UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

PADUA QTECH

Le tecnologie quantistiche
dai fondamenti alle comunicazioni sicure

Paolo Villoresi

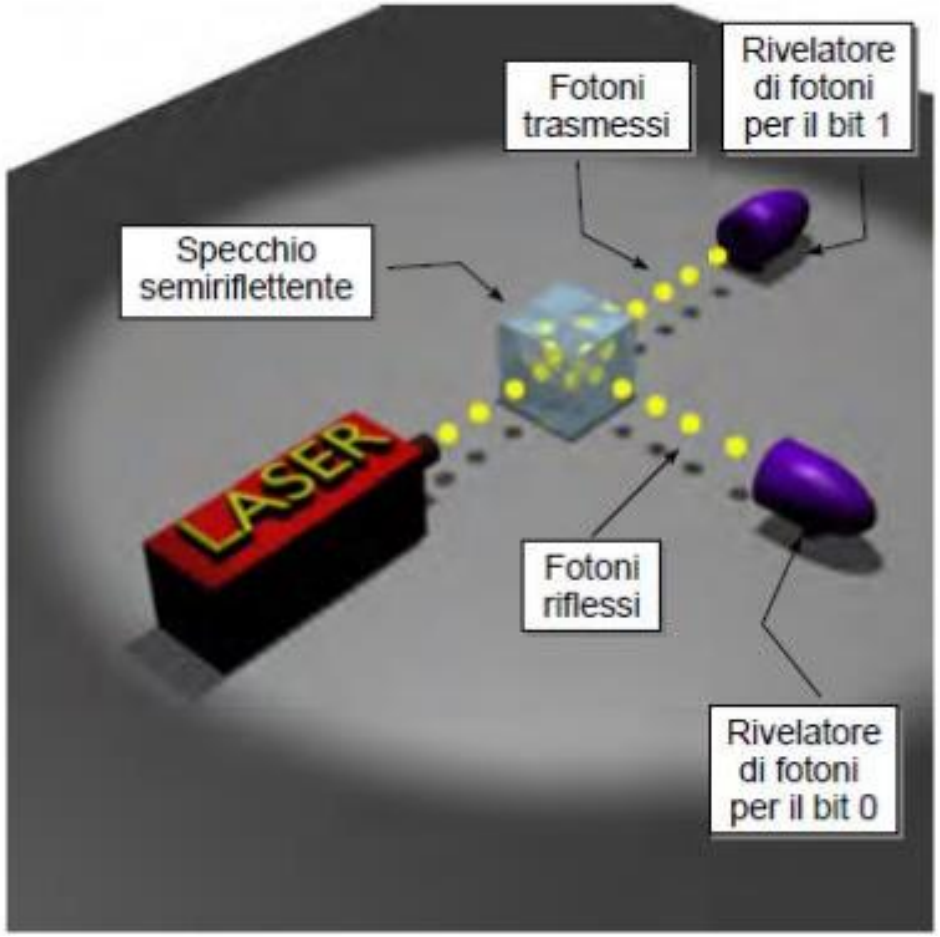
QuantumFuture Research Group
Padua Quantum Technologies Research Center
Dipartimento di Ingegneria dell'Informazione
Università di Padova

Roma 5 Novembre 2026

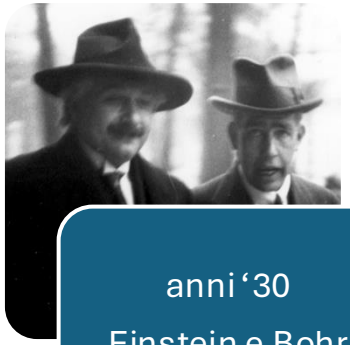


Tecnologie Quantistiche

rappresentano un settore dove si affrontano necessità di **calcolo**, di **comunicazione** e di **misura** utilizzando come **agenti** degli **stati quantistici** (atomi, quanti di luce – fotoni – ioni..)
Gli stati quantistici prendono il posto dei **bit** usati nei metodi convenzionali – *classici* – per sfruttare delle proprietà che rendono *i calcoli più semplici, rivelano i tentativi di spiare una comunicazione o garantiscono che una sequenza casuale non possa essere replicata o predetta.*



Per giungere alle tecnologie si è partiti dalla comprensione del microcosmo e la verifica delle proprietà dei suoi costituenti



anni '30

Einstein e Bohr discutono del significato degli stati quantistici



1964 il teorema di John Bell fissa un limite alle correlazioni classiche



1981 Alain Aspect misura la violazione del limite di Bell: la Natura è quantistica



fine anni '90 Anton Zeilinger realizza diversi protocolli quantistici: crittografia, teletrasporto,



fine anni '10 John Martinis realizza un prototipo di computer quantistico, ora con Michelle Simmons

Università Degli Studi di Padova

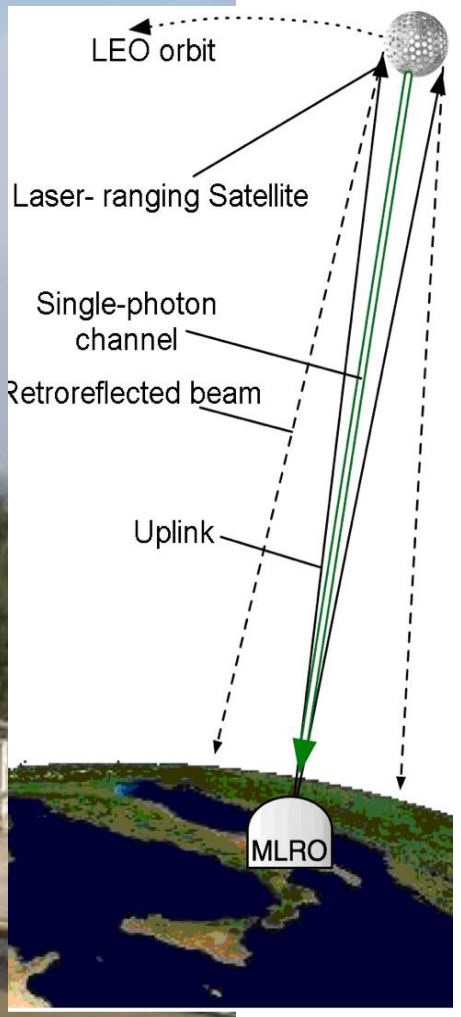
Dipartimento di Ingegneria dell'Informazione

