Dalle disuguaglianze di Bell alla crittografia quantistica:

applicazioni della fisica fondamentale e dell'Informazione Quantistica

Giuseppe Vallone

email: vallone@dei.unipd.it

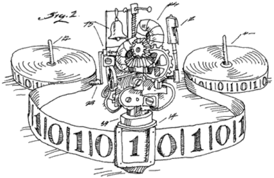
Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Dip. di Fisica, Università di Torino - 5 Giugno 2015

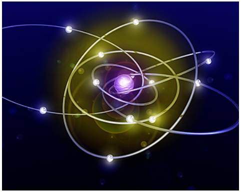
What is Quantum Information?

Information Theory



$\Leftrightarrow$

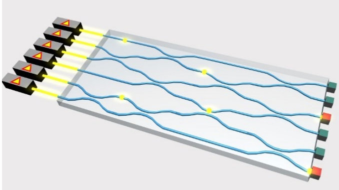
Quantum Mechanics



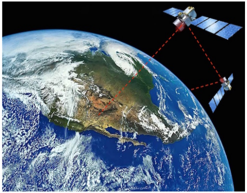
Merging two big XXth century revolutions:
information theory (Shannon, Turing) and Quantum Mechanics.

Examples of applications

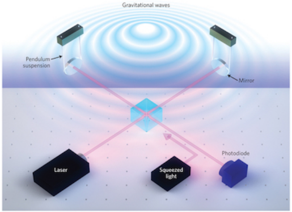
Quantum computer

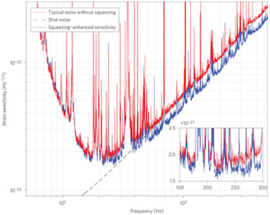


Quantum cryptography



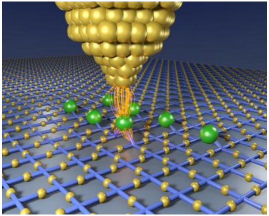
Quantum metrology



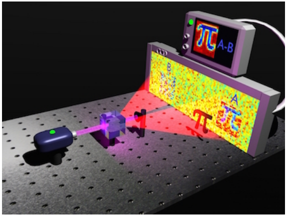


Esempi di applicazioni

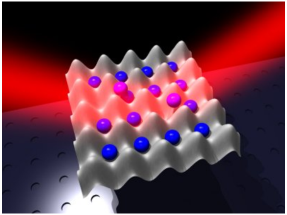
Quantum sensing



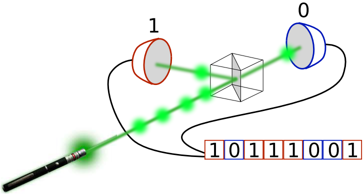
Quantum imaging



Quantum simulation



Quantum random number generation



But...

...be aware of fake!

Summary

1. Quantum Mechanics
2. Quantum Key Distribution
3. Quantum Random Number Generators
4. Entanglement and Bell inequalities
5. Protocols exploiting entanglement
   - Teleportation
   - "Device Independent" protocols
6. Conclusions

Summary

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

4 Entanglement and Bell inequalities

5 Protocols exploiting entanglement
- Teleportation
- "Device Independent" protocols

6 Conclusions

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:

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

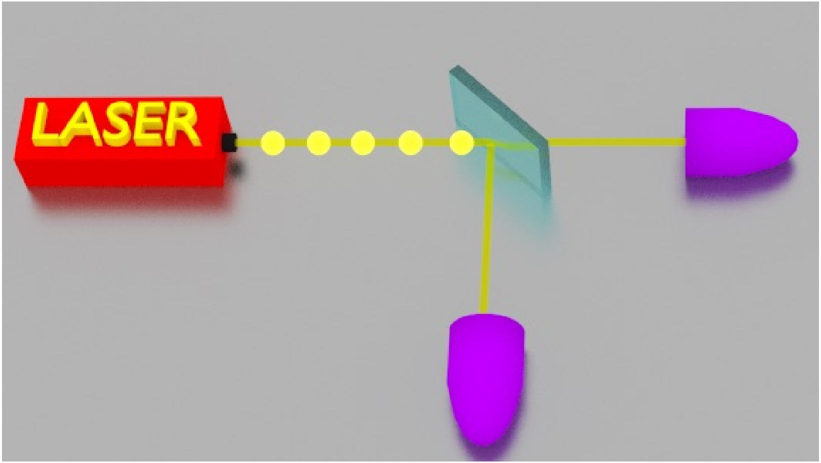
- From classical bit (two orthogonal states $|0\rangle$ and $|1\rangle$) to quantum-bit , or qubit:

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

- indistinguishability $\Rightarrow$ INTERFERENCE!

