Single Photon Detection in Quantum Secure Communication: towards the future Quantum Internet

20211110 OSUG-FOCUS – Erik Kerstel

The Dream: A Global Quantum Information Network

The quantum internet has arrived (and it hasn't), *Nature* **554**, 289 (2018)
On-demand entanglement could lead to scalable quantum networks, *Nature* **558**, 192 (2018)
Quantum internet: A vision for the road ahead, Science **362**, 303 (2018)

Distributed, cloud quantum-computing,
Entanglement-based sensing, clock synchronization,
Quantum physics measurements (gravitational waves, VLB interferometry)
Quantum communications,
…

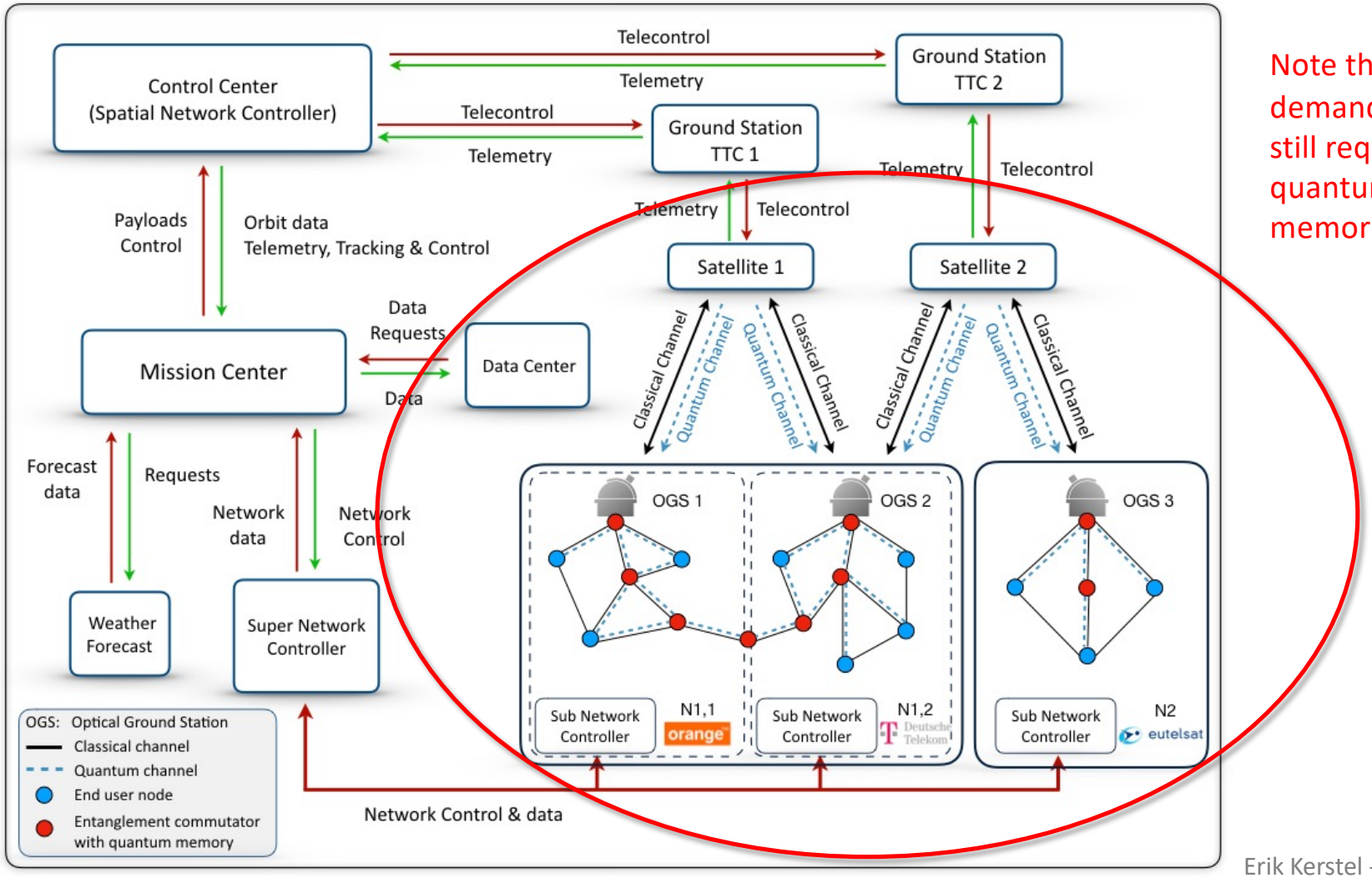
credit:

Optical fibers limited by absorption losses (~100 km),
Free-space optics on Earth limited to line of sight (~100 km)

→ require quantum repeaters or trusted nodes to extend the range

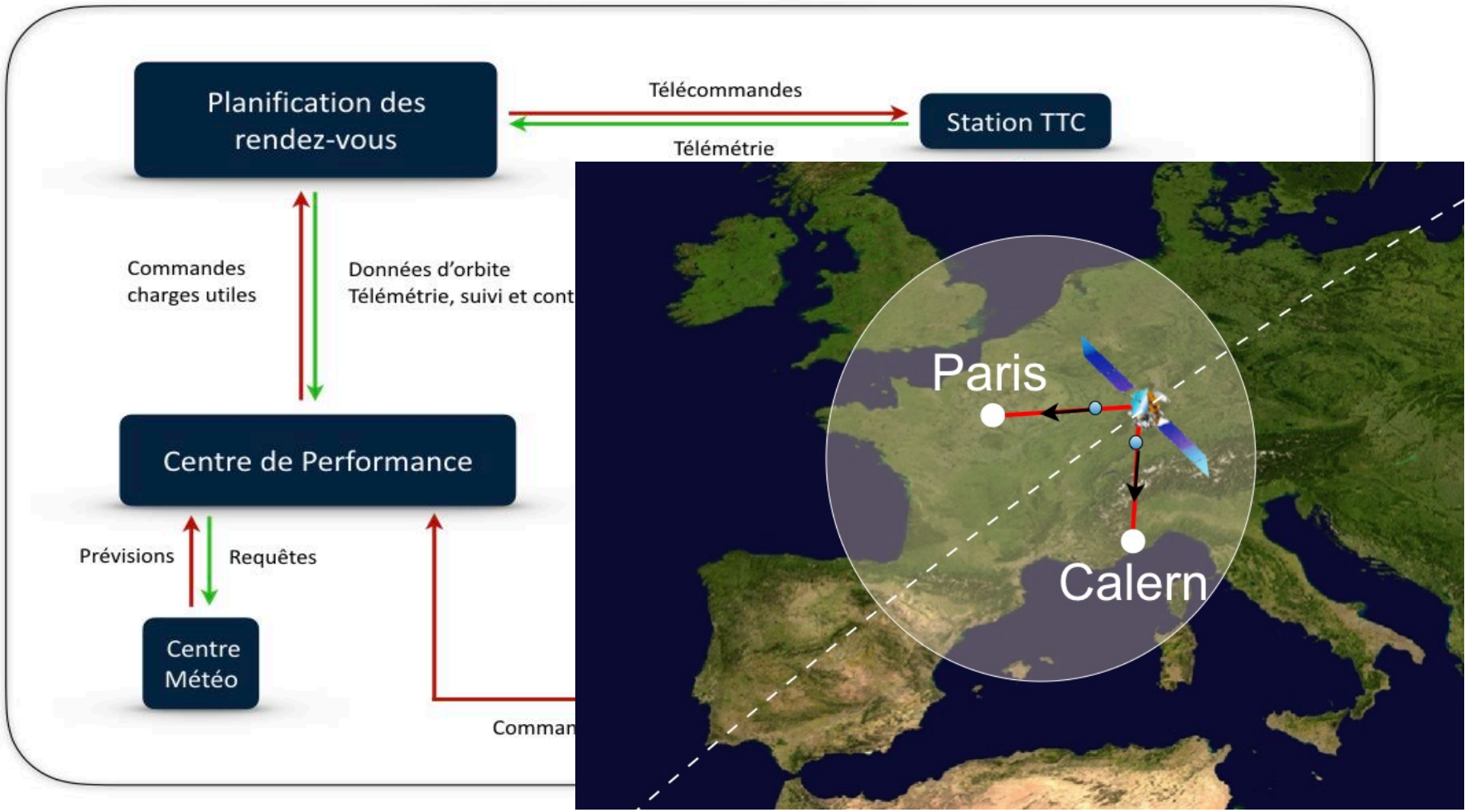
Space QKD can go global while reducing # of trusted nodes …