PROGETTO Q-SPACE

QUANTUM INFORMATION AND COMMUNICATION IN SPACE

Responsabile: Dr. Paolo Villoresi, DEI

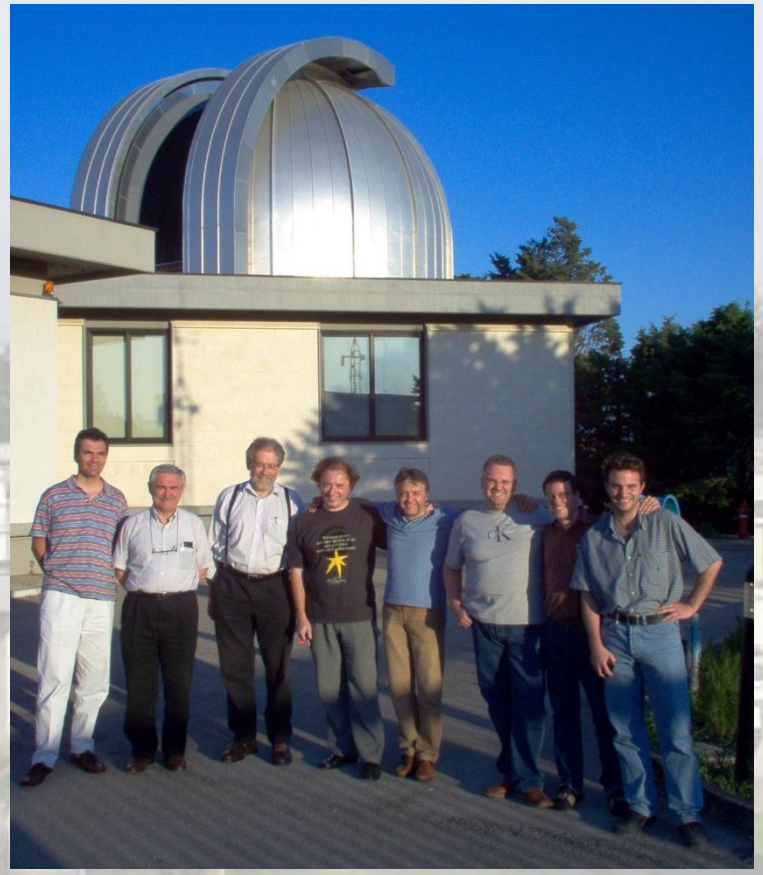
2003-2004

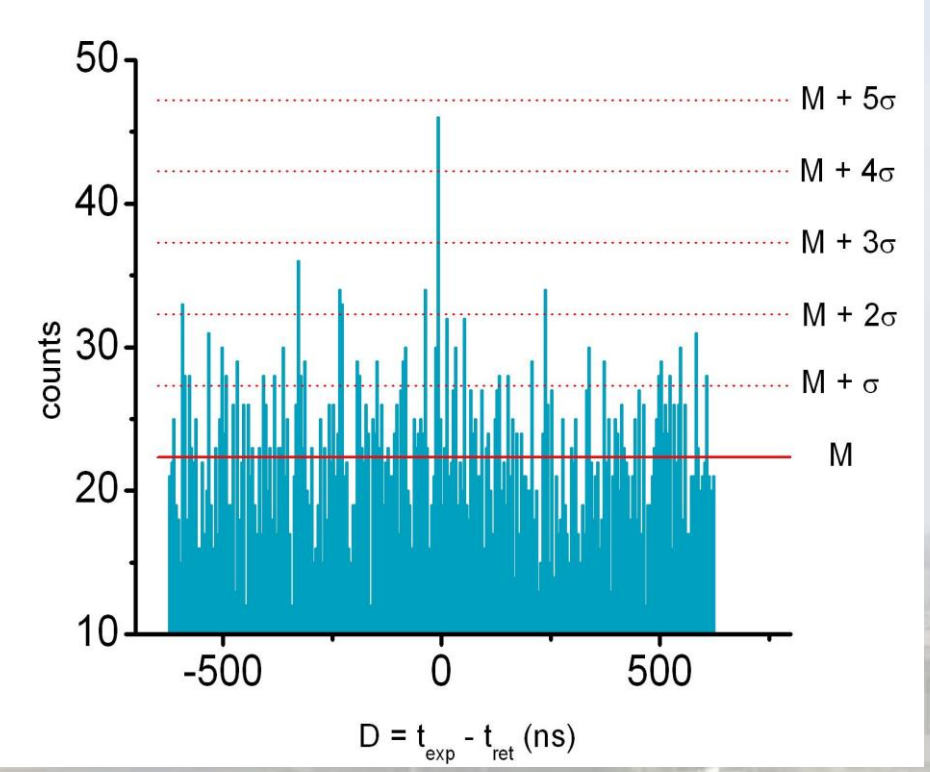


Prima dimostrazione della possibilità di scambiare stati quantistici dallo spazio a terra

Finaziamento Università di Padova, esperimenti svolti presso il Matera Laser Ranging Observatory di Matera - ASI

agenzia spaziale italiana





New Journal of Physics
The open-access journal for physics

Experimental verification of the feasibility of a quantum channel between space and Earth

P Villoresi[1,8], T Jennewein[2], F Tamburini[3], M Aspelmeyer [2,4], C Bonato[1], R Ursin[4], C Pernechele[5], V Luceri[6], G Bianco[7], A Zeilinger [2,4] and C Barbieri[3]

New Journal of Physics **10** (2008) 033038 (12pp)

QuantumFuture
The shift in the communication paradigm

Università degli Studi di Padova

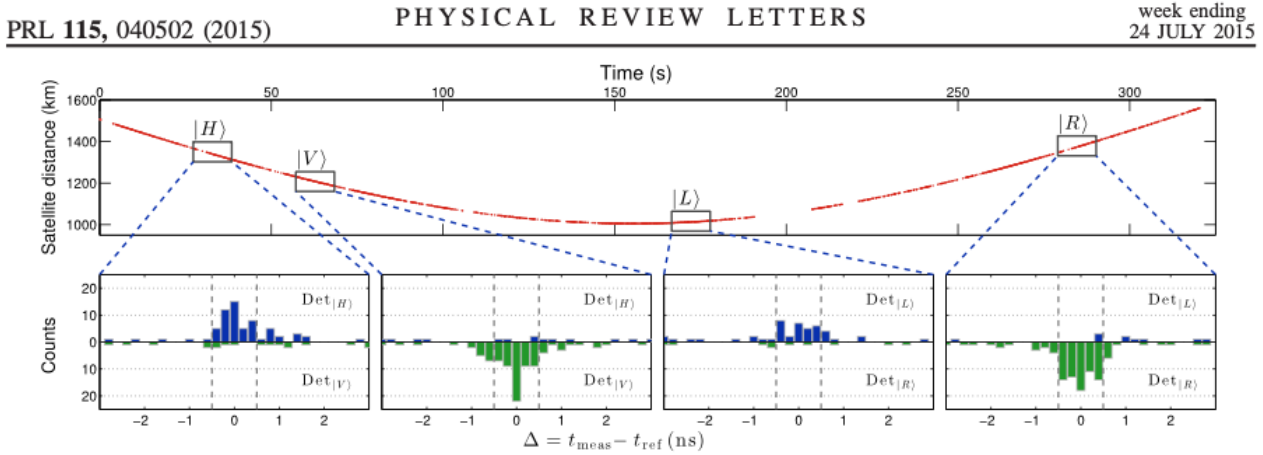
polarization qubits first result LARETS sat

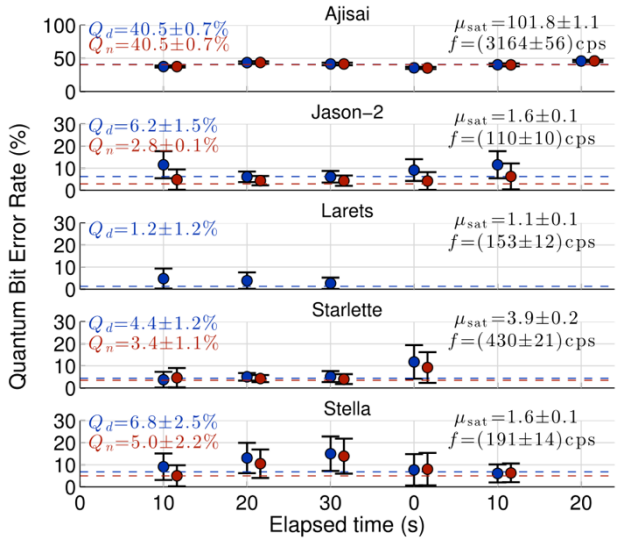




Satellite Orbit height 690 km
24 cm in diameter, 23 kg mass,
60 cube corner retroreflectors (CCR)
Metallic coating on CCR

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





***G. Vallone et al.* Experimental Satellite Quantum Communications**
PRL 115, 040502 (2015)
Return rate 147 cps - 10^4 bits/passage

agenzia spaziale italiana

The road to Space goes through Italy

SEARCH IN ASI OK

THE AGENCY | MISSIONS AND PROJECTS | NEWS | EDUCATIONAL | MULTIMEDIA | PRESS ROOM | CALLS AND OPPORTUNITIES

ASI - AGENZIA SPAZIALE ITALIANA
NEWS

NEWS
News Archive
RSS Feed

+01. EXPLORING SPACE
+02. OBSERVING THE EARTH
+03. LIVING IN SPACE
+04. ACCESSING SPACE
+05. TELECOMMUNICATIONS AND NAVIGATION



Half a century of italian space missions.
The Space history in Italy since 1964.

Home > News > Italy sends first ever quantum transmission sent by satellite

3 2 3

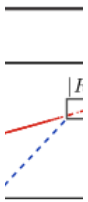
Italy sends first ever quantum transmission sent by satellite

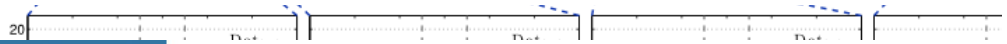
Signal sent 1700km using photons. The experiment conducted by the University of Padua and the Italian Space Agency opens the way for future hacker-proof telecommunications systems



24 June 2015
Sending secure, practically **unhackable information** a **record distance of 1700km** using **photon** bursts "shot" into space and sent back to Earth in a nanosecond, is now possible. The results were achieved by the **University of Padua** and the **ASI space geodesy facility** in Matera, which collaborated to perform the first **quantum satellite transmission** in history.

The experiment, which is currently being considered for publication by Physical Review Letters, was presented by **ASI President Roberto Battiston** at the Agency's headquarters together with **Paolo Villoresi**, leader of the Padua University team that worked on the study, **Giuseppe Vallone**, the first signature on the article entitled Experimental satellite quantum communications and **Giuseppe Bianco**, director of the ASI space geodesy facility.Battiston told the press that "there is international competition to see who can communicate the farthest using a quantum signal," and Italy "has not only **beaten the previous record of 144km by a long shot**, but did so **for the first time ever using a satellite in space**".





NewScientist Space

search New S

Home News In-Depth Articles Opinion CultureLab Galleries Topic Guides Last Word Subscribe Da

SPACE | TECH | ENVIRONMENT | HEALTH | LIFE | PHYSICS&MATH | SCIENCE IN SOCIETY

Home | Space | Physics & Math | Tech | News

First quantum transmission sent through space

› 17:53 26 June 2014 by Jacob Aron



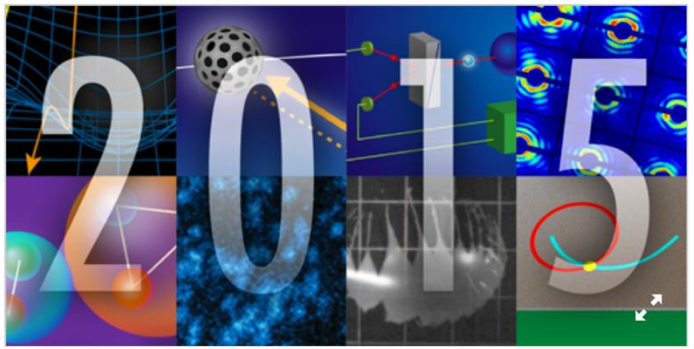
APS physics | Journals | Physics | PhysicsCentral | APS News

Physics ABOUT BROWSE JOURNALISTS

Highlights of the Year

December 18, 2015 • *Physics* 8, 126

Physics **picks its favorite stories from 2015.**



As 2015 draws to a close, we look back on the research covered in *Physics* that really made waves in and beyond the physics community

Wishing everyone an excellent 2016.

