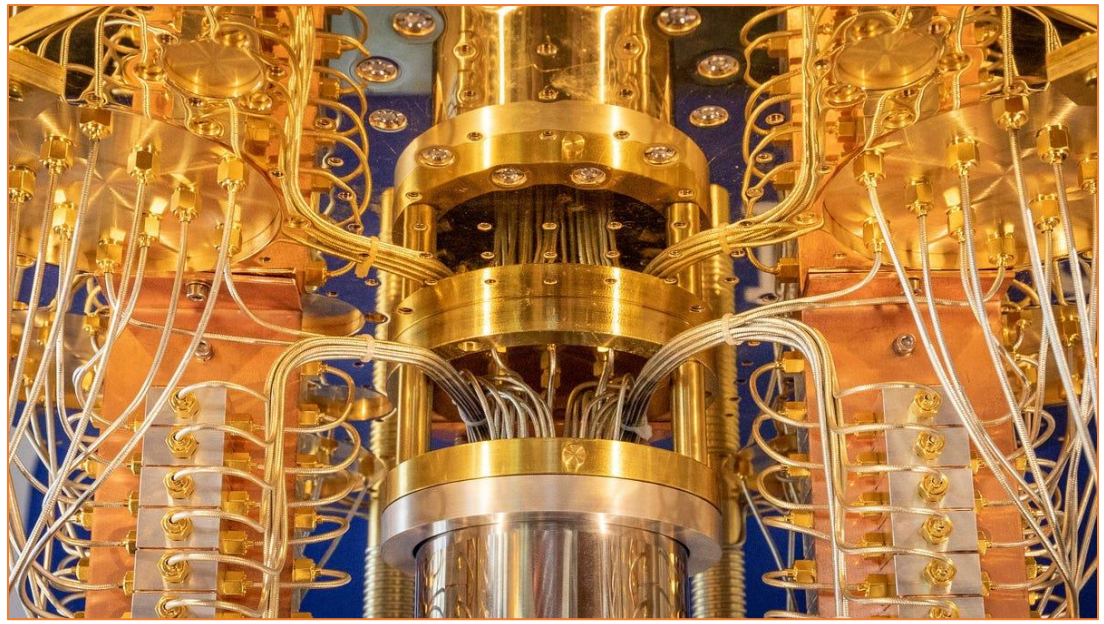
The QKD Network in Padova

Results and new developments

Giulio Foletto
foletto@dei.unipd.it
ITNOG 16 September 2022

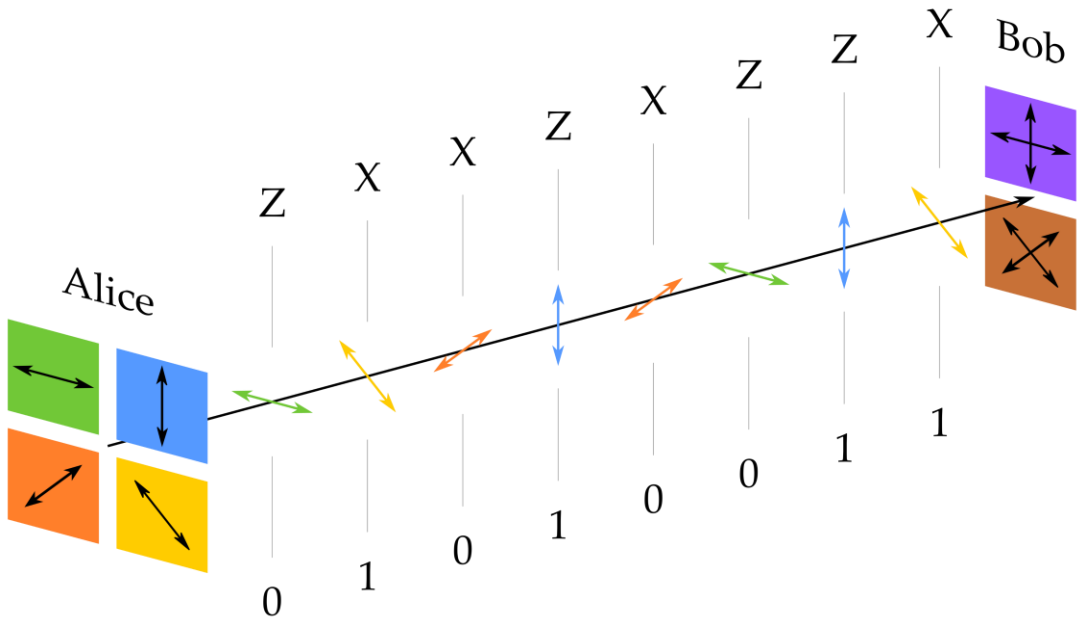
The problem with classical cryptography

- Relies on computationally hard problems
- No formal guarantee of security
- Might be broken by new algorithms or technological developments
- E.g. Shor's algorithm for quantum computers
- Even old data might become vulnerable



