# Quantum Technologies: a new frontier in cyber-security

**Giuseppe (Pino) Vallone**

*email*: vallone@dei.unipd.it

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

WORKSHOP GARR 2019 - 8-10 ottobre 2019

# Summary

# Summary

1 Quantum Key Distribution
- Introduction to QKD
- Our recent achievements

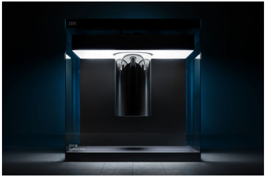
2 Quantum Random Number Generators

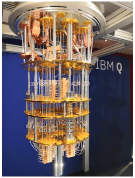
3 Conclusions

# Summary

# 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)






- Post-Quantum crypto

# QKD: quantum key distribution

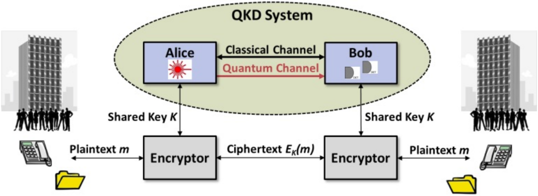
- A novel approach for unconditionally secure communications: Security based on physics and not on **computational complexity**

# QKD: quantum key distribution

- A novel approach for unconditionally secure communications: Security based on physics and not on **computational complexity**
- Exploit quantum mechanics laws for establishing secure keys

# QKD: quantum key distribution

- A novel approach for unconditionally secure communications: Security based on physics and not on **computational complexity**
- Exploit quantum mechanics laws for establishing secure keys
- Single photon transmission to create keys and classical channel for send encrypted message



# OpenQKD


- Develop an experimental testbed based on QKD and to test the interoperability of equipments
- Preparation of the future pan-European QKD infrastructure
- Over 25 use-case trials already been determined and will be complimented by open calls.

# One time pad

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

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| message | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

$$\oplus$$

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| random key | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

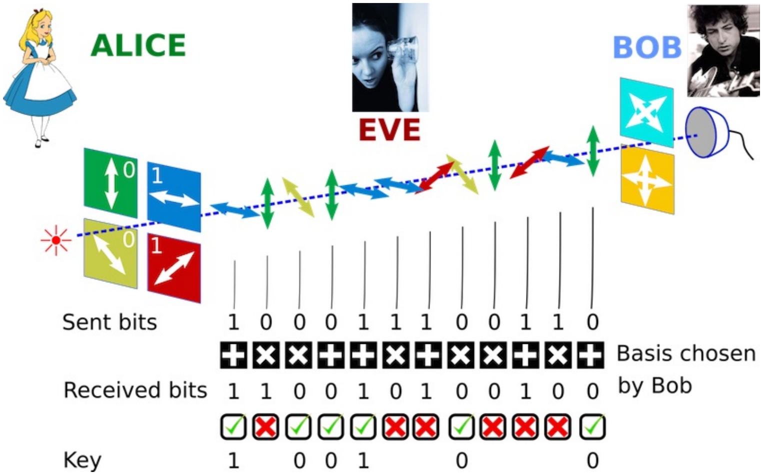
$$=$$

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| encrypted message | 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

QKD can achieve unconditional security



V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Secret key rate

QKD can achieve unconditional security

$$\left.\begin{array}{l}\text{▶ two non-commuting basis}\\ \text{▶ no-cloning theorem}\\ \text{▶ any measurement (generally) perturbs the systems}\end{array}\right\} \Rightarrow \text{Eve detection!}$$



V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Secret key rate

QKD can achieve unconditional security

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

$\Rightarrow$ Eve detection!

Secret key rate related to **Quantum Bit Error Rate** $Q$:

$$\boxed{r = 1 - 2h_2(Q)}$$

with

$$h_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$$



V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Secret key rate

QKD can achieve unconditional security

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

$\Rightarrow$ Eve detection!

Secret key rate related to **Quantum Bit Error Rate** $Q$:

$$\boxed{r = 1 - 2h_2(Q)}$$

with

$$h_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$$

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



V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Real life implementation: decoy state

Are true single photon sources necessary?



V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Real life implementation: decoy state

Are true single photon sources necessary?
NO, if the decoy state method is implemented


V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Real life implementation: decoy state

Are true single photon sources necessary?
NO, if the decoy state method is implemented

- Use a classical laser attenuated to the single photon level.

