SECRET

SECuRe quantum communication based on Energy-Time/time-bin entanglement

Giuseppe (Pino) Vallone

800 1222·2022 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

INFN PADOVA
Istituto Nazionale di Fisica Nucleare
Sezione di Padova

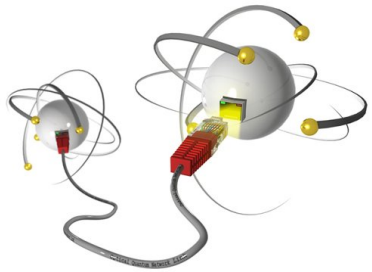
Quantum Technologies within INFN: status and perspectives

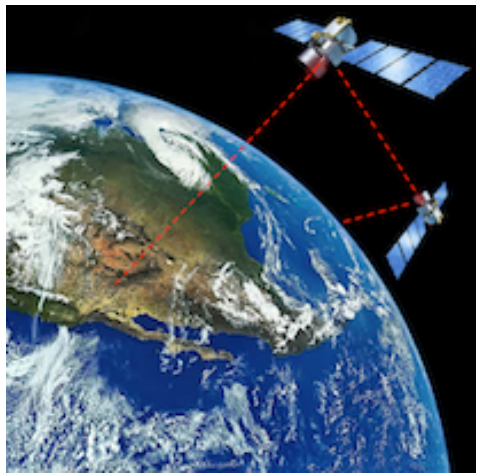
Summary

Summary

What is Quantum Communication?

- Quantum Communications is the ability of faithful transmit quantum states between two distant locations
- Creation of a quantum network
- Applications in security: QKD
- Ground QKD have progressed up to commercial stage using fiber-cables

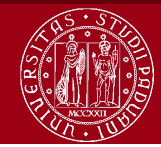




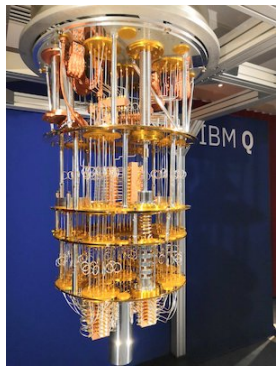
Possible issues with classical cryptography

- Classical cryptography is based on (currently) hard computational problems
- Breakthrough in classical algorithm can broke security

Possible issues with classical cryptography

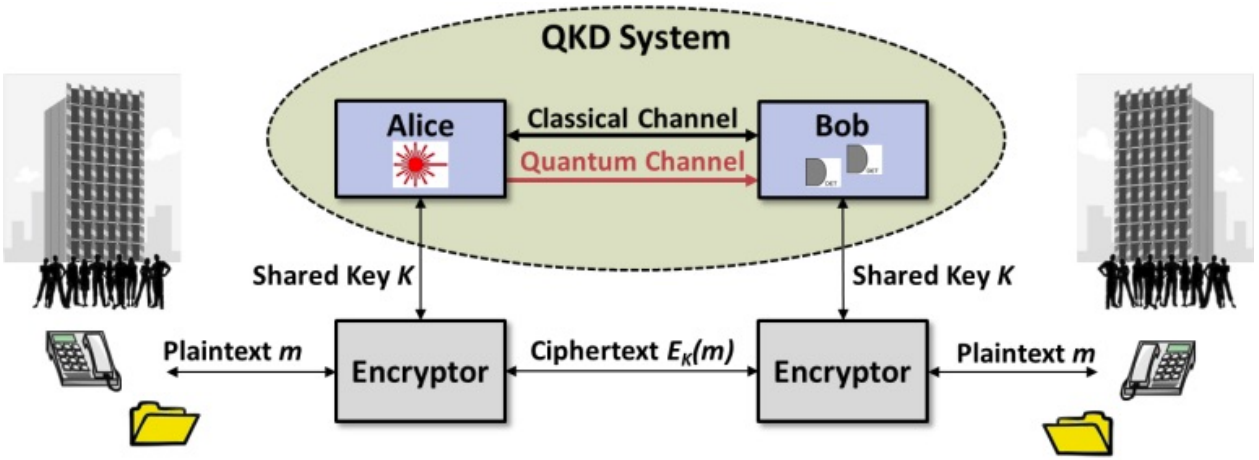


- Classical cryptography is based on (currently) hard computational problems
- Breakthrough in classical algorithm can broke security
- Quantum computer will broke some classical cryptograpic scheme (RSA)



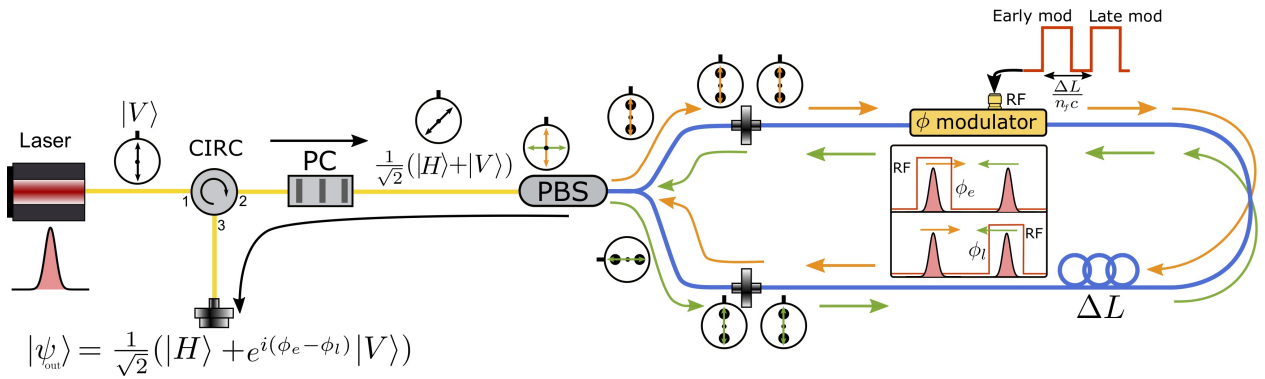
QKD: quantum key distribution

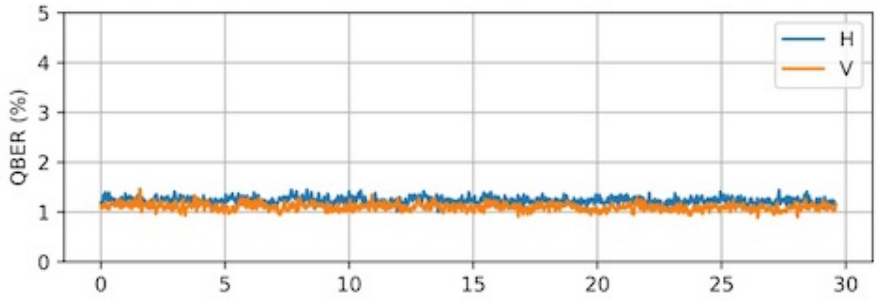
- QKD: security based on physics
- Exploit quantum mechanics laws for establishing secure keys

