Experimental quantum communication in Space

G. Vallone

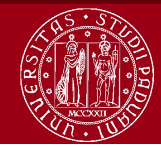
email: vallone@dei.unipd.it

UNIVERSITÀ DEGLI STUDI DI PADOVA

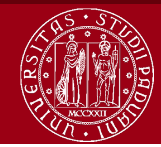
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

23 Maggio 2016

Summary

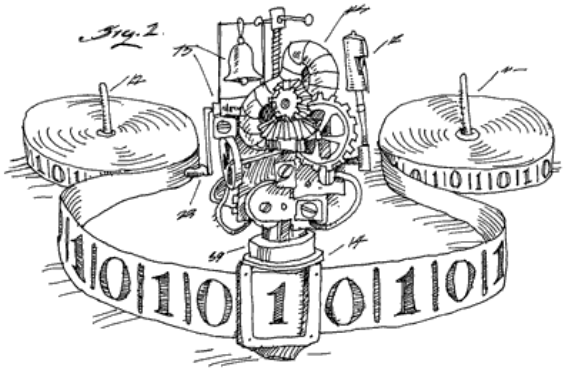


Summary



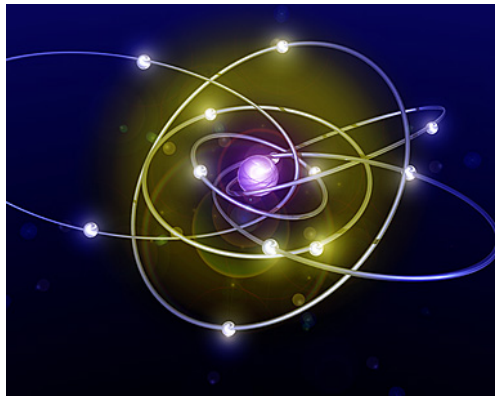
What is Quantum Information?

Information Theory



$\Leftrightarrow$

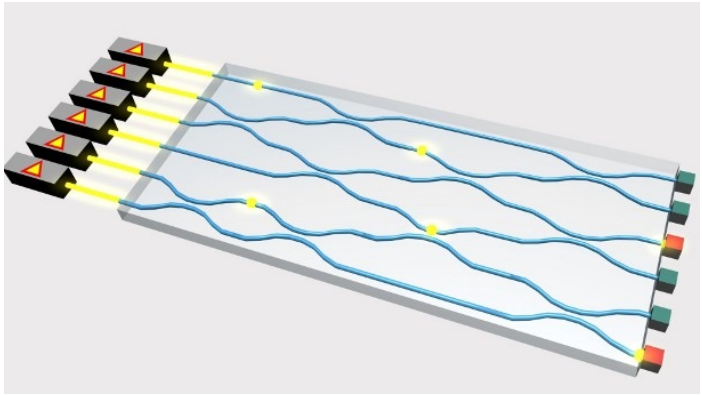
Quantum Mechanics



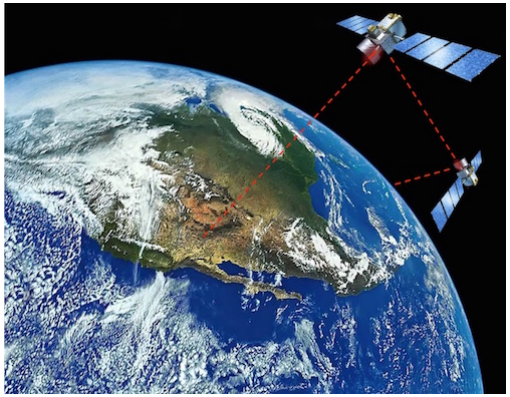
Merging two big XXth century revolutions:
information theory (Shannon, Turing) and Quantum Mechanics.

Examples of applications

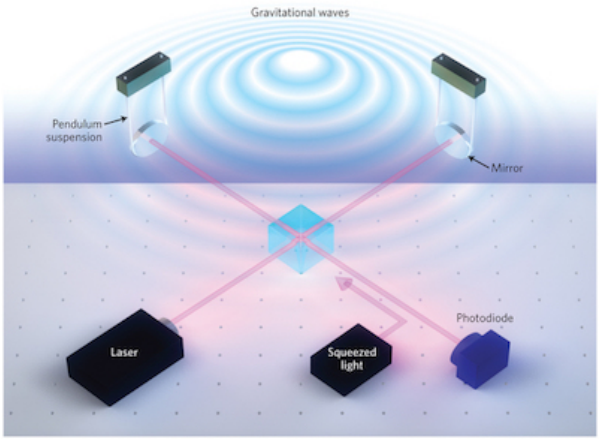
Quantum computer

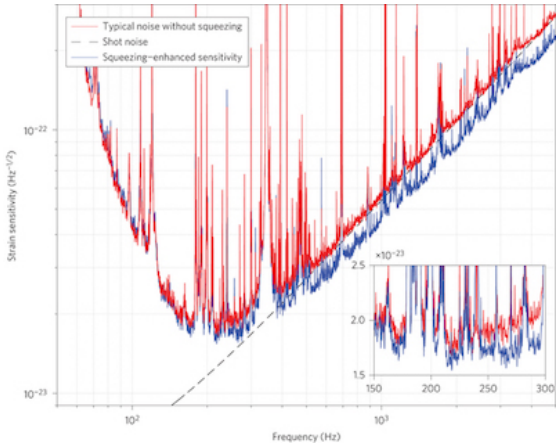


Quantum cryptography



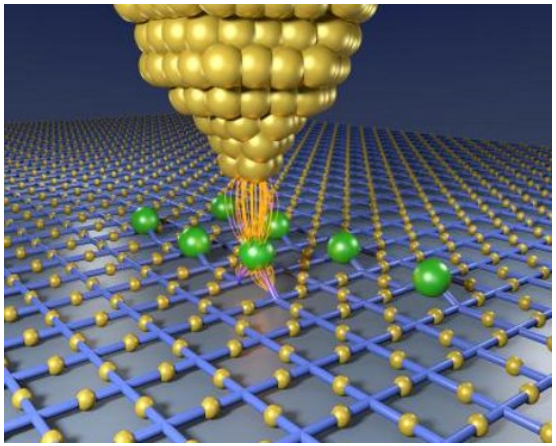
Quantum metrology



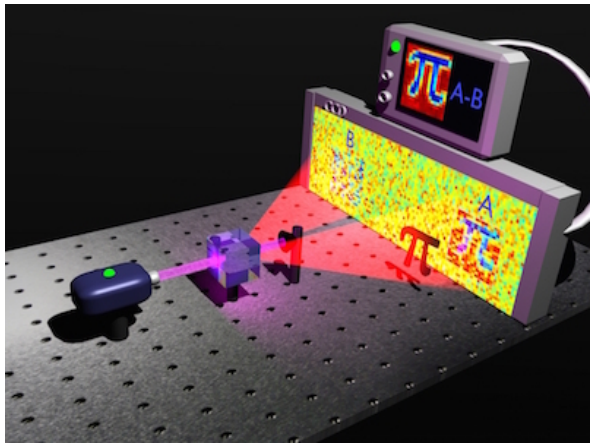


Examples of applications

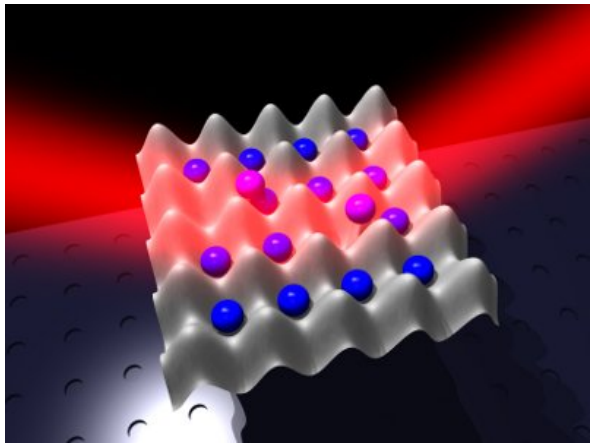
Quantum sensing



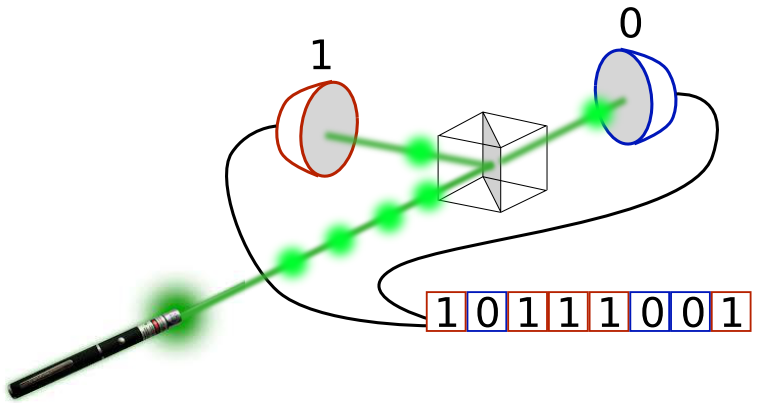
Quantum imaging



Quantum simulation



Quantum random number generation

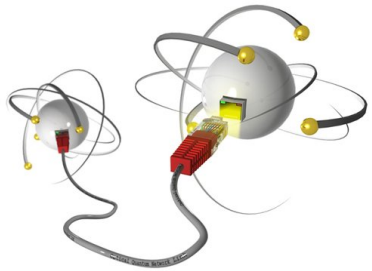


But...

...be aware of fake!

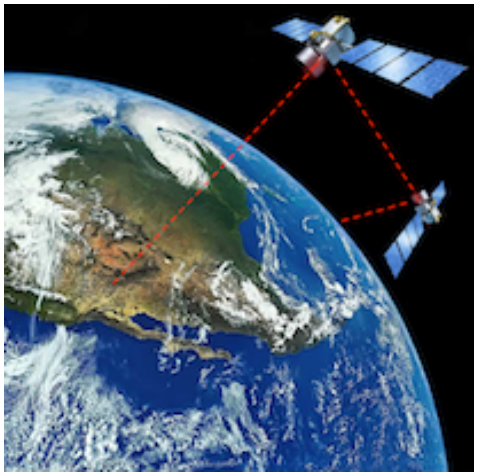
What is Quantum Communication?

- Quantum Communications is the ability of faithful transmit qubit (or generic quantum states) between two distant locations

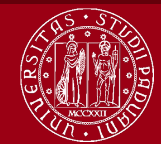


- Application of ground QC: commercial QKD using fiber-cables

- Quantum Communications on planetary scale require complementary channels including ground and satellite links



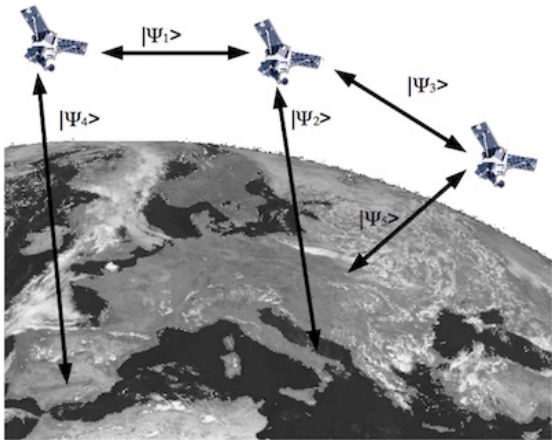
Motivation



Why free-space quantum communications?

Motivation

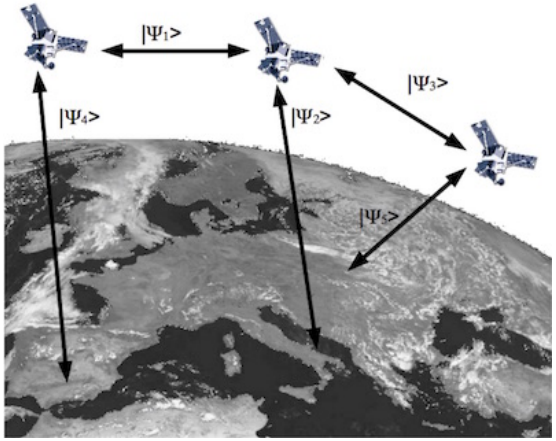
Why free-space quantum communications?

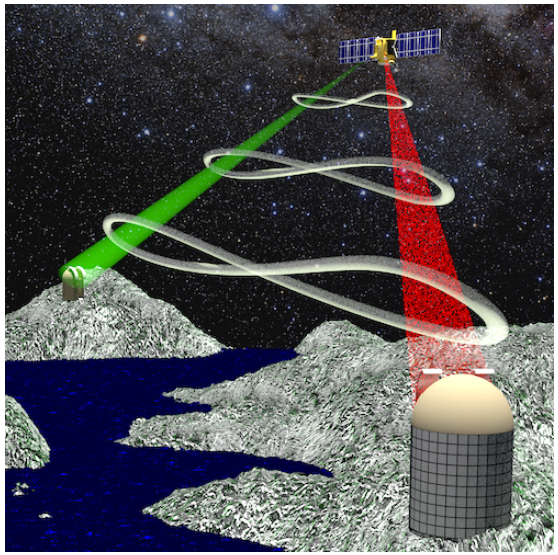


- Creation of a **worldwide quantum network**: overcome fiber-loss limitations

Motivation

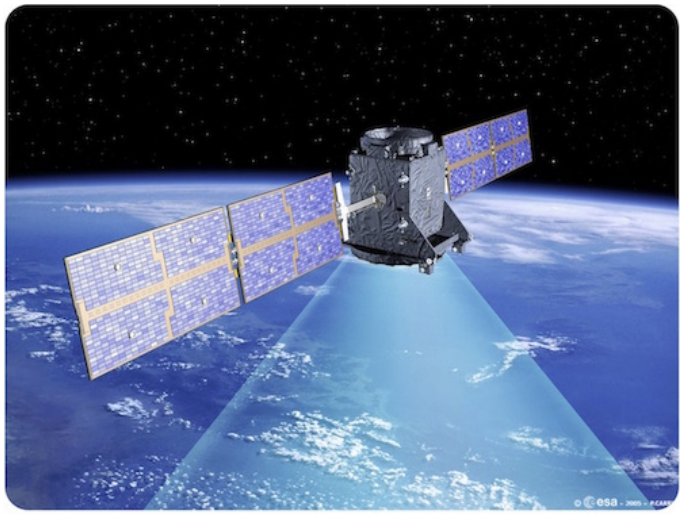
Why free-space quantum communications?





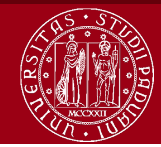
- Creation of a **worldwide quantum network**: overcome fiber-loss limitations
- **Explore the limits of Quantum Mechanics** and quantum correlations over very long distances

Context

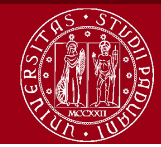


- On May 24, 2014 Japan's NICT launched SOTA on Socrates satellite.
- Ongoing programs for QC on satellite in China and Canada as well as in Singapore and USA.

Summary



Superposition principle



- Physical states are representes as vectors $|\psi\rangle$

Superposition principle

- Physical states are representes as vectors $|\psi\rangle$
- Superposition principle: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are physical states, any linear combination is a physical state:

$$|\Psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \qquad a, b \in \mathbb{C}$$

Superposition principle

- Physical states are representes as vectors $|\psi\rangle$
- Superposition principle: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are physical states, any linear combination is a physical state:

$$|\Psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \qquad a, b \in \mathbb{C}$$

- From classical bit (two orthogonal states $|0\rangle$ and $|1\rangle$) to quantum-bit , or qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}\,, |\alpha|^2 + |\beta|^2 = 1$$

Superposition principle

- Physical states are representes as vectors $|\psi\rangle$
- Superposition principle: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are physical states, any linear combination is a physical state:

$$|\Psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \qquad a, b \in \mathbb{C}$$

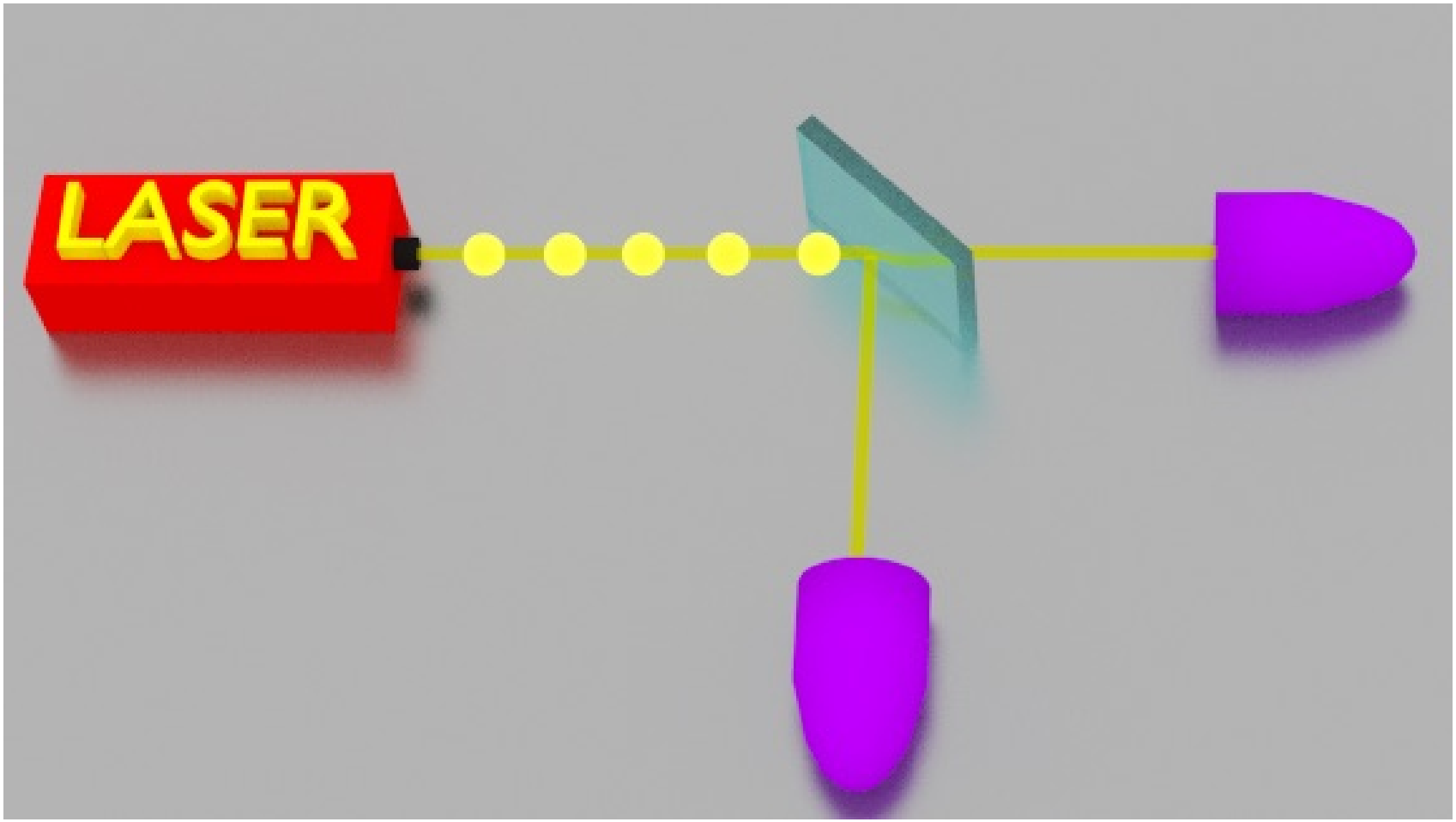
- From classical bit (two orthogonal states $|0\rangle$ and $|1\rangle$) to quantum-bit , or qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}\,, |\alpha|^2 + |\beta|^2 = 1$$

- indistinguishability $\Rightarrow$ INTERFERENCE!

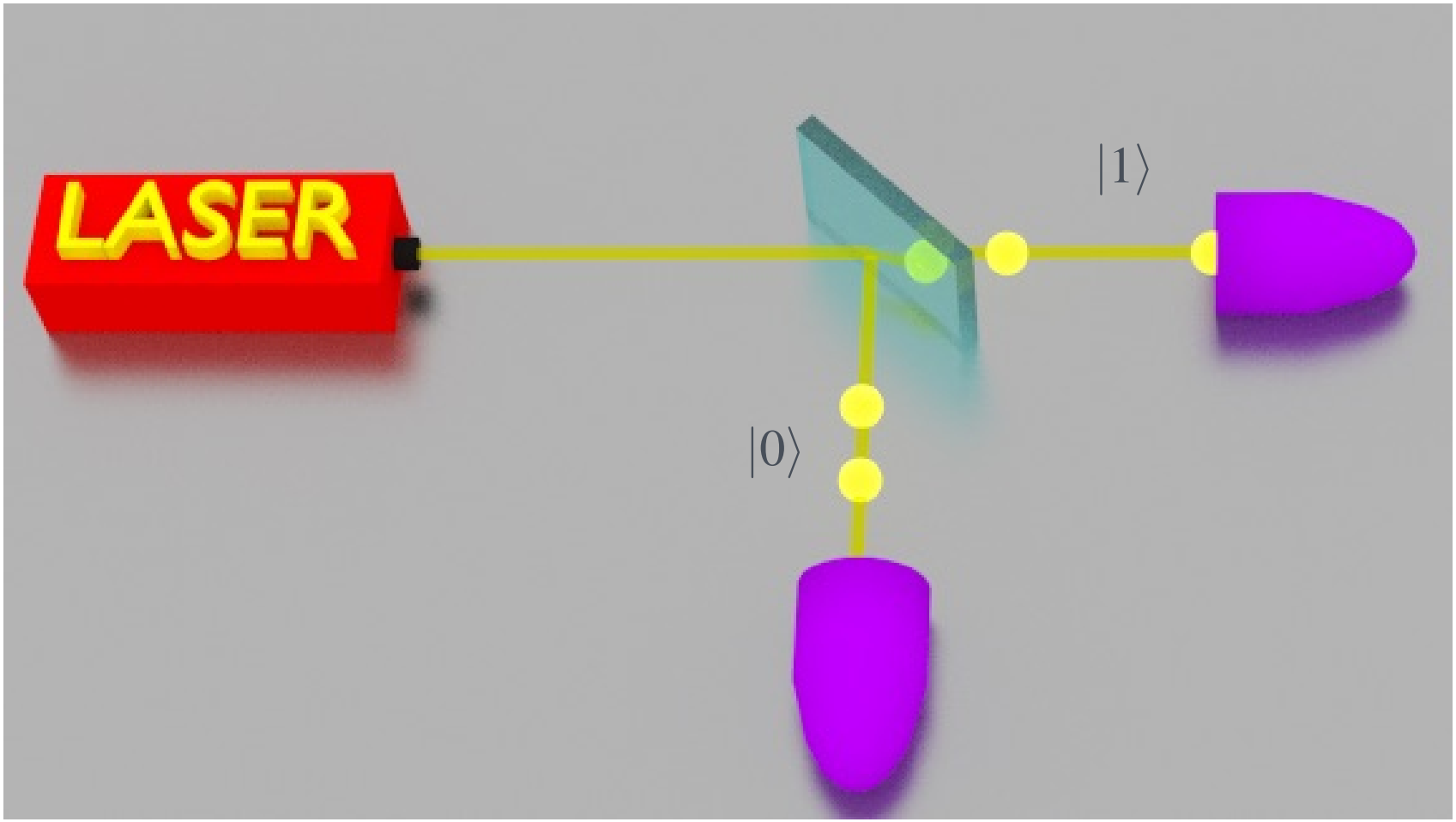
State superposition

Example : photons on a semi-reflective mirror (beam splitter)