–The Editors

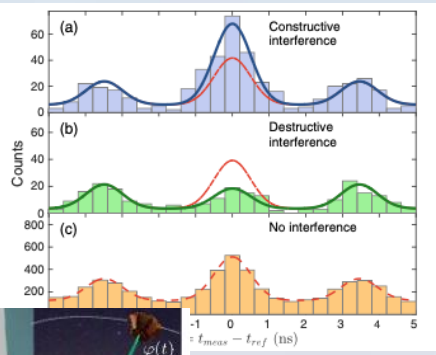
ıntum Communications

PRL 116, 253601 (2016) PHYSICAL REVIEW LETTERS week ending 24 JUNE 2016

Interference at the Single Photon Level Along Satellite-Ground Channels

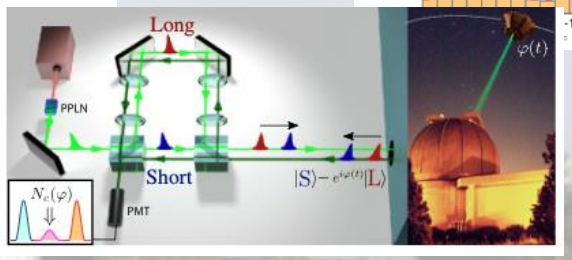
Giuseppe Vallone,[1] Daniele Dequal,[1] Marco Tomasin,[1] Francesco Vedovato,[1] Matteo Schiavon,[1] Vincenza Luceri,[2] Giuseppe Bianco,[3] and Paolo Villoresi[1,*]





time bins qubits to reveal special relativity effects

wave-particle duality tested along space-to ground links



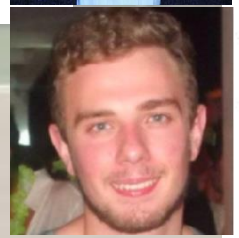
SCIENCE ADVANCES | RESEARCH ARTICLE

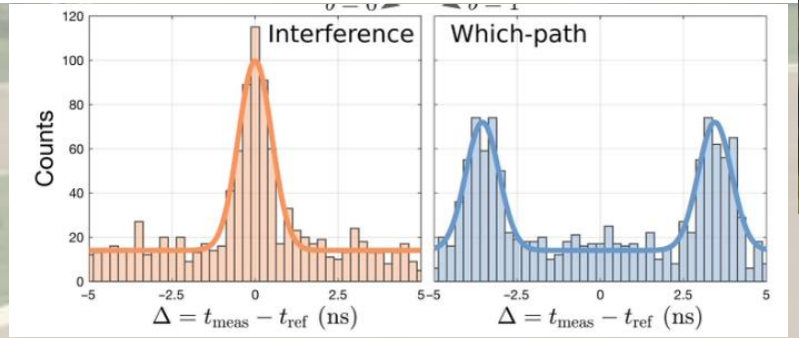
QUANTUM MECHANICS

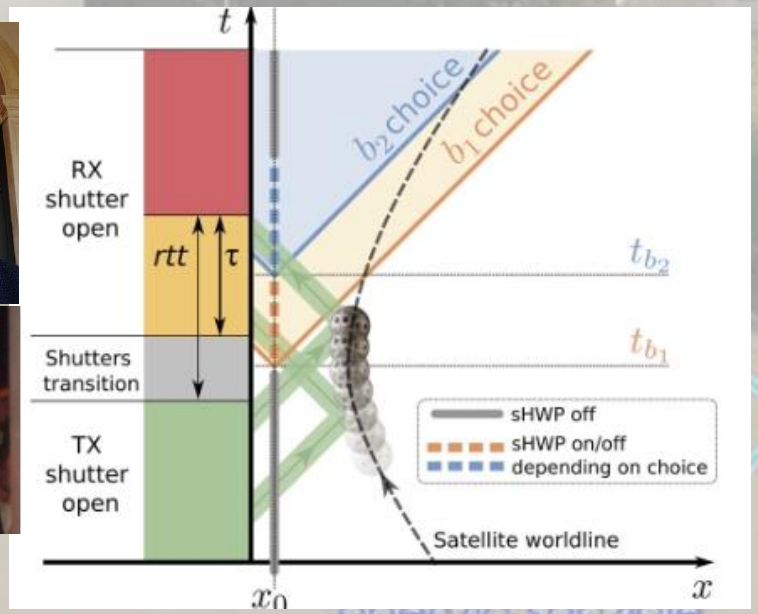
Extending Wheeler's delayed-choice experiment to space

Francesco Vedovato,[1]* Costantino Agnesi,[1]* Matteo Schiavon,[1] Daniele Dequal,[1,2] Luca Calderaro,[1] Marco Tomasin,[1] Davide G. Marangon,[1] Andrea Stanco,[1] Vincenza Luc
Giuseppe Bianco,[2] Giuseppe Vallone,[1] Paolo Villoresi[1†]



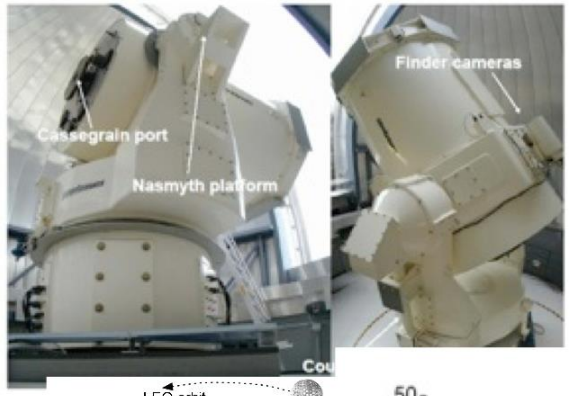


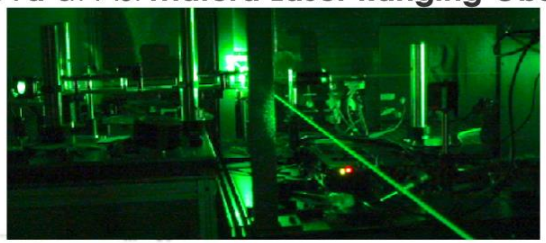


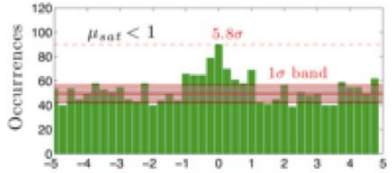


Italian Space Quantum Communications

Experimental results since 2003 by QuantumFuture Research Group of University of Padova at ASI **Matera Laser Ranging Observatory,** using its **1.5 m telescope**

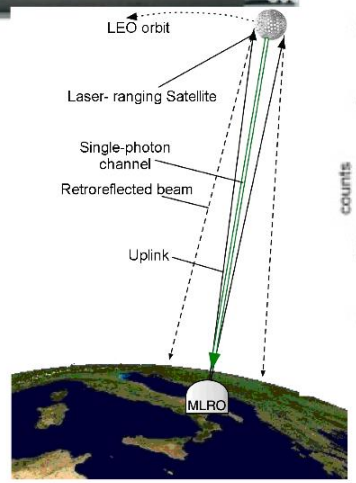


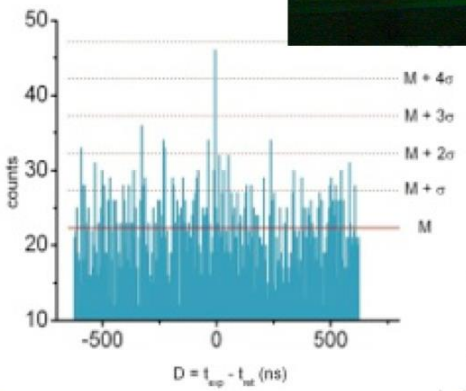




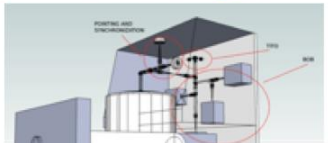


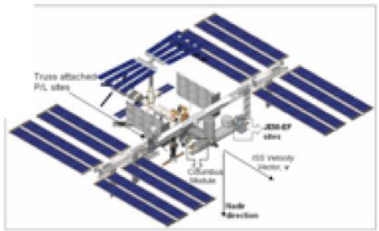


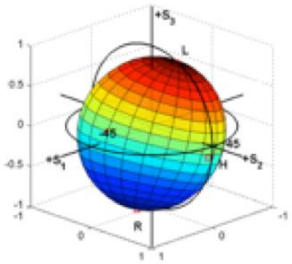




P. Villoresi et al.
New J. Phys.
10 033038 (2008)







G. Vallone et al. Phys. Rev. Lett. vol 115 040502 (2015)



2003 – UniPD SpaceQ project: single photon transceiver @ MLRO

2008 – first single-photon return from Ajisai announced

2009 ASI Feasibility study Q payload for the ISS

2009-2011 Characterizati on of MLRO Mueller Matrix

2012 - Analysis of response for different satellites CCR

2013 state preparation and analysis, satellite synch

2014 – Q-Comm on satellites demonstrated

2015 Temporal modes demonstrated in satellite qubit

2016 – New limit in single photon exchange at 7000 km

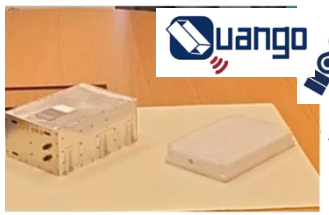
2017-Testing wave-particle duality in Space