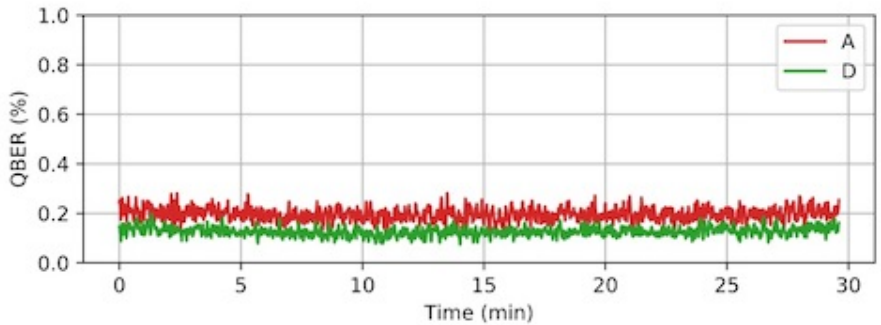


Quantum state encoder

POGNAC = POlarization saGNAC







6 May 2019

OSA The Optical Society | 100 Since 1916

New All-Fiber Device Simplifies Free-space Based Quantum Key Distribution

Robust encoder switches polarization 1 billion times a second; could facilitate global quantum encryption network

ScienceDaily

Your source for the latest research news

New all-fiber device simplifies free-space based quantum key distribution

Robust encode
bal quantum en

Date: May 6

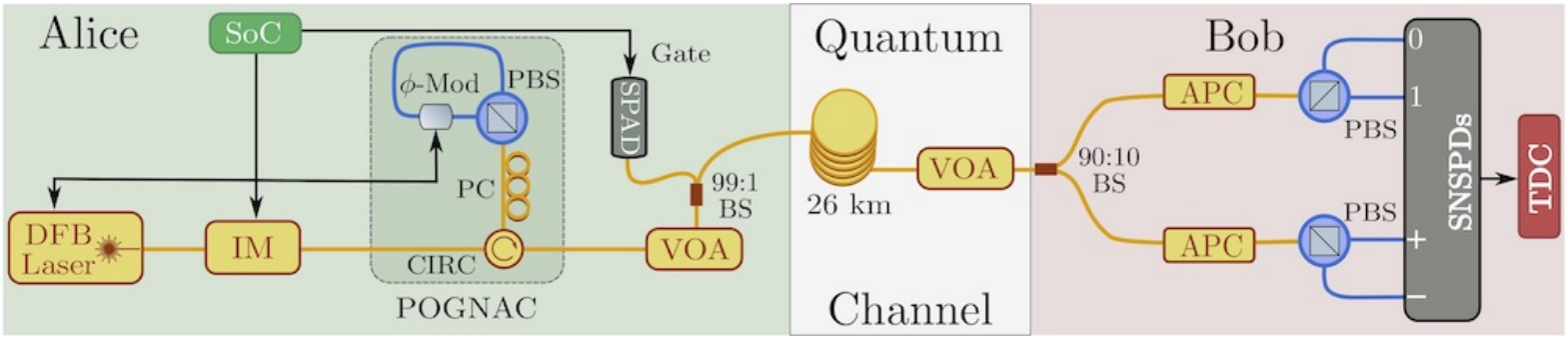
PHYS.ORG

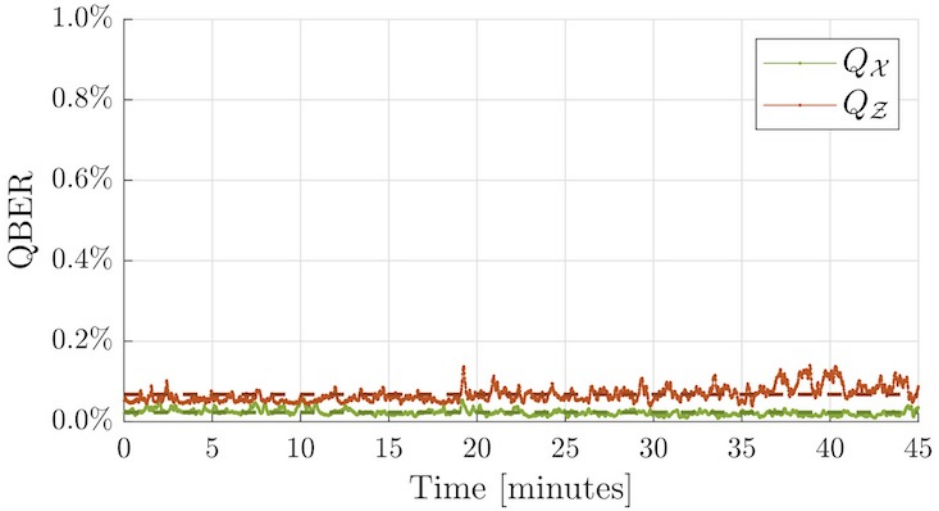
New all-fiber device simplifies free-space based quantum key distribution