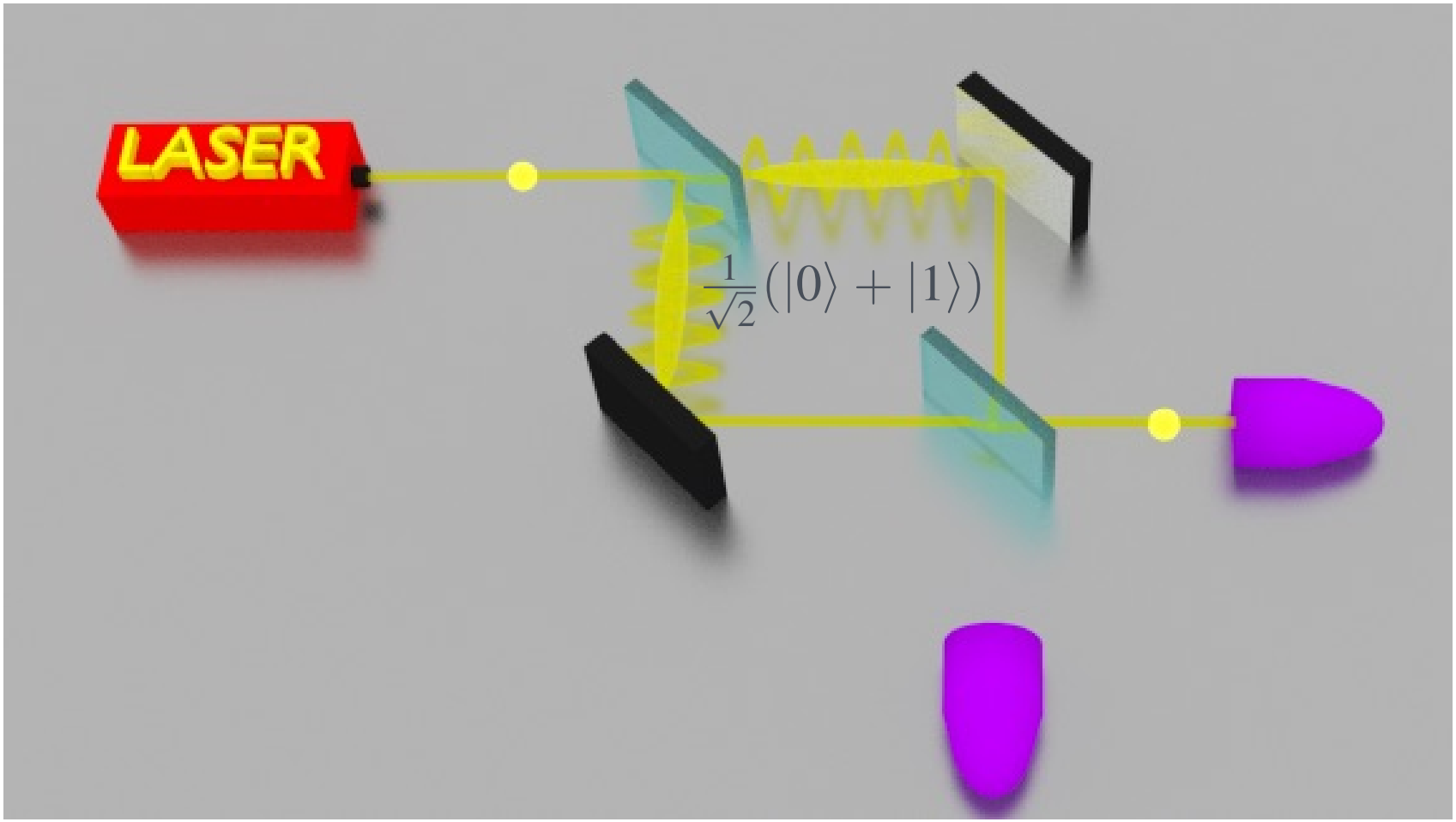
State superposition

Example : photons on a semi-reflective mirror (beam splitter)



State superposition

Example : photons on a semi-reflective mirror (beam splitter)



State superposition

Example 2: two-slit experiment

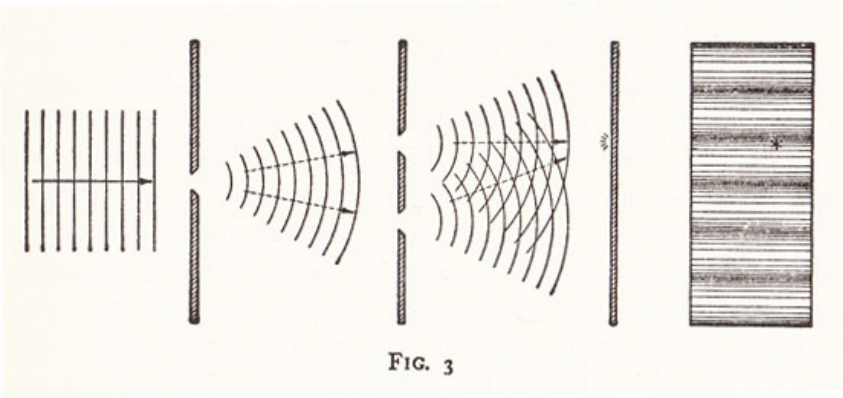
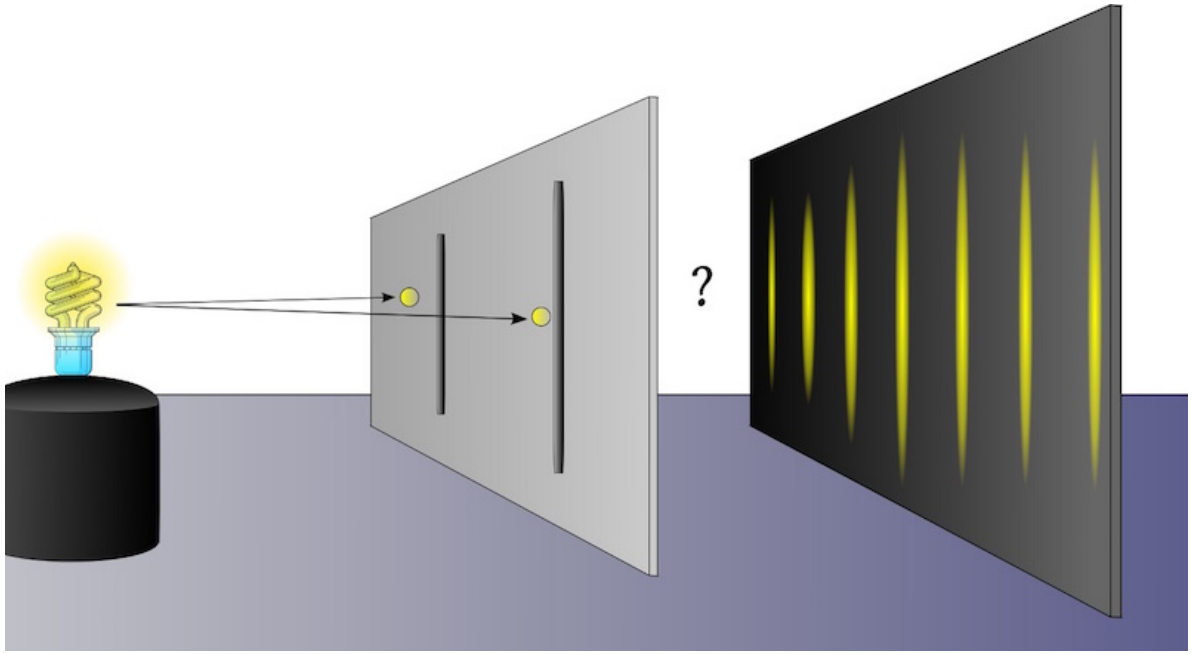


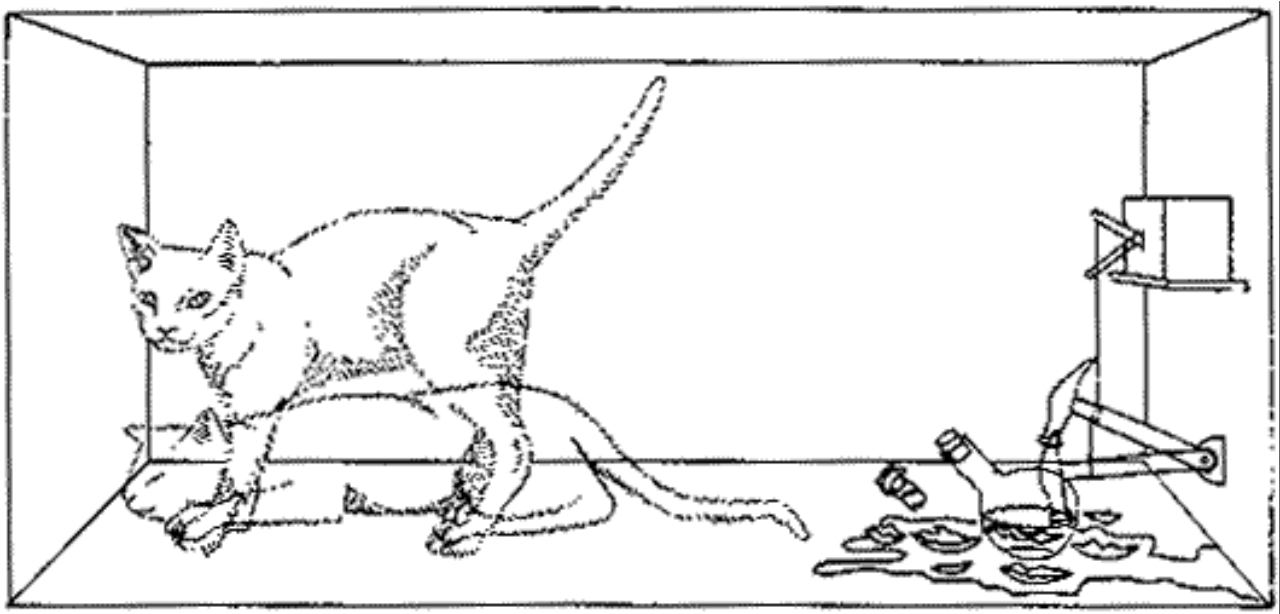
FIG. 3



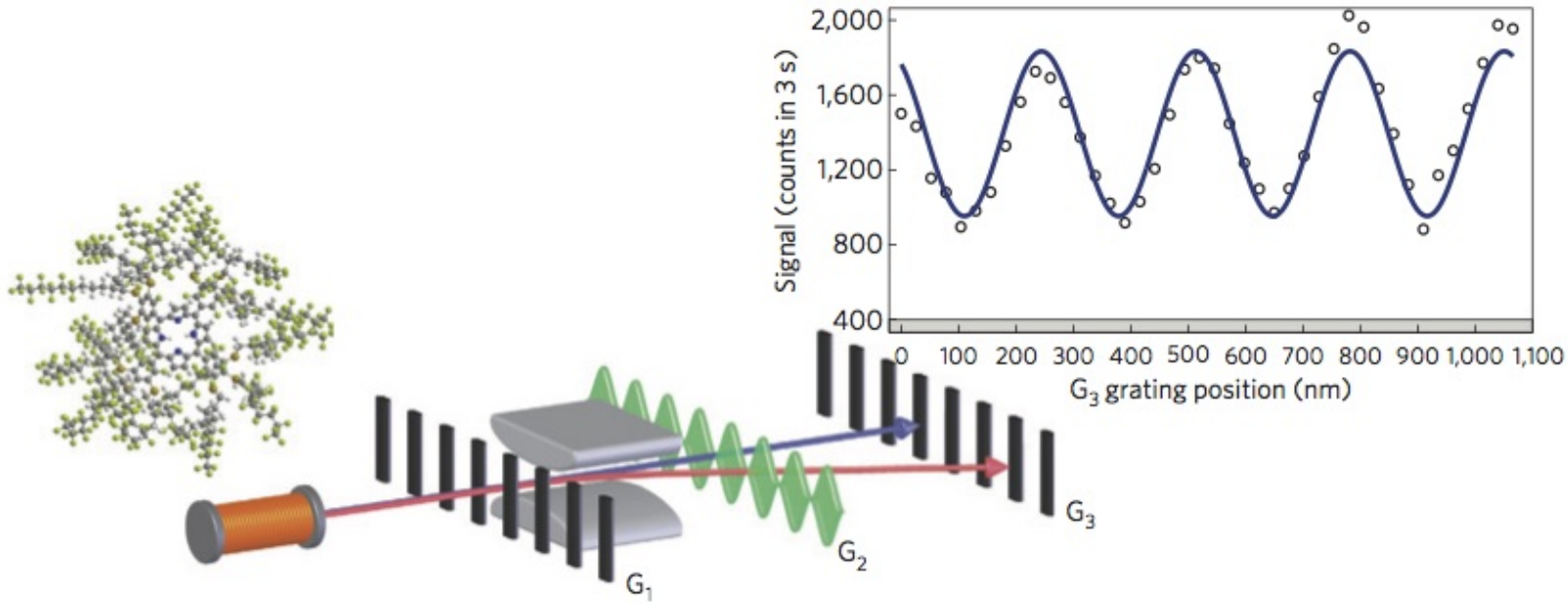
State superposition

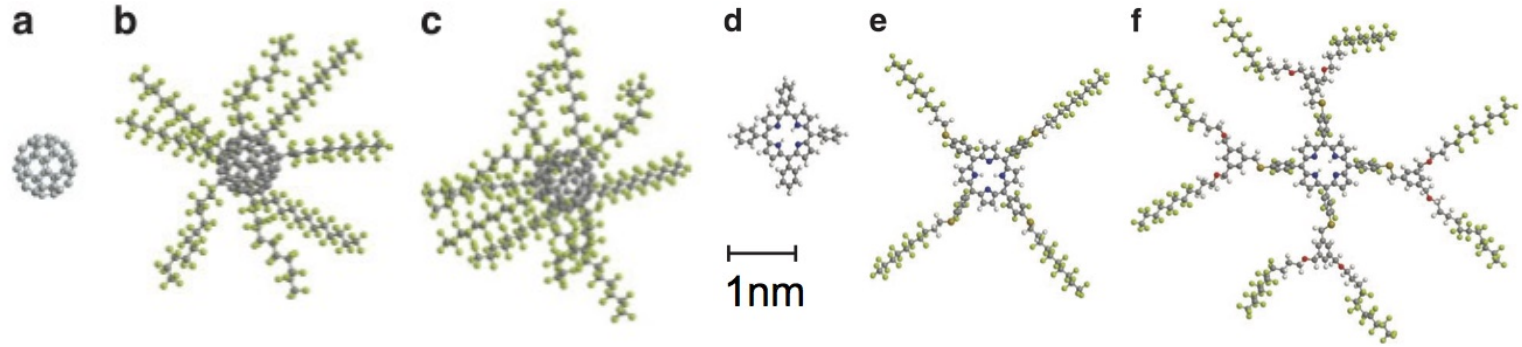
Example 3: Schrödinger cat

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\text{live}\rangle + |\text{dead}\rangle)$$



State superposition



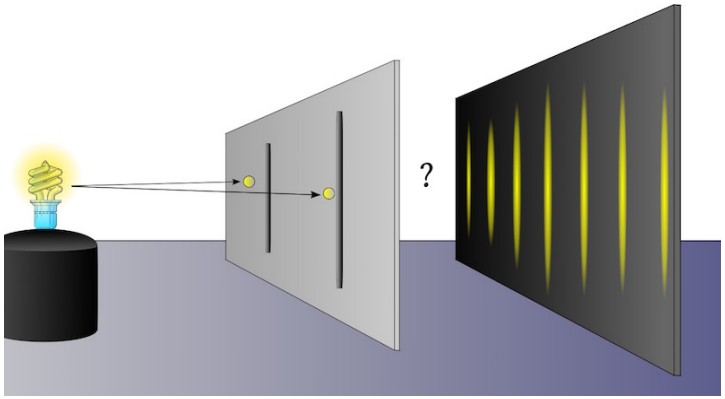


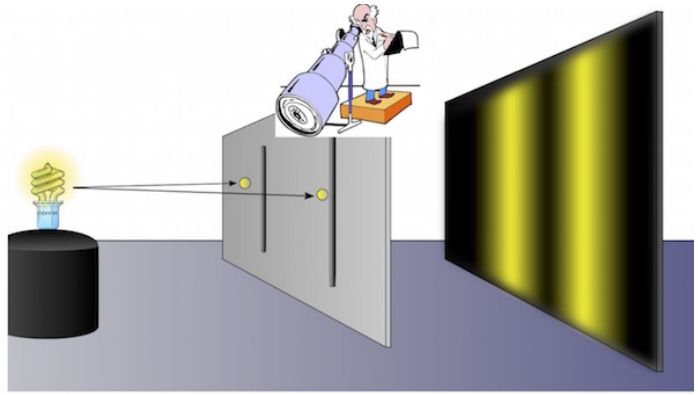
up to 6910 AMU, 430 atoms

Quantum interference of large organic molecules, **Nature Communication 2, 263 (2011)**

Measurement and no-cloning

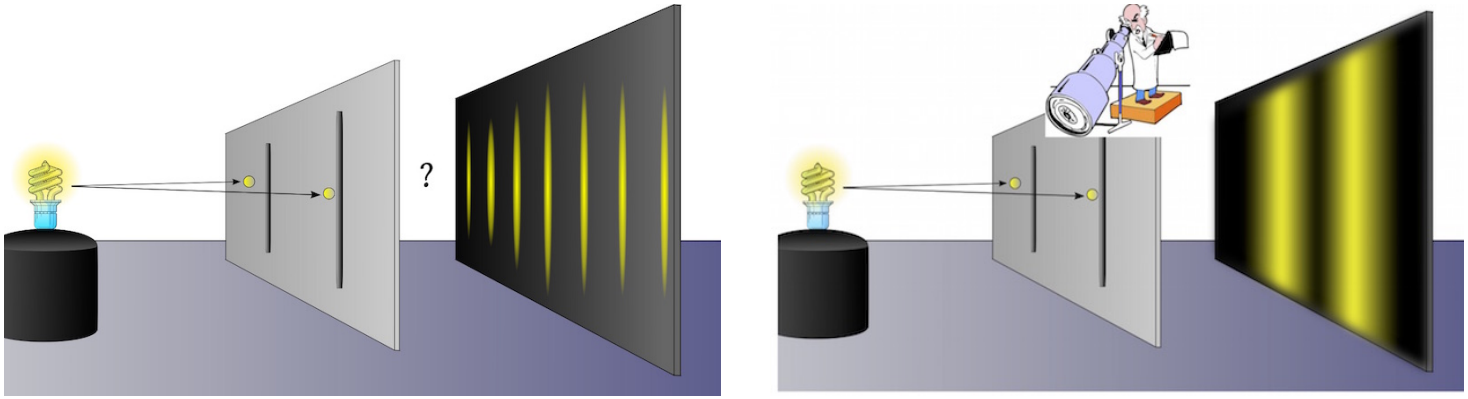
- The measurement (in general) perturbs quantum states





Measurement and no-cloning

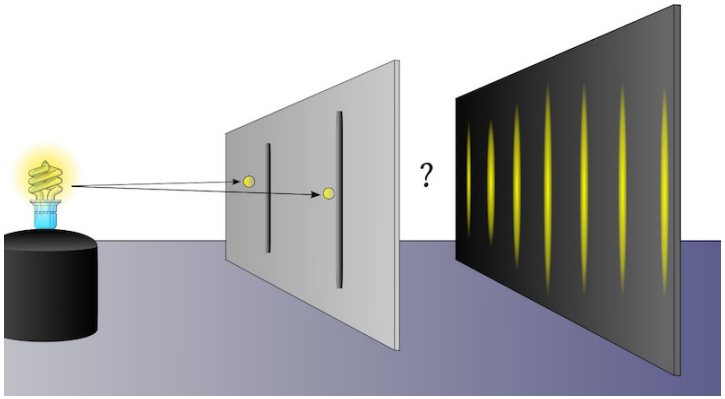
- The measurement (in general) perturbs quantum states

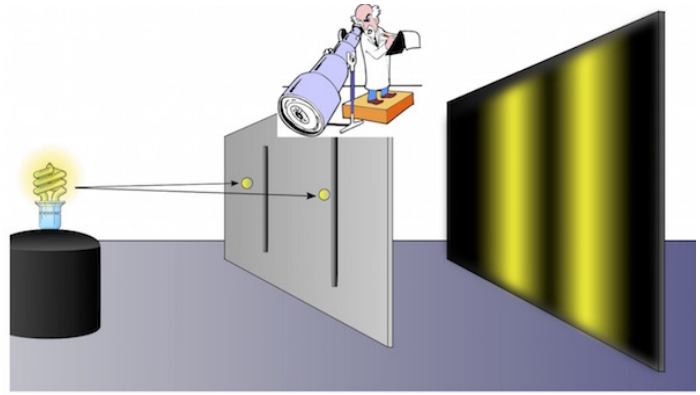


- The output of a measurement is probabilistic (if the state is not an eigenstate of the observable)

Measurement and no-cloning

- The measurement (in general) perturbs quantum states





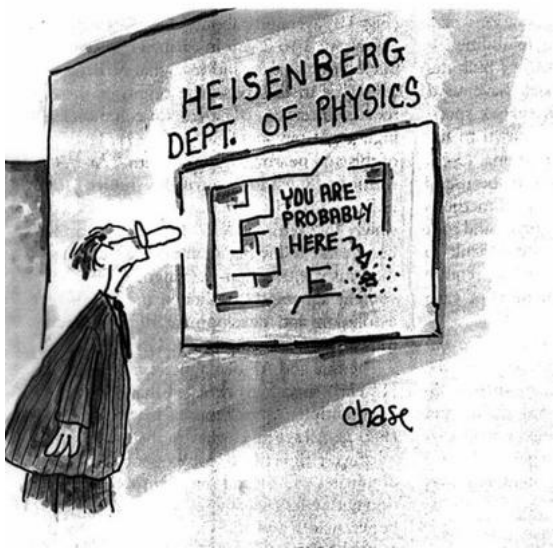
- The output of a measurement is probabilistic (if the state is not an eigenstate of the observable)
- Impossibility of perfect cloning: quantum copy-machine is not physical

$$\nexists \mathcal{U} \mid \mathcal{U}|\psi\rangle_A \rightarrow |\psi\rangle_A|\psi\rangle_B \qquad \forall|\psi\rangle$$

Uncertainty principle

- Bound on the precision of non-commuting observables: Heisenberg uncertainty principle

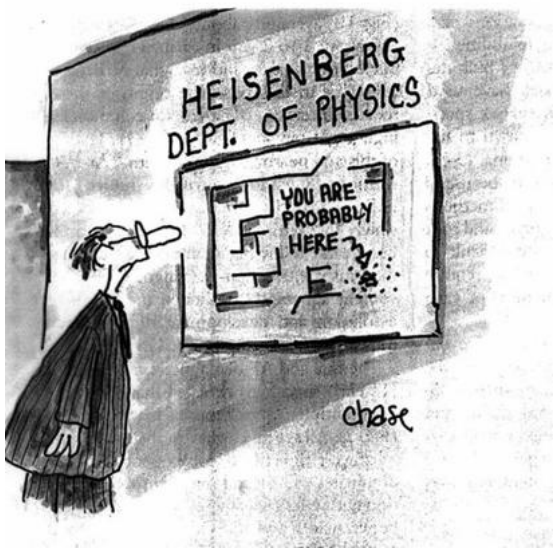
$$\Delta x \Delta p \geq \frac{\hbar}{2}$$



Uncertainty principle

- Bound on the precision of non-commuting observables: Heisenberg uncertainty principle