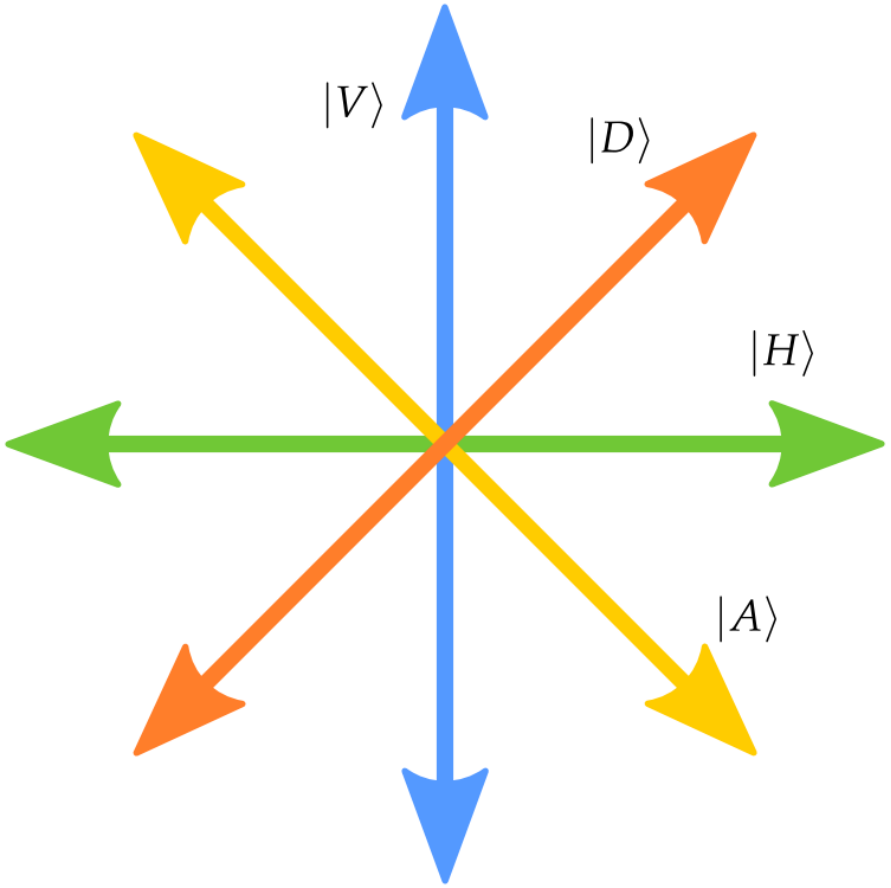
Quantum Key Distribution

- Protocols to distribute a secret cryptographic key through quantum systems
- Unconditional security guaranteed by quantum physics
- Can be used with (unconditionally secure) symmetric encryption
- Research pushes for new schemes and technology
- First commercial applications are ready