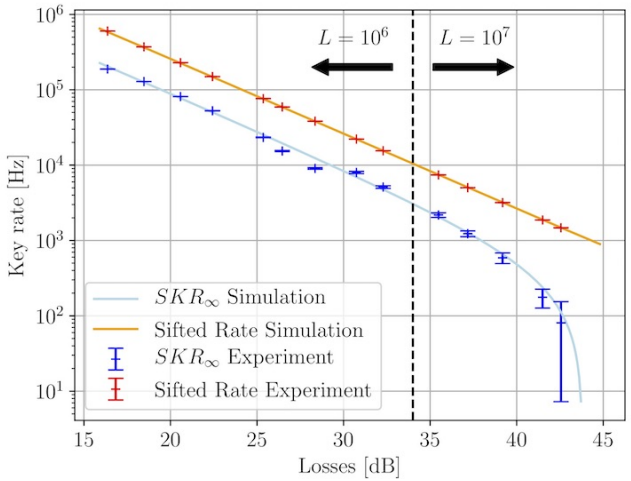
6 May 2019

C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, **GV**, *Optics Letters 44, 2398 (2019)*

Test with fiber-link







- Lowest intrinsic QBER ever reported (<0.07%)

C. Agnesi, *et. al.* **[arXiv: 1909.12703]**

Summary

QuantERA project

SECRET

Secure quantum communication based on energy-time/time-bin entanglement

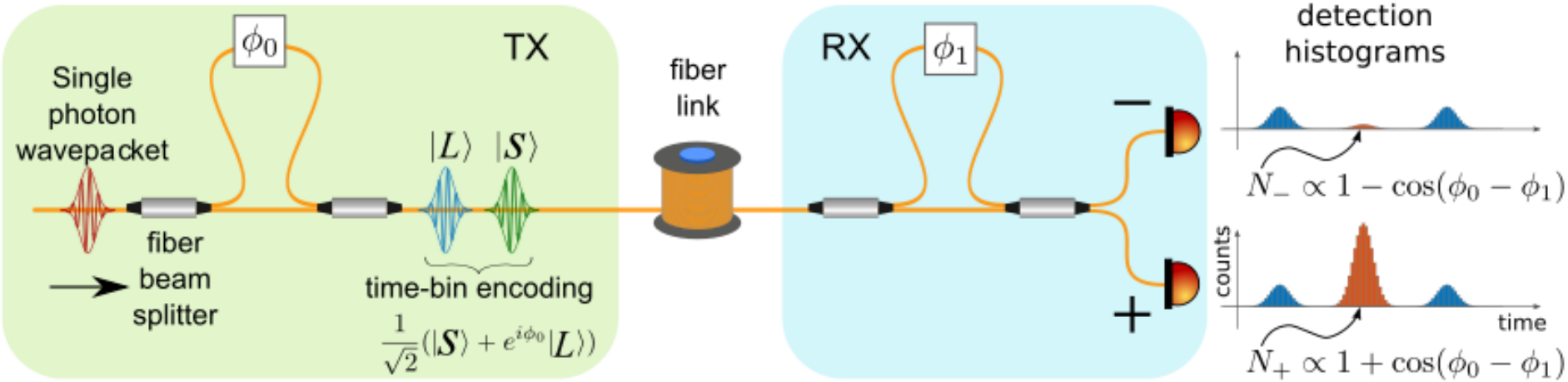
Partners:

- PI: Linköping University - **Sweden**
- INFN/UniPD - **Italy**
- Universidad de Sevilla - **Spain**

Time-bin encoding

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|S\rangle + e^{i\phi_0}|L\rangle)$$

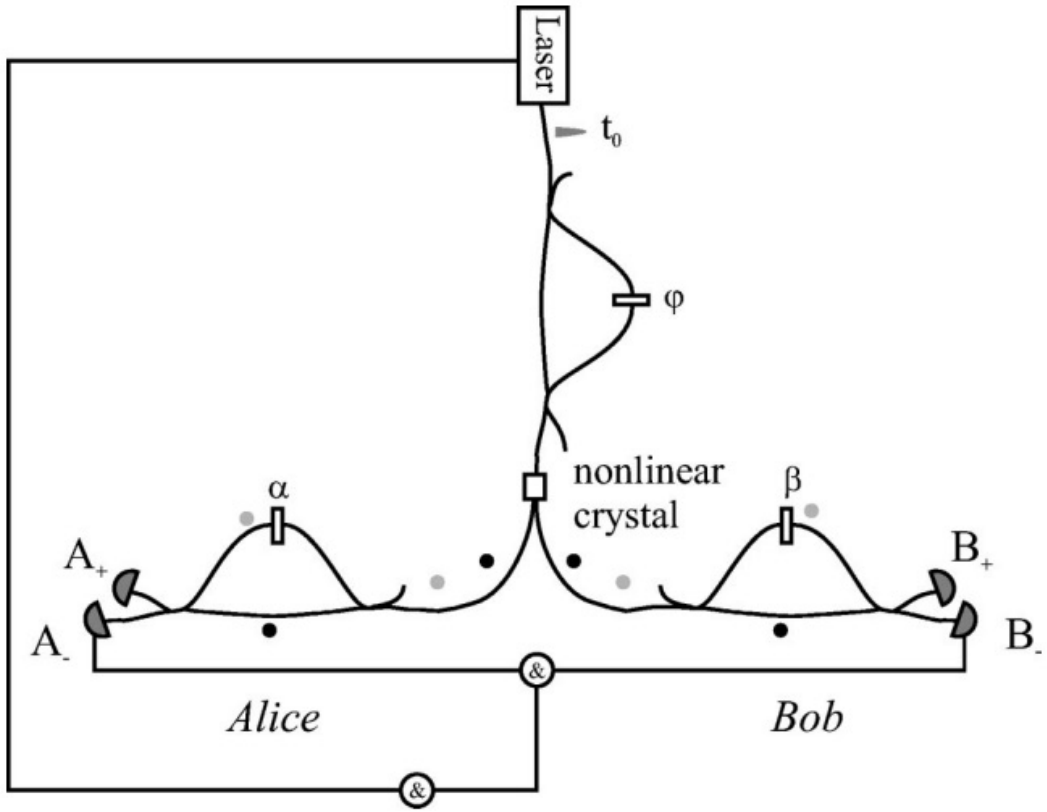
Relative phase to encode the qubit



Time-bin is robust in fiber-optic propagation!