2018 New limit in single photon exchange from MEO 20000 km

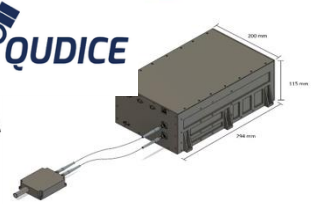
2019 sub-ns resolution - daylight free-space QKD

2020 daylight QComms and <0.001 QBER





A




Quantum Manifesto
A New Era of Technology
May 2016
http://qurope.eu/manifesto

The Guardian
Eur
News | Opinion | Sport | Culture | Lifestyle
World Europe US news Americas Asia Australia Middle East Africa Inequality Global develop

The NSA files

This article is more than 13 years old

NSA monitored calls of 35 world leaders after US official handed over contacts

- Agency given more than 200 numbers by government official
- NSA encourages departments to share their 'Rolodexes'
- Surveillance produced 'little intelligence', memo acknowledges

(C) Customers Can Help SID Obtain Targetable Phone Numbers

FROM: [redacted] and [redacted]
A&P Staff's Access Interface Portfolio (S203A)
Run Date: 10/27/2006

(C) From time to time, SID is offered access to the personal contact databases of US officials. Such "rolodexes" may contain contact information for foreign political or military leaders, to include direct line, fax, residence and cellular numbers.

The NSA memo suggests that such surveillance was not isolated as the agency routinely monitors world leaders. Photograph: Guardian

James Ball

Fri 25 Oct 2013 08.50 CEST

The Guardian
Eur
News | Opinion | Sport | Culture | Lifestyle
World Europe US news Americas Asia Australia Middle East Africa Inequality Global develop

Angela Merkel

This article is more than 13 years old

Angela Merkel's call to Obama: are you bugging my mobile phone?

Germany sees credible evidence of US monitoring of chancellor as NSA surveillance row intensifies
Live coverage of reaction to reports of Merkel surveillance

Ian Traynor *in Brussels,* Philip Oltermann *in Berlin, and* Paul Lewis *in Washington*

Thu 24 Oct 2013 09.10 CEST

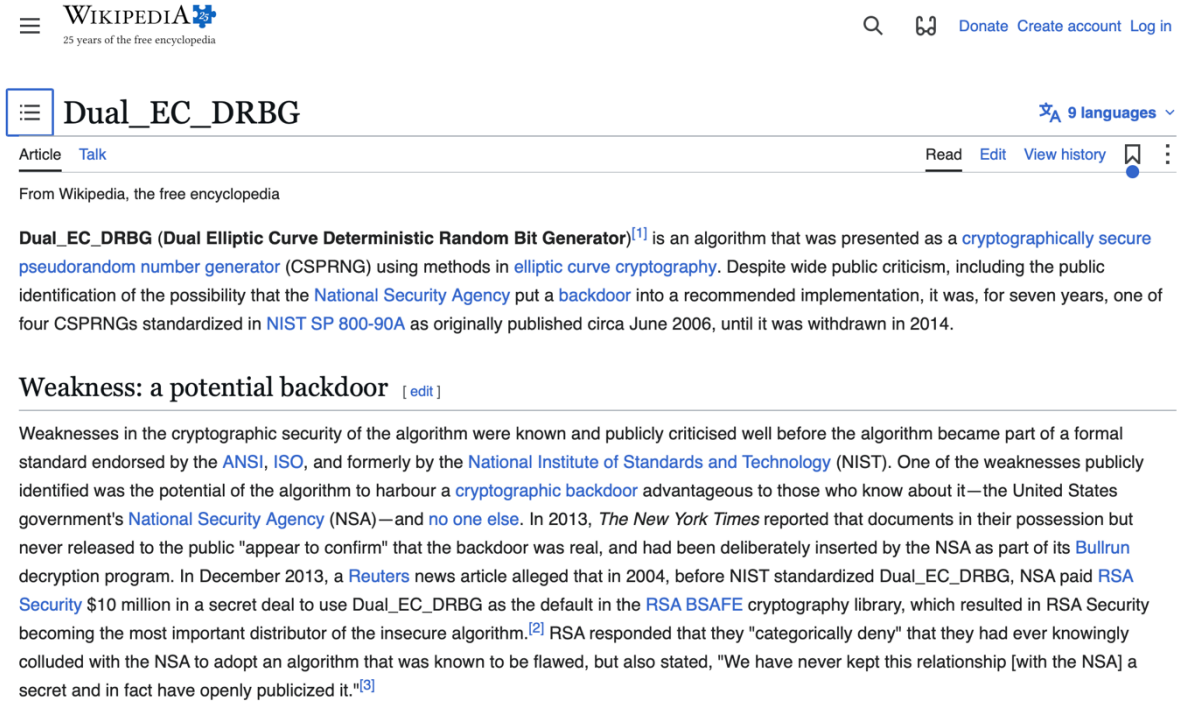


NOT SO RANDOM NUMBERS

Report: NSA paid RSA to make flawed crypto algorithm the default

The NSA apparently paid RSA $10M to use Dual EC random number generator.

ARS STAFF – 20 DIC 2013 23:14 | 87



WIKIPEDIA
25 years of the free encyclopedia

Donate Create account Log in

Dual_EC_DRBG

9 languages

Article Talk Read Edit View history

From Wikipedia, the free encyclopedia

Dual_EC_DRBG (**Dual Elliptic Curve Deterministic Random Bit Generator**)[1] is an algorithm that was presented as a cryptographically secure pseudorandom number generator (CSPRNG) using methods in elliptic curve cryptography. Despite wide public criticism, including the public identification of the possibility that the National Security Agency put a backdoor into a recommended implementation, it was, for seven years, one of four CSPRNGs standardized in NIST SP 800-90A as originally published circa June 2006, until it was withdrawn in 2014.

Weakness: a potential backdoor [edit]

Weaknesses in the cryptographic security of the algorithm were known and publicly criticised well before the algorithm became part of a formal standard endorsed by the ANSI, ISO, and formerly by the National Institute of Standards and Technology (NIST). One of the weaknesses publicly identified was the potential of the algorithm to harbour a cryptographic backdoor advantageous to those who know about it—the United States government's National Security Agency (NSA)—and no one else. In 2013, *The New York Times* reported that documents in their possession but never released to the public "appear to confirm" that the backdoor was real, and had been deliberately inserted by the NSA as part of its Bullrun decryption program. In December 2013, a Reuters news article alleged that in 2004, before NIST standardized Dual_EC_DRBG, NSA paid RSA Security $10 million in a secret deal to use Dual_EC_DRBG as the default in the RSA BSAFE cryptography library, which resulted in RSA Security becoming the most important distributor of the insecure algorithm.[2] RSA responded that they "categorically deny" that they had ever knowingly colluded with the NSA to adopt an algorithm that was known to be flawed, but also stated, "We have never kept this relationship [with the NSA] a secret and in fact have openly publicized it."[3]

UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

Thierry Breton

COMMISSIONER (2019-2024)



Internal Market

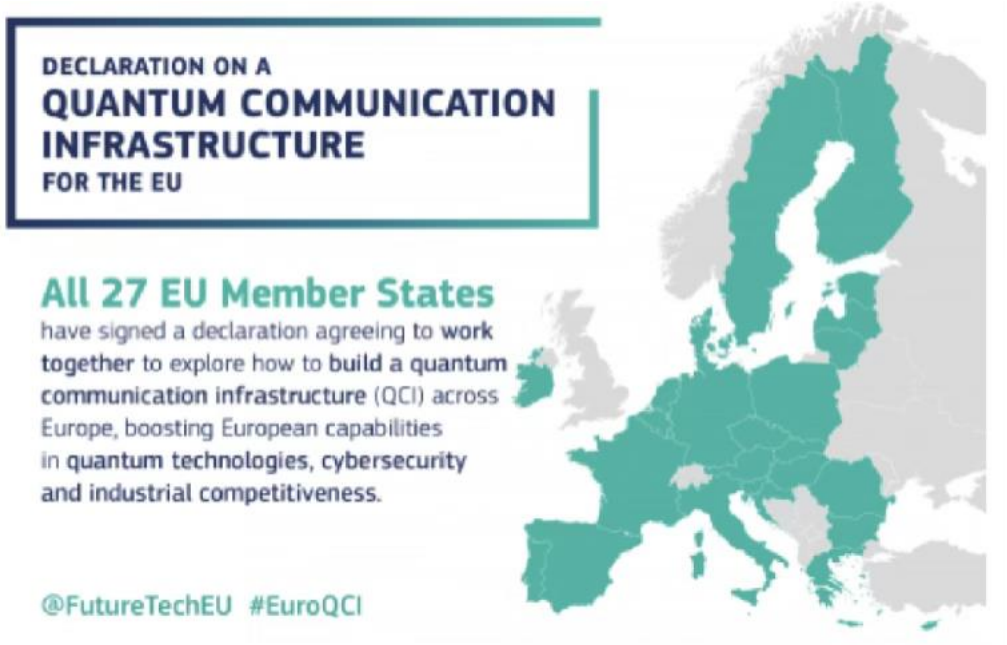
European Commission > Strategy > Shaping Europe's digital future > News >