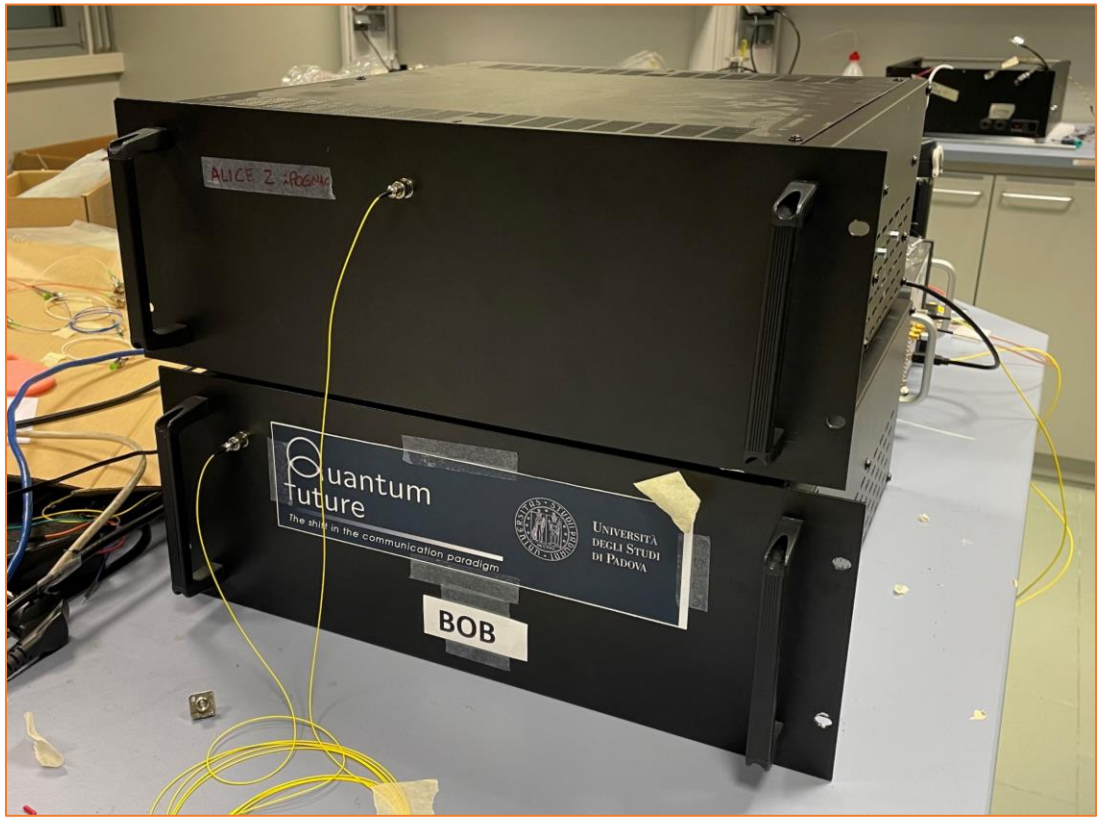
BB84

- Proposed by Bennett and Brassard in 1984
- Uses four two-dimensional quantum states in two mutually unbiased bases
- Security based on the no-cloning theorem
- Typically implemented with «single» photons