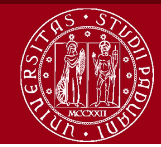
Time-bin entanglement

time-bin entanglement: $|\psi\rangle = \frac{1}{\sqrt{2}}(|S\rangle_A|S\rangle_A + e^{i\phi}|L\rangle_A|L\rangle_B)$



Phys. Rev. A 66, 062308 (2002)

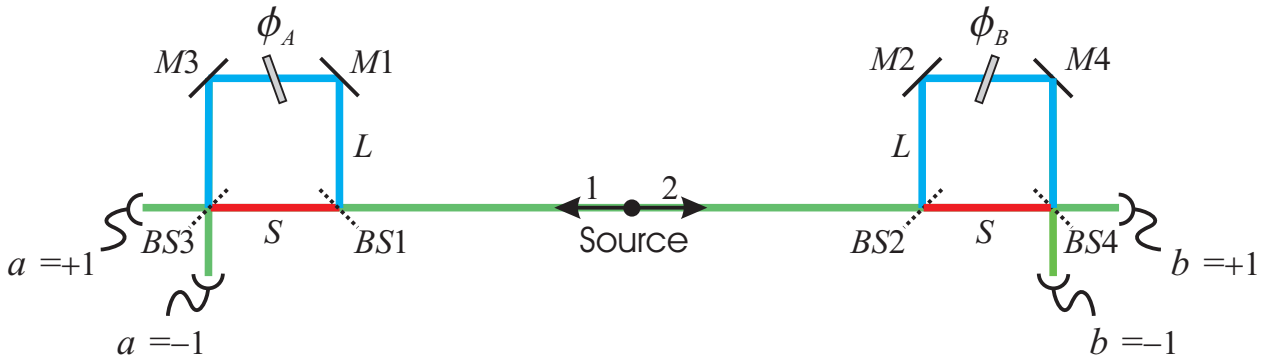
Time-bin Bell's inequality loophole



- Bell's inequality: if violated, the experiment cannot be described by a local deterministic theory.

Time-bin Bell's inequality loophole

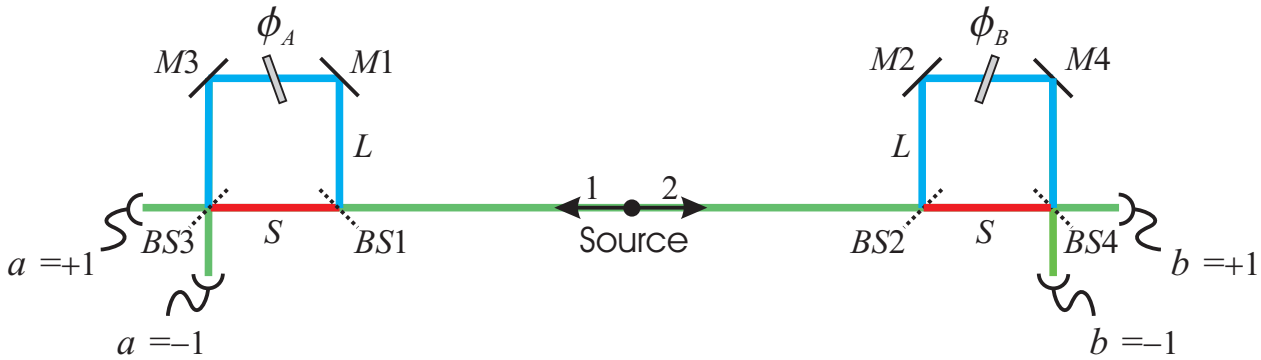
- Bell's inequality: if violated, the experiment cannot be described by a local deterministic theory.
- loophole for time-bin entanglement: the subensemble of selected events can depend on the phase settings



S. Aerts, P. G. Kwiat, J.-Å. Larsson, and M. Zükowski, Phys. Rev. Lett. 83, 2872 (1999)

Time-bin Bell's inequality loophole

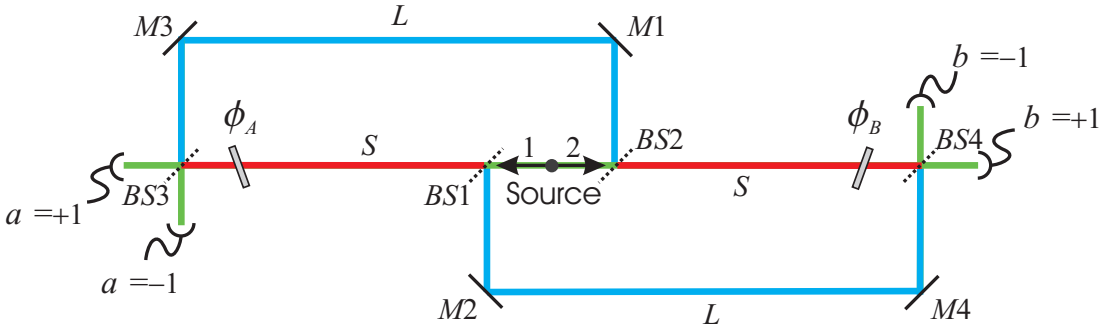
- Bell's inequality: if violated, the experiment cannot be described by a local deterministic theory.
- loophole for time-bin entanglement: the subensemble of selected events can depend on the phase settings



S. Aerts, P. G. Kwiat, J.-Å. Larsson, and M. Zükowski, Phys. Rev. Lett. 83, 2872 (1999)

- classical model is possible due to post-selection.