Global QIN: Satellites distribute entangled photon pairs



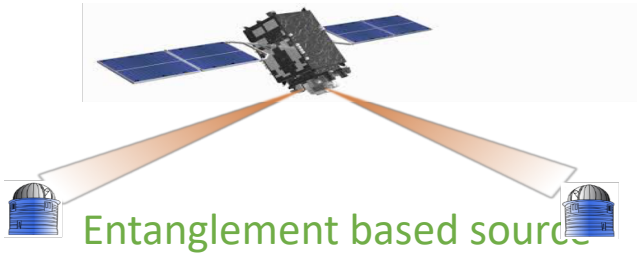
Note that an on-demand network still requires quantum memories (●)

Demonstrator Simplified Diagram



Scenarios

Entanglement distribution



Entanglement based source

Holy Grail: Satellite not trusted

Limited range (~1200 km)
Squared losses

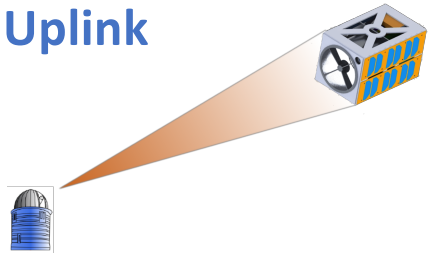
Very complex: source on-board

Big satellite (Micius 620 kg)

Expensive

Detectors on the ground

Uplink



Satellite is trusted node

Global
'Shower curtain' losses (~10 dB)
(Adaptive optics compensation!)

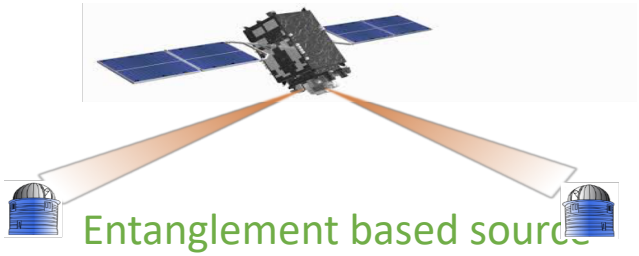
Low on-board count rate & storage

Space segment less complex,
more robust

CubeSat standard platform
Space segment cheaper, faster
Detectors in the satellite
Versatile: BB84, E91, ...

Scenarios

Entanglement distribution



Entanglement based source

Holy Grail: Satellite not trusted

Limited range (~1200 km)

Squared losses

Very complex: so

Big satellite (Mici

Expensive

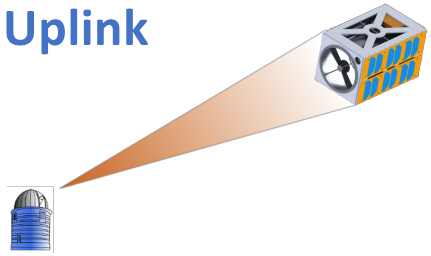
Detectors on the ground

CNES-Thales+ « RIQS » project

Early demonstrator

« NanoBob » project

Uplink



Satellite is trusted node

Global

'Shower curtain' losses (~10 dB)

(Adaptive optics compensation!)