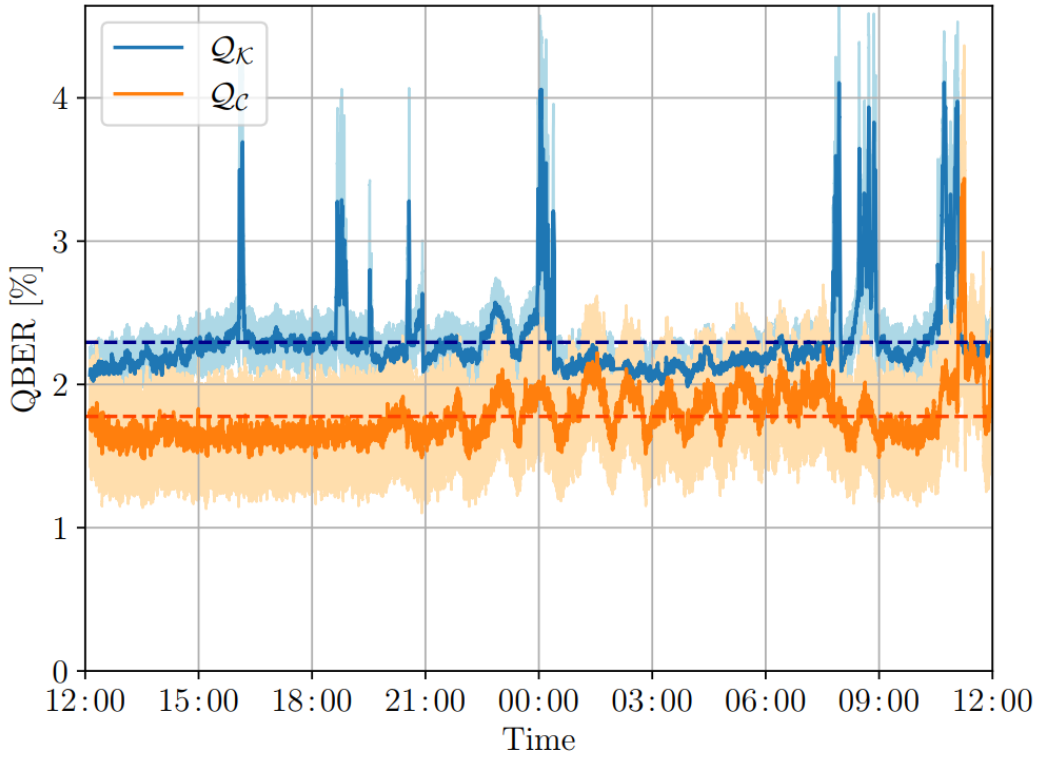


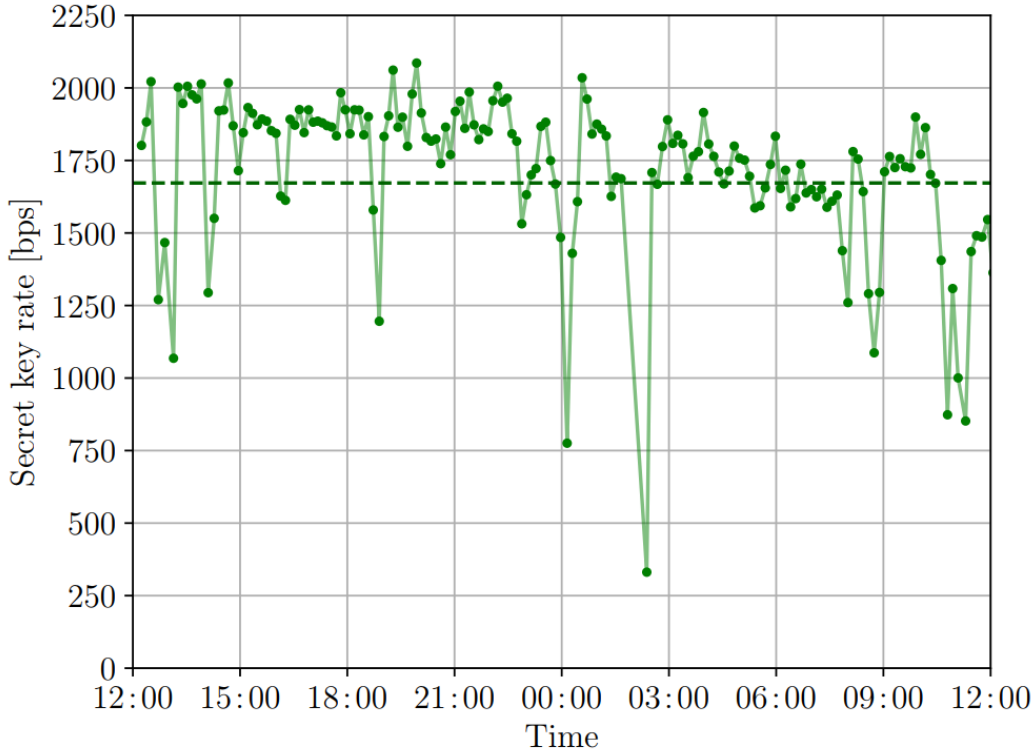
Prototype Devices

- BB84 protocol
- Photon polarization
- Telecom wavelength
- Patented iPognac polarization encoder
- Time-multiplexing scheme at the receiver to use only one single photon detector
- Portable and compact in size