Shaping Europe's digital future

DIGIBYTE | 13 June 2019

The future is quantum: EU countries plan ultra-secure communication network





EUROPEAN QUANTUM TECHNOLOGIES
FUNDING OPPORTUNITIES

erc

MARIE CURIE ACTIONS

HORIZON EUROPE
2021-2027

RESEARCH BASED

HORIZON EUROPE

QUANTUM FLAGSHIP

Bring quantum **technologies** from the **lab** to the **market** and consolidate European scientific **leadership** in quantum research

- **FUNDAMENTAL R&D**
- **TECHNOLOGY SUPPLY**

QSN PARTNERSHIP

QUANTUM FLAGSHIP

DIGITAL EUROPE
DIGITAL SKILLS, CYBERSECURITY, SUPERCOMPUTING

INFRASTRUCTURES

DIGITAL EUROPE

ADVANCED DIGITAL SKILLS

Develop short term **training courses** and **Master programmes** in key capacity areas

QUANTUM COMMUNICATION INFRASTRUCTURE (EuroQCI)

Build and **deploy** in the next decade a certified secure pan-European end-to-end QCI for **cybersecurity services**

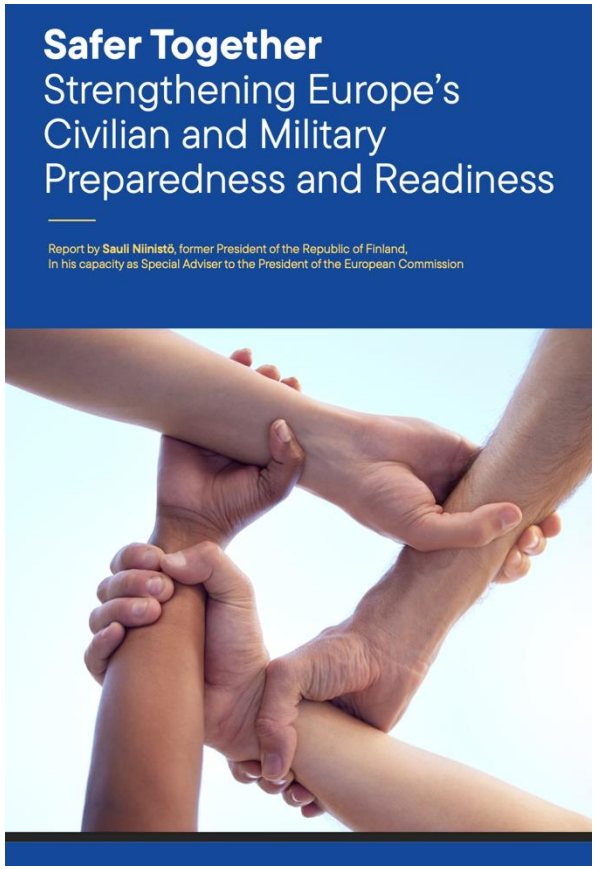
- **QKD INFRASTRUCTURE**
- **TESTING OF CROSS-BORDER QCI LINKS**

QUANTUM COMPUTING INFRASTRUCTURE (EuroHPC)

Build and **deploy** an infrastructure for big data, artificial intelligence, high performance computing, among others

- **QT/HPC HYBRID**
- **QUANTUM SIMULATION/ COMPUTATION**

Evoluzione Europea del contesto nelle comunicazioni sicure



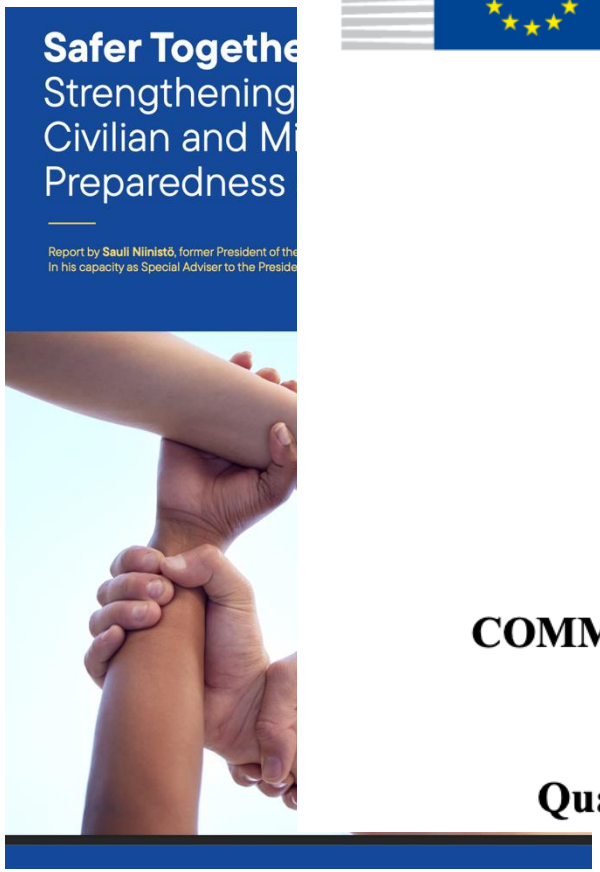
→ The race to control disruptive technologies will intensify.

Disruptive technologies can shift economic performance to a higher level. Controlling them can add to the arsenal for power and global influence. The pace of innovation, spurred on by AI-enabled technologies, will only further rise. Disruptive technologies offer untold possibilities, but also come with **new vulnerabilities and security concerns**. Unmanned air and naval systems, enabled by artificial intelligence, will further **change our societies as well as the nature of warfare**. Quantum computing can set off a new wave of innovation, while posing severe risks to encryption keys used worldwide.

In particular in view of geopolitical confrontations, the EU needs to be more resilient and to minimise **external dependencies in critical sectors that are vital for society in crisis situations.** This requires the EU to focus even more on **regaining and strengthening its innovative and competitive edge**, while stepping up its work to enhance supply chain resilience and to de-risk unwanted dependencies. The Union needs to protect its science and technology potential and **safeguard its ability to access, develop, operate, control, produce and secure critical goods and technologies, including those related to military capabilities.**

https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

Evoluzione Europea del contesto nelle



EUROPEAN
COMMISSION

Brussels, 2.7.2025
COM(2025) 363 final

r level. Controlling them
innovation, spurred on by
untold possibilities, but also
naval systems, enabled by
ture of warfare. Quantum
s to encryption keys used

nore resilient and to mini-
y in crisis situations. This
novative and competitive
de-risk unwanted depen-
and **safeguard its ability**
oods and technologies,

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Quantum Europe Strategy: Quantum Europe in a Changing World

https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

Padua Quantum Technologies Research Center

L'obiettivo primario di QTech è la ricerca nel campo delle scienze quantistiche e l'approfondimento e la diffusione delle tecnologie quantistiche nel campo del calcolo, delle simulazioni, delle comunicazioni e dell'informazione:

- promuovere, sostenere e coordinare le attività di ricerca e di insegnamento finalizzate allo studio delle tecnologie quantistiche;
- provvedere alla comunicazione, all'integrazione e allo sviluppo delle conoscenze tra studiosi di diversa estrazione scientifica;

Direttore dalla fondazione nel 2020 Paolo Villoresi

Vicedirettore Simone Montangero



UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

Evoluzione Italiana del contesto nelle comunicazioni sicure

3.1.4 Comunicazione quantistica

Obiettivo OSc-4A	**Realizzazione di reti di comunicazione quantistica sicure e integrate** *Sviluppare le reti di comunicazione quantistica, rendere quantum-ready e quantum-resilient le attuali reti di comunicazione ed integrare la comunicazione quantistica sicura nelle reti classiche*

Linee di azione

a) Completare la dorsale quantistica italiana e collegarla a EuroQCI integrando comunicazioni quantistiche satellitari, connessioni transfrontaliere in fibra ottica e reti metropolitane;

b) Definire una roadmap per EuroQCI e la dorsale quantistica italiana, valorizzando in particolare le risorse presenti a livello locale;