rd count rate & storage

ent less complex,

t

ndard platform

ent cheaper, faster

Detectors in the satellite

Versatile: BB84, E91

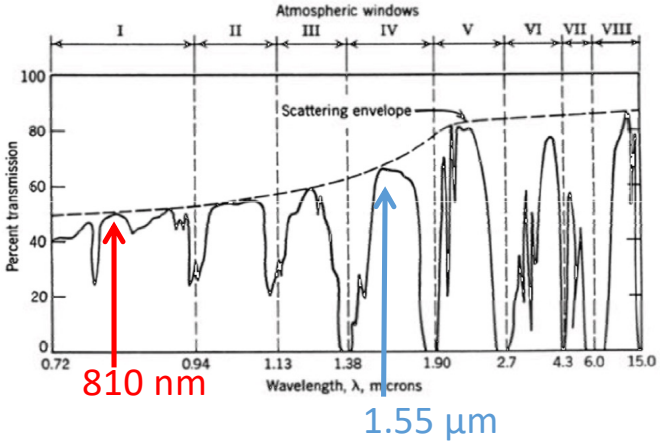
Sofar: extensive mission analyses for both scenarios with trade-offs for:

- Satellite orbit (LEO, MEO, inclination, …)
- Quantum channel wavelength
- Single Photon Detectors

NanoBob: Single Photon Detectors in Space

810-nm (Silicon) versus 1550-nm (InGaAs or MCT) spectral range:

Infrastructure/day compatibility	InGaAs or MCT
Atmospheric transmission	1.55 µm (-0.8 dB)
Turbulence limited diffraction	1.55 µm (-0.6 dB)
Detector Efficiency	Si or MCT (+3 dB)
Detector operating temp.	< -80 °C (InGaAs & MCT) vs. -30 °C (Si)
Dark counts	Si or InGaAs
Timing jitter	Si or MCT
Space heritage (radiation!)	Si



Wavelength range	VIS (800 nm)	NIR (1550 nm)	NIR (1550 nm)
Technology	Si-APD	InGaAs/InP-APD	MCT
Active area diameter (µm)	50 - 100	fiber coupled	160
Operating temperature (°C)	> -30	**-90**	**-120**
Dark count rate (Hz)	20	200	**1000 ?**
Quantum efficiency	40%	< 25%	> 60%
Timing resolution (ps)	90	200	< 100 ps
Pulse width (ns)	<100	100	0.3
Dead time (µs)	1	> 2 (up to 100)	< 1
Manufacturer/ Model	MPD/ RE-SPAD	IDQuantique/ ID230	CEA-Sofradir

Currently, Si-based single photon detectors are only practical alternative for the Space segment

« RIQS » Single Photon Detector: Requirements

Wavelength (atm. Transmission)	1550 nm or 810 nm	
Photon Detection Efficiency (PDE)	> 0.5	
Dark Count Rate (DCR)	< 250 cps	(100 cps)
Timing jitter (τ)	< 500 ps	(200 ps)
Count Rate (CR)	> 100 Mcps	(1 Gcps, potentially through parallelization)
Dead-time (τ_d)	< 10 ns	
After-pulsing	< 2%	

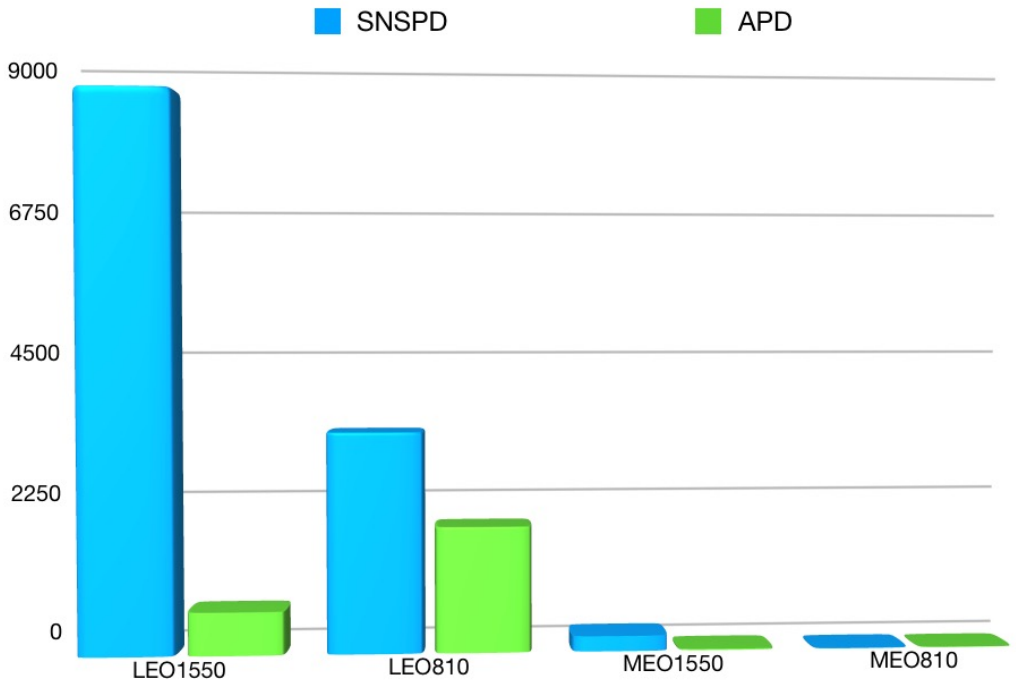
« RIQS » Single Photon Detector: State-of-the-Art