 V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Real life implementation: decoy state

Are true single photon sources necessary?
NO, if the decoy state method is implemented

- Use a classical laser attenuated to the single photon level.
- Modulate the intensity and


choose randomly between three possible values of the pulse mean photon number $\mu$ of the laser:

1. $\mu_1 = 0.5$
2. $\mu_2 = 0.1$
3. $\mu_3 = 0$

 V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Summary



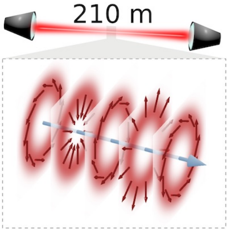


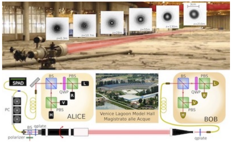
V. Scarani, *et al.*, *The security of practical quantum key distribution*, **Rev. Mod. Phys. 81, 1301 (2009)**

# Long distance free-space quantum communication

**Phys. Rev. Lett. 113, 060503 (2014)**

Rotation invariant QKD by OAM

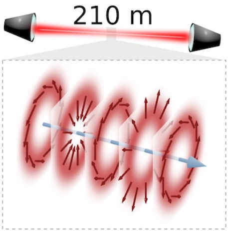


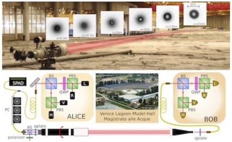



# Long distance free-space quantum communication

**Phys. Rev. Lett. 113, 060503 (2014)**

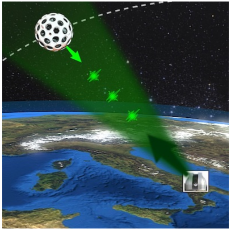
Rotation invariant QKD by OAM




**Phys. Rev. Lett. 113, 060503 (2014)**

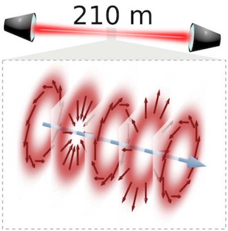
Experimental satellite quantum communication

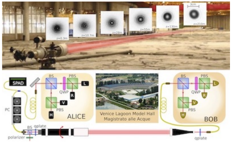


# Long distance free-space quantum communication

**Phys. Rev. Lett. 113, 060503 (2014)**

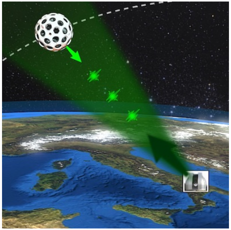
Rotation invariant QKD by OAM



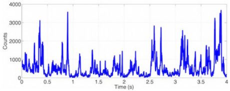

**Phys. Rev. Lett. 113, 060503 (2014)**

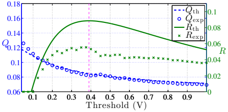
Experimental satellite quantum communication



**Phys. Rev. A 91, 042320 (2015)**

Mitigating turbulence in free-space QKD

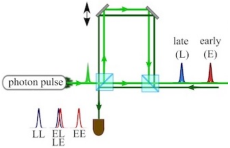



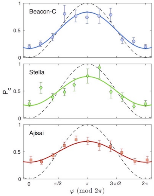



# Long distance free-space quantum communication

**Phys. Rev. Lett. 116, 253601 (2016)**

Single photon interference in space channels

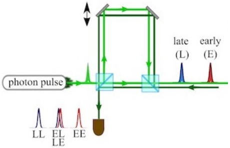


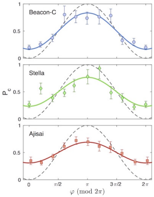



# Long distance free-space quantum communication

**Phys. Rev. Lett. 116, 253601 (2016)**

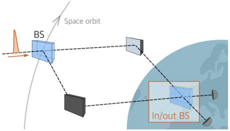
Single photon interference in space channels