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

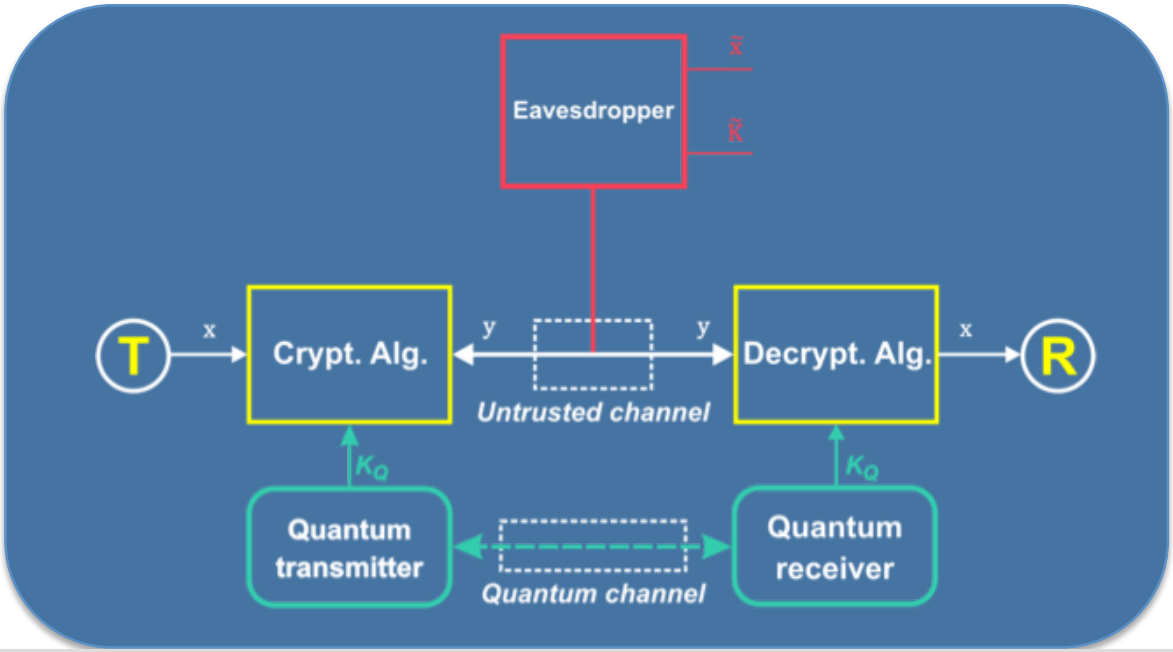


- The lower is the uncertainty on the position, the larger is the uncertainty on the momentum (and viceversa)

Summary

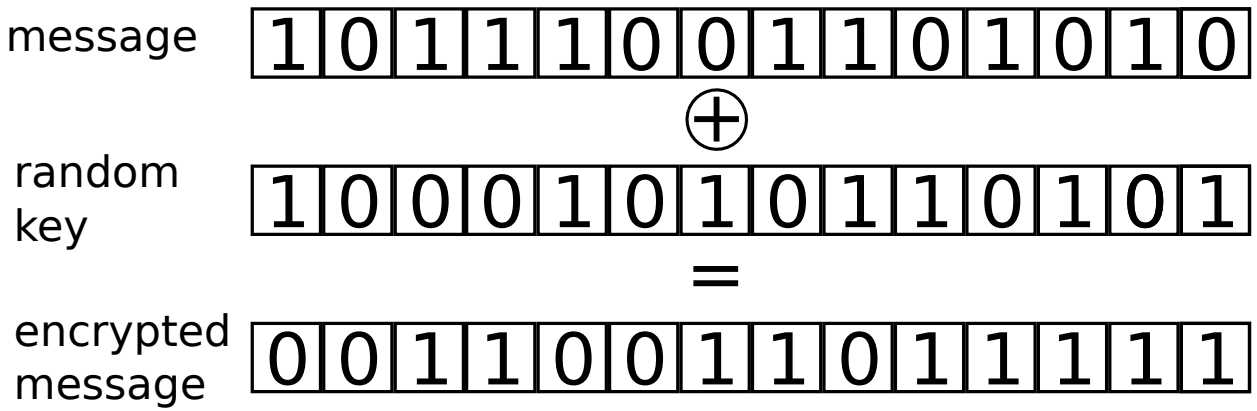
QKD: quantum key distribution

- A novel approach towards unconditionally secure communications
- Exploit quantum mechanics laws for establishing secure keys
- Single photon transmission for create keys and classical channel for send encrypted message



QKD principles

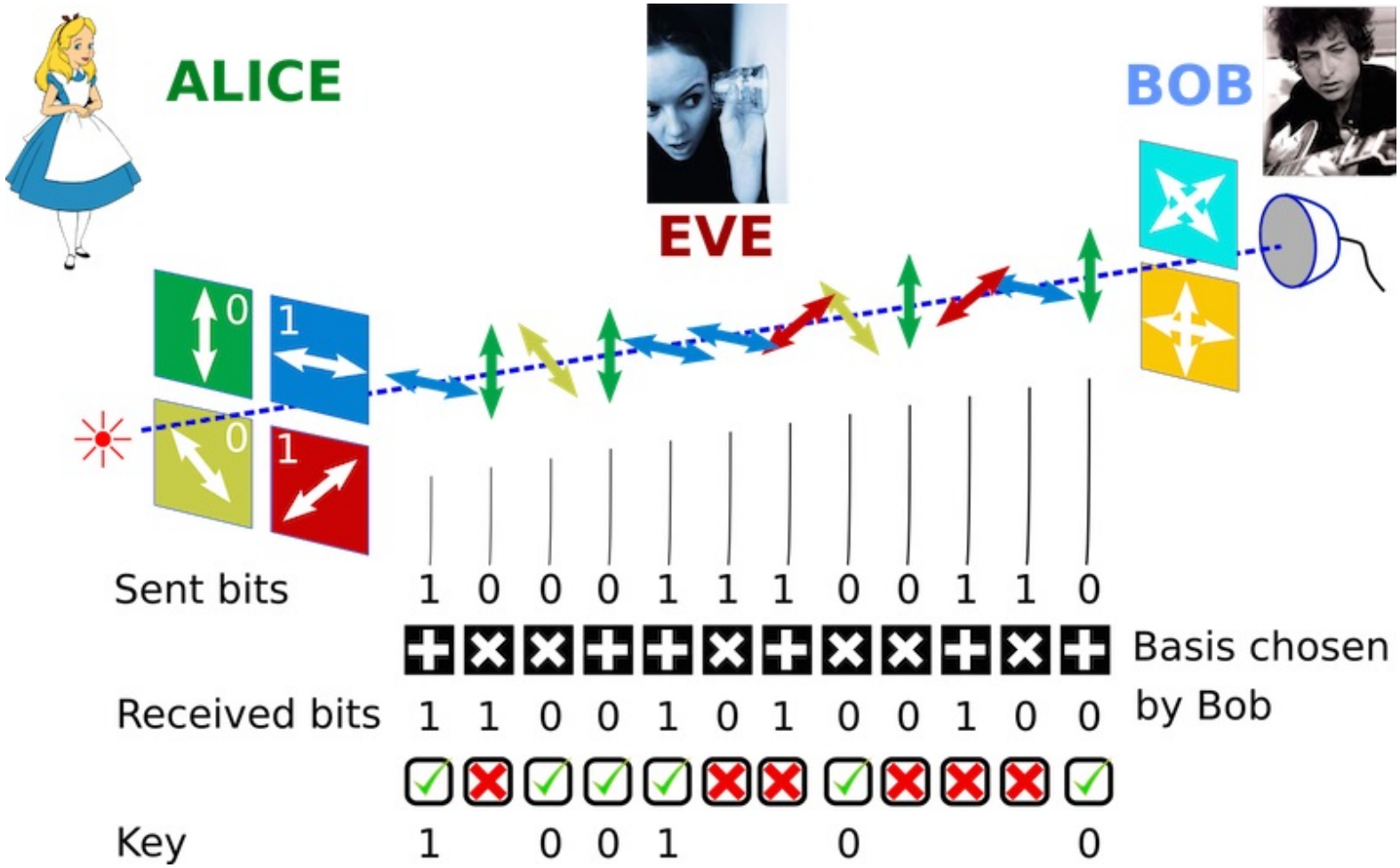
The best method to encrypt a message is the One-Time-Pad (OTP) protocol: for a n-bit message, a n-bit secure key is needed



Quantum key distribution (QKD) allows two users to exchange random and secret keys

QKD in a nutshell

BB84 protocol



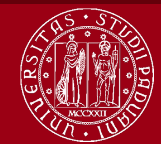
Secret key rate

Basic tools:

- two non-commuting basis
- no-cloning theorem
- any measurement (generally) perturbs the systems

$\Rightarrow$ Eve detection!

Secret key rate



Basic tools:

- two non-commuting basis
- no-cloning theorem
- any measurement (generally) perturbs the systems

$\Rightarrow$ Eve detection!

Secret key rate:

$$r = 1 - 2h_2(Q)$$

with

$$Q = \mathrm{QBER} \qquad h_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$$

Secret key rate

Basic tools:

- two non-commuting basis
- no-cloning theorem
- any measurement (generally) perturbs the systems

$\Rightarrow$ Eve detection!

Secret key rate:

$$r = 1 - 2h_2(Q)$$

with

$$Q = \mathrm{QBER} \qquad h_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$$

If Eve is gaining information on the key, the key is discarded.
Eve has no information on the secret message

Commercial QKD

First commercial example of security protocol based on Quantum Mechanics

ID Quantique (CH)

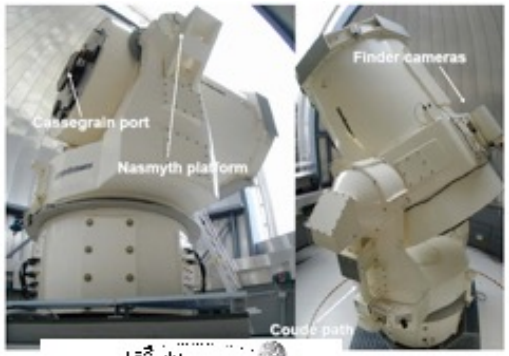
MagiQ (US)

Quintessence (AU)

SeQurenet (FR)

Toshiba (UK)

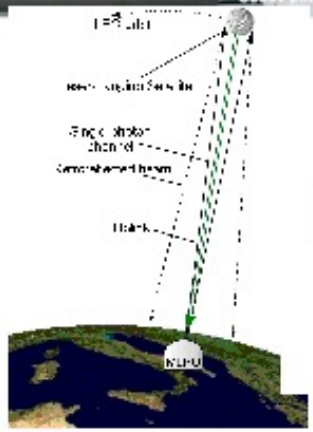
Timeline of quantum communications in space

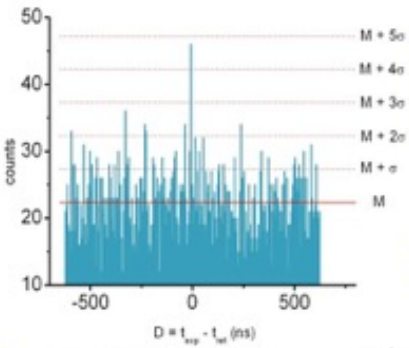


Space Qcomms timeline

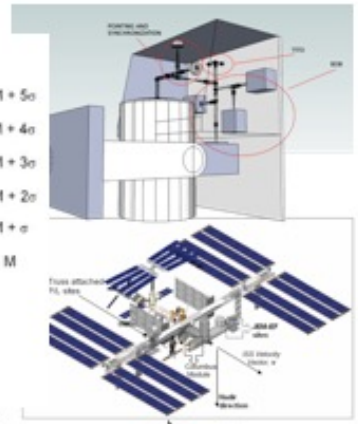
We operated at **Matera Laser Ranging Observatory**, owned by the **Italian Space Agency** and directed by Dr. Giuseppe "Pippo" Bianco.

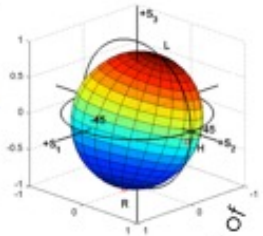
With its **1.5 m telescope an millimeter resolution in SLR**, Matera is our research hub for Space Quantum Communications since 2003.

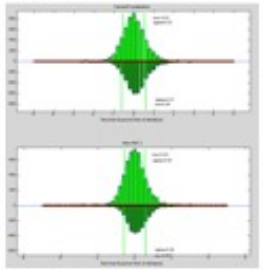




P. Villoresi et al.
New J. Phys.
10 033038 (2008)







2003 – UniPD SpaceQ project

2008 – first single-photon return from Ajisai announced

2009 - Feasibility study for a quantum payload for the ISS

2012 - Analysis of response for different satellites CCR

2014 – Q-Comm on satellites downlink demonstrated

st MLRO tests

Optical front-end, high rep rate laser installed and single photon eiver @ MLRO

Setup for the returns search

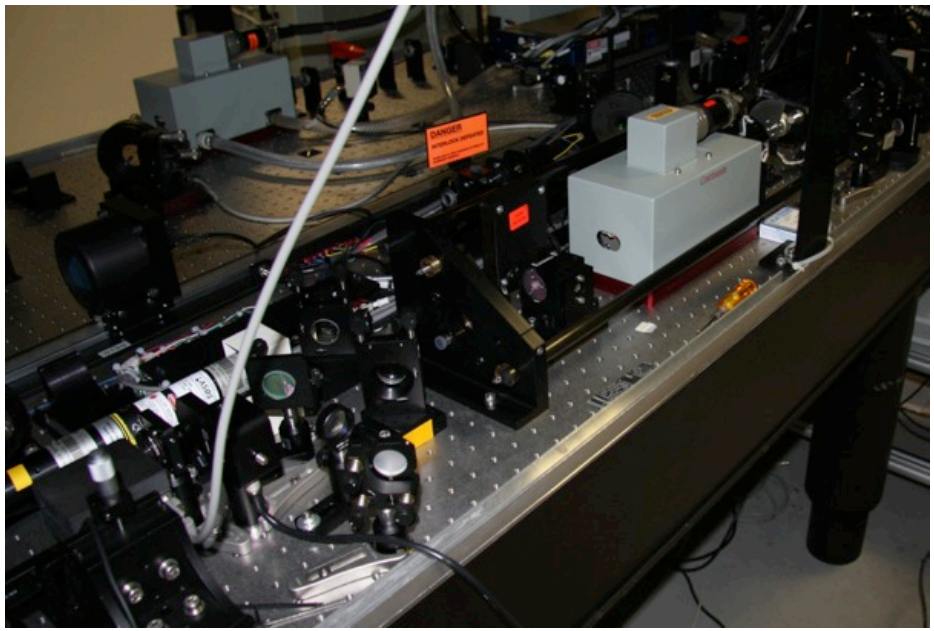
Design and test of setup for polarization analysis

Characterization of MLRO Mueller Matrix

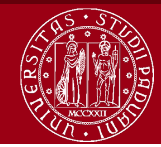
2013 – state reparation, state nalysis – satellite ynchronization

MLRO as quantum hub

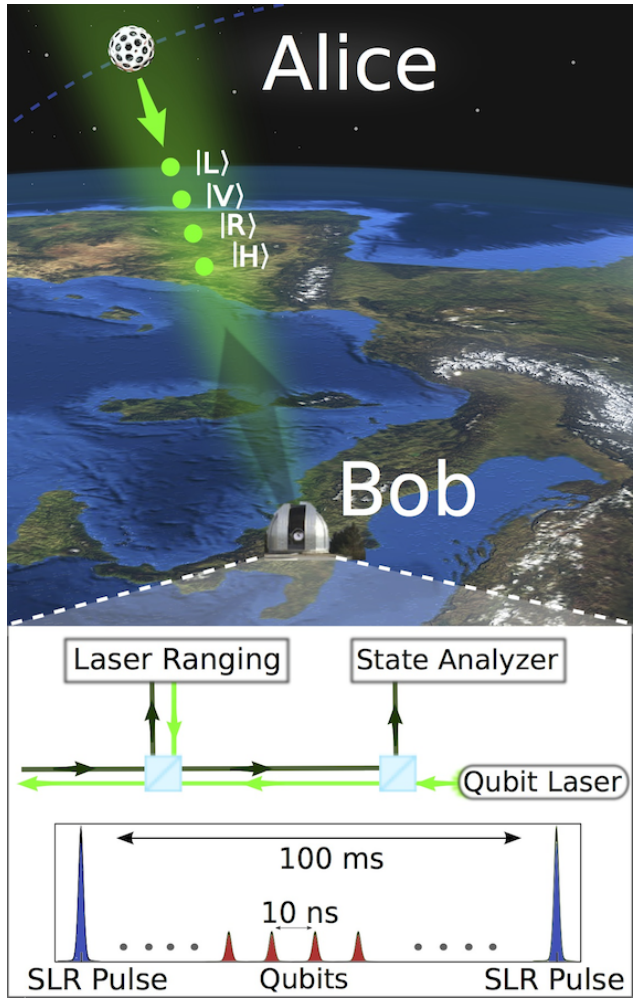
MLRO: research hub for Space QC since 2003



Summary



Objectives of the recent q-comm experiment

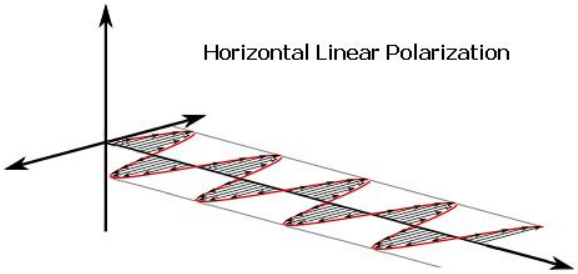


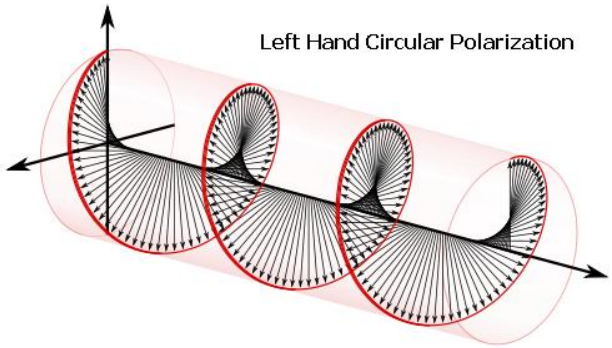
- To simulate a qubit source in Space using orbiting retroreflectors
- To demonstrate the measurement of quantum states in the downlink
- To address the mitigation of the background noise
- To demonstrate quantum communication of a generic qubits from Space to ground

Qubit encoding

Polarization encoding

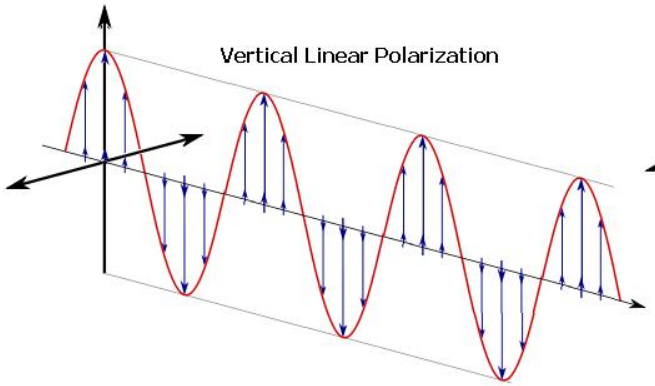
$|0\rangle$

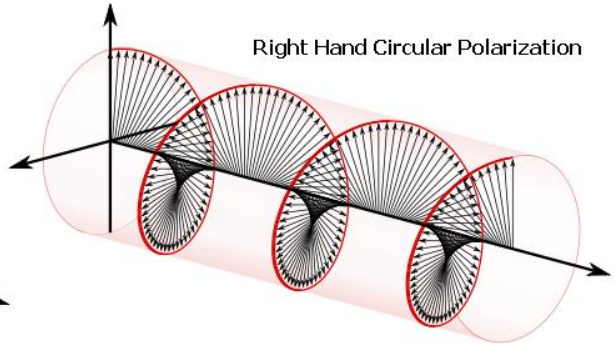




$|0\rangle - i|1\rangle$

$|1\rangle$



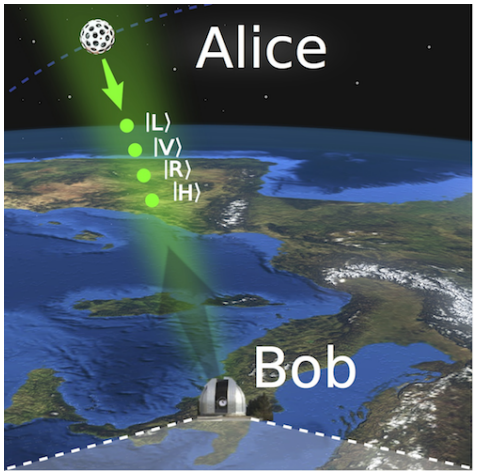


$|0\rangle + i|1\rangle$

The making of the qubits

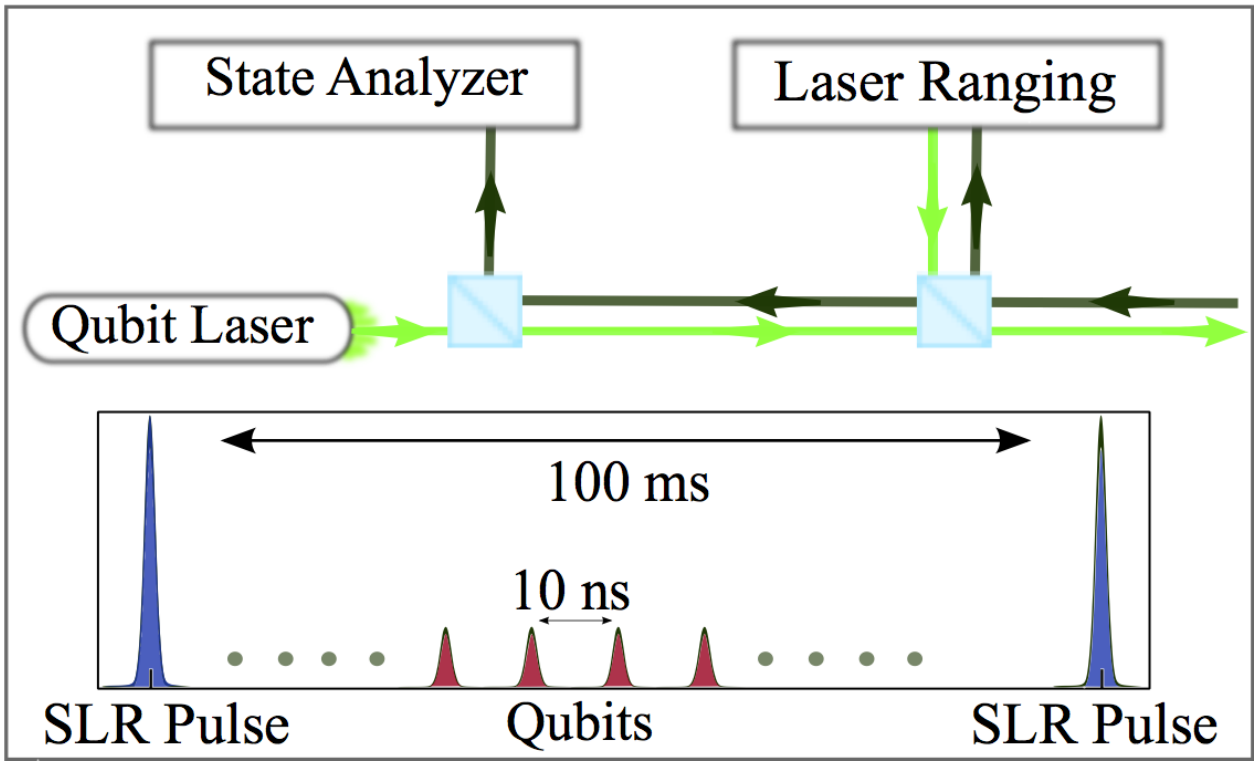
- Source on satellite simulated by a CCR
- Source (Alice) need to be at the single photon level
- Downlink attenuation from $\sim 3\ cm$ LEO sources in the range of 55-70 dB.
- Short pulses necessary for background rejection
- Not too short to prevent bandwidth opening and noise increasing