	APD-Si	APD-InGaAs	SNSPD	SNSPD	MCT
Wavelength (nm)	810	1550	810	1550	1550
Photon Detection Efficiency	> 70%	> 25%	> 90%	> 90%	> 60%
Dark Count Rate (cps)	< 100	< 250	< 10	< 10	> 1000 ?
Timing jitter (ps)	< 100	< 200	< 80	< 80	< 100
Count Rate (Mcps)	> 100	> 100	~10	~10	1000
Complexity/cost	$	$$	$$$$$	$$$$$	$$$

« RIQS » Simulation input parameters

Parameter	Description	Value
λ	Quantum channel wavelength	810 nm / 1550 nm
H	Satellite altitude	LEO: 600 km / MEO: 8000 km
D_R	Ground receiver telescope diameter	80 cm @LEO / 100 cm @MEO
D_T	Onboard transmitter telescope diameter	30 cm @LEO / 50 cm @MEO
$A_{atm,0}$	Atmospheric attenuation at zenith	3 dB @810 nm, 2 dB @1550 nm
T_R	Receiver transmission factor (FSO @810 nm, fibre coupling @1550 nm)	0.8 @810 nm, 0.5 @1550 nm
T_T	Transmitter transmission factor (FSO @810 nm, fibre coupling @1550 nm)	0.8 @810 nm, 0.5 @1550 nm
L_p	Pointing losses	0.2 (with precision $\leq 10\mu$rad)
q	Basis reconciliation factor	0.5
f	Biderectional error correction efficiency	1.22
τ	Coincidence time window	200 ps
μ	Average number of photon pairs per pulse	0.02
D	Detector dark count rate (same detector in Paris and Calern)	100 cps
B	Background (stray light) count rate	400 cps @810 nm, 100 cps @1550 nm
PDE	Single photon detector efficiency	0.9(SNSPD) /0.68(APD-Si) /0.25(APD-IGA)
T_{opt}	Combined optics efficiency (satellite/station)	0.64 @810 nm, 0.25 @1550 nm
η_x	Quantum channel efficiency, with A_x the losses in channel $x = 1, 2$	$\eta_x = T_{opt}.PDE.10^{-A_x/10}$
e_0	Error probability for dark- and background counts	0.5
e_p	Error probability of photon arriving on wrong detector	0.01
Δt	Time step	10 seconds
T_{final}	Total simulation duration	12 months

« RIQS » Simulation results



1550 nm	810 nm
Low Earth Orbit (h = 600 km)	Medium Earth Orbit (h = 8000 km)

Conclusion:

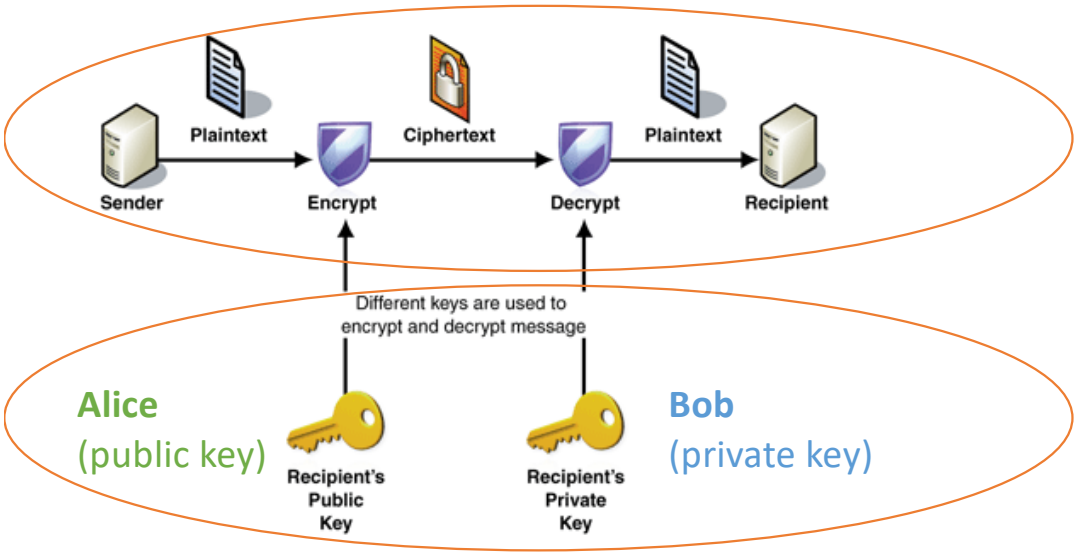
If cost plays no role:
Parallelized SNSPDs at both wavelengths

If cost/complexity/cooling is a concern:
Si-APDs at 810 nm
Great potential for MCT developments for access to 1550 nm (telecom), e.g., in mobile optical ground stations or in the satellite! (cooling, arrays)

LEO is always to be preferred

Classical cryptography/key distribution

Asymmetric classical protocol

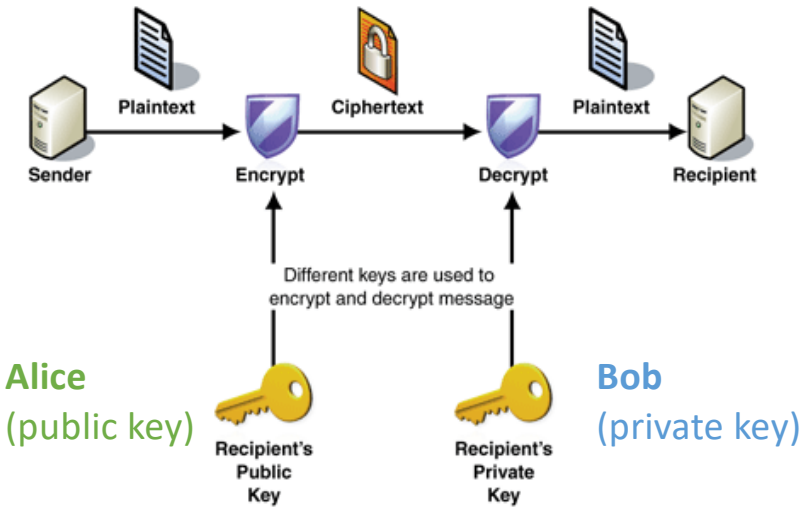


Cryptography: (de-) ciphering a message

Secret Key Distribution

Classical cryptography/key distribution

Asymmetric classical protocol



- 2 different keys are used
- **No security proof exists**

Currently widely used RSA protocol (Rivert, Shamir, Adleman, 1978) can be broken!

→ 768-bit RSA now takes about 2 years on a 100-core computer to crack … future ??

→ Future **Quantum Computers** ?!