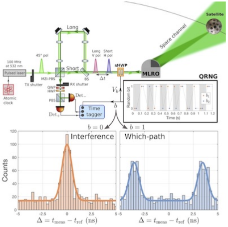



**Science Advances 3, e1701180 (2017)**

Wheeler's delayed choice in space

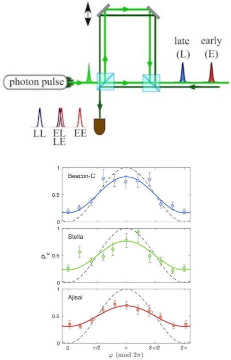


# Long distance free-space quantum communication

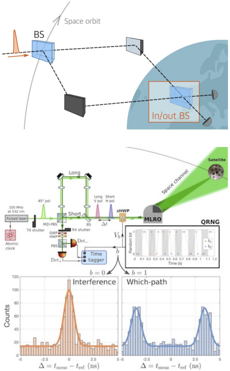
**Phys. Rev. Lett. 116, 253601 (2016)**

Single photon interference in space channels



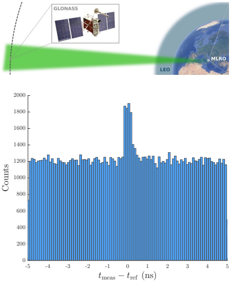

**Science Advances 3, e1701180 (2017)**

Wheeler's delayed choice in space



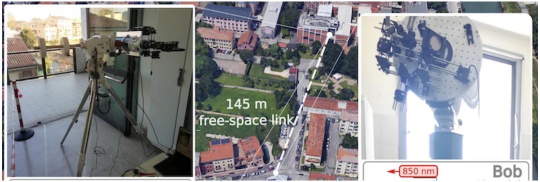

**Quantum Science and Tech. 4, 015012 (2019)**

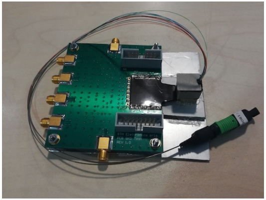
Single-photon exchange with GNSS satellite (20000 km)

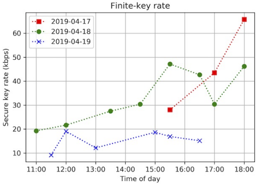


# Daylight operation of free-space QKD

M. Avesani, *et. al.*, **[arXiv:1907.10039]**



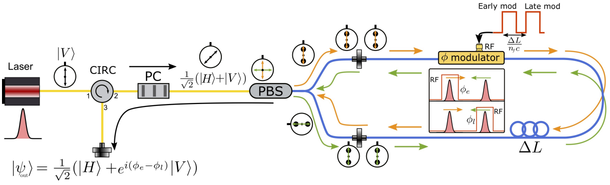



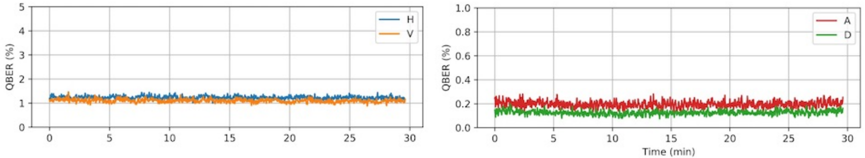


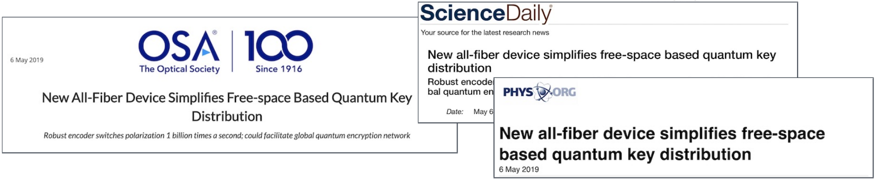

- QKD from 11:00 to 18:00. Full daylight
- Photonic integrated chip source

# Quantum state encoder

## POGNAC = POlarization saGNAC



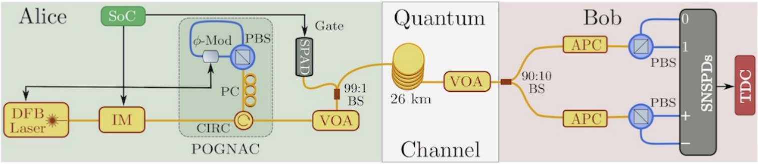



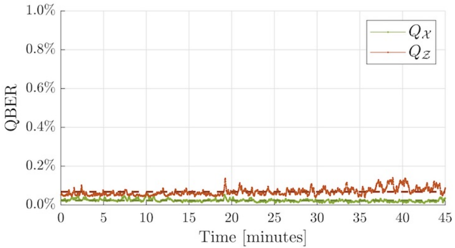



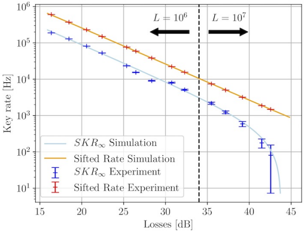



C. Agnesi, *et. al.* **Optics Letters 44, 2398 (2019)**

# Test with fiber-link



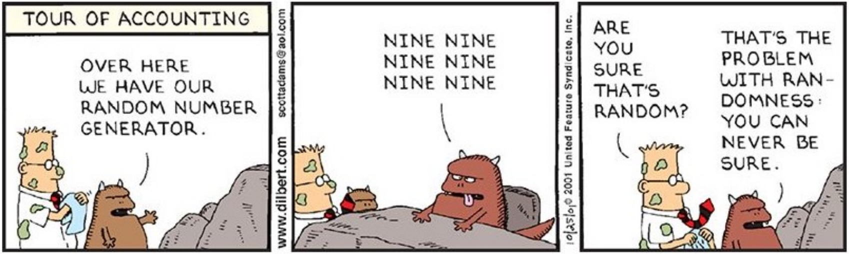

- Lowest intrinsic QBER ever reported (<0.07%)