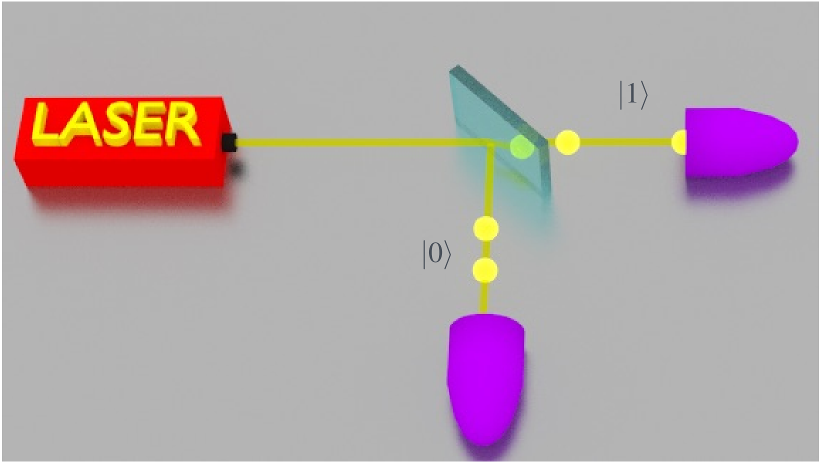
State superposition

Example 1: photons on a semi-reflective mirror (beam splitter)



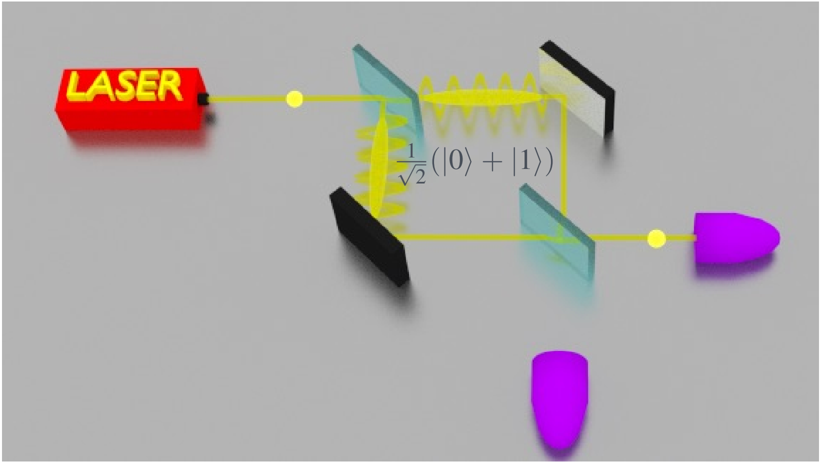
State superposition

Example 1: photons on a semi-reflective mirror (beam splitter)



State superposition

Example 1: photons on a semi-reflective mirror (beam splitter)



State superposition

Example 2: two-slit experiment

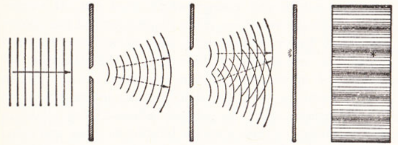
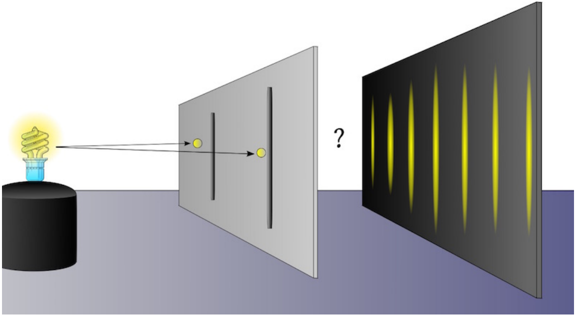