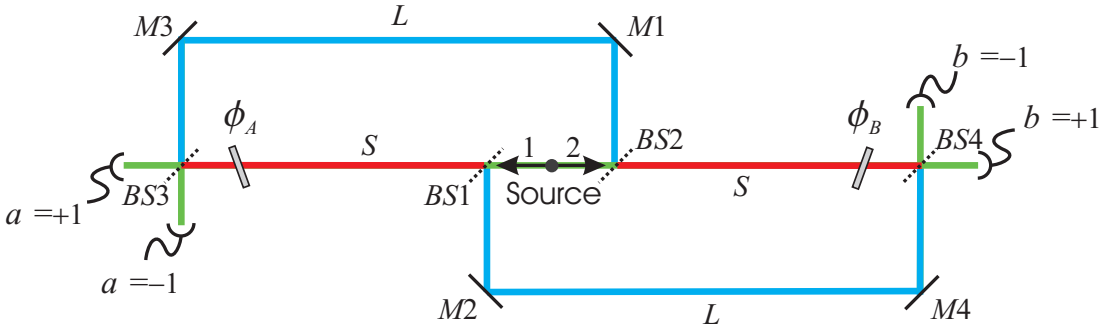
Removing the loohole



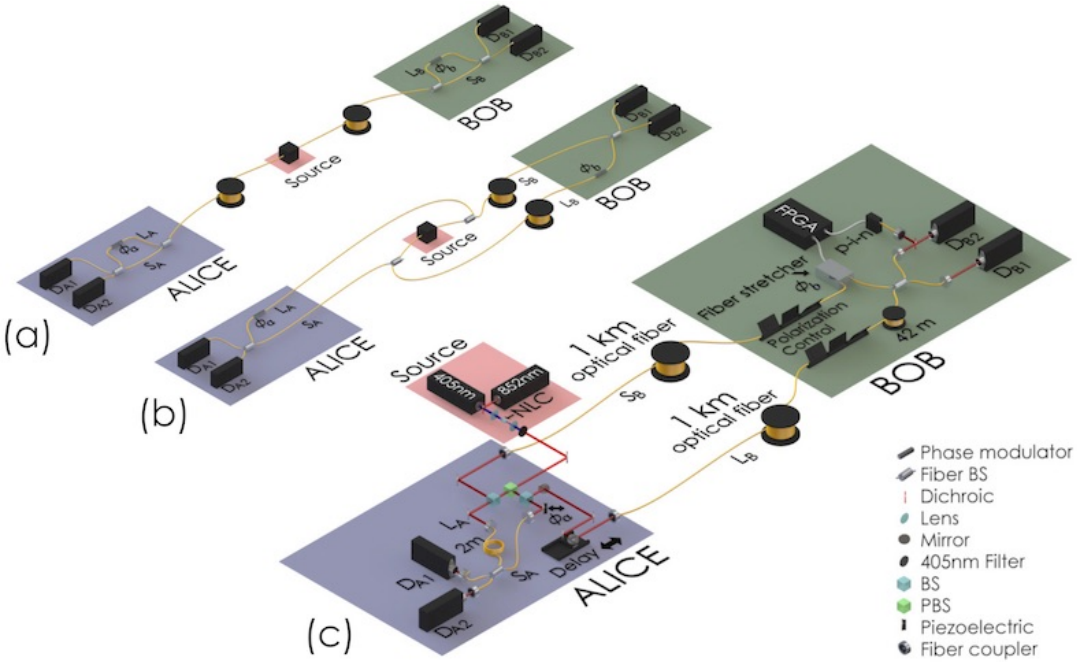
A. Cabello, A. Rossi, **GV**, F. De Martini, P, Mataloni

Phys. Rev. Lett. 102, 040401 (2009)

Removing the loohole



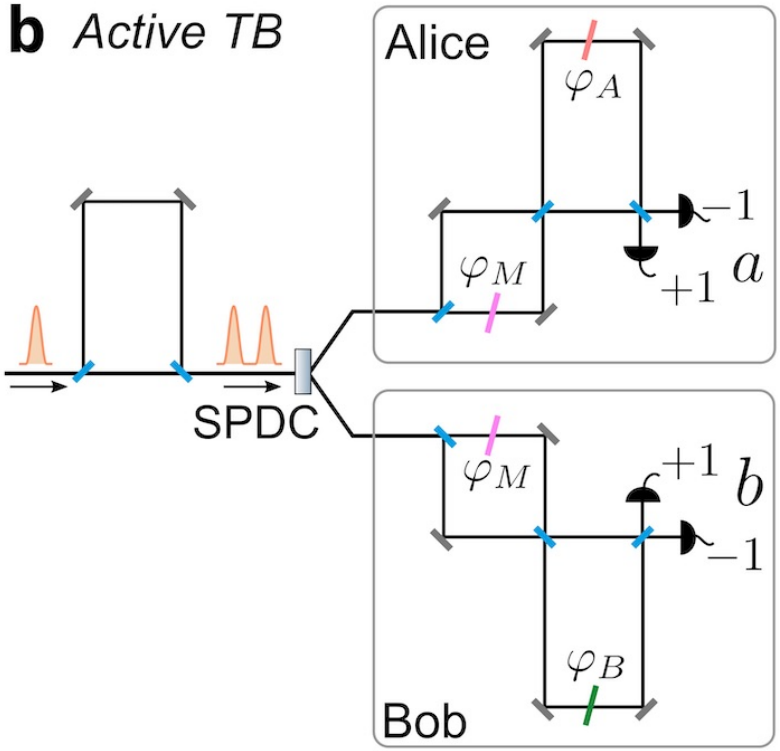
A. Cabello, A. Rossi, **GV**, F. De Martini, P, Mataloni
Phys. Rev. Lett. 102, 040401 (2009)

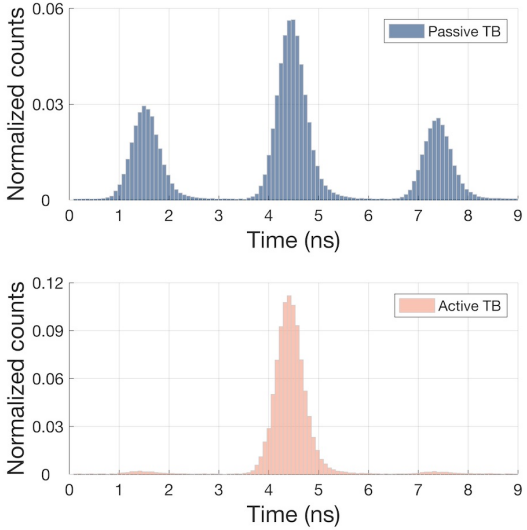


Nat. Commun. 4, 2871 (2013)
Phys. Rev. Lett. 115, 030503 (2015)