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

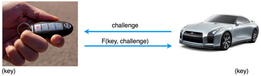
# Summary

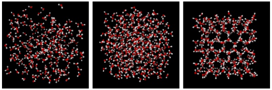
# What is a random number

A random number is a number generated by an unpredictable process



# Why random numbers?

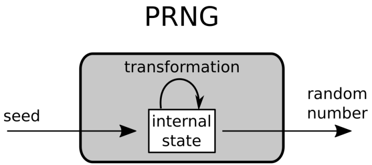



Random numbers are crucial in several applications:

1. Information technology and security (also QKD)
2. Scientific simulation (meteorology, biology, physics...)
3. Lottery/gaming

# Pseudo Random Number Generators




Pseudo-random numbers are generated by a deterministic algorithm that produces a sequence that "resemble" a random sequence

## PROS

- simple
- fast

## CONS

- period
- not-uniformity
- correlations

# but....

## Von Neumann (1903-1957)

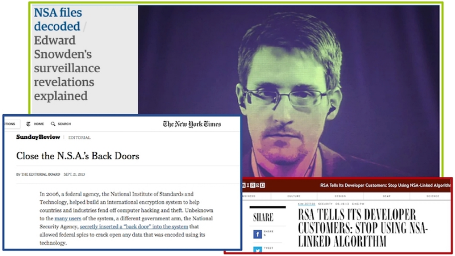
(among the father of information theory

*"Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin"*

# Flaws in PRNG!

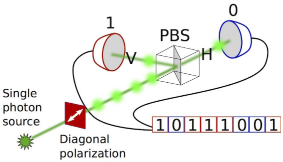
## NSA (National Security Agency) scandal

NSA inserted a “backdoor" in the generator Dual_EC_DRBG certified by NIST



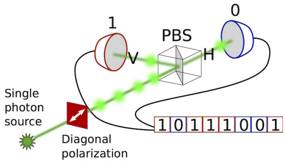

Dual_EC_DRBG was used in several RSA products. In 2013, RSA officially discouraged his clients to use their products with Dual_EC_DRBG.

# Why QRNG?




- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

# Why QRNG?

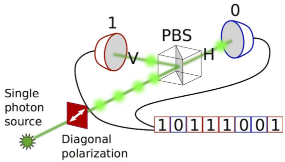



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

What QRNG offer:

- intrinsic randomness of quantum measurements

# Why QRNG?

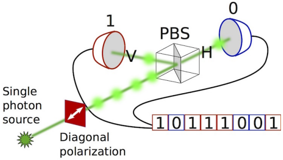



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

What QRNG offer:

- intrinsic randomness of quantum measurements
- outputs not predictable even if the initial state is known

# Why QRNG?

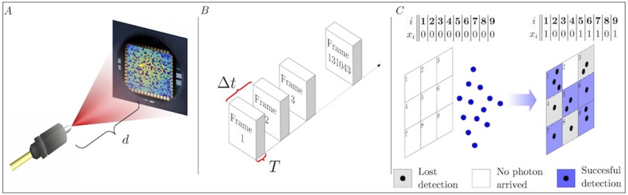



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

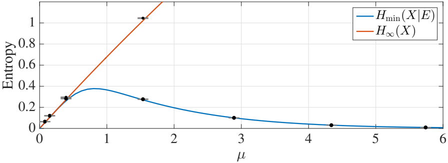
What QRNG offer:

- intrinsic randomness of quantum measurements
- outputs not predictable even if the initial state is known
- randomness is not due to ignorance on the initial conditions (like coin tossing)

# Photon position: single-photon camera QRNG



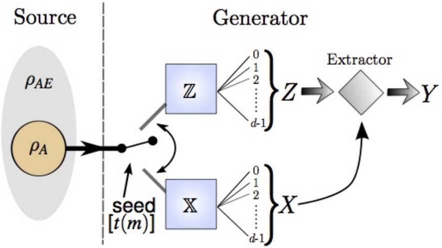

- The eavesdropper knows the number of photons emitted by the source
- Detection inefficiency modeled by perfect detectors activated, with probability $\eta$, by the eavesdropper