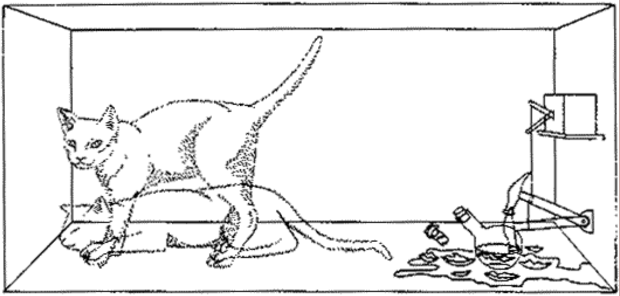
FIG. 3



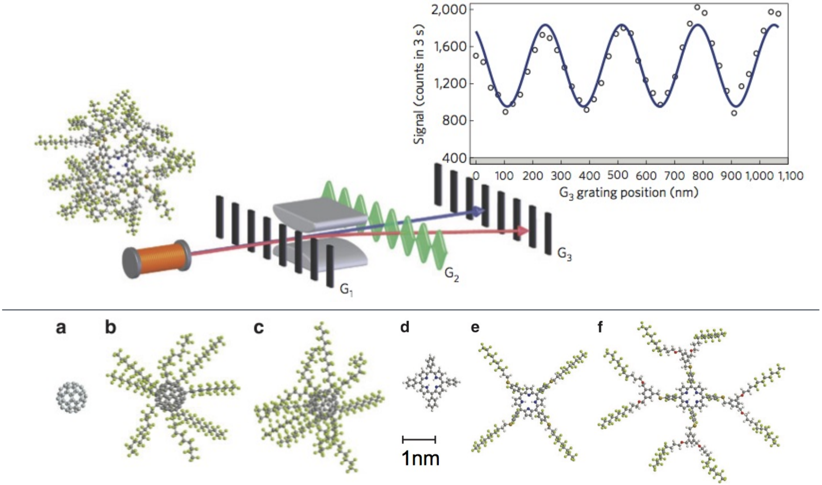
State superposition

Example 3: Schrödinger cat

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



State superposition

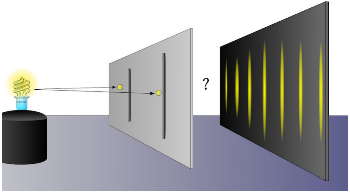


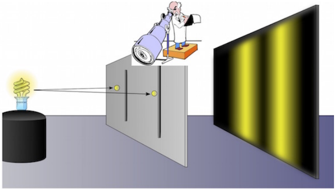
up to 6910 AMU, 430 atoms

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

Misurement and no-cloning

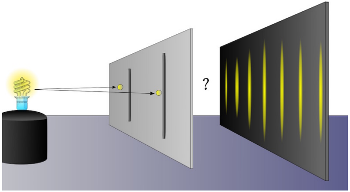
- The measurement (in general) perturbs quantum states

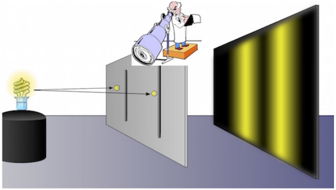




Misurement and no-cloning

- The measurement (in general) perturbs quantum states

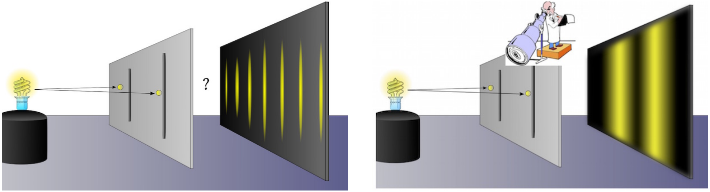




- The output of a measurement is probabilistic (if the state is not an eigenstate of the observable)

Misurement and no-cloning

- The measurement (in general) perturbs quantum states



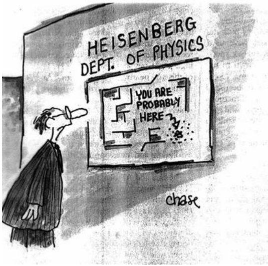
- The output of a measurement is probabilistic (if the state is not an eigenstate of the observable)
- Impossibility of perfect cloning: quantum copy-machine is not physical

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

Uncertainty principle

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

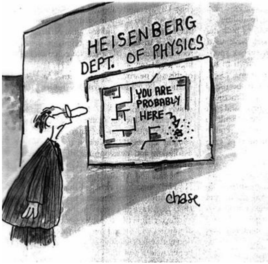
$$\Delta x \Delta p \geq \frac{\hbar}{2}$$