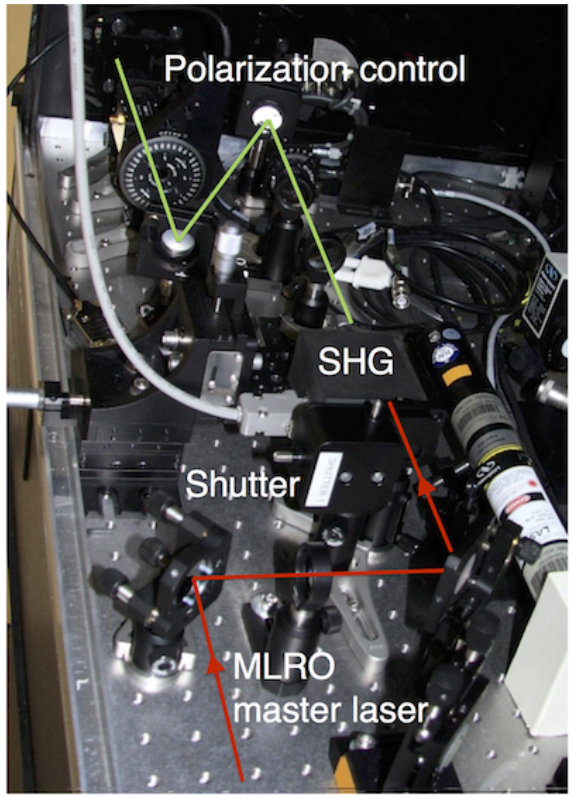
CCR:
Corner-Cube
Retroreflector



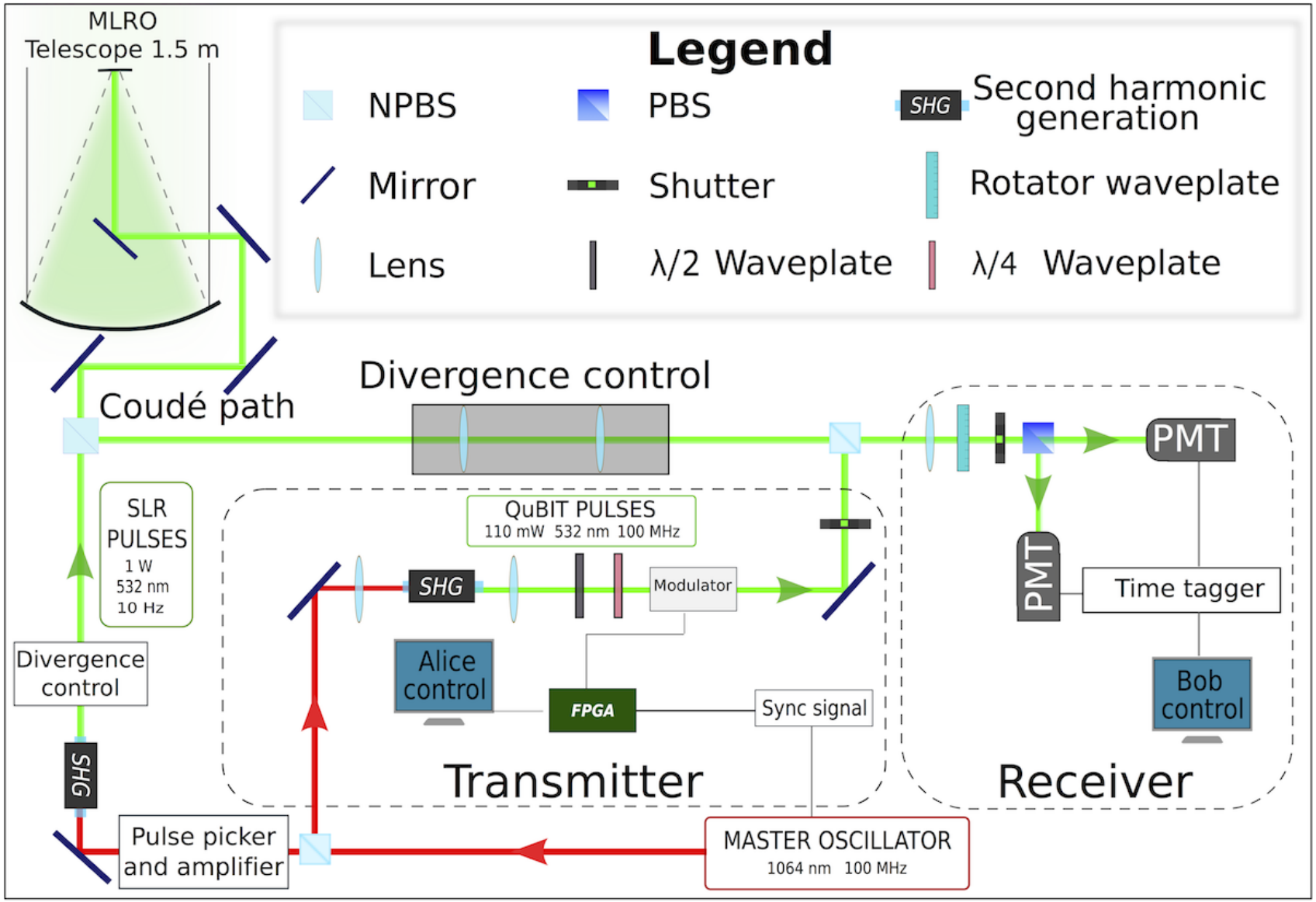
The making of the qubits

MLRO master laser provided the solution: 100 MHz, 100 ps, 300 mW, 1064 nm

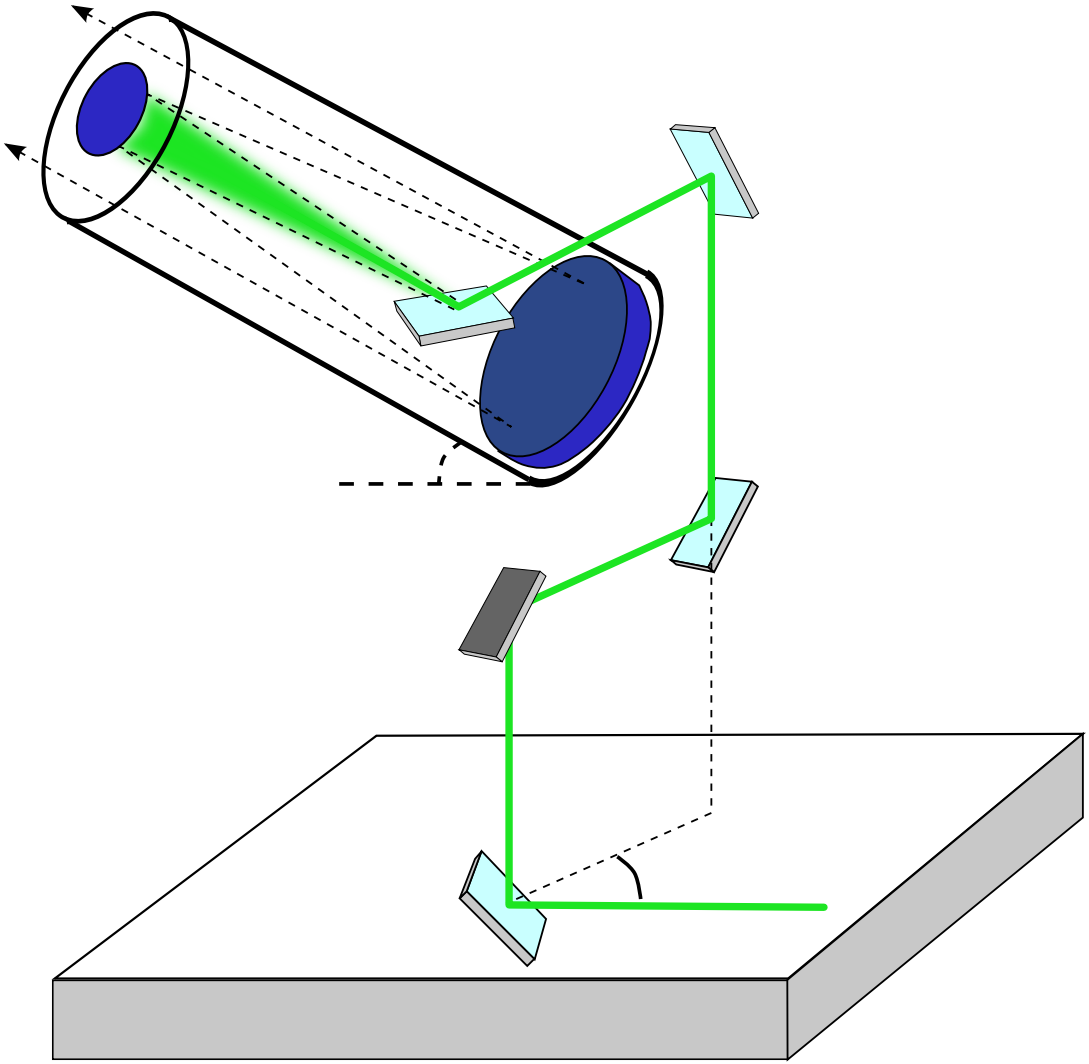




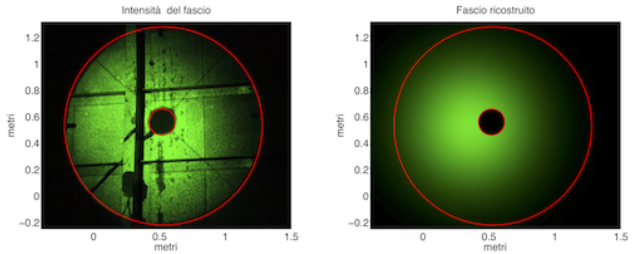
Setup


MLRO
Telescope 1.5 m
Legend
NPBS
PBS
SHG
Second harmonic generation
Mirror
Shutter
Rotator waveplate
Lens
λ/2 Waveplate
λ/4 Waveplate
Coudé path
Divergence control
PMT
SLR PULSES
1 W
532 nm
10 Hz
QuBIT PULSES
110 mW 532 nm 100 MHz
SHG
Modulator
PMT
Time tagger
Divergence control
Alice control
FPGA
Sync signal
Bob control
SHG
Transmitter
Receiver
Pulse picker and amplifier
MASTER OSCILLATOR
1064 nm 100 MHz

Coudé path of in-and-out

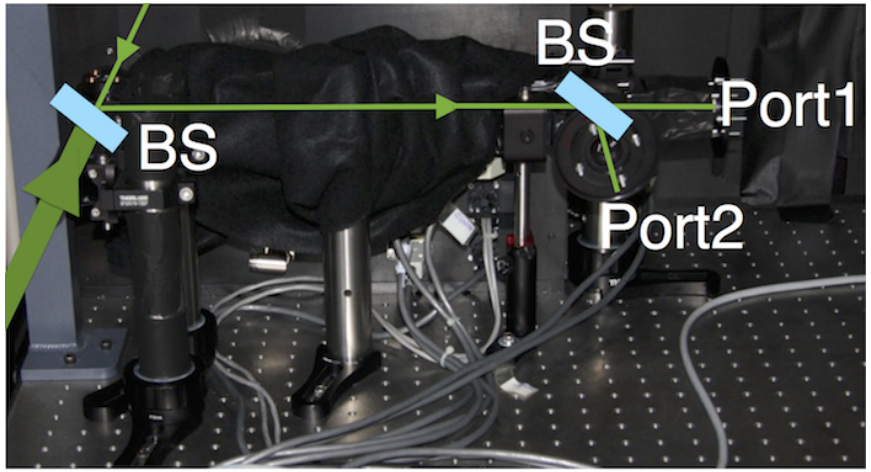


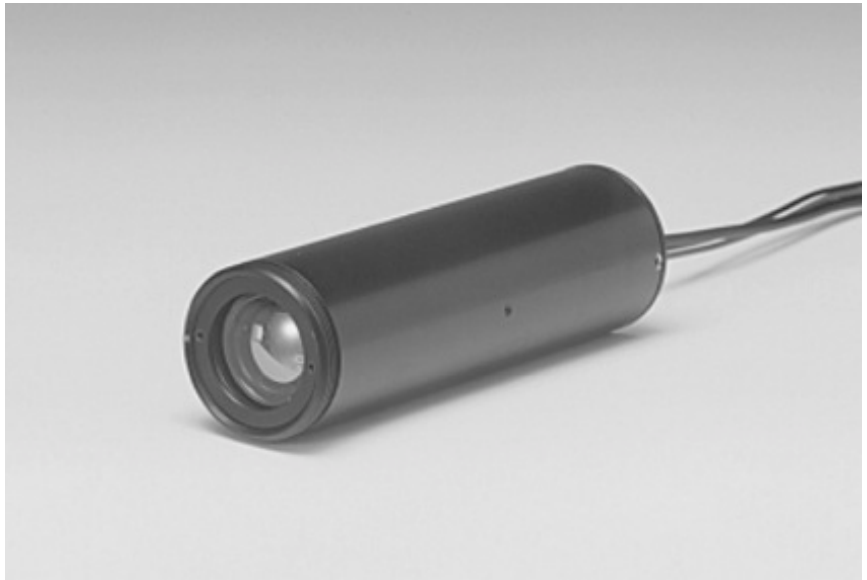
- Characterization of the polarization transformation
- Assessment of total transmission efficiency
- Mutual alignement of SLR and Qubit beams



Measuring the qubits

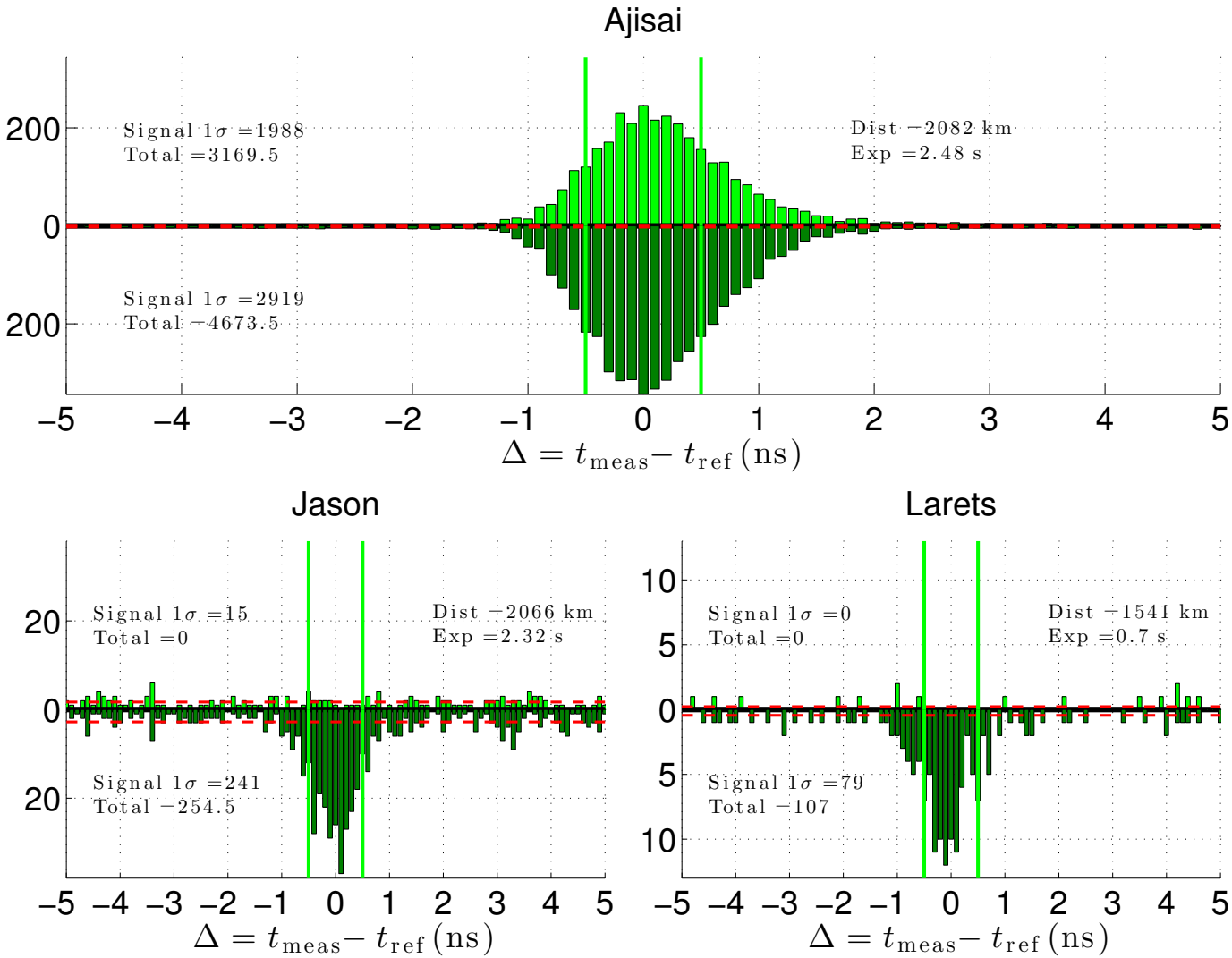
- The Coudé path is used in both directions for both the SLR beam and the qubits
- The upward and inward beams are combined using a non polarizing beam splitter (BS)
- Two large ares SPADs mounted to the exit ports, designed to address the velocity-aberration
- 81 ps timetagging of 8 channels





Single photon returns

Histogram of the counts

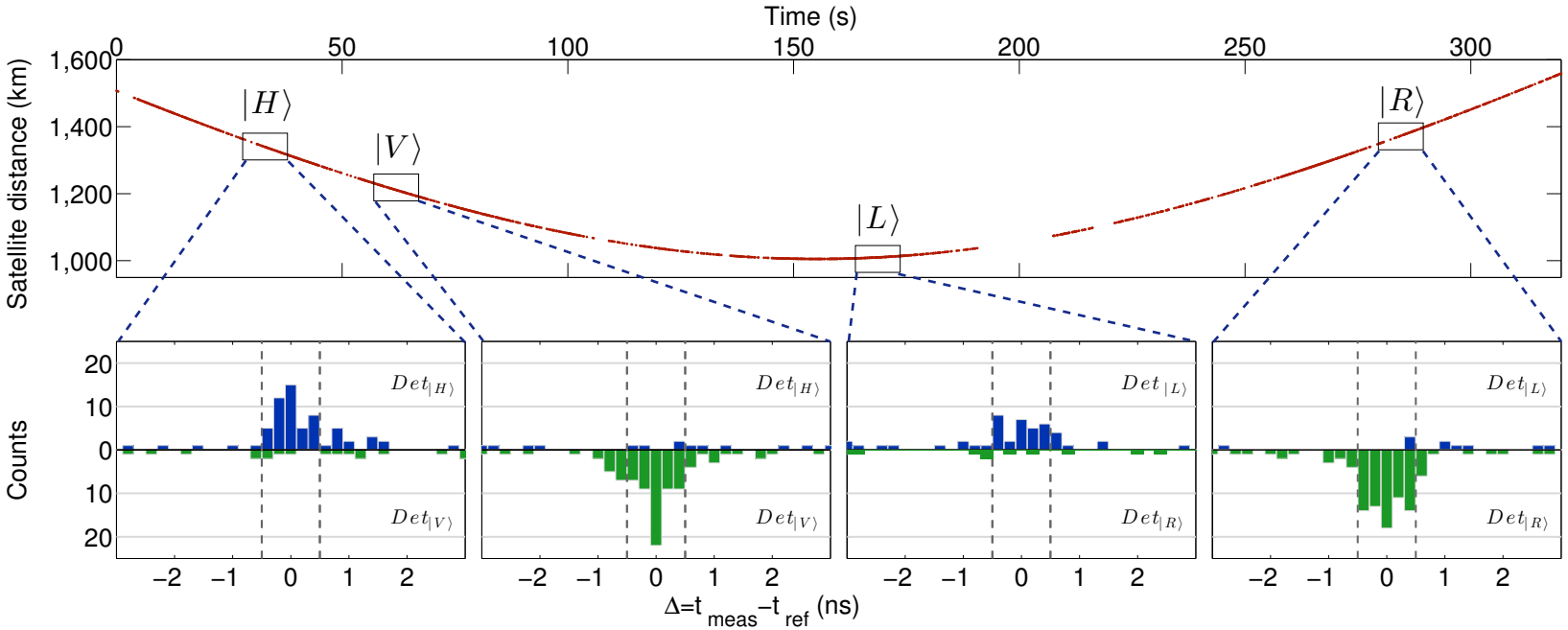


Single passage of LARETS

Orbit height 690 km - spherical brass body
24 cm in diameter, 23 kg mass,

60 Metallic coated Corner-Cube Retroreflectors

Apr 10th, 2014, start 4:40 am CEST



Detection of four polarization states received from satellite
10 s windows

QBER: Quantum Bit Error Rate

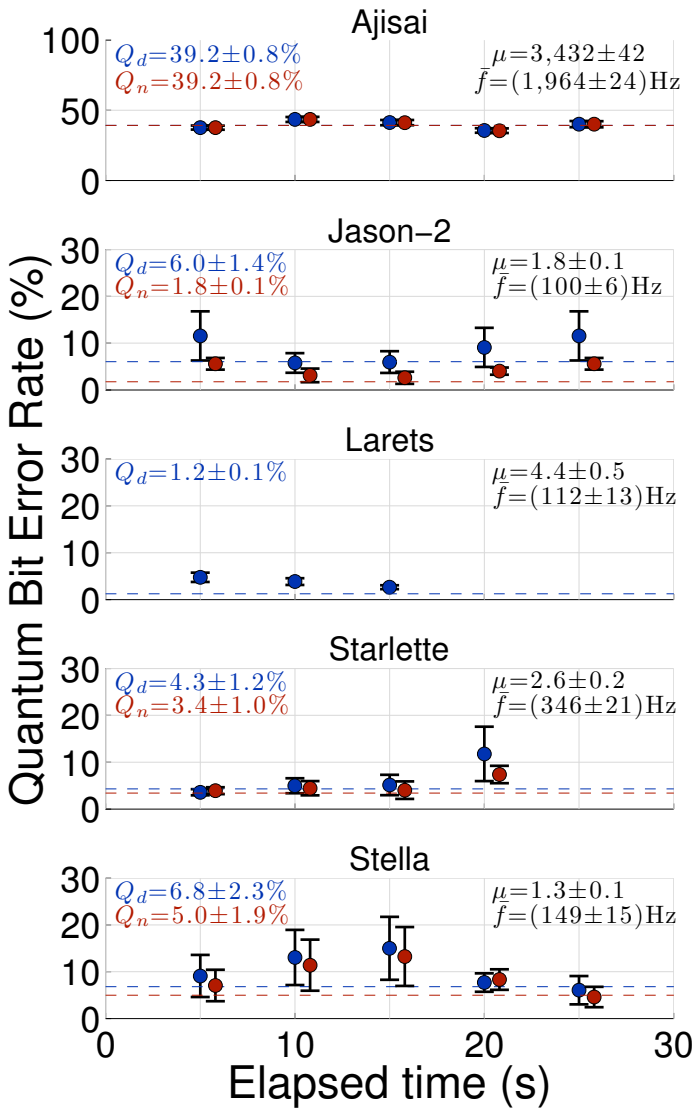
Ajisai

Non polarization maintaining CCR:
Polarization Q-Comm not possible

Jason-2, Larets, Starlette, Stella

Polarization maintaining CCR:

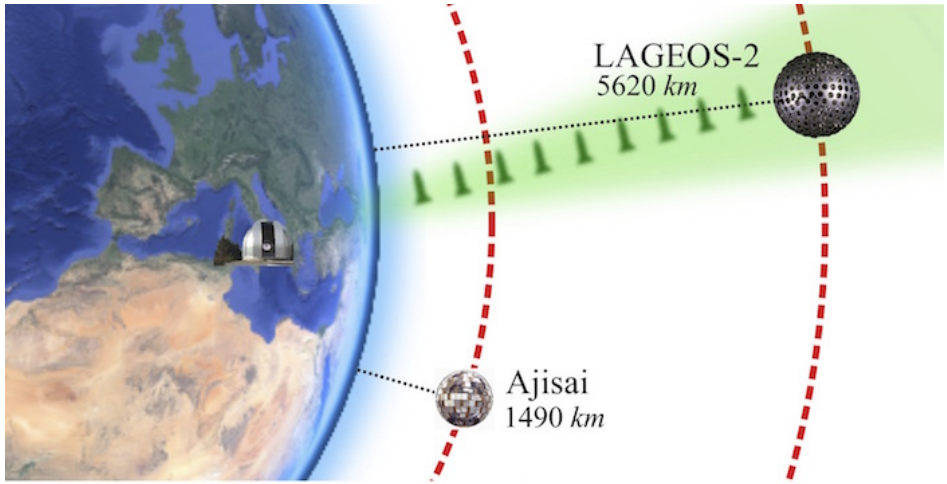
- QBER compatible with applications
- Demonstration of stable QBER over extended link duration