D.G. Marangon, GV, U. Zanforlin, P. Villoresi, **Quantum Sci. Technol. 1, 015005 (2016)**

# QRNG certified




- $Z$ is the random sequence
- $X$ is the sequence used to evaluate the randomness in $Z$.
- $Y$ is the final random sequence

$$H_{\min}(Z|E) \geq \log_2 d - \log_2 [\sum_x \sqrt{p_x}]^2$$

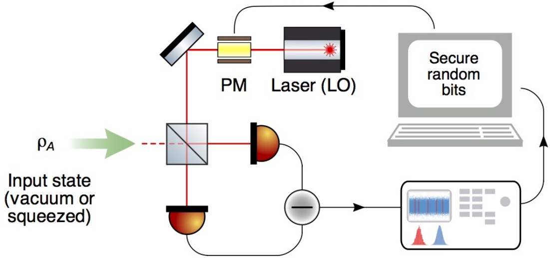
$$\Downarrow$$

$$P_{\text{guess}}(Z) \leq \frac{1}{d} (\sum_x \sqrt{p_x})^2$$



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

# Source-device-independent QRNG with CV

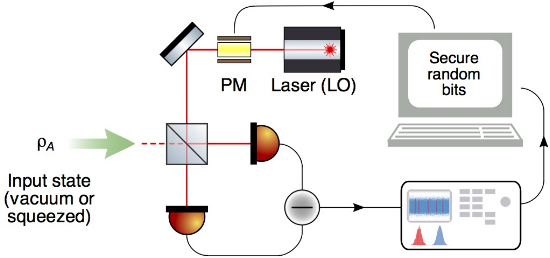



Switch between two conjugate quadratures $\hat{p}$ and $\hat{q}$



D. G. Marangon, GV, P. Villoresi, **Phys. Rev. Lett. 118, 060503 (2017)**

# Source-device-independent QRNG with CV

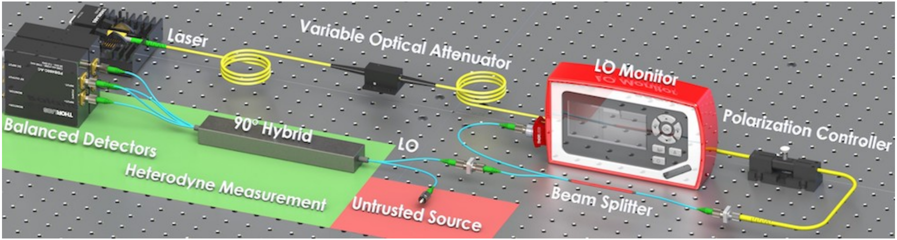



Switch between two conjugate quadratures $\hat{p}$ and $\hat{q}$

Secure bit generation rate of approximately 1.76 Gbit/s


D. G. Marangon, GV, P. Villoresi, **Phys. Rev. Lett. 118, 060503 (2017)**

# QRNG based on heterodyne




Secure heterodyne-based QRNG at 17 Gbps


M. Avesani, D. G. Marangon, G. Vallone, P. Villoresi, **Nature Communications 9, 5365 (2018)**

# Summary

# Conclusions

- QKD is able to generate unconditional secure keys between two users

# Conclusions

- QKD is able to generate unconditional secure keys between two users
- QKD guarantees forward security: protect critical infrastructure for long time in the future

# Conclusions

- QKD is able to generate unconditional secure keys between two users
- QKD guarantees forward security: protect critical infrastructure for long time in the future
- QRNGs guarantees unpredictability of the generated numbers by physical laws

# Conclusions

- QKD is able to generate unconditional secure keys between two users
- QKD guarantees forward security: protect critical infrastructure for long time in the future
- QRNGs guarantees unpredictability of the generated numbers by physical laws
- QKD and QRNG could be employed in all classical security algorithm (xoring technique)

# The group

## FACULTY


P. Villoresi


G. Vallone

## POST-DOC


F. Vedovato

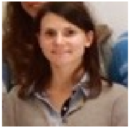

L. Calderaro


A. Stanco

## PHD

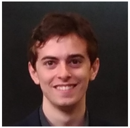

C. Agnesi


M. Avesani


A. Scriminich


H. Tebyanian


L. Zahidy


G. Foletto


F. Picciariello

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/