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

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

4 Entanglement and Bell inequalities

5 Protocols exploiting entanglement
- Teleportation
- “Device Independent” protocols

6 Conclusions

QKD principles

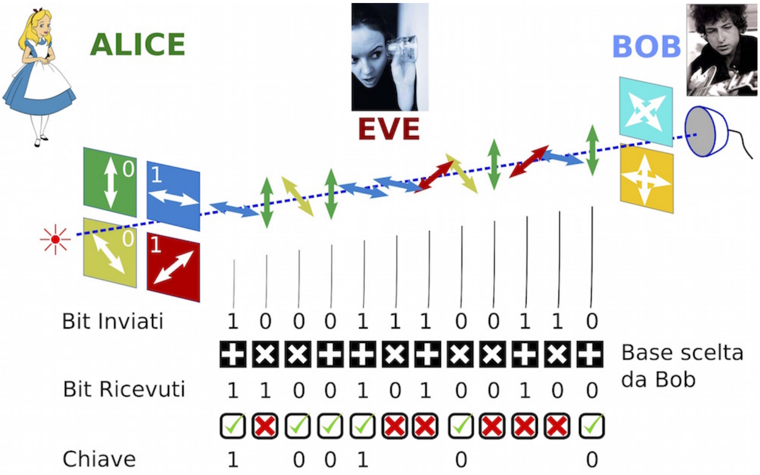
The best method to encrypt a message is the One-Time-Pad (OTP) protocol: for a n-bit message, a n-bit secure key is needed

Messaggio	1	0	1	1	1	0	0	1	1	0	1	0	1	0
							$\oplus$							
Chiave random	1	0	0	0	1	0	1	0	1	1	0	1	0	1
							=							
Messaggio cifrato	0	0	1	1	0	0	1	1	0	1	1	1	1	1

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:

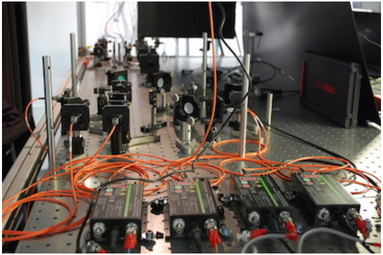
$$r = 1 - 2h_2(Q)$$

with

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

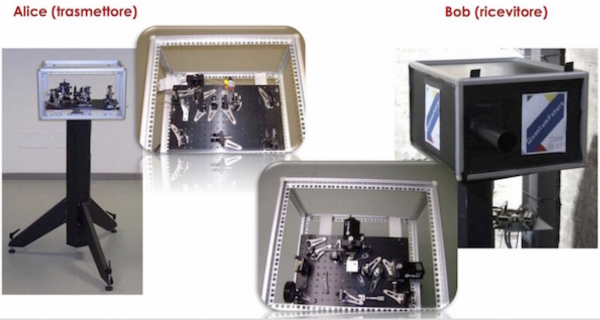
If Eve is gaining information on the key, the key is discarded.
Eve has no information on the secret message

QKD in the lab

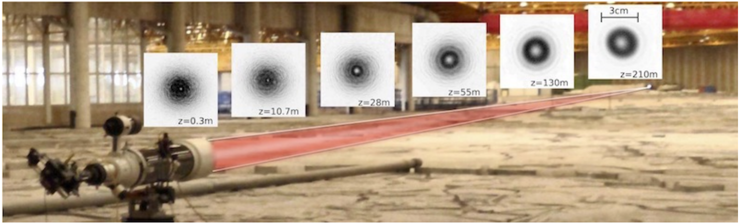


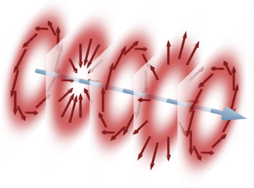
QKD system for BB84 protocol

Free-space QKD prototype



Aligment-free OAM QKD: 210m free space link

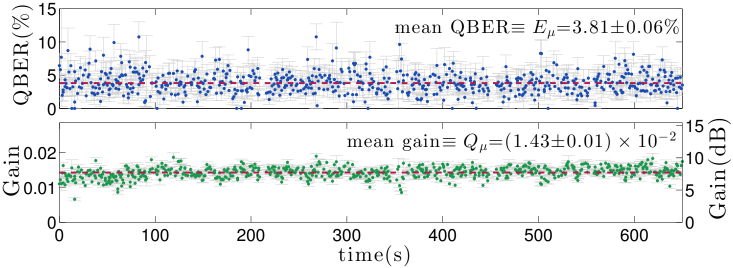




Hybrid qubit: $\alpha|L\rangle_\pi \otimes |r\rangle_O + \beta|R\rangle_\pi \otimes |l\rangle_O$
Rotaton-invariant states!

