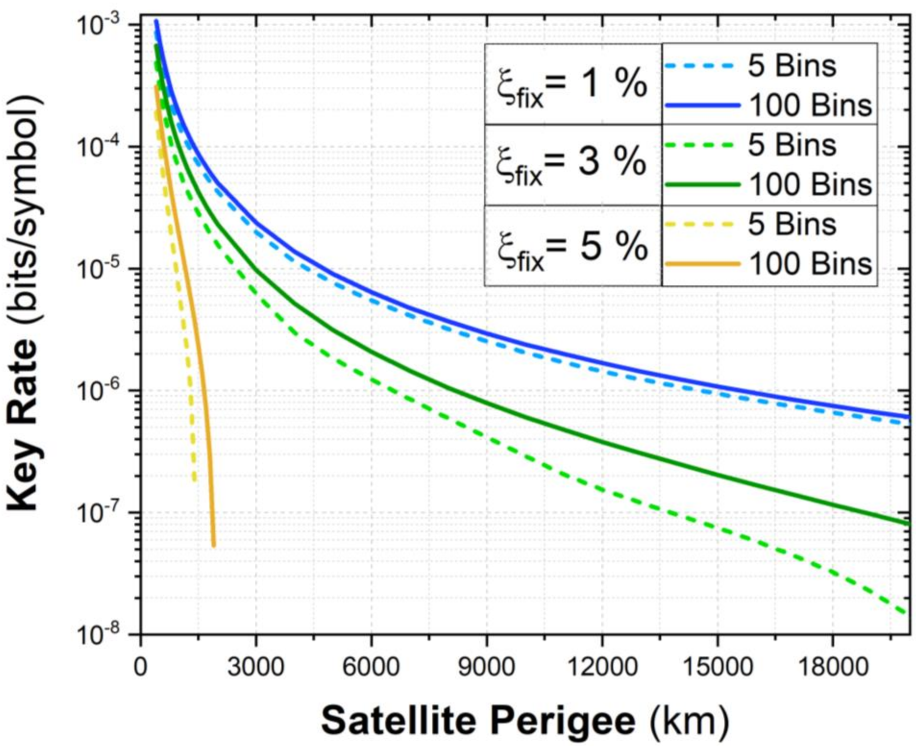
$$\xi_{\text{total}} = \xi_{\text{fixed}} + \xi_{\text{fading}}$$

Channel division

To reduce variance of the fading process →

Classical beacon to estimate transmission efficiency

'Binning' of data according to transmission efficiency, security analysis for each group

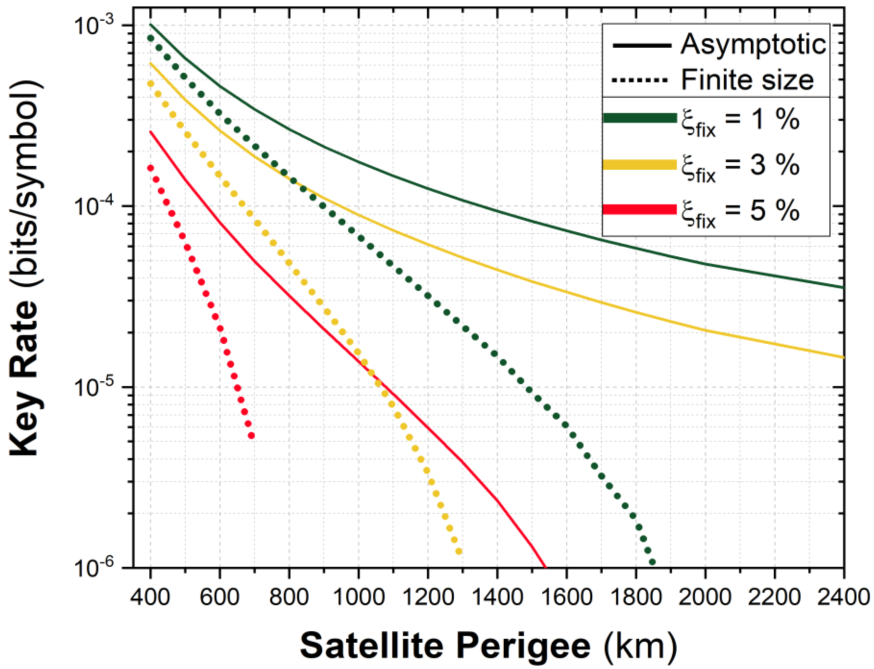


Parameter	Symbol	Reference value
Pointing error	θ_{point}	1 μ rad
Divergence angle	θ_{div}	10 μ rad
Fixed attenuation	τ_{fix}	5.8 dB
Electronic noise	ν_{el}	10% S.N.U.
Detection efficiency	η	0.4
Fixed excess noise	ξ_{fix}	1-5% S.N.U.
Reference laser power	P_{ref}	100 mW
Reconciliation efficiency	β	0.95
Transmission frequency	f_{TX}	1 GHz

Finite size effects

Finite size effects are related to statistical uncertainties in parameter estimation

Trade-off between finite size and fading noise in channel division



Conclusion

Quantum satellite communications will be part of the future quantum-safe infrastructure

CV-QKD is feasible for LEO with realistic assumptions, and provides high throughput

Finite-size effects prevent key generation at higher orbits → increasing transmission rate and using multiple passages may help

Next steps:

Study of inclined orbits, adaptive optics, lab validation, realistic architecture with specific ground stations, measurement device independent configuration