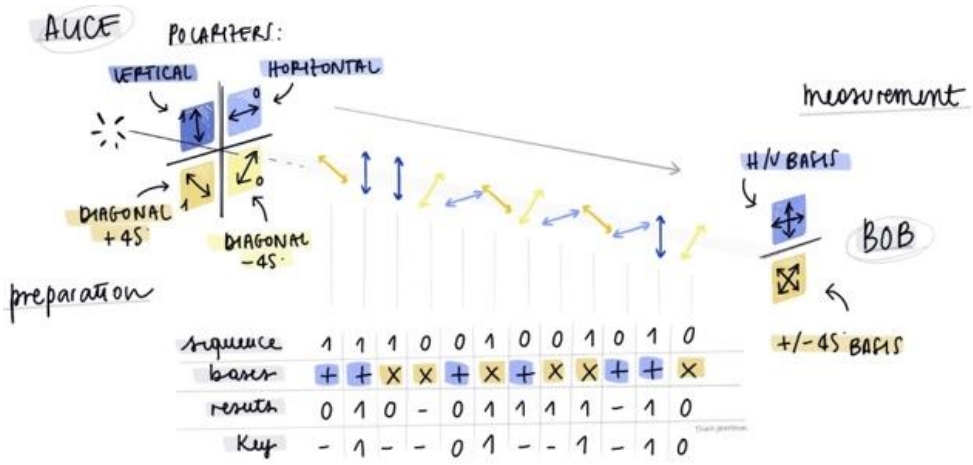
c) Progettare architetture e protocolli per reti quantistiche nella prospettiva di uno stack protocollare quantistico, con il duplice obiettivo: i) rispondere ad esigenze pratiche riducendo i requisiti hardware richiesti, ii) massimizzare l'interplay/interoperabilità tra infrastruttura classica di comunicazione ed infrastruttura quantistica, abilitando la coesistenza tra traffico classico e traffico quantistico e/o integrando i protocolli quantistici e lo stack protocollare classico;

https://www.mur.gov.it/sites/default/files/2025-09/QIS_FINAL_IT%200809.pdf



La distribuzione quantistica di chiavi crittografiche, **Quantum Key Distribution (QKD)**

- sfrutta le proprietà della fisica quantistica
- consente la distribuzione di chiavi crittografiche attraverso la trasmissione di Qubit nelle comuni reti di telecomunicazioni in fibra
- garantisce una sicurezza instrinseca, superiore a quella fornita dagli attuali protocolli basati sulla complessità computazionale



UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

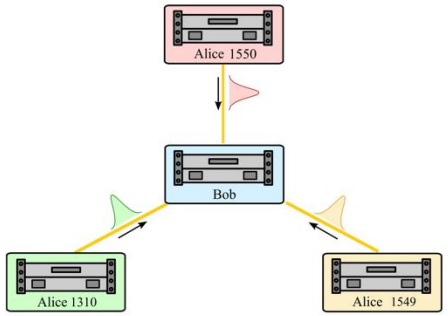
Sviluppi dalla ricerca

payload per satelliti

nuovi encoders di qubit

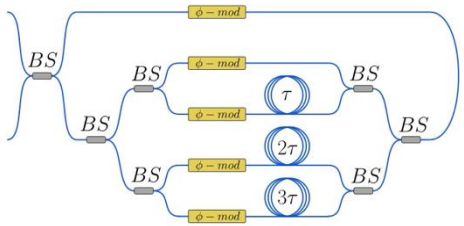
studio dei fondamenti



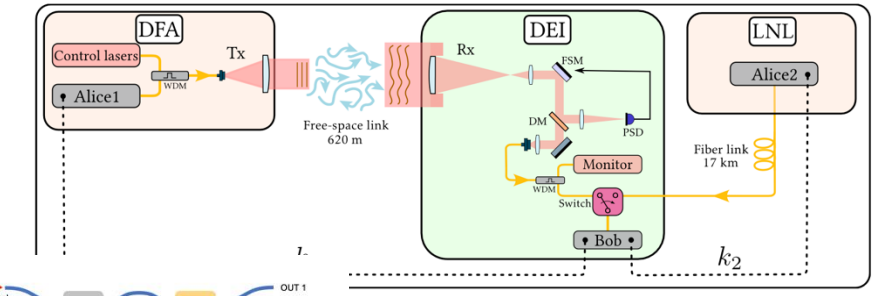






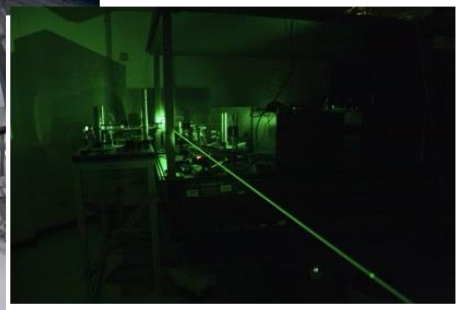




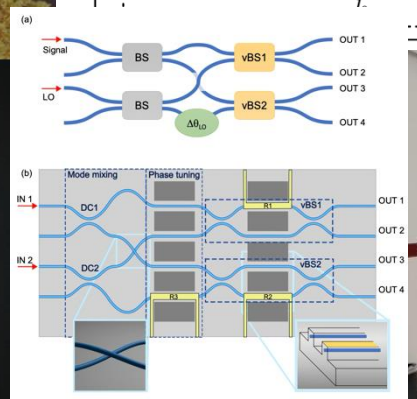


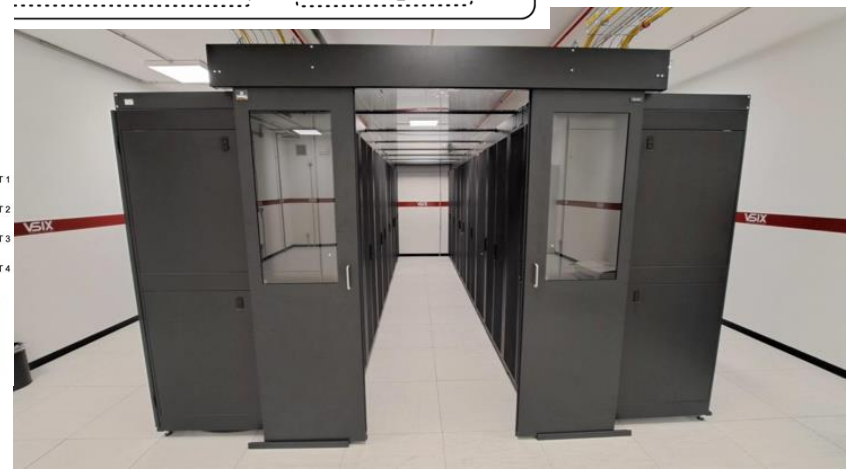












Sviluppi dalla ricerca

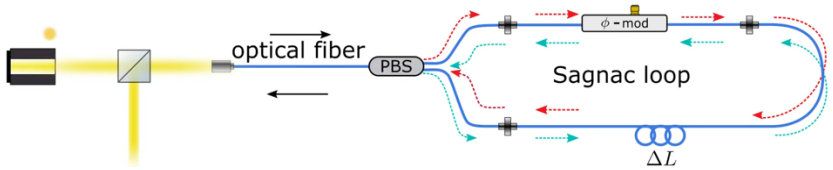
network in fibra

collegamenti in orizzontale senza fibra

network intermodale - canali spaziali

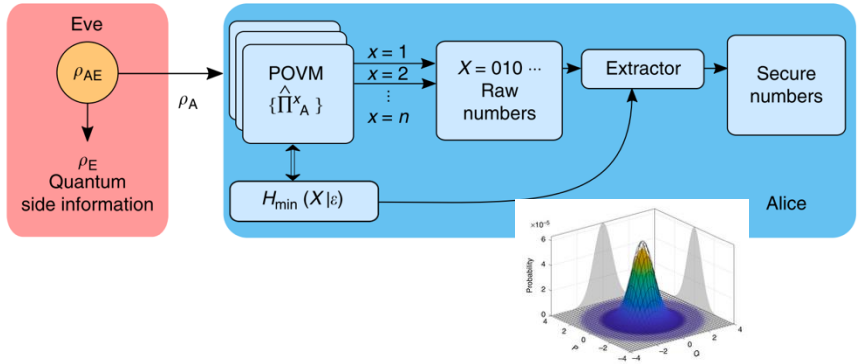






1. Agnesi C. et al. Opt. Lett. 44, 2398 (2019) - patented
2. Agnesi C. et al. Optica 7, 284 (2020)
3. Avesani M. et al. Opt. Lett. 45, 4706 (2020)

+



Avesani, M., Marangon, D. G., Vallone, G. & Villoresi, P. *Source-device-independent heterodyne-based quantum random number generator at 17 Gbps* Nature Commun. 9, 5365 (2018) - patented

+



=

ThinKQUANTUM

spinoff of University of Padua
founded in 2021 together with
Officina Stellare spa Italy

Comunicazioni sicure mediante tecnologie quantistiche

il supporto alla ricerca è strategico

sostenere sostanzialmente roadmap nazionali e europee

affrancare le infrastrutture critiche con tecnologie fidate

Evoluzione Italiana del contesto nelle comunicazioni sicure

L'Alleanza Quantistica Italiana (AQI), con sede a Padova, è un associazione che riunisce università, enti di ricerca, industrie e istituzioni pubbliche che riconoscono il ruolo strategico delle tecnologie quantistiche per il futuro dell'Italia. L'associazione nasce con l'obiettivo di costruire un ecosistema nazionale unificato e competitivo a livello internazionale, capace di valorizzare le eccellenze italiane e di integrare in una visione comune il mondo accademico, scientifico, industriale e politico.

Le attività di AQI coprono tutti i principali ambiti del settore: calcolo quantistico, comunicazioni quantistiche, sensori, simulazioni, metrologia, intelligenza artificiale quantistica e quantum networking.