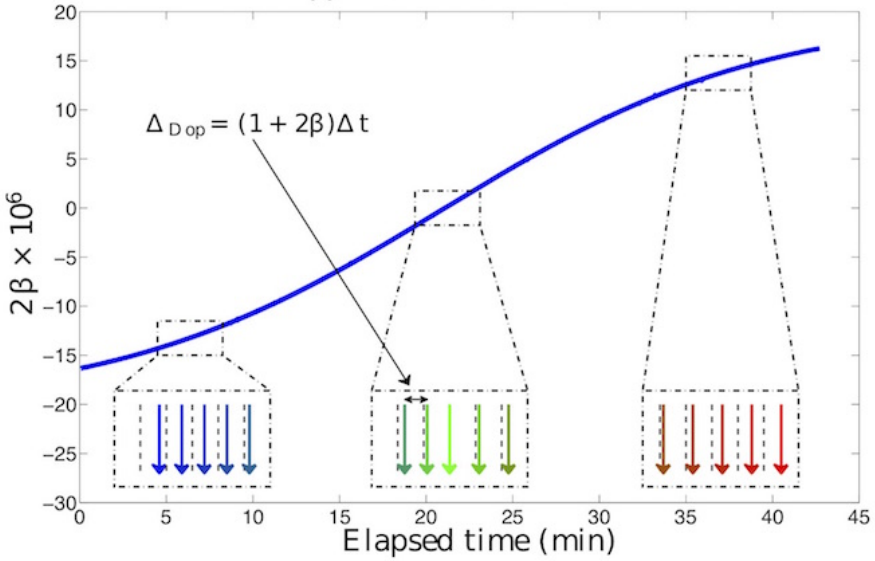
Summary

Extending QC to MEO satellites

MEO=Medium-Earth-Orbit

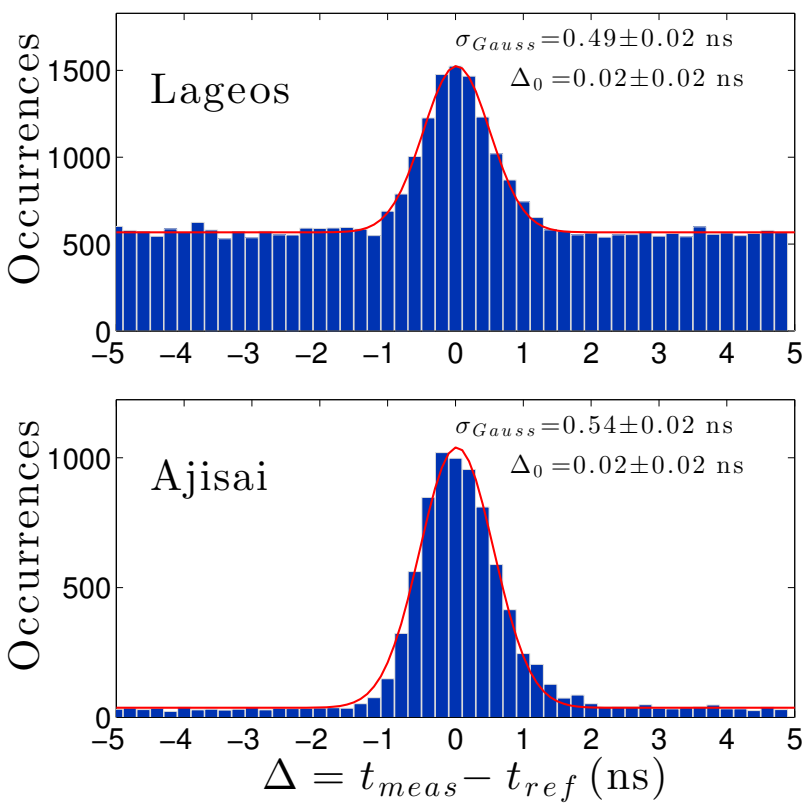


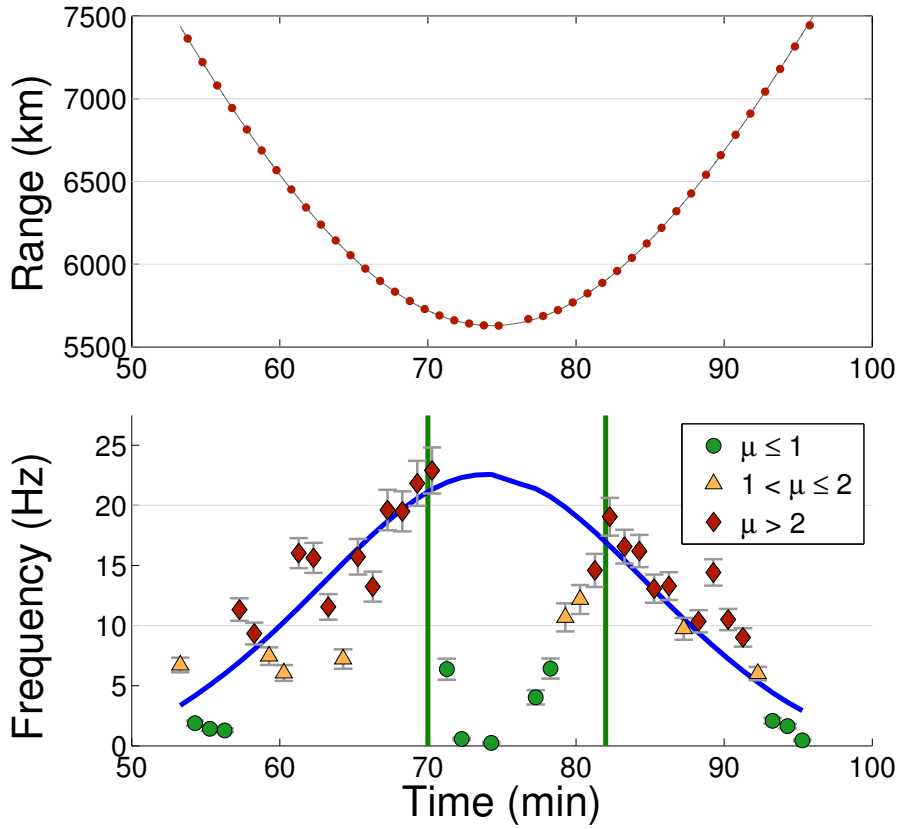
Doppler effect for LAGEOS–2



Single photon returns

Histogram of the counts

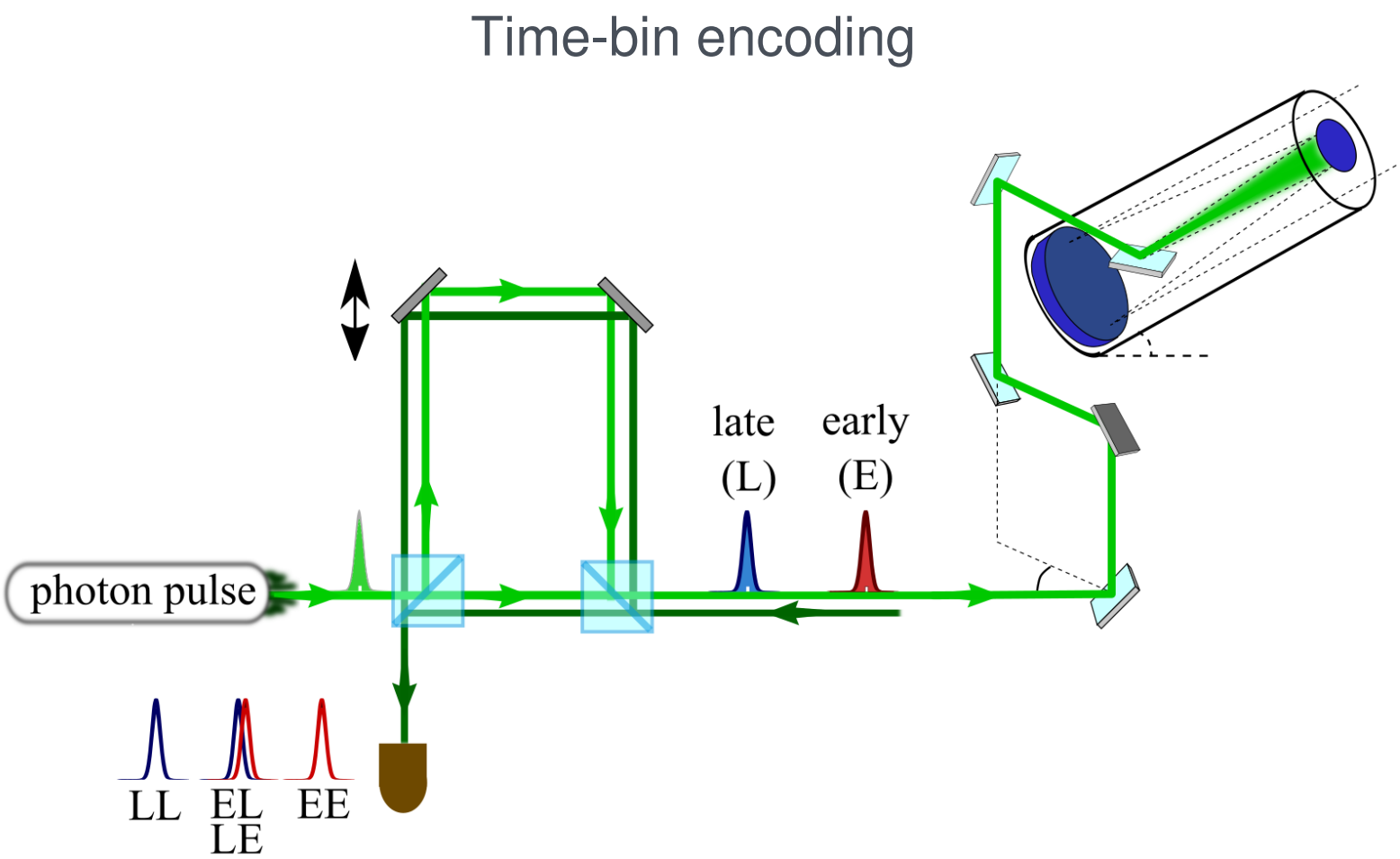




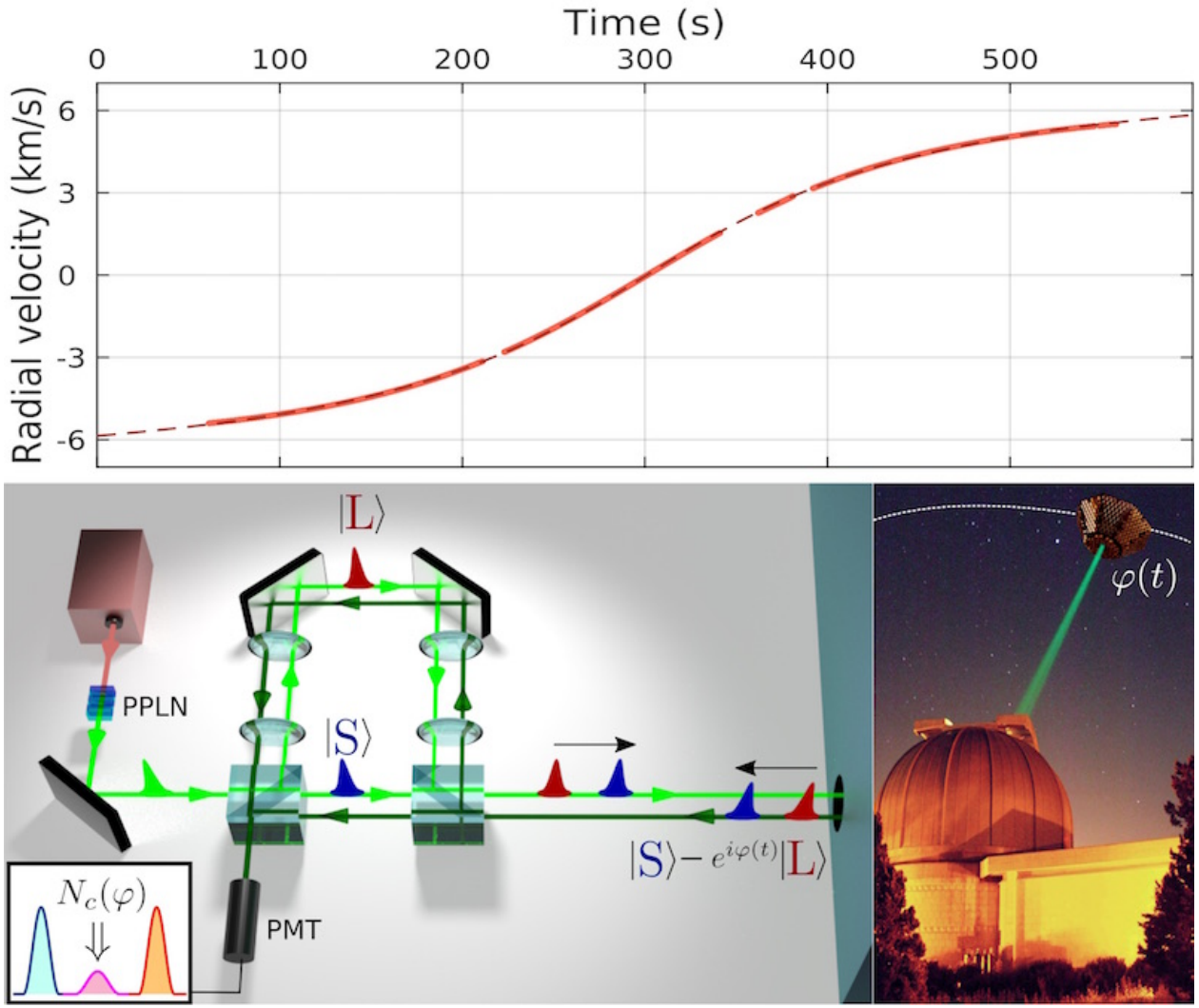
7000km link

Summary

Qubit with time-bin

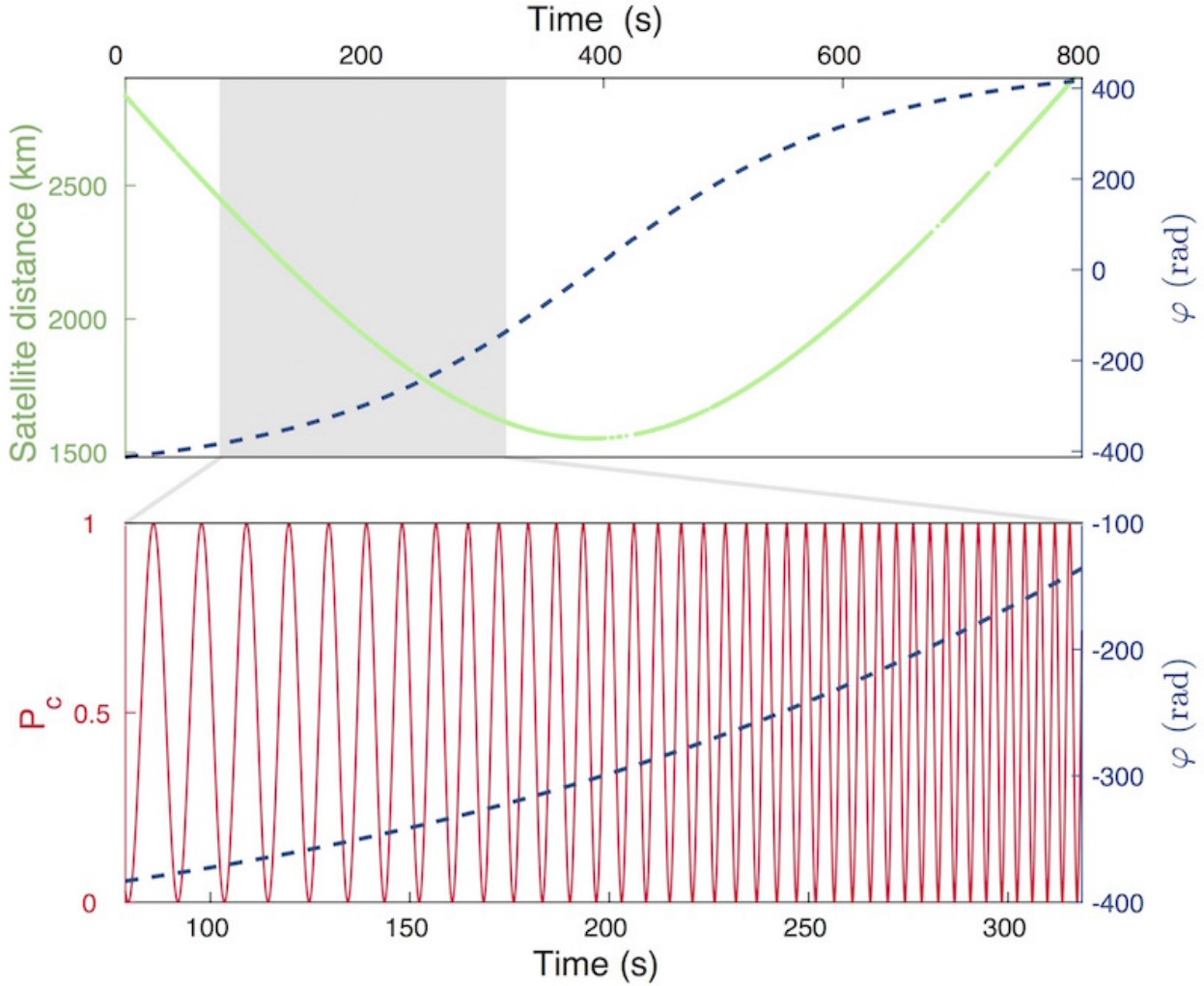


Time-bin setup



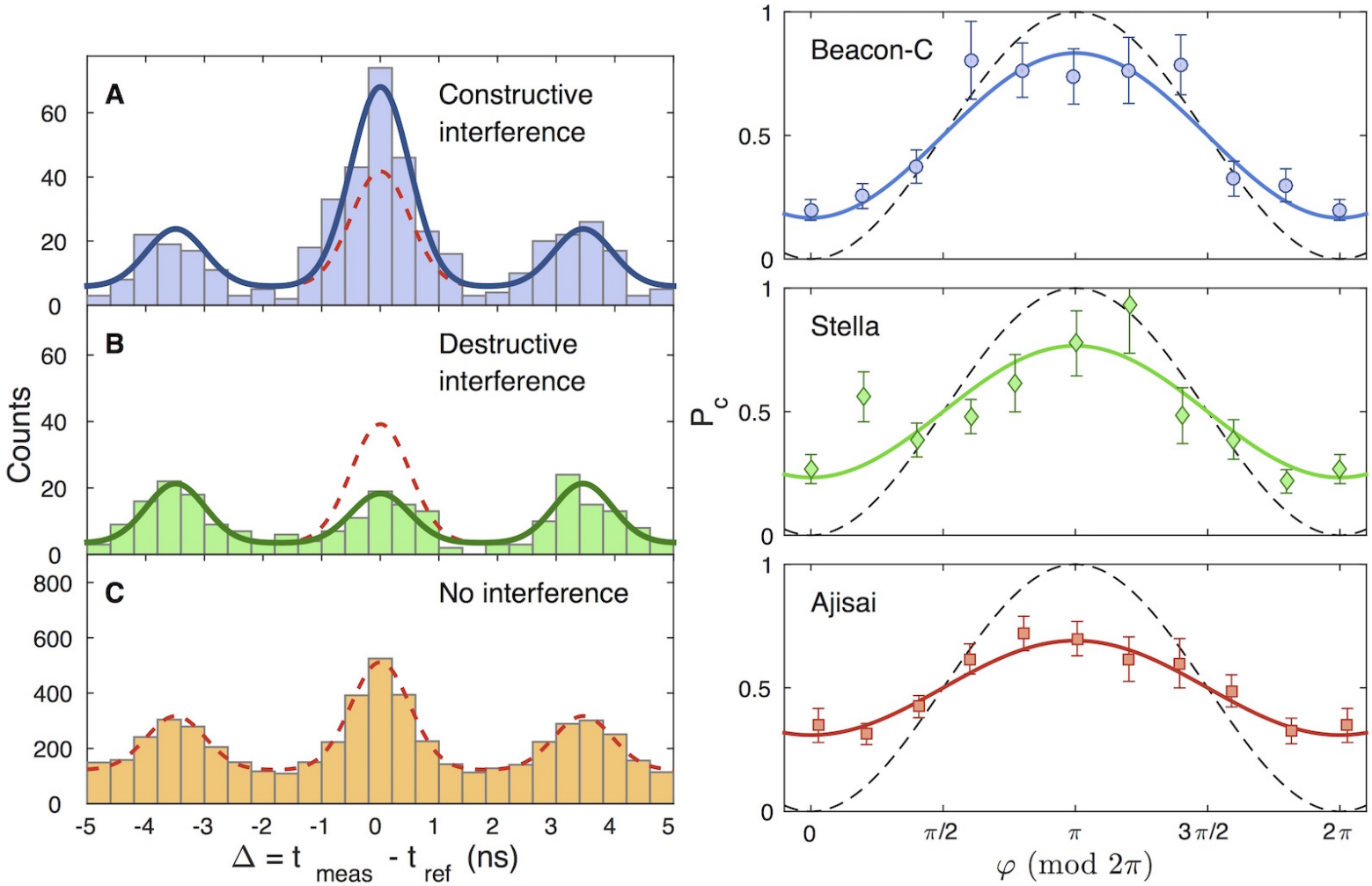
Dynamical phase

Phase changes during the satellite passage

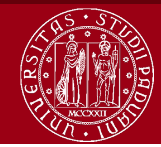


Quantum interference

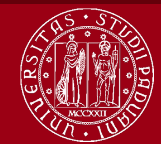
Interference pattern



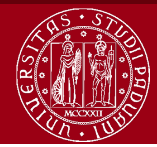
Summary



Summary



Free-space QKD with different degrees of freedom



- Polarization is maintained in propagation.
- Can we exploit other degrees of freedom to encode the qubit?
- Can we **increase the information** sent for single photon by increasing the dimension of the Hilbert space?