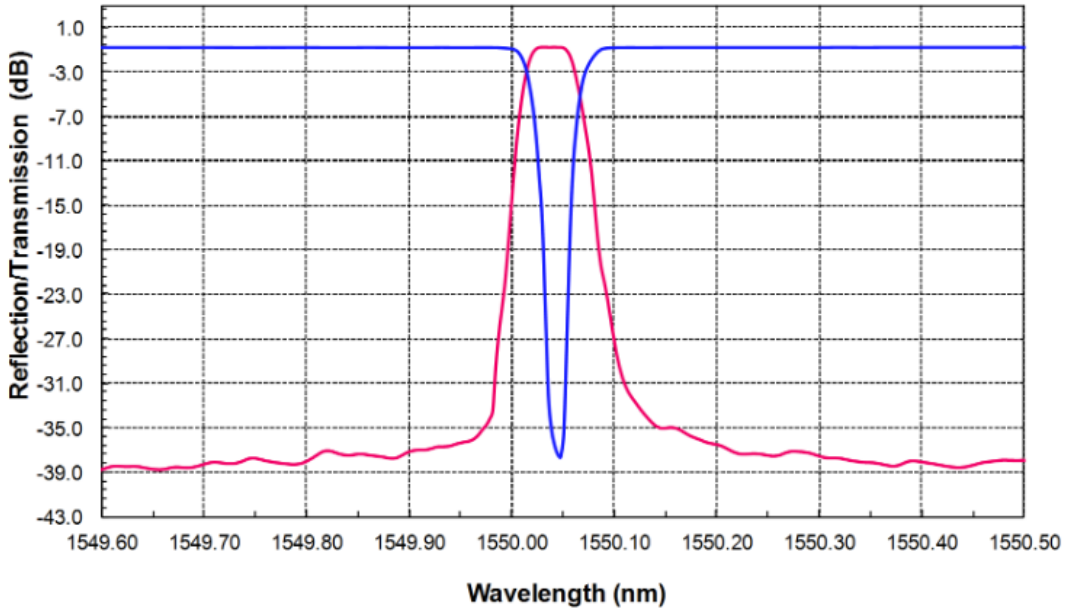
Some results



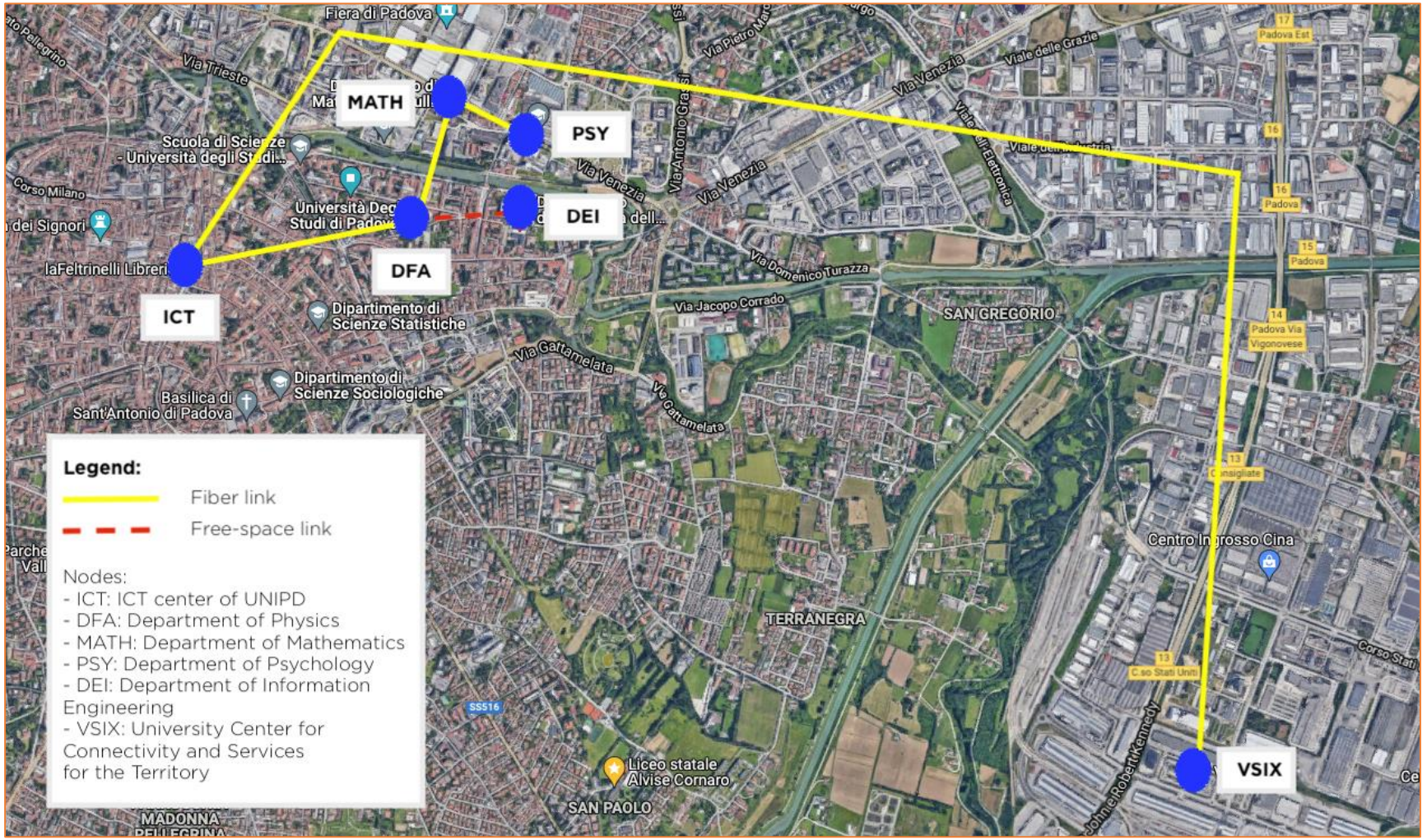


Challenges

- For underground fibers, polarization stability is not an issue
- Multiplexing with classical communication needs strong filtering
- Free-space links need some form of adaptive optics



Future steps for the network



Quantum Random Number Beacon

- Quantum measurements are inherently random, and can be used to produce random bits
- In collaboration with VSIX, we have installed a QRNG that acts as an internet beacon of public random numbers

Conclusions

- QKD makes key distribution invulnerable to future algorithmic or technological developments
- Albeit strikingly different from classical encryption devices, the first prototypes are already available on the market
- Technological challenges remain when integrating this technology with deployed infrastructure
- Research and development are moving at a rapid pace

Contact: foletto@dei.unipd.it