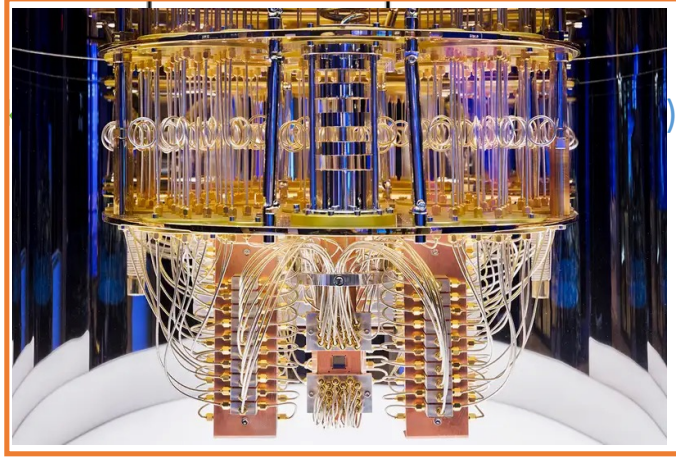
Classical cryptography?

Asymmetric classical protocol

Currently widely used RSA protocol (Rivert, Shamir, Adleman, 1978) can be broken!

→ 768-bit RSA now takes about 2 years on a 100-core computer to crack … future ??

→ Future **Quantum Computers** ?!

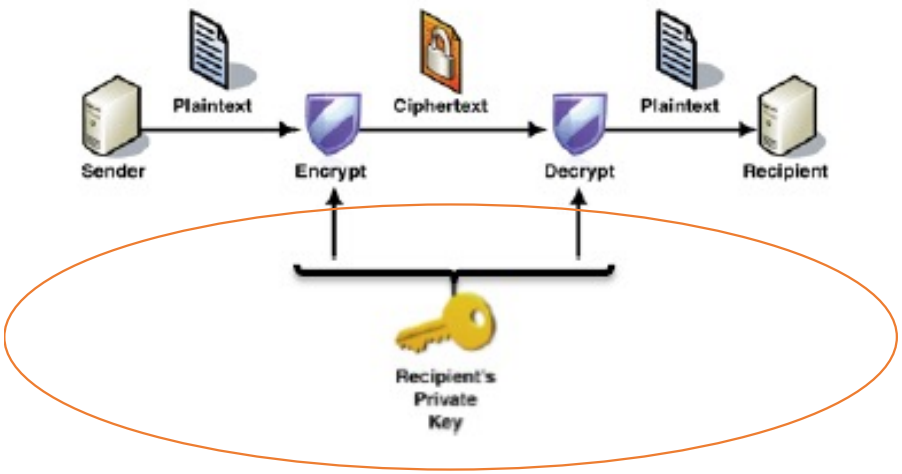


IBM Research Quantum Computer

- A polynomial-time algorithm for prime factorization already exists (Peter Shor, 1994)
- Arrival of the quantum computer is only a matter of time

Classical cryptography the secure way

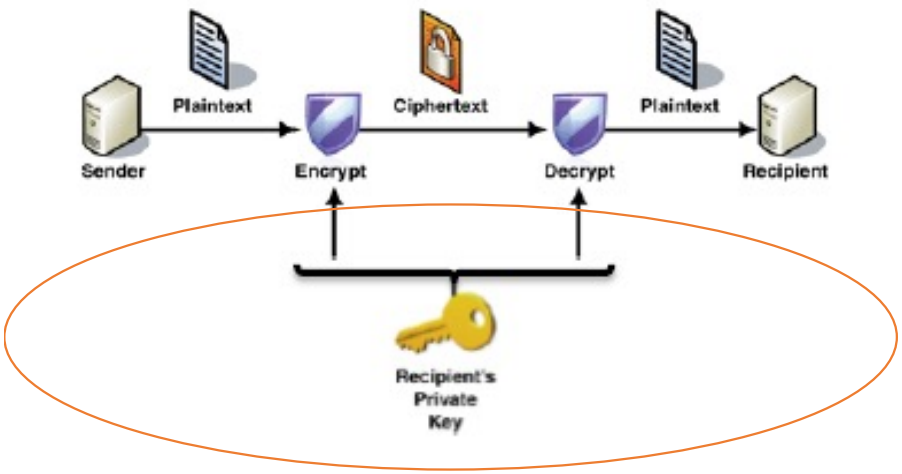
Symmetric protocol



- Random Key
- 1 key used only once (“one-time pad”)
- **Provably secure implementation**