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Free-space QKD with different degrees of freedom

- Polarization is maintained in propagation.
- Can we exploit other degrees of freedom to encode the qubit?
- Can we **increase the information** sent for single photon by increasing the dimension of the Hilbert space?

$$\Downarrow$$

Orbital Angular Momentum (OAM) of Light

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Orbital Angular Momentum of light

- Total angular momentum of light beam

$$\vec{J} = \epsilon_0 \int \vec{r} \times (\vec{E} \times \vec{B}) \mathrm{d}^3 \vec{r}$$

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Orbital Angular Momentum of light

- Total angular momentum of light beam

$$\vec{J} = \epsilon_0 \int \vec{r} \times (\vec{E} \times \vec{B}) \mathrm{d}^3 \vec{r}$$

- In paraxial approximation split into SPIN and Orbital Angular Momentum (OAM)

$$J_z = J_z^{\mathrm{spin}} + J_z^{\mathrm{OAM}}$$

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Orbital Angular Momentum of light

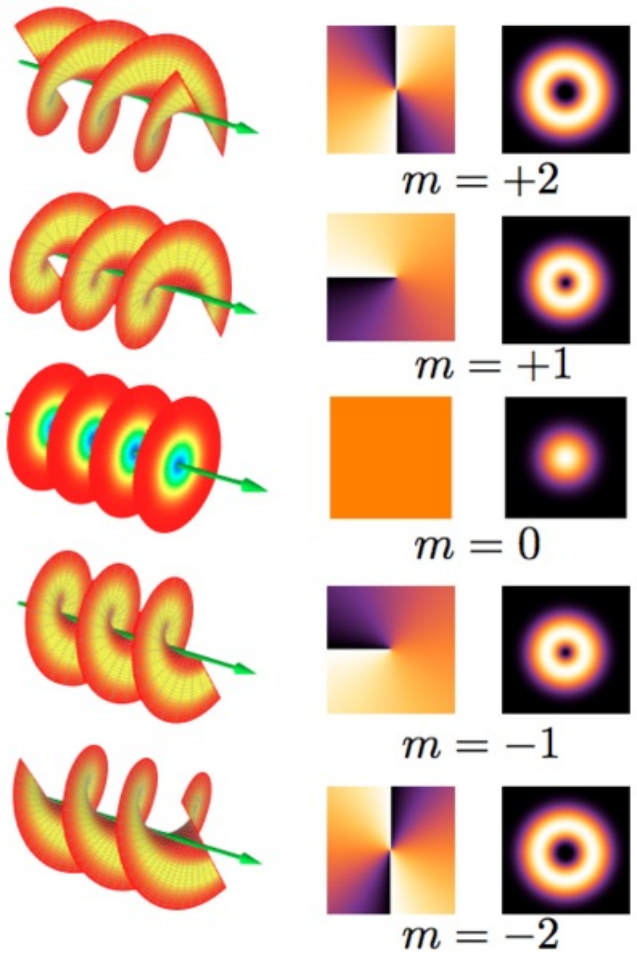
- Total angular momentum of light beam

$$\vec{J} = \epsilon_0 \int \vec{r} \times (\vec{E} \times \vec{B}) \mathrm{d}^3 \vec{r}$$

- In paraxial approximation split into SPIN and Orbital Angular Momentum (OAM)

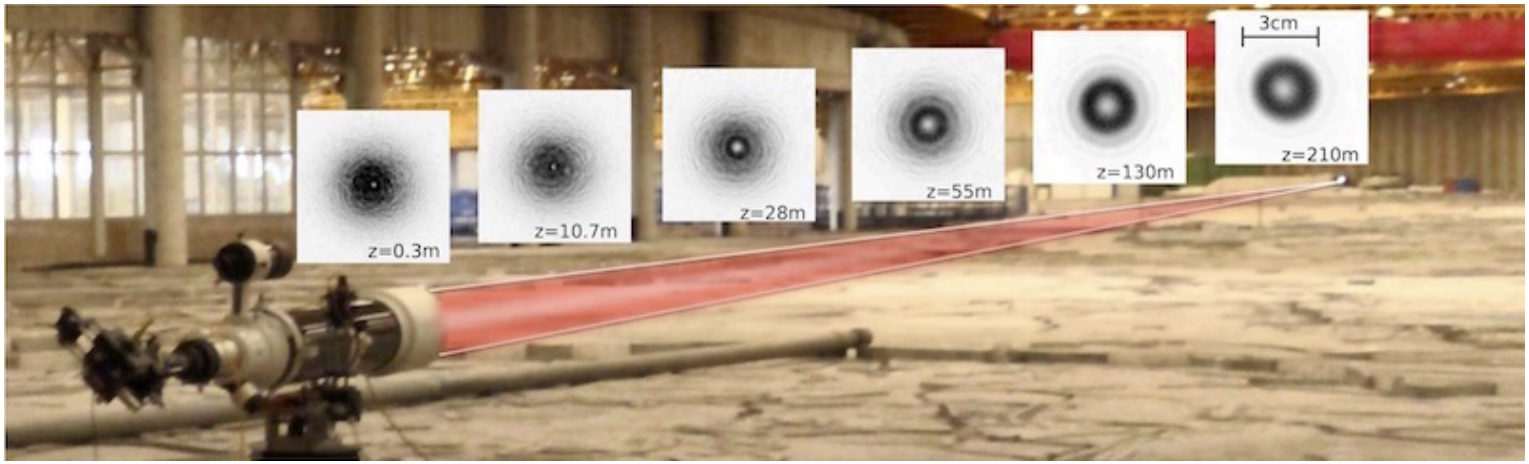
$$J_z = J_z^{\mathrm{spin}} + J_z^{\mathrm{OAM}}$$

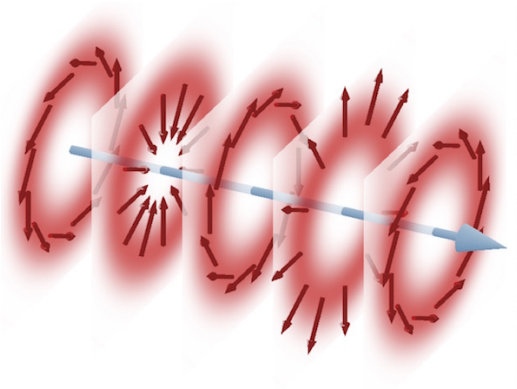
- OAM related to the phase $e^{im\phi}$ $(m \in \mathbb{Z})$ in the transverse plane. Each photon carries $m\hbar$ of angular momentum.



G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Aligment-free OAM QKD: 210m free space link



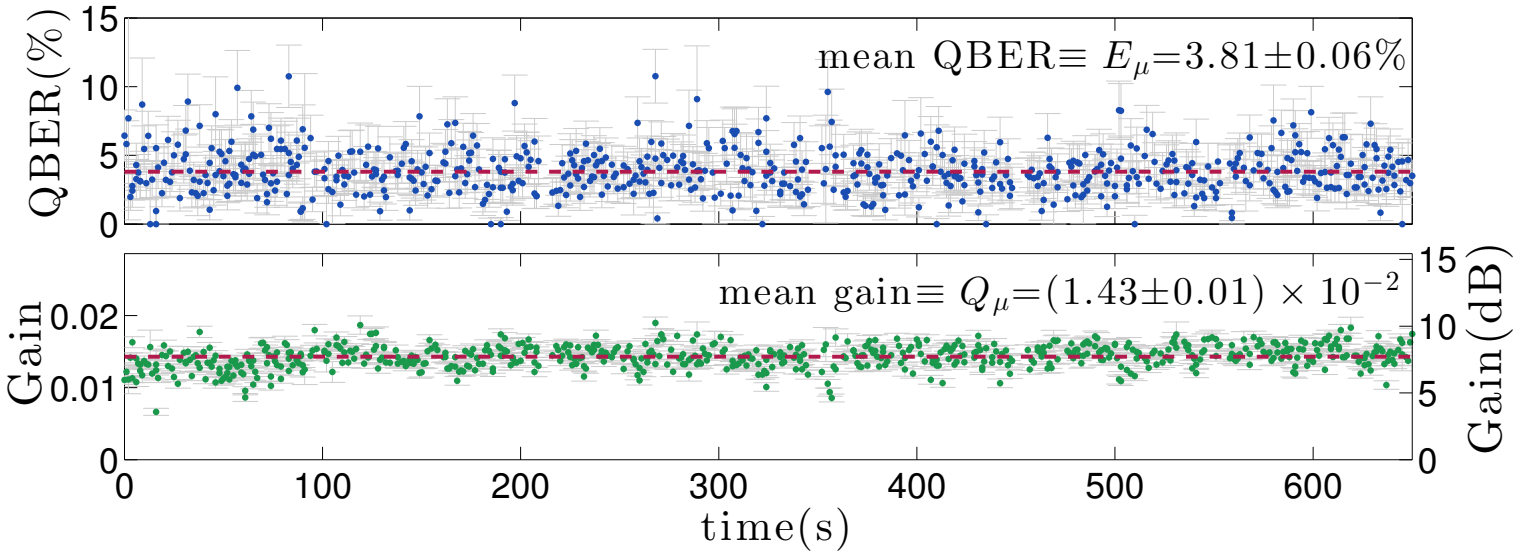


Hybrid qubit: $\alpha|L\rangle_\pi \otimes |r\rangle_O + \beta|R\rangle_\pi \otimes |l\rangle_O$

Rotaton-invariant states!

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

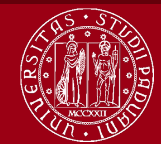
Gain and QBER



The data show 10 minutes of acquisition. Dashed lines represent mean values. QBER and gain fluctuations from block to block are due to transmission fluctuation caused by the channel turbulence and to the finite size of the blocks.

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Summary



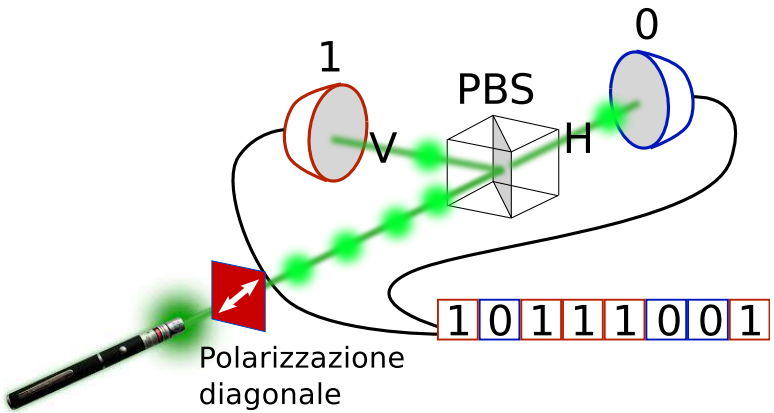
G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

Random number in everyday life

- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks)
- All classical security protocols used in e-commerce or credit card are based on RANDOM NUMBERS

G. Vallone, *et al.*, **Phys. Rev. Lett. 113, 060503 (2014)**

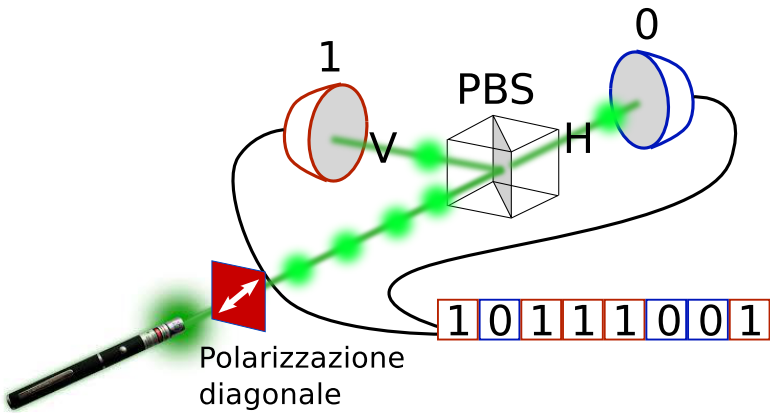
Quantum Random Number Generators (QRNG)



- intrinsic randomness of quantum measurements

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

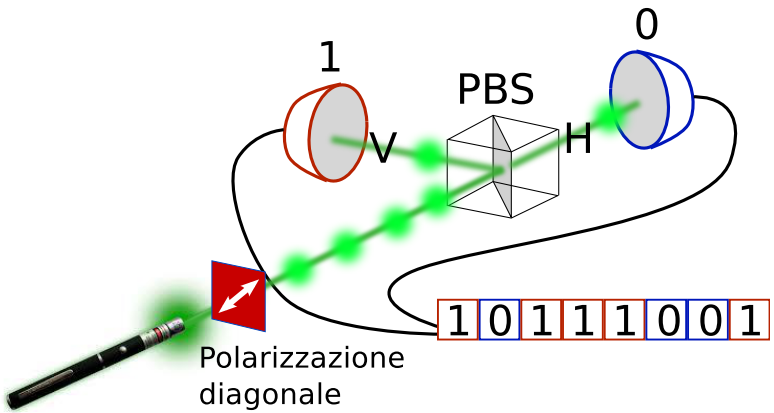
Quantum Random Number Generators (QRNG)



- intrinsic randomness of quantum measurements
- The output of the measurement cannot be predicted (even if the initial state is perfectly known)

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

Quantum Random Number Generators (QRNG)



- intrinsic randomness of quantum measurements
- The output of the measurement cannot be predicted (even if the initial state is perfectly known)
- Randomness is not due to ignorance on the initial conditions (like coin tossing)

How to distinguish

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \quad \text{(quantum randomness)}$$

from

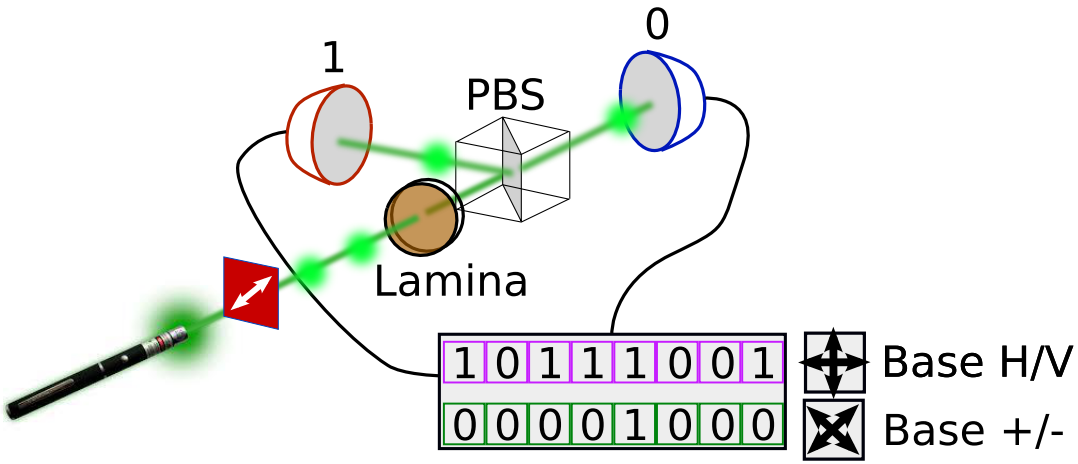
$$\rho = \frac{1}{2}|H\rangle\langle H| + \frac{1}{2}|V\rangle\langle V| \quad \text{(classical randomness)?}$$

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

QRNG certified by the uncertainty principle

For mutually unbiased basis $\mathbb{Z}$ and $\mathbb{X}$ in d dimensions, the Entropic Uncertainty Principle is:

$$H_{\min}(Z|E)_\rho + H_{\max}(X|B)_\rho \geq \log_2 d$$



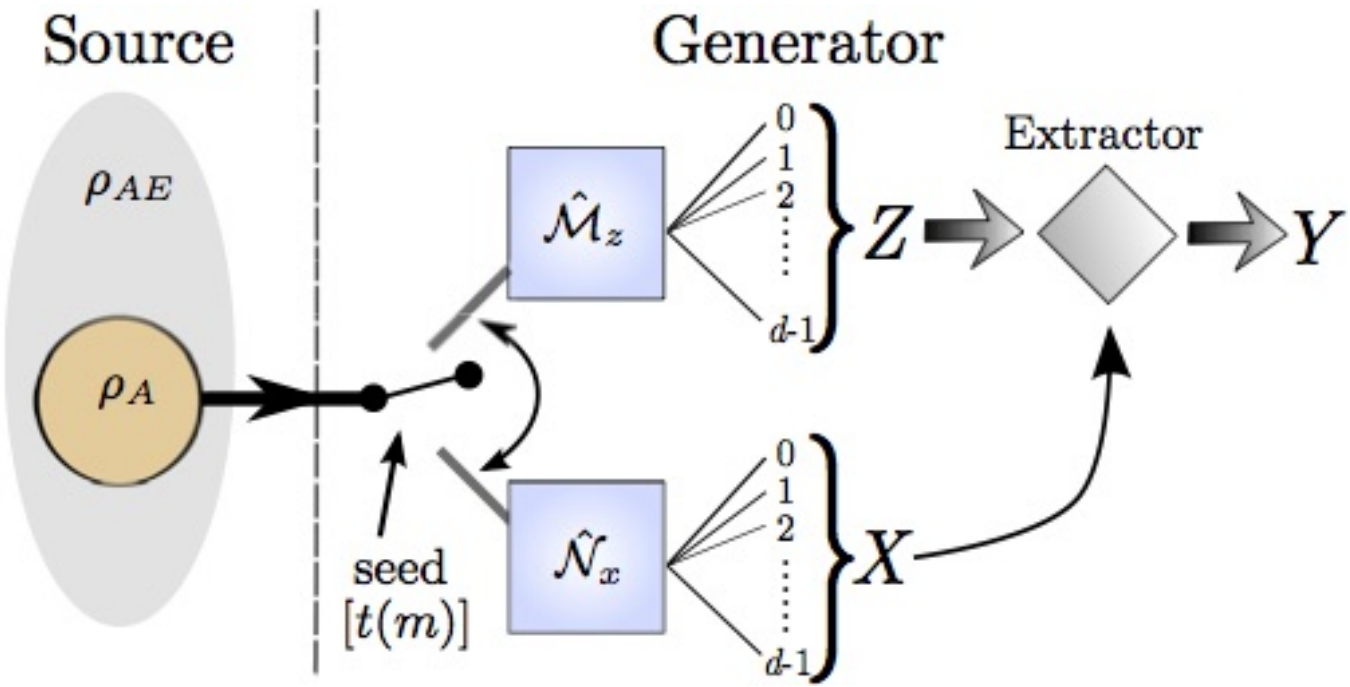
Base $\mathbb{Z}$: $\{|H\rangle/|V\rangle\}$
Random bits

Base $\mathbb{X}$: $\{|+\rangle/|-\rangle\}$
Randomness certification

$$p_{\text{guess}}(Z|E) \leq \frac{1}{d}\left(\sum_x \sqrt{p_x}\right)^2$$

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

Scheme of the QRNG certified by the UP

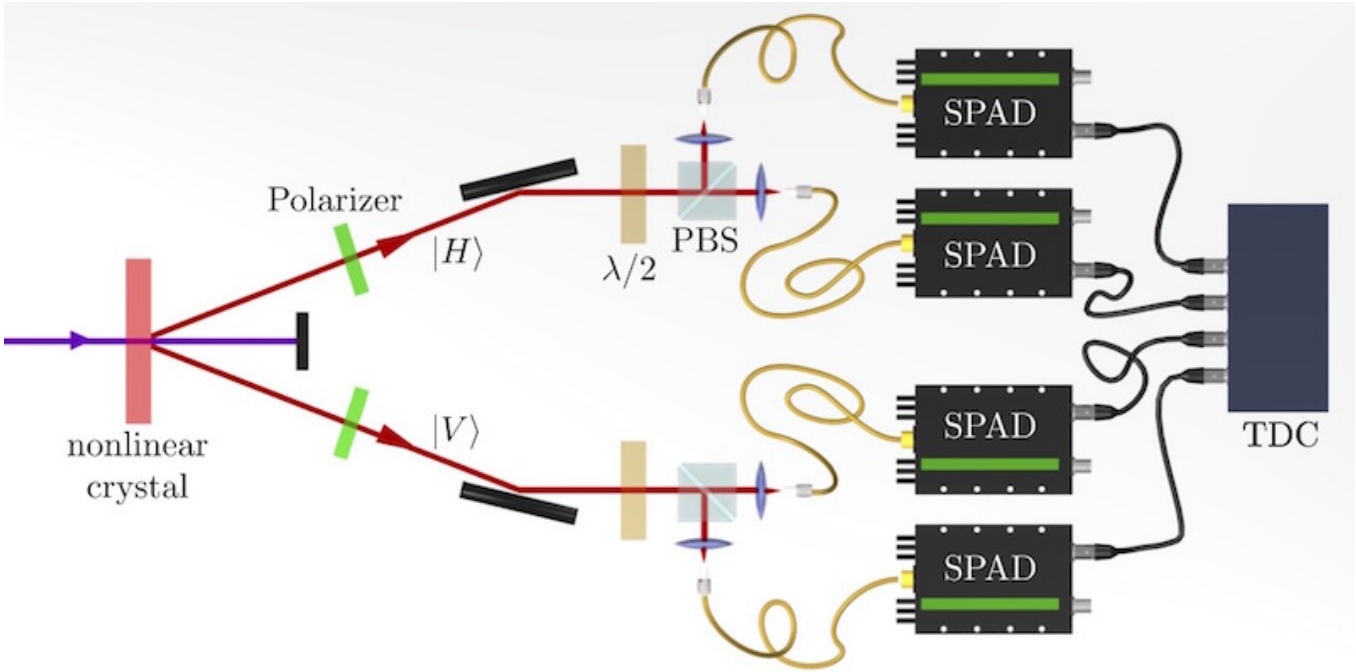


By switching between the $\{|z\rangle\}$ and $\{|x\rangle\}$ basis, the random variables Z and X are extracted. The variable Z is used to generate the random sequence, while the variable X is used to evaluate how many true random bits can be extracted by Z. Y represents the final true random sequence.

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

Experimental realization

Proof of principle realization with qubit and ququart

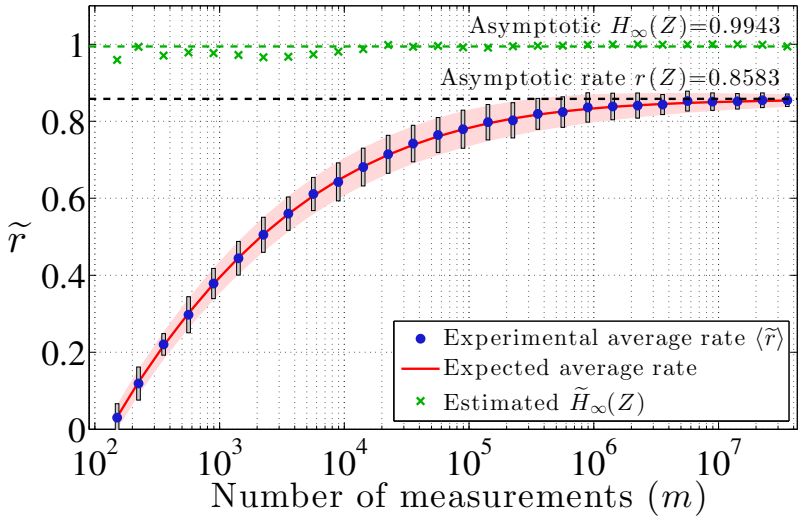


qubit $\Rightarrow$ heralded single photon in $|H\rangle$

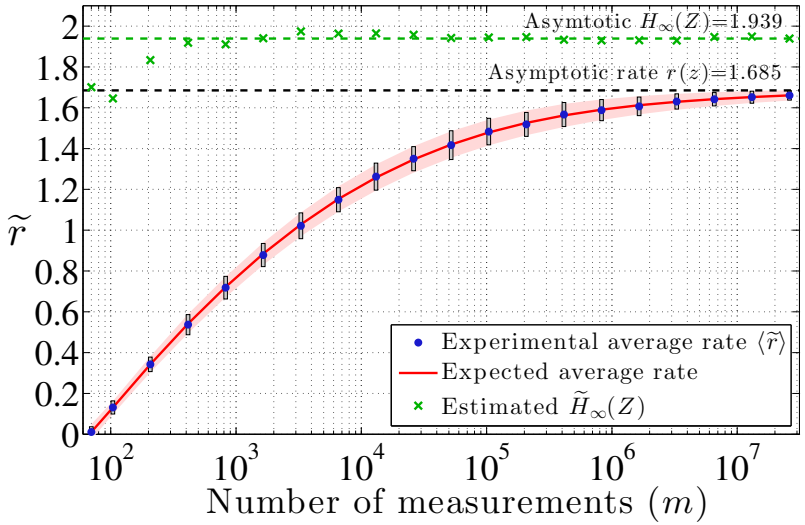
ququart $\Rightarrow$ pair of photons in $|HV\rangle$

G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

Random generation rates



Random generation rate for a generator based on qubits (2-level system)



Random generation rate for a generator based on ququarts (4-level system)

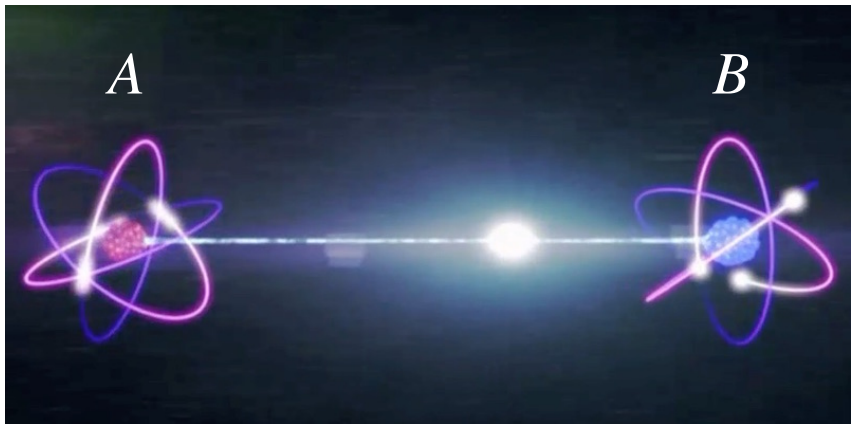
G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, **Phys. Rev. A 90, 052327 (2014)**

What is Entanglement?