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

Gain and QBER



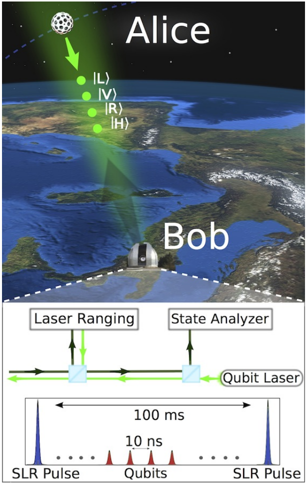
The data show 10 minutes of acquisition. Dashed lines represent mean values. QBER and gain fluctuations from block to block are due to transmission fluctuation caused by the channel turbulence and to the finite size of the blocks.

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

Satellite quantum communication

- Source on satellite simulated by a CCR

CCR: Corner-Cube Retroreflector



- Source (Alice) need to be at the single photon level
- Short pulses necessary for background rejection: qubit interleaving strong SLR pulses

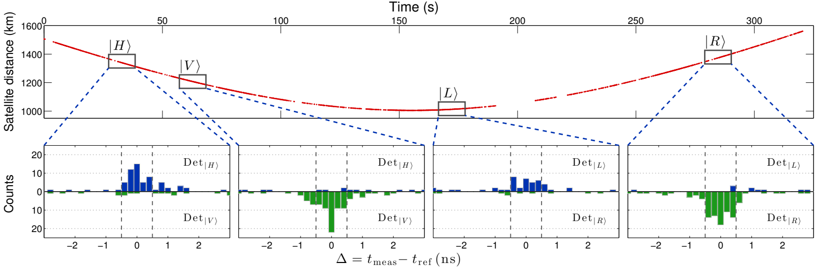
G. Vallone, *et al.*, *Experimental Satellite Quantum Communication*, **Phys. Rev. Lett. (in press)**

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: arrival time within $0.5ns$ from predictions

G. Vallone, *et al.*, *Experimental Satellite Quantum Communication*, **Phys. Rev. Lett. (in press)**

Commercial QKD

First commercial example of security protocol based on Quantum Mechanics

ID Quantique (CH)

MagiQ (US)

Quintessence (AU)

SeQurenet (FR)

Toshiba (UK)

Summary

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

4 Entanglement and Bell inequalities

5 Protocols exploiting entanglement
- Teleportation
- "Device Independent" protocols

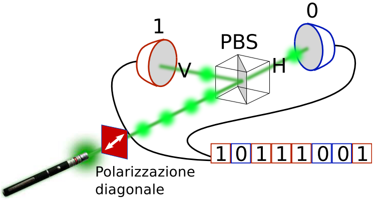
6 Conclusions

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

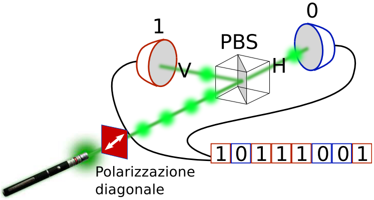
Quantum Random Number Generators (QRNG)



- intrinsic randomness of quantum measurements

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

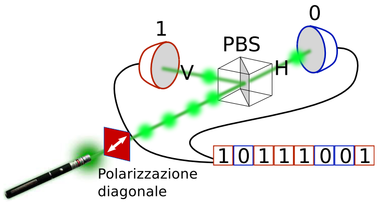
Quantum Random Number Generators (QRNG)



- 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

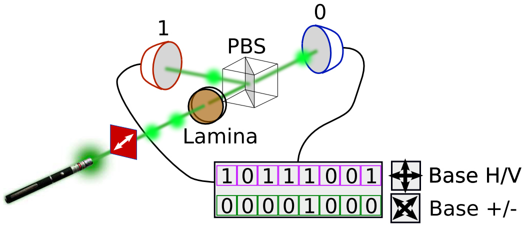
$$\rho = \frac{1}{2}|H\rangle\langle H| + \frac{1}{2}|V\rangle\langle V| \quad \text{(classical randomness)}?$$

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)**

Summary

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

4 Entanglement and Bell inequalities

5 Protocols exploiting entanglement
- Teleportation
- “Device Independent” protocols

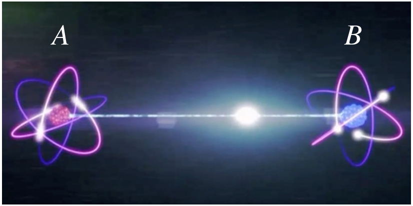
6 Conclusions

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

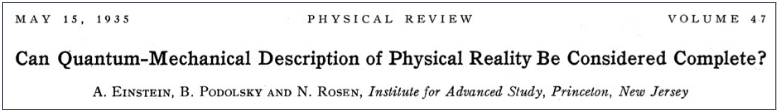
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

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.