AQI si propone di favorire sinergie strategiche tra ricerca e industria, promuovendo una roadmap condivisa per lo sviluppo delle scienze e tecnologie quantistiche italiane. L'associazione sostiene la formazione di nuove competenze, il trasferimento tecnologico, la creazione di infrastrutture nazionali e paneuropee, nonché un coordinamento unitario nei confronti delle istituzioni politiche italiane ed europee.

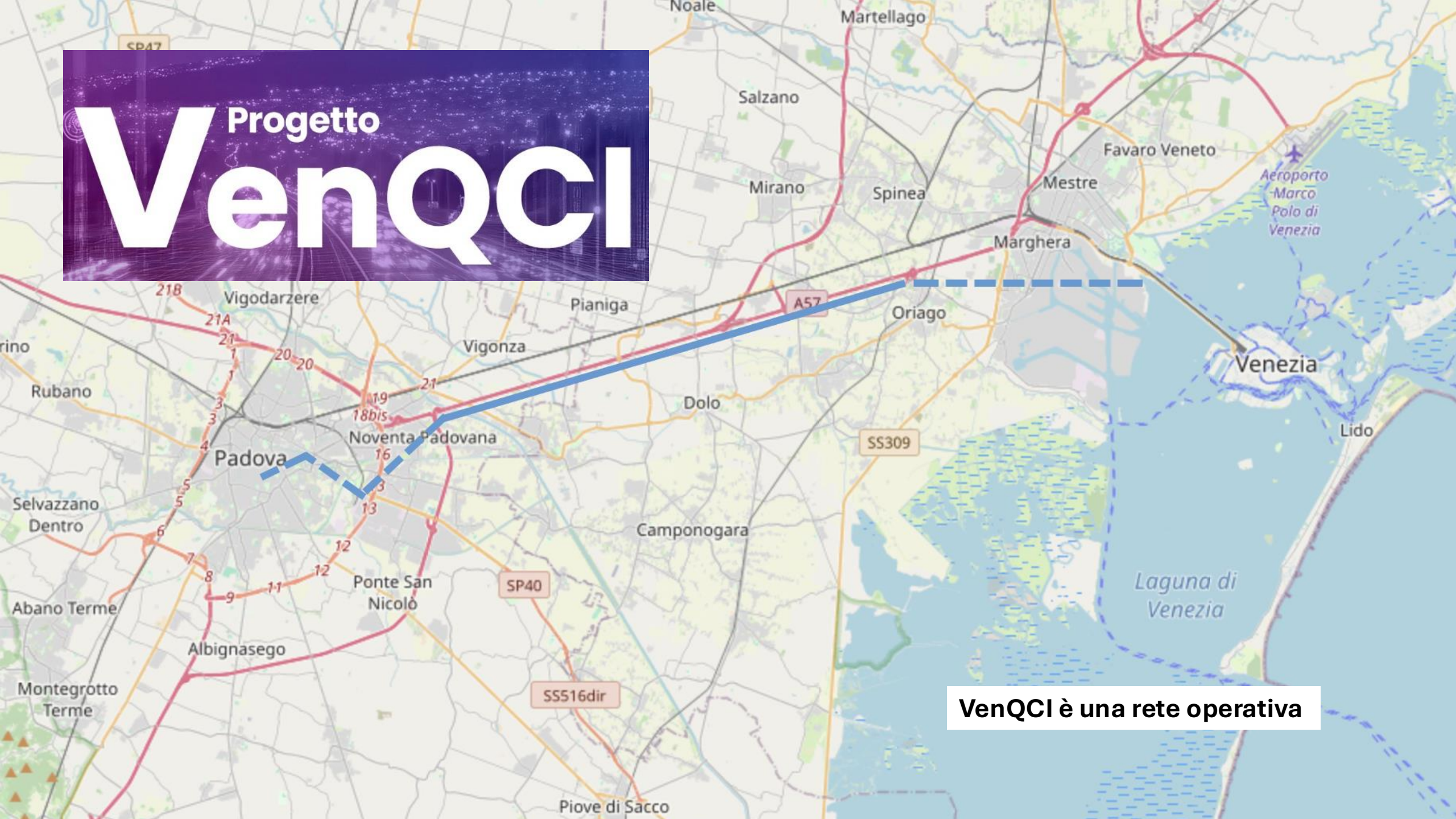
https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

Il progetto VenQCI

Il **progetto VenQCI** *(Veneto Quantum Communication Infrastructure)* si prefigge di realizzare una rete regionale quantistica che consenta di introdurre le **tecnologie quantistiche** per la distribuzione di chiavi crittografiche con l'obiettivo di innalzare il profilo di **cyber sicurezza del territorio**

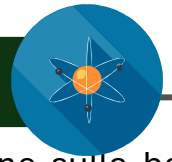
L'iniziativa è svolta attraverso una convenzione (12/2023) e la collaborazione tra partners

- *Agenzia Digitale del Veneto per* ***Regione Veneto***
- ***QTech*** *Center e* ***Vsix*** *per l'****Università degli Studi di Padova***
- ***CAV*** *Concessioni Autostradali Venete, coordinatore del progetto*


Progetto
VenQCI
Noale
Martellago
Salzano
Favaro Veneto
Mirano
Spinea
Mestre
Aeroporto Marco Polo di Venezia
Marghera
Vigodarzere
Pianiga
A57
Oriago
Vigonza
Venezia
Rubano
Dolo
Noventa Padovana
Padova
SS309
Lido
Selvazzano Dentro
Camponogara
Laguna di Venezia
Ponte San Nicolò
SP40
Abano Terme
Albignasego
Montegrotto Terme
SS516dir
Piove di Sacco
VenQCI è una rete operativa

VenQCI: Obiettivi

Obiettivi



- Far nascere la progettazione sulla base di **CASI D'USO** reali ovvero sulle necessità, presenti e future, di ciascun partner (Disaster recovery, business continuity, …)
- **Realizzazione** e messa in esercizio di un'infrastruttura come rete quantistica regionale
- Identificazione di **scenari di governance** per sviluppi futuri

Rete quantistica regional



- **Cross-partner**
- Permanente e operativa **"in produzione"**
- **Multi-nodo** (5+)
- Scalabile e predisposta alla crescita

Casi d'uso



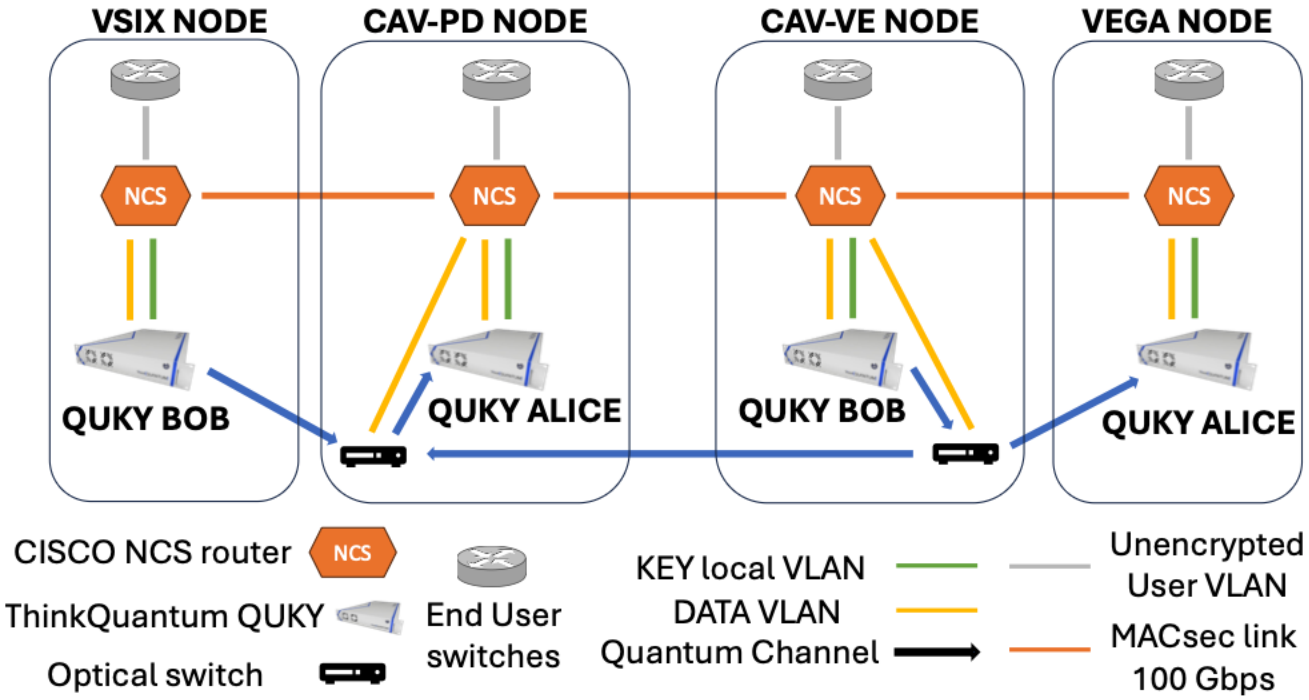
- Disaster Recovery & Business Continuity
- Authentication & Integrity (i.e. VPN, VideoCall, Research projects)
- Mobility Hub, CAV Cloud Services @ Vsix
- Dynamic Back-up / load balance / Metro Cluster