Correlation and superposition. In Schrödinger word:

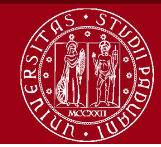
"the characteristic trait of quantum mechanics"

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B) = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B)$$
$$\neq |\varphi_1\rangle_A \otimes |\chi_2\rangle_B$$



Correlations that cannot be obtained by classical systems!

EPR paradox: the beginning...



Einstein, Podolsky e Rosen (EPR), 1935:

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

EPR paradox: the beginning...

Einstein, Podolsky e Rosen (EPR), 1935:

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

1. Reality: if, without disturbing a system a physical quantità can be predicted, then an **element of reality** is associated to such quantity;

EPR paradox: the beginning...

Einstein, Podolsky e Rosen (EPR), 1935:

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

1. Reality: if, without disturbing a system a physical quantità can be predicted, then an **element of reality** is associated to such quantity;
2. Completeness: every **element of reality** must be contained in the physical theory;

EPR paradox: the beginning...

Einstein, Podolsky e Rosen (EPR), 1935:

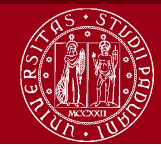
MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

1. Reality: if, without disturbing a system a physical quantità can be predicted, then an **element of reality** is associated to such quantity;
2. Completeness: every **element of reality** must be contained in the physical theory;
3. Locality: any action on a system A (Alice) cannot change the physical reality of a system B (Bob) spatially separated.

The "paradox"



- EPR aim was to demonstrate that Quantum Mechanics is NOT a complete theory.

The "paradox"

- EPR aim was to demonstrate that Quantum Mechanics is NOT a complete theory.
- The "EPR paradox" is based on entangled states:

$$|\Psi^-\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right)$$

The "paradox"

- EPR aim was to demonstrate that Quantum Mechanics is NOT a complete theory.
- The "EPR paradox" is based on entangled states:

$$|\Psi^-\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right)$$

- If Alice (on the first particle) and Bob (on the second particle) measure the polarization (or spin) in the same direction the obtain always opposite results.

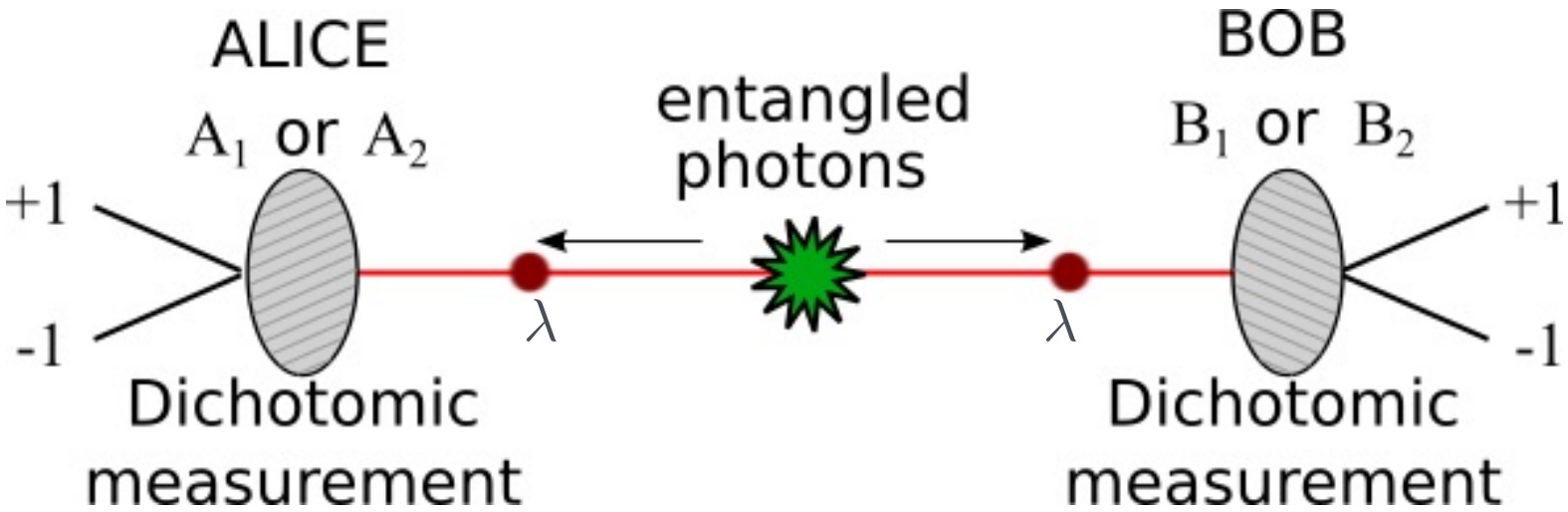
Hypotesis: Locality and Realism

$\Downarrow$

EPR paradox: QM is not complete!

Local hidden variable model

Does an alternative model exist?



λ : Hidden variable (real and local)

Correlation: $\langle A_i B_j \rangle = p(A_i = B_j) - p(A_i \neq B_j)$

Bell Inequality

- Bell inequality: for any local hidden variable theory it holds:

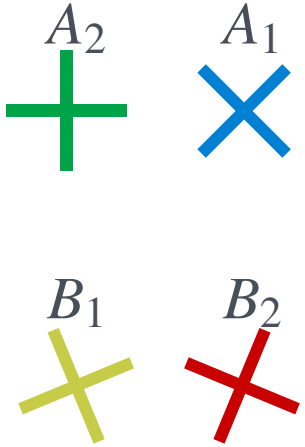
$$S_{CH} \equiv |\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle| \leq 2$$

Bell Inequality

- Bell inequality: for any local hidden variable theory it holds:

$$S_{CH} \equiv |\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle| \leq 2$$

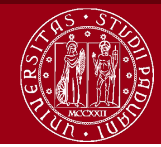
- The inequality is violated by a (singlet) entangled state with A_1, A_2, B_1 and B_2 chosen as in figure:



Quantum Mechanics predicts:

$$\langle S_{CH} \rangle_{\text{entangled state}} = 2\sqrt{2} > 2$$

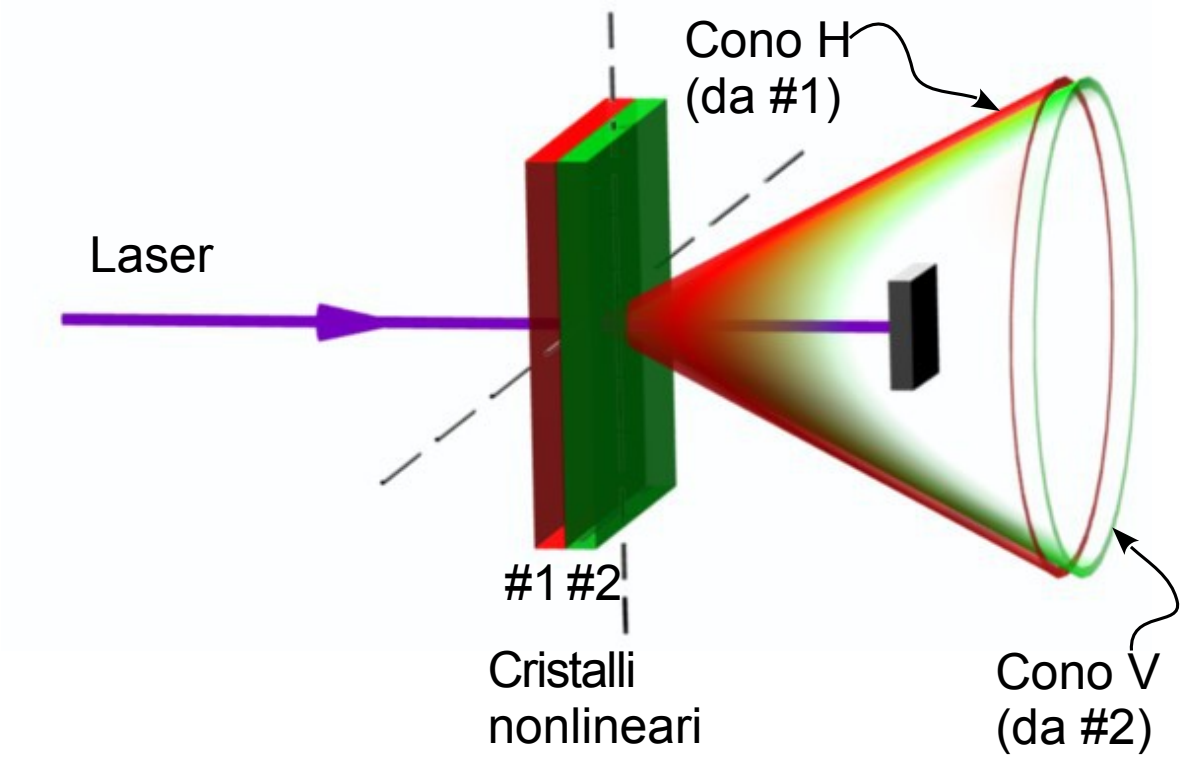
Conseguences



- It is not possible to describe nature with a local hidden variable theory
- Neither the particle "knows" in advance the output of the measurement
- Loopholes...

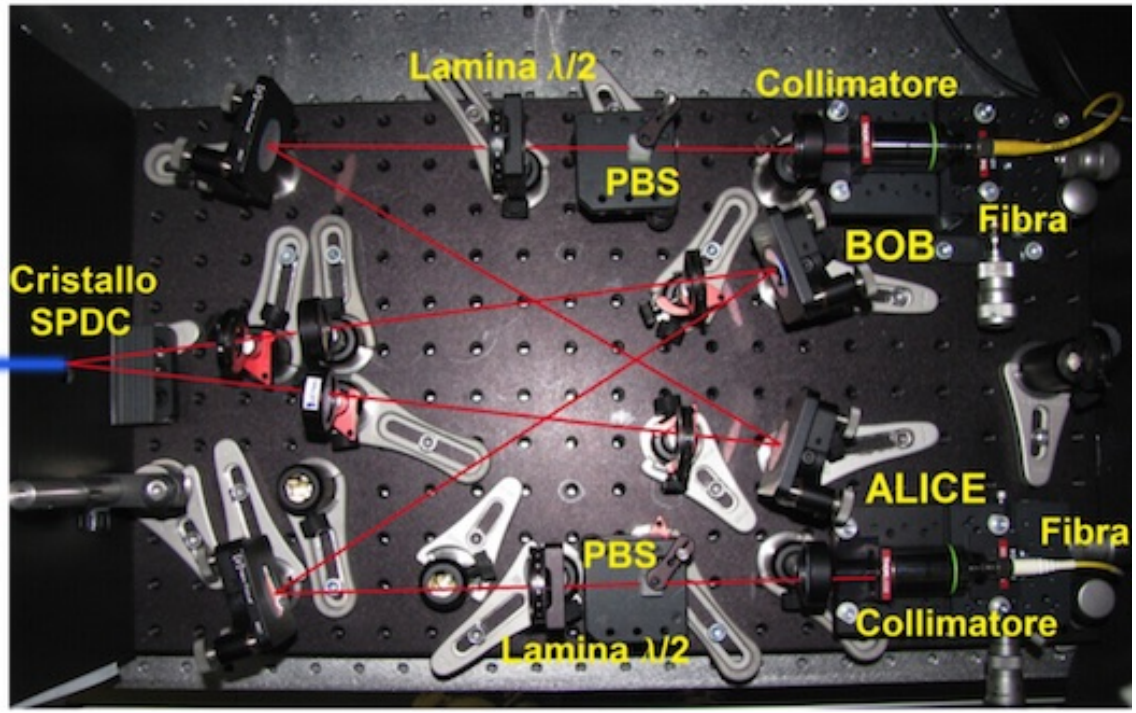
How entanglement can be generated?

Parametric down-conversion (probabilistic effect)



What is the measured value of S_{CH}?

In the lab:

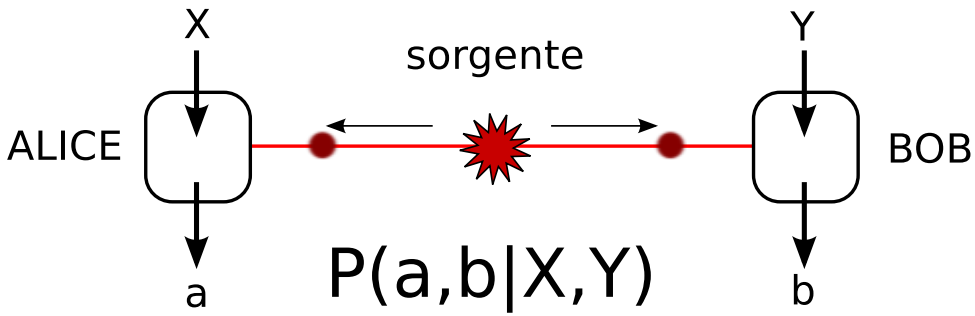


$$\langle S_{\mathrm{CH}} \rangle_{\mathrm{exp}} = 2.80 \pm 0.04 > 2\,, \qquad 2\sqrt{2} \simeq 2.8284$$

Device Independent Protocols

- Bell inequality was introduced to deal with fundamental problems: the reality and locality of quantum mechanics
- It has been violated in many different experiments (photons, ions, diamonds, atoms....)
- close to loophole-free violations
- The Bell inequality is now used as a tool to certify entanglement: device-independent protocols

Device Independent Protocols



ALICE
X: choice of the measurement basis
a: output of the measurement

BOB
Y: choice of the measurement basis
b: output of the measurement

The following probabilities are measured:

$$P(a, b|X, Y)$$

If the above probabilities violate a Bell Inequality, entanglement between Alice and Bob can be proved

Device Independent QKD

- In standard QKD system, the security is based on the working mechanism of the devices
- In Device-Independent QKD, the devices are **BLACK BOXES**: no assumption on their functioning
- Key rate related to the violation of the Bell inequality

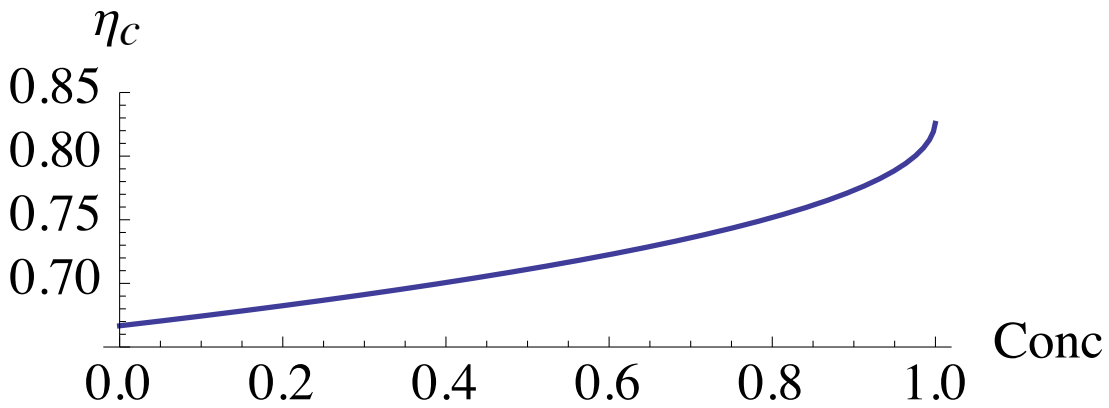
$$r = 1 - h_2(Q) - h_2[f(S_{\mathrm{CH}})]$$

con $f(S_{\mathrm{CH}}) = \frac{1+\sqrt{(S_{\mathrm{CH}}/2)^2-1}}{2}$ e Q =QBER.

- If the inequality is not violated, a vanishing key rate is obtained

DI-QKD with non-maximally entangled states

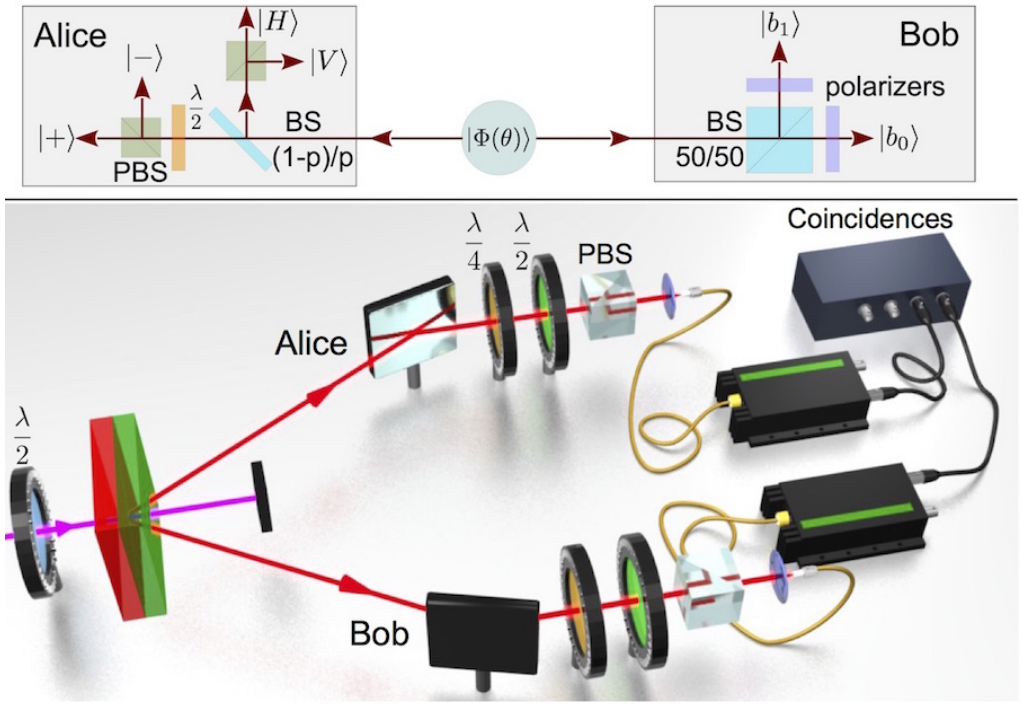
- DI protocols requires high detection efficiency in order to close the detection looholes
  - Non-maximally entangled states requires lower threshold efficiency η_c compared to maximally entangled states

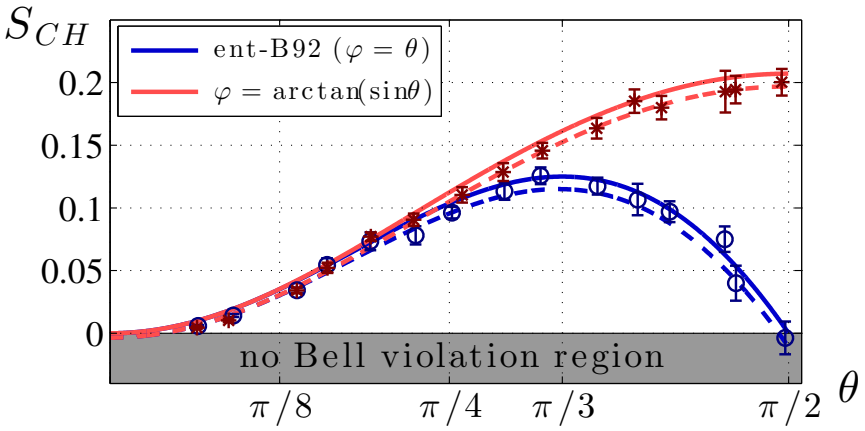


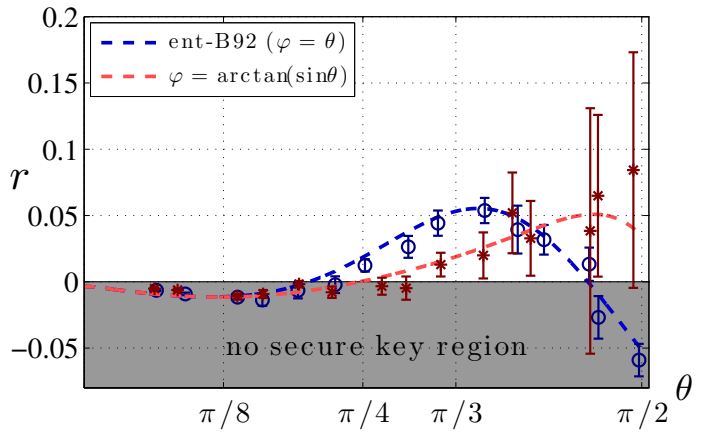
$\Rightarrow$ Define a protocol with non-maximally entangled states for DI-QKD

G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, **New J. Phys. 16, 063064 (2014)**.

Experimental key rates

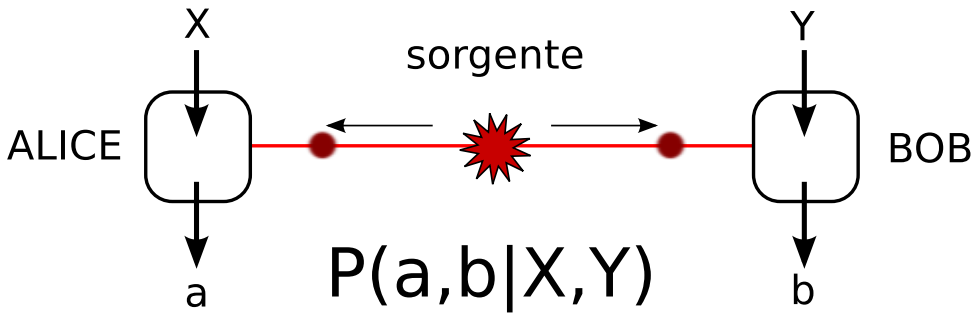






G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, **New J. Phys. 16, 063064 (2014)**.

Device Independent QRNG



- Random bit generation rate:

$$r = -\log_2\left[1-\log_2\left(1+\sqrt{2-\frac{S_{\mathrm{CH}}^2}{4}}\right)\right]$$

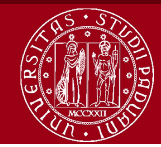
- Vanishing rate if $S_{\mathrm{CH}} \leq 2$

G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, **New J. Phys. 16, 063064 (2014)**.

Summary

G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, **New J. Phys. 16, 063064 (2014)**.