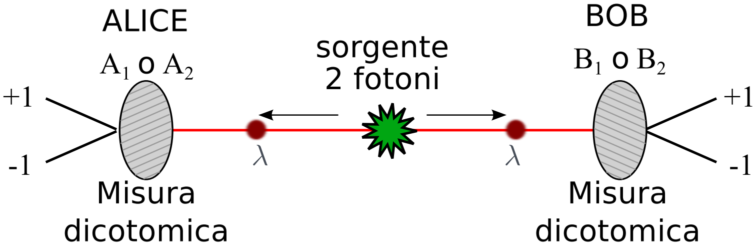
Hypotesis: Locality and Realism

$\Downarrow$

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:

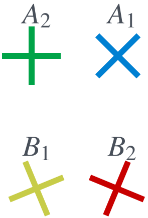
$$S_{CH} \equiv |\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle| \leq 2$$

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:

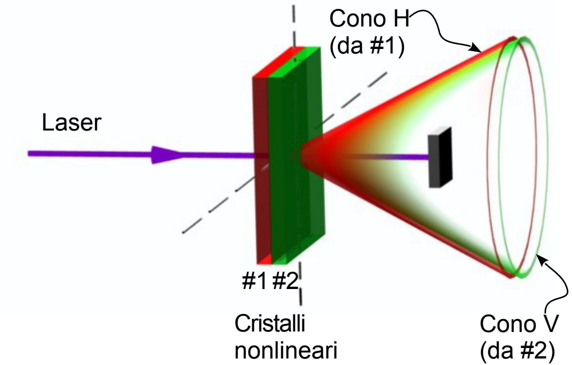
$$\langle S_{CH} \rangle_{\text{entangled state}} = 2\sqrt{2} > 2$$

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...

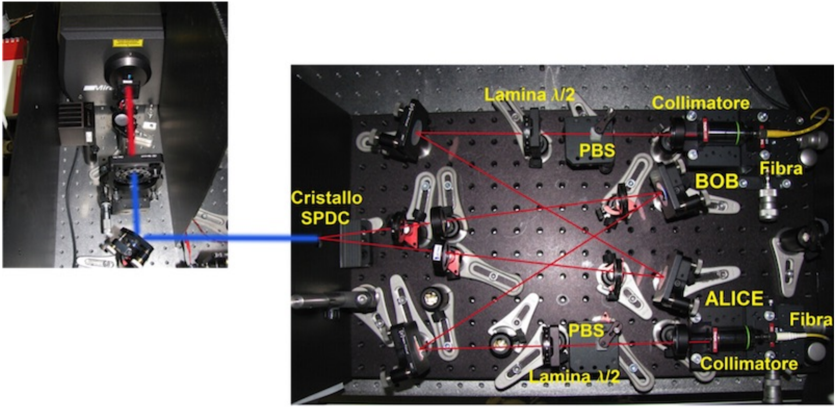
How entanglement can be generated?

Parametric down-conversion (probabilistic effect)



What is the measured value of S_{CH}?

In the lab:



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

Summary

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

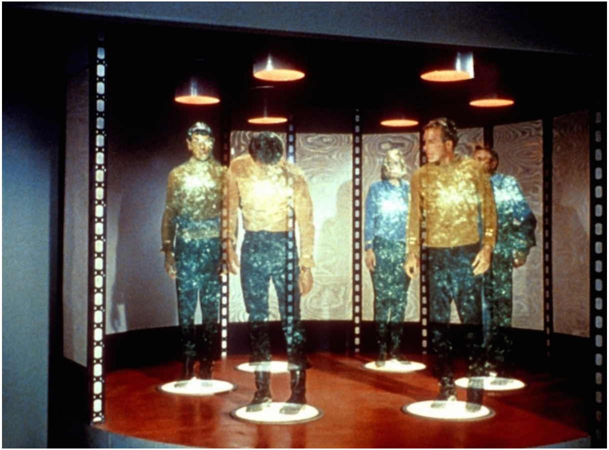
4 Entanglement and Bell inequalities

5 Protocols exploiting entanglement
- Teleportation
- “Device Independent” protocols

6 Conclusions

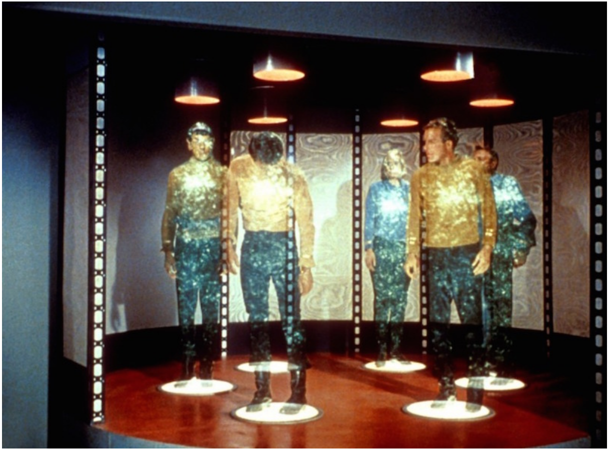
Quantum Teleportation

Like Star Trek?



Quantum Teleportation

Like Star Trek?

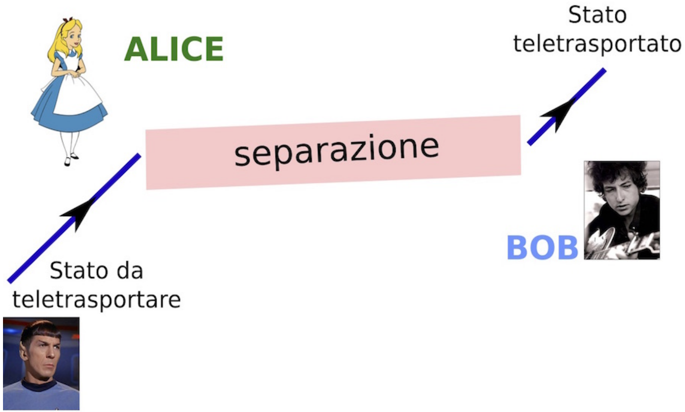


almost....

Quantum Teleportation of a qubit

IMPORTANT:

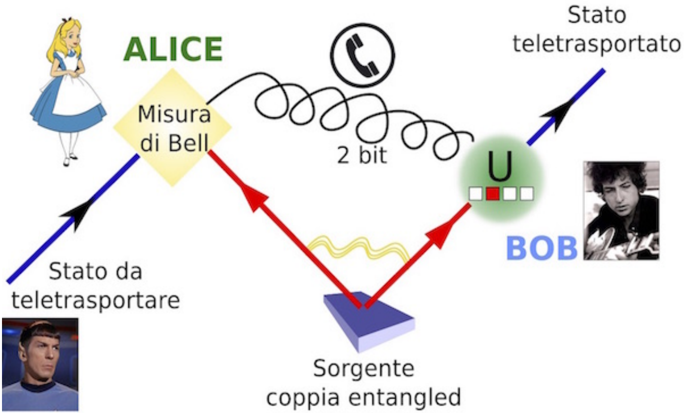
Alice does not know the state that must be teleported to Bob.
It is impossible for Alice to copy the qubit state.



Quantum Teleportation of a qubit

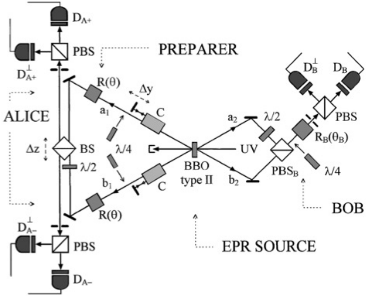
IMPORTANT:

Alice does not know the state that must be teleported to Bob.
It is impossible for Alice to copy the qubit state.

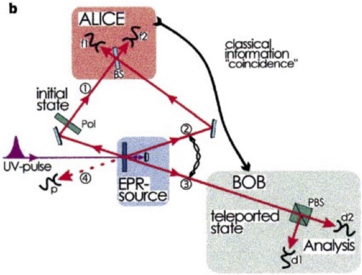


First experimental realization: 1997

Esperimento di Roma



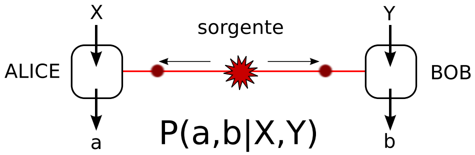
Esperimento di Vienna



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

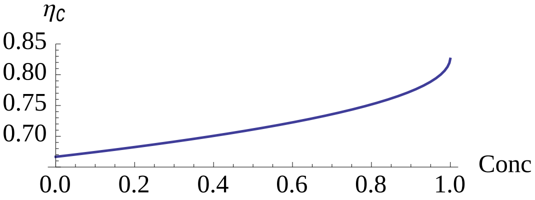
$$r = 1 - h_2(Q) - h_2[f(S_{\mathrm{CH}})]$$