Classical cryptography the secure way

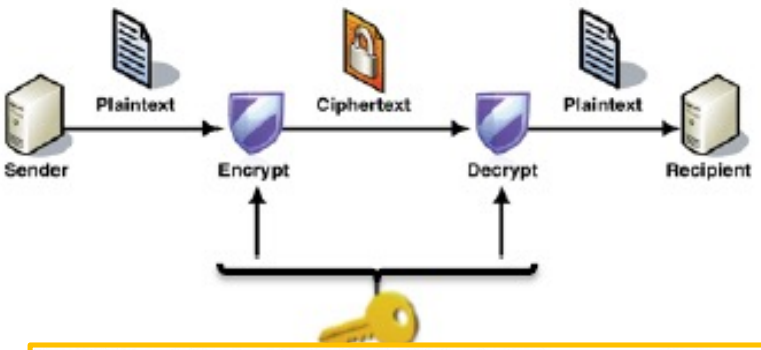
Symmetric protocol



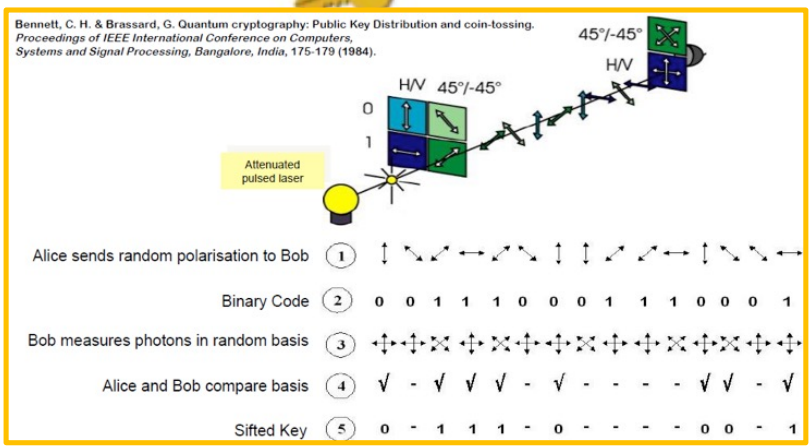
- Random Key
- 1 key used only once (“one-time pad”)
- **Provably secure implementation**
- **But, how to share the key ?**

Quantum cryptography

Symmetric protocol



- Random Key
- 1 key used only once ("one-tim
- Provably secure implementati
- **But, how to share the key ?**



Solution is Quantum Key Distribution

- **Single photons** carrying the quantum bit information in their polarization state
- Statistics of photon states allow testing the trustworthiness of the key by a test of the **Bell inequality** ("Ekert91")

TAS-F (Laurent De Parny, Mathias Van Den Bosche)
CNES (Patrick Gelard)
IQOQI (Rupert Ursin, Siddarth K. Joshi, and Matthias Fink),
INPHYNI (Sebastien Tanzilli, O Alibart),
LIP6 (Eleni Diamanti, M Schiavon),
OCA (E Samain, C Courde, J Chabé),
Bristol (SKJ, John Rarity),
Onera (Nicolas Vedrenne),
and other industrial partners

CSUG (E Kerstel, S Gressani, J Debaud, A Metrat), and the entire **UGA-CSUG Team**!

EPJ-QT 2018. https://rdcu.be/1uEO

The CSUG NanoBob Team:

Yves Gilot (STMicroelectronics), Etienne LeCoarer (UGA), Juana Rodrigo (Rolls Royce), Thierry Sequies (UGA), *Vincent Borne* (UGA), *Guillaume Bourdarot* (UGA), *Jean-Yves Burlet* (UGA), *Alexis Christidis* (UGA), *Jesus Segura* (UGA), Benoit Boulanger (UGA), Veronique Boutou (UGA), Mylene Bouzat (Air Liquide), Mathieu Chabanol (UGA), Laurent Fesquet (UGA), Hassen Fourati (UGA), Michel Moulin, Jean-Michel Niot (Air Liquide), Rodrigo Possamai Bastos (UGA), Bogdan Robu (UGA), Etienne Rolland (UGA), and Sylvain Toru (UGA).