Long term opportunities



Unique opportunity of Quantum Physics in Space

Possibility of testing quantum physics in new environment and probing the laws of nature at very large distance

Long term opportunities

Unique opportunity of Quantum Physics in Space

Possibility of testing quantum physics in new environment and probing the laws of nature at very large distance

- Distribution of entanglement from Earth to Space
- Test of Bell's Inequalities with unprecedented conditions: LEO or GEO-orbit, moving terminals, gravitational field

Long term opportunities

Unique opportunity of Quantum Physics in Space

Possibility of testing quantum physics in new environment and probing the laws of nature at very large distance

- Distribution of entanglement from Earth to Space
- Test of Bell's Inequalities with unprecedented conditions: LEO or GEO-orbit, moving terminals, gravitational field
- Teleportation from Earth to Space
- Quantum technologies in long distance applications

Long term opportunities

Unique opportunity of Quantum Physics in Space

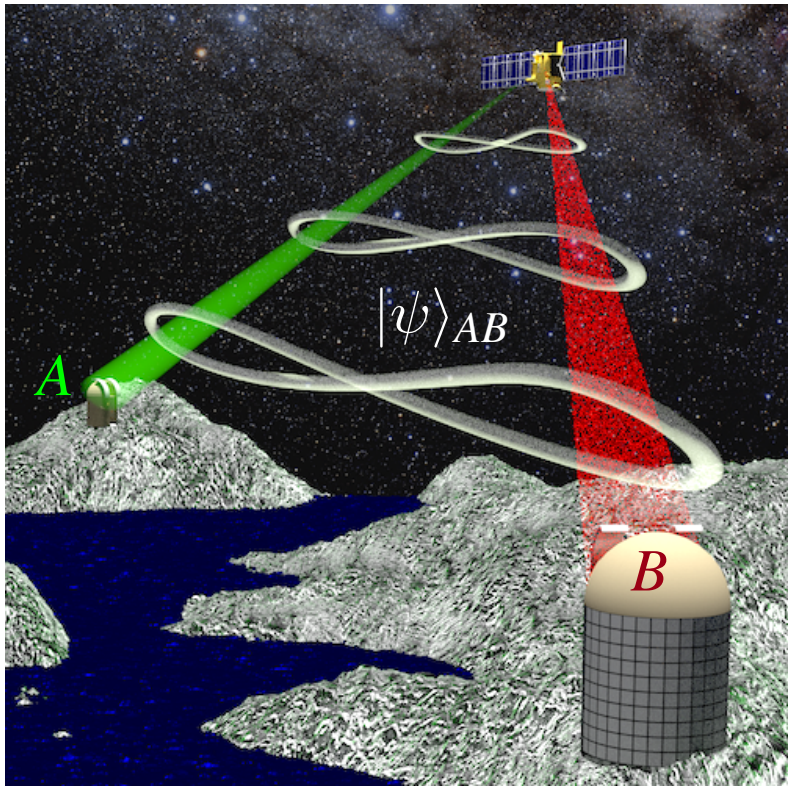
Possibility of testing quantum physics in new environment and probing the laws of nature at very large distance

- Distribution of entanglement from Earth to Space
- Test of Bell's Inequalities with unprecedented conditions: LEO or GEO-orbit, moving terminals, gravitational field
- Teleportation from Earth to Space
- Quantum technologies in long distance applications
- Test of foundations of quantum field theory and general relativity

Entanglement distribution

$$|\psi\rangle_{AB} \neq |\phi\rangle_A \otimes |\chi\rangle_B$$

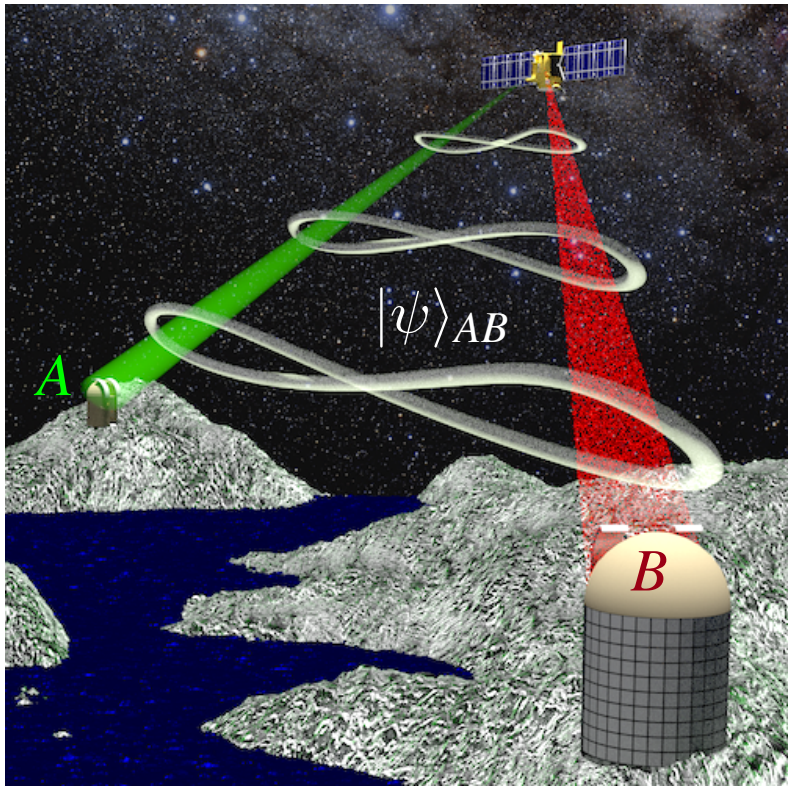
- Entanglement is a unique resource for Quantum Information applications (teleportation, dense coding, etc..)



Entanglement distribution

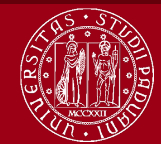
$$|\psi\rangle_{AB} \neq |\phi\rangle_A \otimes |\chi\rangle_B$$

- Entanglement is a unique resource for Quantum Information applications (teleportation, dense coding, etc..)



- Limits on the distance between two entangled systems?
- Is entanglement limited to certain mass and length scales or altered under specific gravitational circumstances?

Bell's test



If a set of correlation do not satisfy the Bell's inequality $S \leq 2$, the correlations cannot be explained by a local realistic theory.

Bell's test

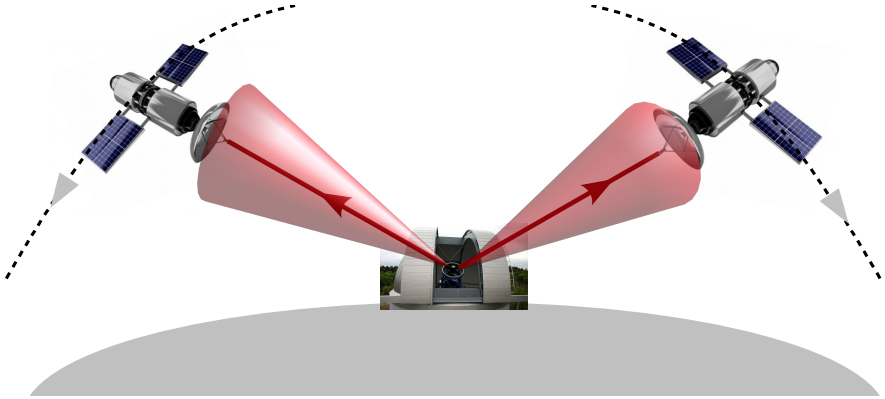
If a set of correlation do not satisfy the Bell's inequality $S \leq 2$, the correlations cannot be explained by a local realistic theory.

- Bell'inequality violated between fixed location: "spooky action at distance" at speed greater than $10^4 c$.

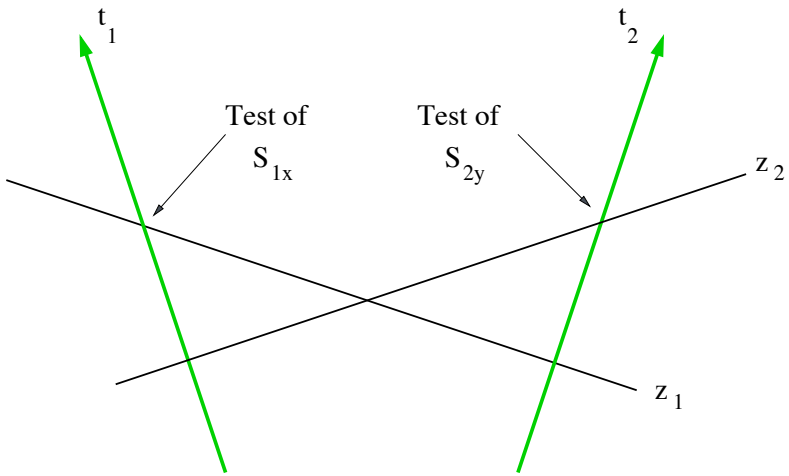
Bell's test

If a set of correlation do not satisfy the Bell's inequality $S \leq 2$, the correlations cannot be explained by a local realistic theory.

- Bell'inequality violated between fixed location: "spooky action at distance" at speed greater than $10^4 c$.
- Bell's test with moving terminals

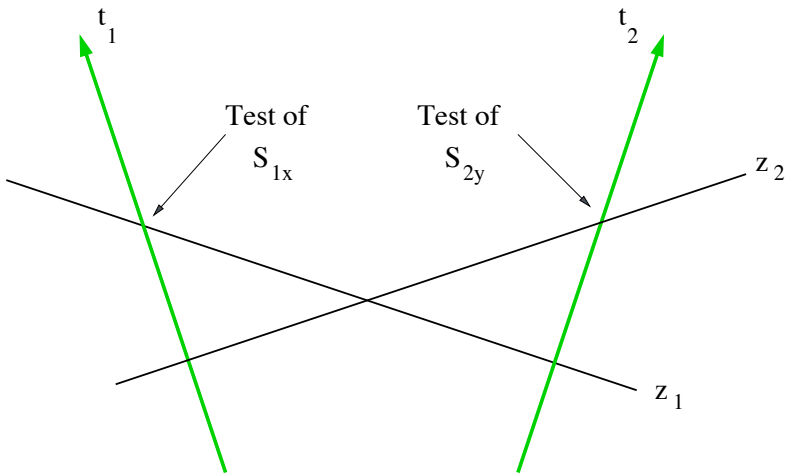


Bell's test with detectors in relative motion



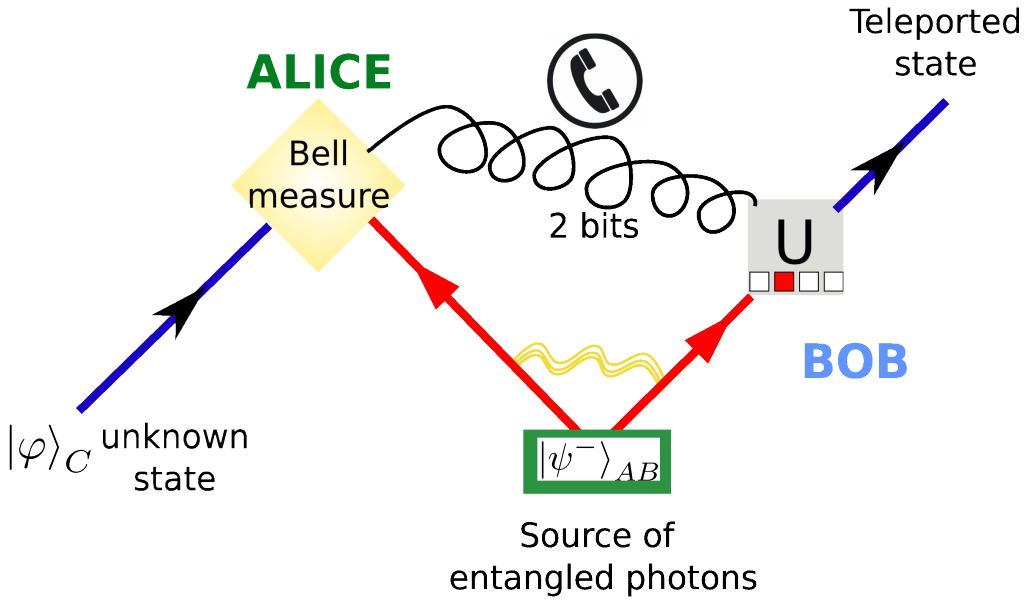
- the two observers disagree on the relative time ordering of the measurement events

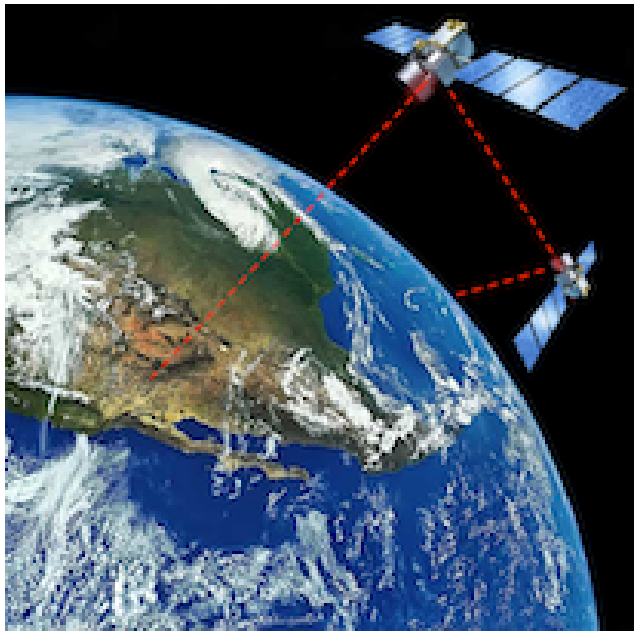
Bell's test with detectors in relative motion



- the two observers disagree on the relative time ordering of the measurement events
- The probabilities predicted by quantum theory do not depend on the time-ordering of spacelike events, so its predictions will not be changed.
- understanding the physical reality of quantum states and the non-local collapse of the wave functions.

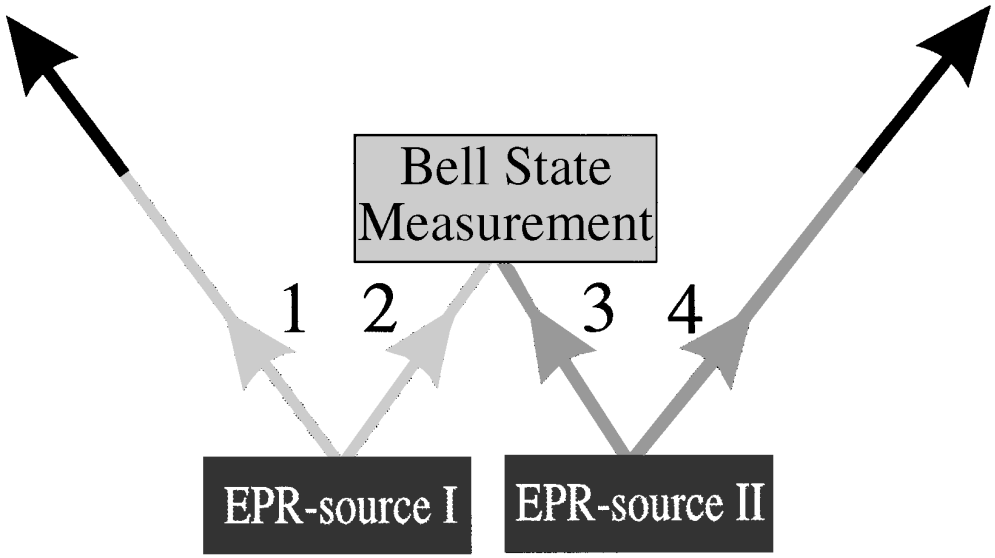
Quantum teleportation





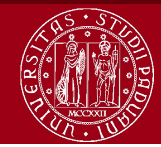
Standard quantum theory places no bound on the distance at which teleportation may be accomplished

Entanglement swapping



Entangling photons that never interacted

Conclusions



- We have experimentally demonstrated Quantum Communication from several satellites acting as quantum transmitter and with MLRO as the receiver

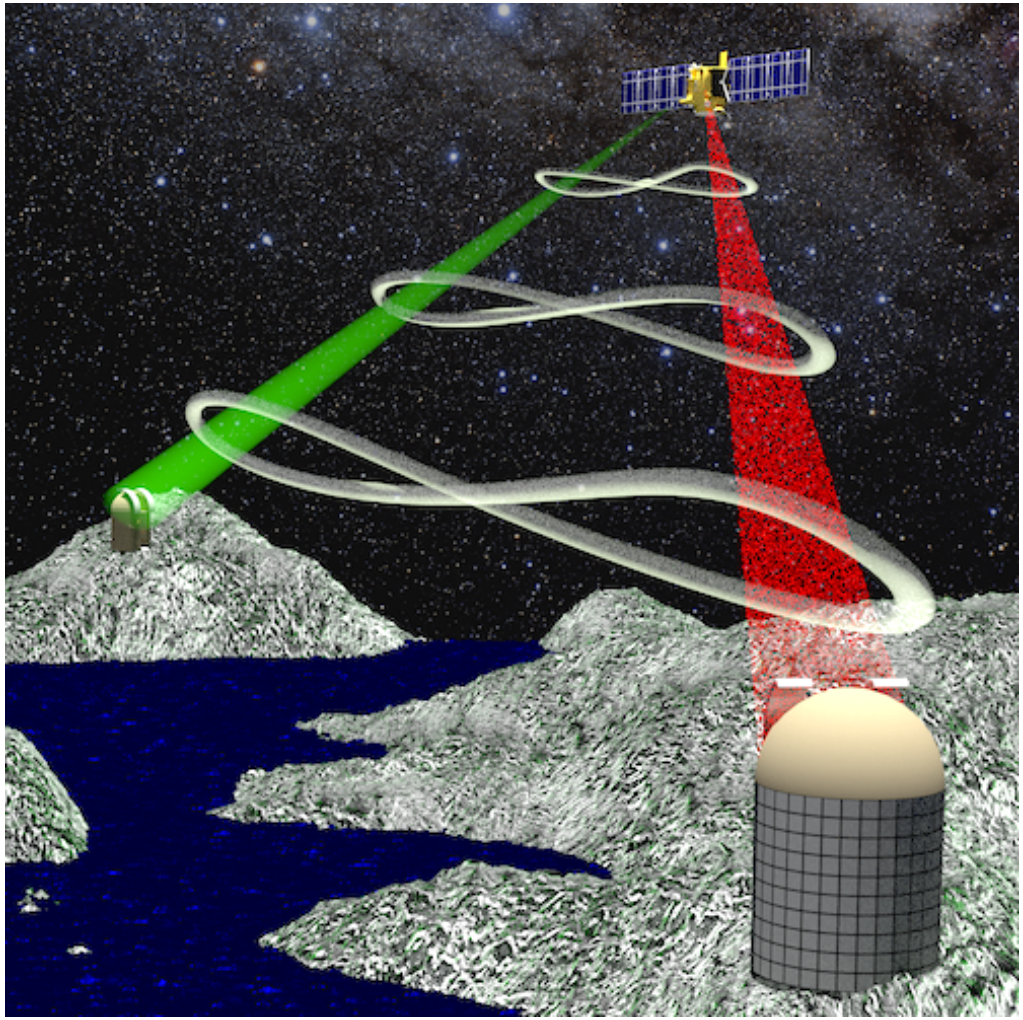
Conclusions

- We have experimentally demonstrated Quantum Communication from several satellites acting as quantum transmitter and with MLRO as the receiver
- QBER was found low enough to demonstrate the feasibility of quantum information protocols such as QKD along a Space channel

Conclusions

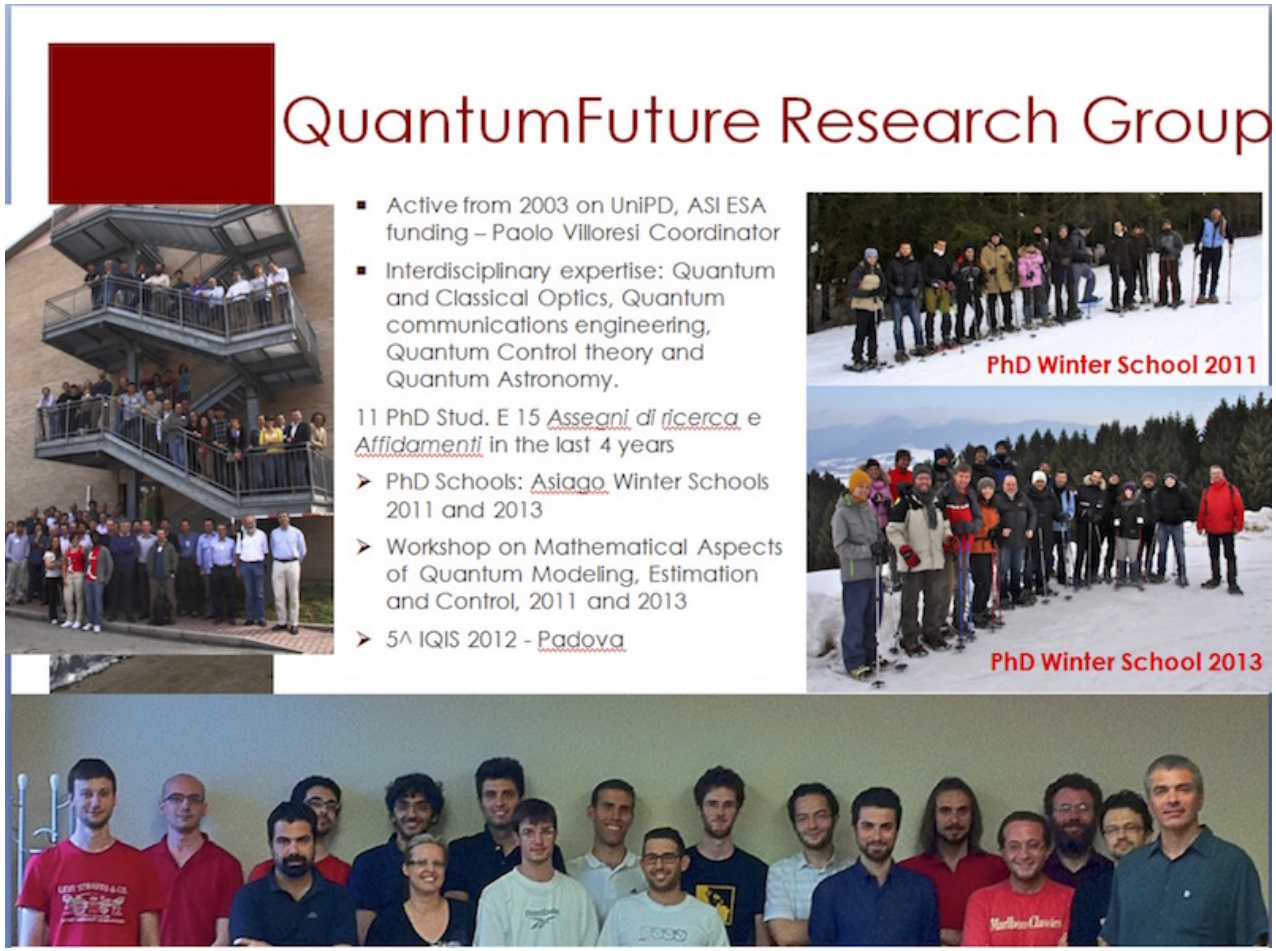
- We have experimentally demonstrated Quantum Communication from several satellites acting as quantum transmitter and with MLRO as the receiver
- QBER was found low enough to demonstrate the feasibility of quantum information protocols such as QKD along a Space channel
- The ability of propagating quantum correlation over large distance will have a great impact for fundamental physics and quantum information applications

Perspectives



Explore the limits of Quantum Mechanics and quantum correlations over very long distances

Research group: QuantumFuture



email: vallone@dei.unipd.it

http://quantumfuture.dei.unipd.it/

REFERENCES

- G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, P. Villoresi, *Quantum interference along satellite-ground channels*, **[arXiv:1509.07855]**.
- G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, *Experimental Satellite Quantum Communications*, **Phys. Rev. Lett. 115, 040502 (2015), Editors' suggestions**
- D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, *Experimental single photon exchange along a space link of 7000 km*, **Phys. Rev. A 93, 010301(R) (2015), (2016), Rapid Communications**.
- I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, P. Villoresi, *Impact of turbulence in long range quantum and classical communications*, **Phys. Rev. Lett. 109, 200502 (2012)**.
- G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, *Loss tolerant device-independent quantum key distribution: a proof of principle*, **New J. Phys. 16, 063064 (2014).**
- G. Vallone, *et al.*, *Free-space QKD by rotation-invariant twisted photons*, **Phys. Rev. Lett. 113, 060503 (2014)**.
- G. Vallone, D. Marangon, M. Tomasin, P. Villoresi, *Quantum randomness certified by the uncertainty principle*, **Phys. Rev. A 90, 052327 (2014)**.
- D. Bacco, M. Canale, N. Laurenti, G. Vallone, P. Villoresi, *Experimental quantum key distribution with finite-key security analysis for noisy channels*, **Nature Communications 4, 2363 (2013)**