New post-selection free

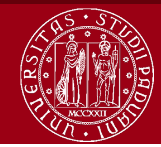
Post-selection-loophole-free Bell violation
with genuine time-bin entanglement





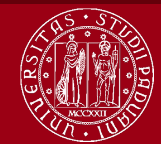
F. Vedovato, et al., Phys. Rev. Lett. 121, 190401 (2018)

SECRET project



So far, only Bell's inequality violation with genuine time-bin entanglement

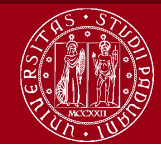
SECRET project



So far, only Bell's inequality violation with genuine time-bin entanglement

Main target of SECRET:
genuine energy-time entanglement-based quantum communication applications

SECRET project



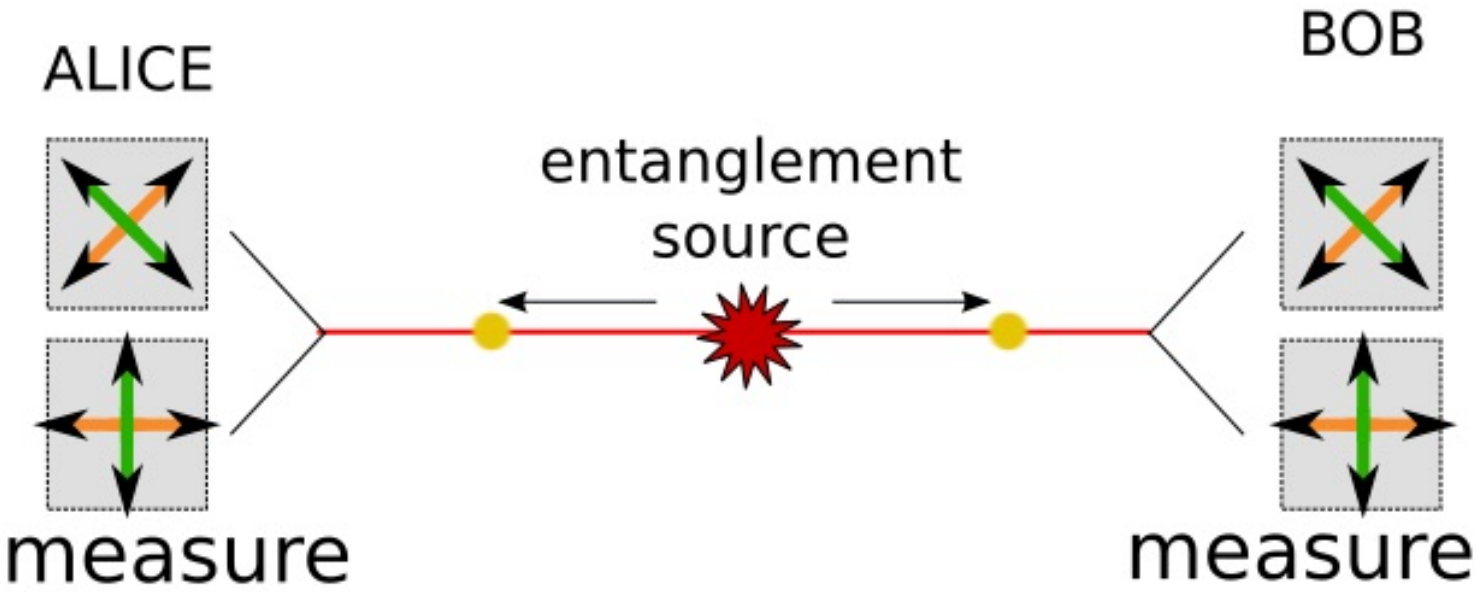
So far, only Bell's inequality violation with genuine time-bin entanglement

Main target of SECRET:
genuine energy-time entanglement-based
quantum communication applications

- **Objective 1**: Quantum communication
- **Objective 2**: entanglement swapping and/or teleportation
- **Objective 3**: integrated photonics technology

Objective 1

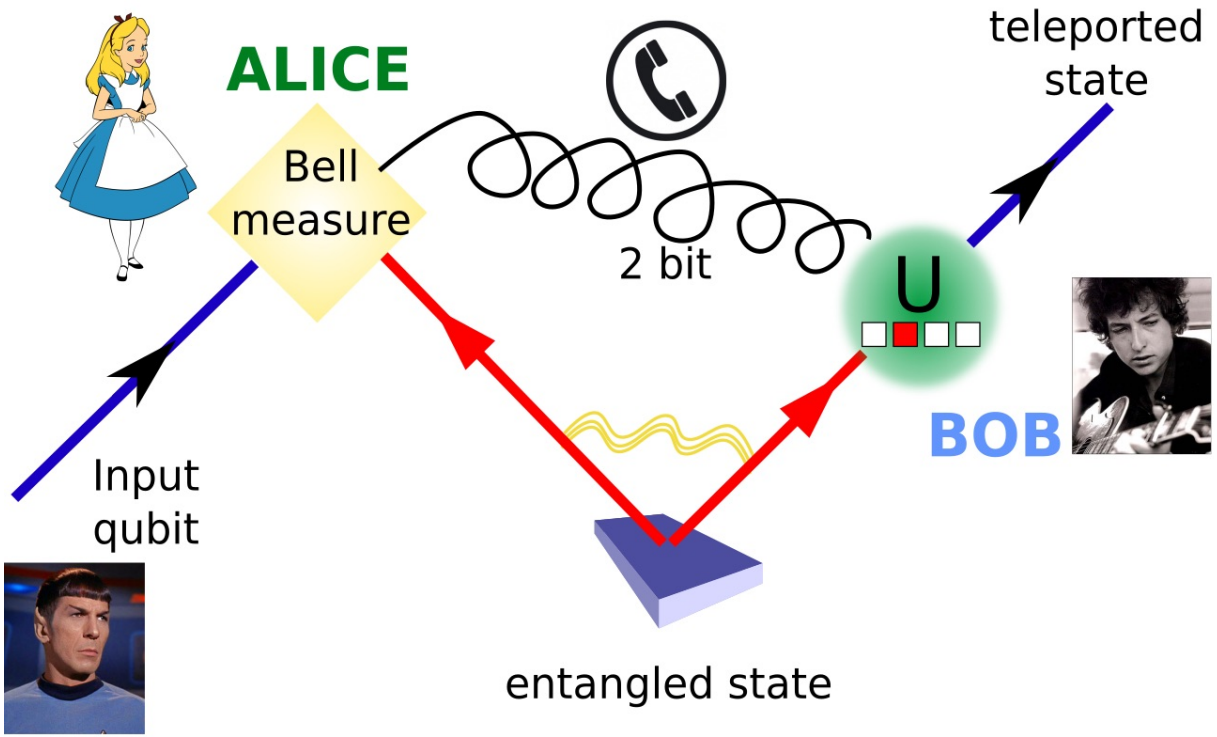
Quantum communication exploiting
ET entanglement without post-selection loophole