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

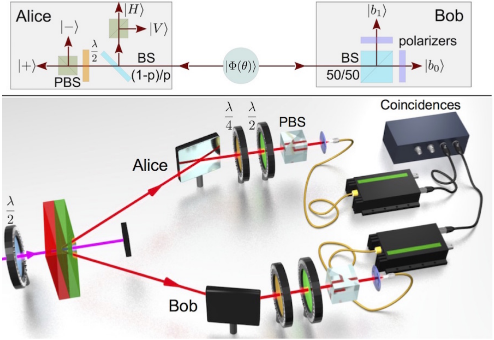
- DI protocols requires high detection efficiency in order to close the detection looholes
  - Non-maximally entangled states requires lower threshold efficiency η_c compared to maximally entangled states

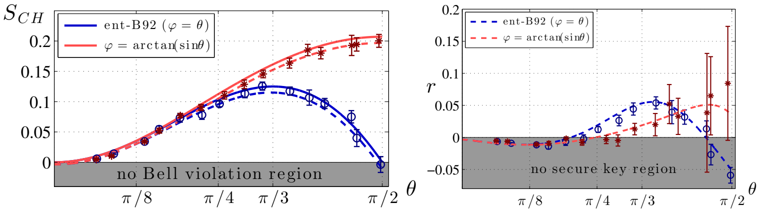


$\Rightarrow$ Define a protocol with non-maximally entangled states for DI-QKD

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

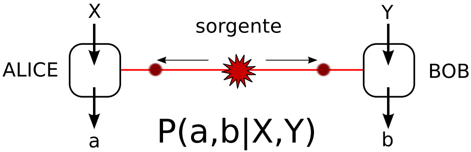
Experimental key rates





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

Device Independent QRNG



- Random bit generation rate:

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

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

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

Summary

1 Quantum Mechanics

2 Quantum Key Distribution

3 Quantum Random Number Generators

4 Entanglement and Bell inequalities

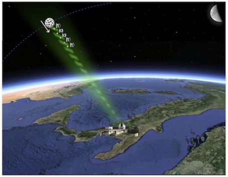
5 Protocols exploiting entanglement
- Teleportation
- "Device Independent" protocols

6 Conclusions

Conclusions

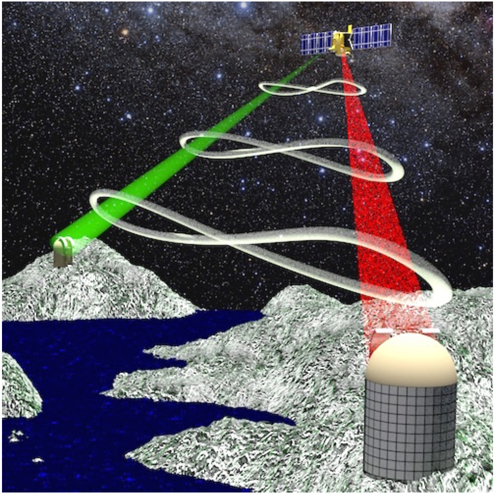
- Deep connection between fundamental physics and applications

- Quantum communications in space: towards satellite quantum network



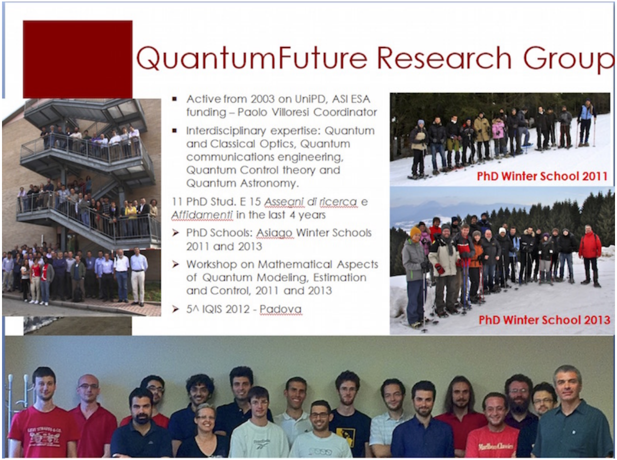
- QRNG in commercial devices

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. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, *Experimental Satellite Quantum Communications*, **Phys. Rev. Lett. (in press)**
- G. Vallone, *et. al.*, *Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels*, **Phys. Rev. A 91, 042320 (2015)**.
- 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)**.
- 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)**.