Governance



- Studio ed analisi del contesto e di iniziative internazionali
- Definizione di scenari per la gestione della rete
- Predisposizione all'estensione a nuovi partner pubblico/privati
- Identificazione di kpi per l'infrastruttura ed il servizio

VenQCI al lavoro: analisi estesa dell'operatività

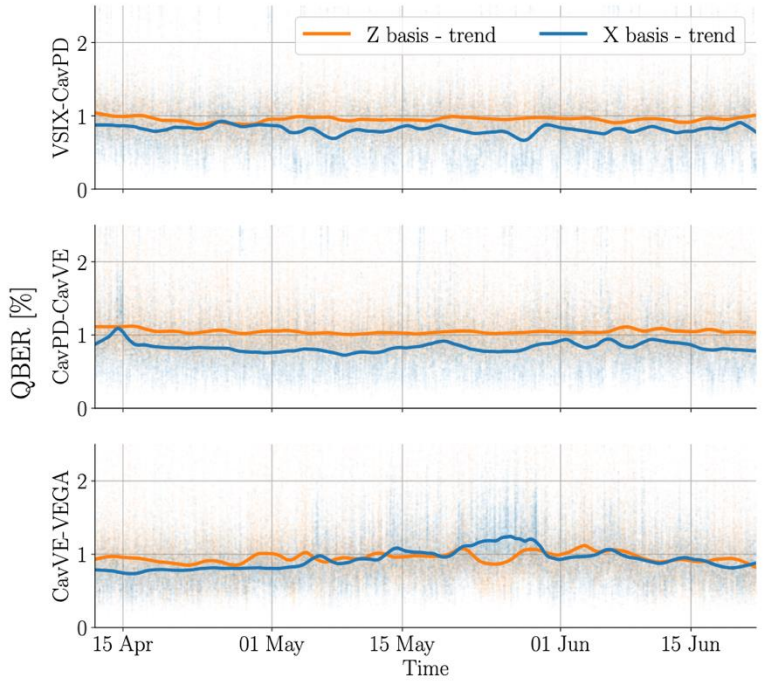


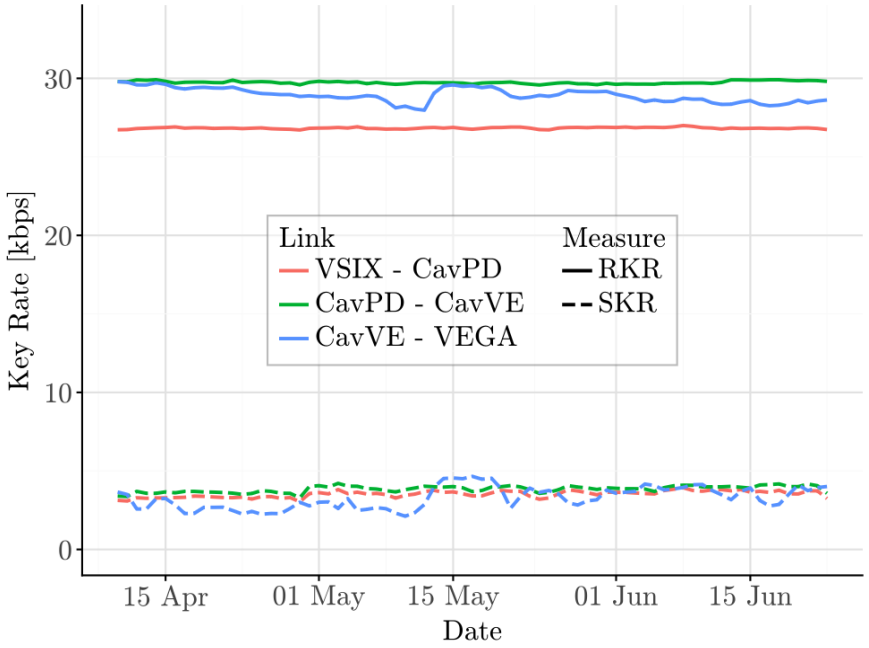


implementazione dello switching per rendere flessibile il network

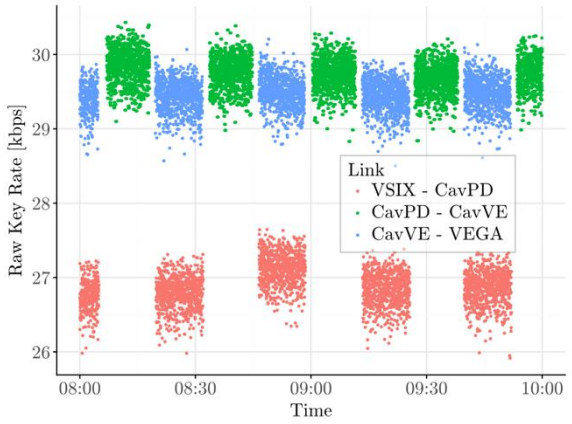
A. De Toni et al. Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment https://arxiv.org/abs/2510.16867

VenQCI al lavoro: analisi estesa dell'operatività







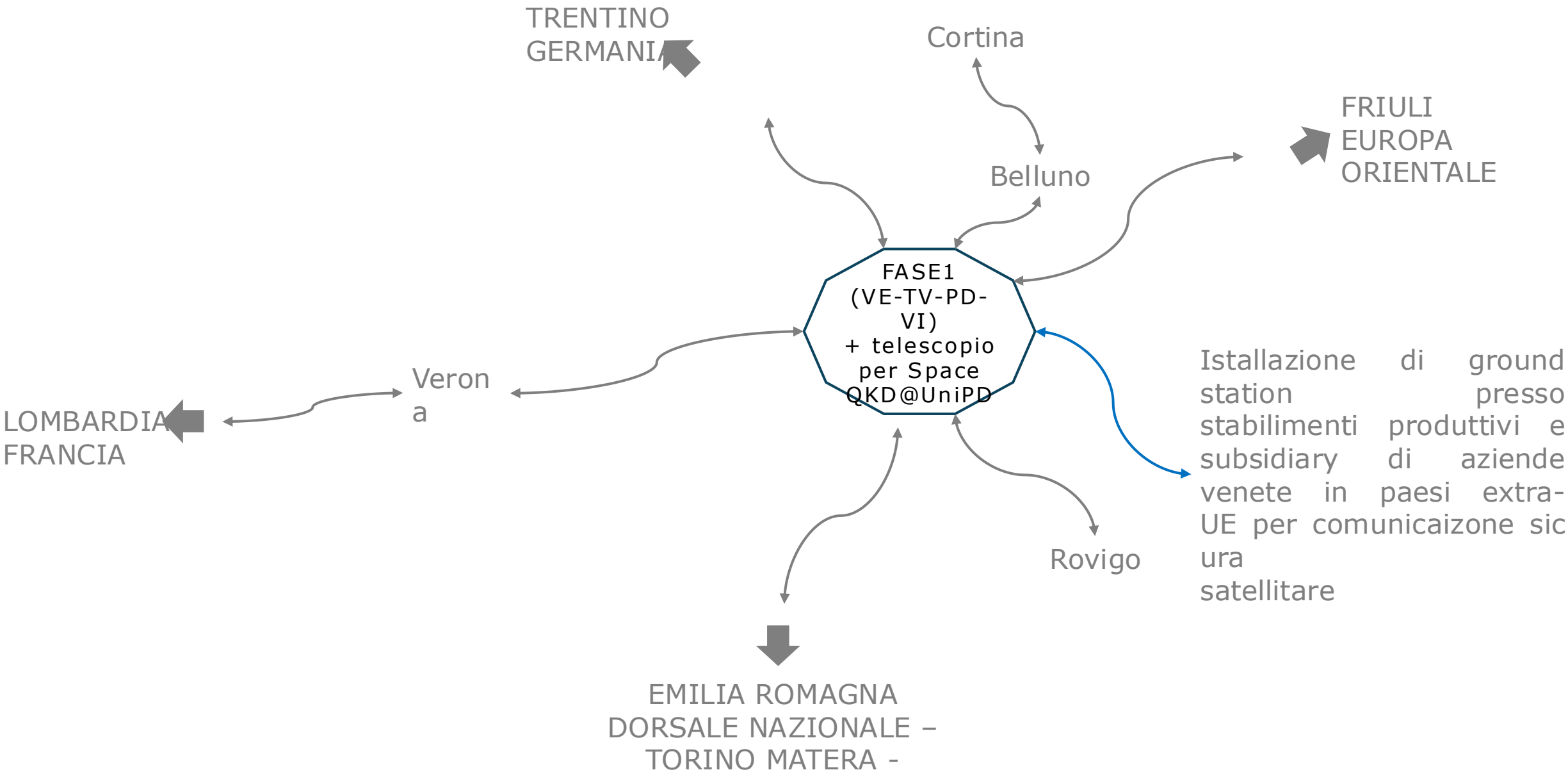


distribuzione continua delle chiavi monitorata nell'arco di due mesi

A. De Toni et al. Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment https://arxiv.org/abs/2510.16867

UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

Prospettiva di crescita e integrazione continentale



UNIVERSITÀ DI PADOVA
Centro interdipartimentale
di Ricerca Padua Quantum
Technologies Research Center

Progetto VenQCI



paolo.villoresi@unipd.it
www.qtech.unipd.it