QKD by entangled photons with untrusted entangled-source

Objective 2

Development of novel building blocks based on genuine energy-time entanglement: entanglement swapping and/or teleportation



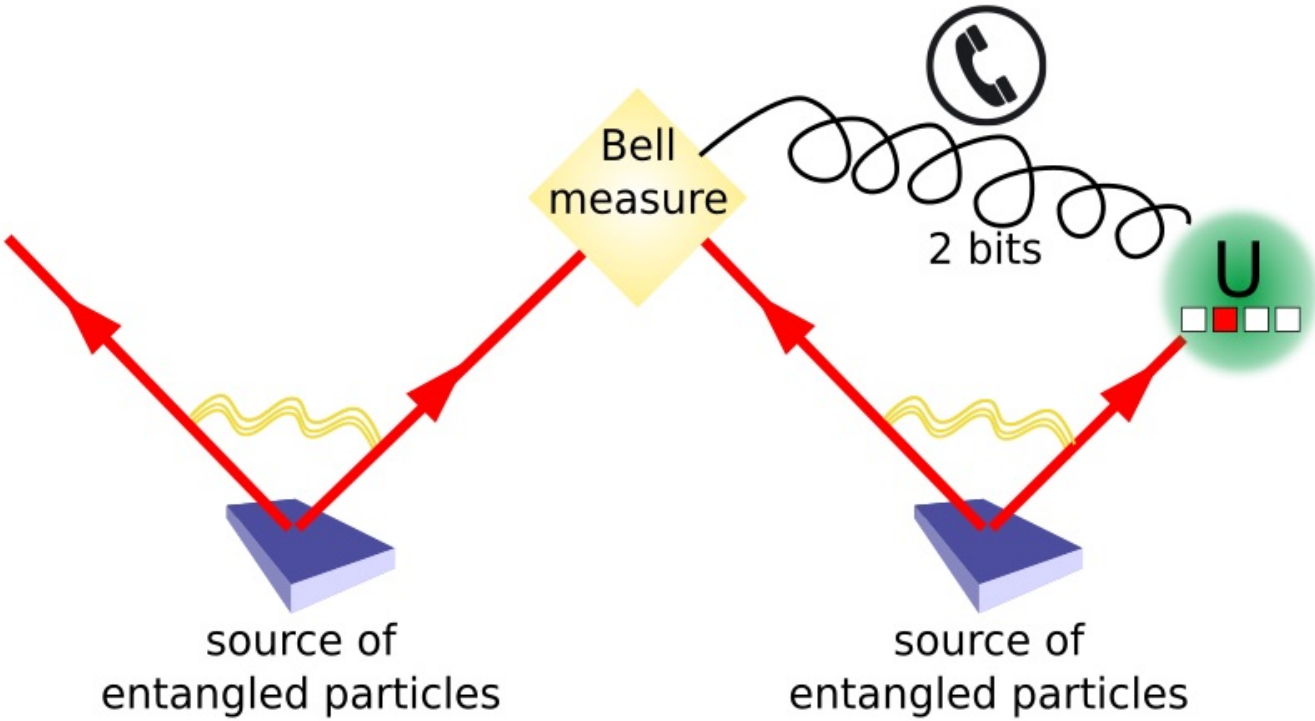
Objective 2

Development of novel building blocks based on genuine energy-time entanglement: entanglement swapping and/or teleportation

entanglement between particles that never interact

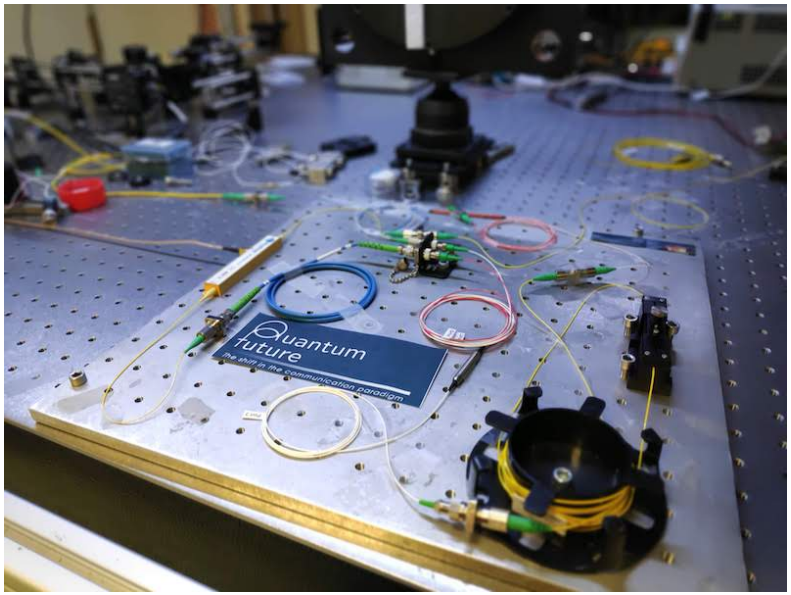
Objective 2

Development of novel building blocks based on genuine energy-time entanglement: entanglement swapping and/or teleportation

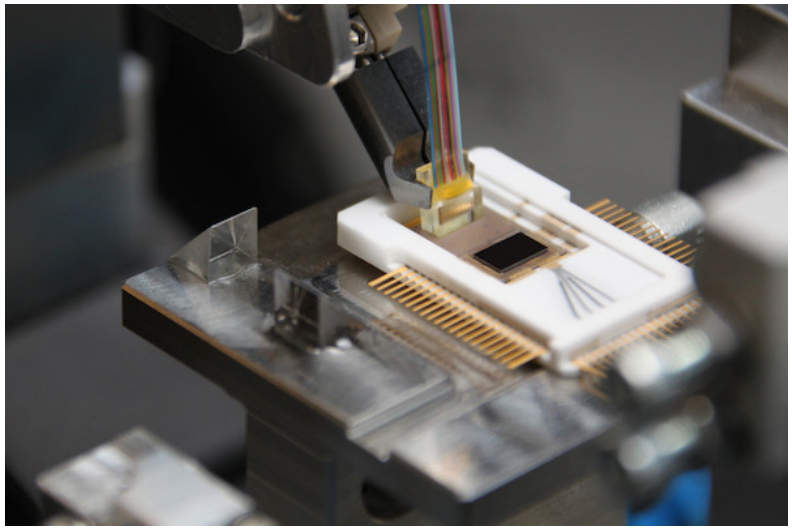


Objective 3

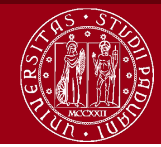
Implementation of genuine ET entanglement by using integrated photonics technology



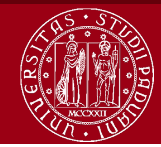
$\Rightarrow$



Summary

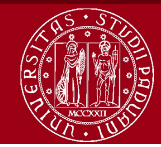


Device Independent Protocols



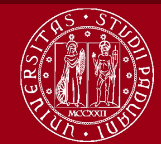
- Bell inequality introduced to rule out local deterministic theory.

Device Independent Protocols



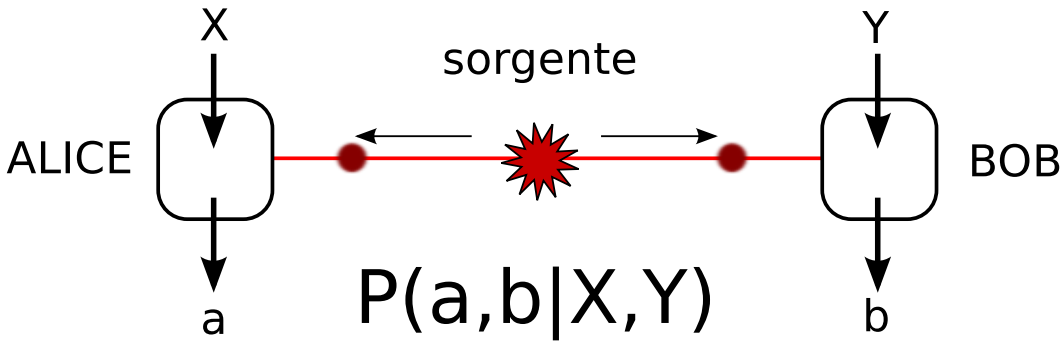
- Bell inequality introduced to rule out local deterministic theory.
- It has been violated in many different experiments (photons, ions, diamonds, atoms....) and also loophole-free violations demonstrated

Device Independent Protocols



- Bell inequality introduced to rule out local deterministic theory.
- It has been violated in many different experiments (photons, ions, diamonds, atoms....) and also loophole-free violations demonstrated
- The Bell inequality can be 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:

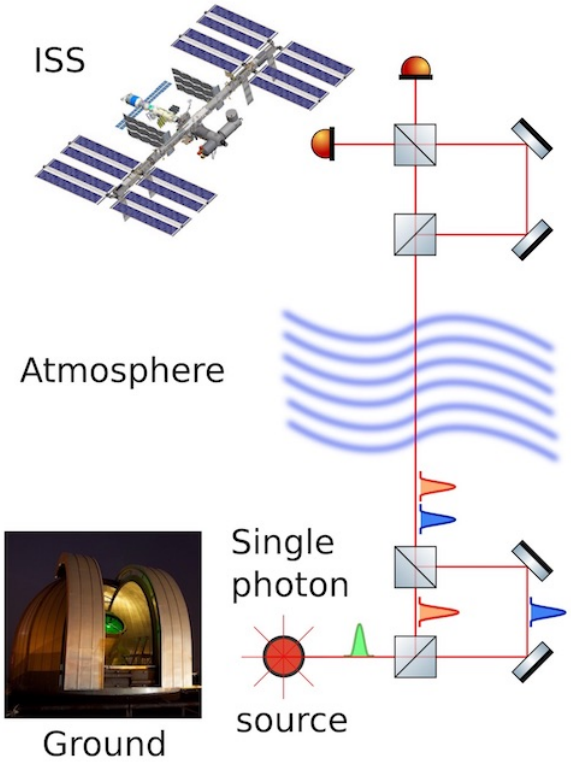
$$P(a, b|X, Y)$$

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

Phys. Rev. Lett. **98**, 230501 (2008); New Journal of Physics **11**, 045021 (2009)

Fundamental physics

Gravitational redshift with single photons



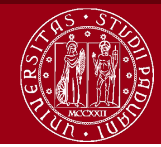
$$\lambda = 800 \text{ nm}$$
$$h \sim 400 \text{ km}$$
$$\ell = 6 \text{ km}$$

$$\Delta\phi = \frac{2\pi\ell}{\lambda}\frac{gh}{c^2} \sim 2 \text{ rad.}$$

- Possibility of measuring space-time curvature on quantum interference
- No predicted effect on photons in the Newtonian limit

Rideaut, *et al.*, Class. Quantum Grav. 29 224011 (2012)

Summary



Conclusions

- Energy-time entanglement fundamental for the future Quantum Internet: compatible with the optical fiber infrastructure

- Tool to connect quantum computers in different locations.
- Integrated photonic circuits can provide large advantages for interferometric stabilization, and speed of operation

THANK YOU FOR YOUR ATTENTION!

QuantumFuture

The shift in the communication paradigm

UNIVERSITÀ DEGLI STUDI DI PADOVA

email: vallone@dei.unipd.it

http://www.dei.unipd.it/∼vallone

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