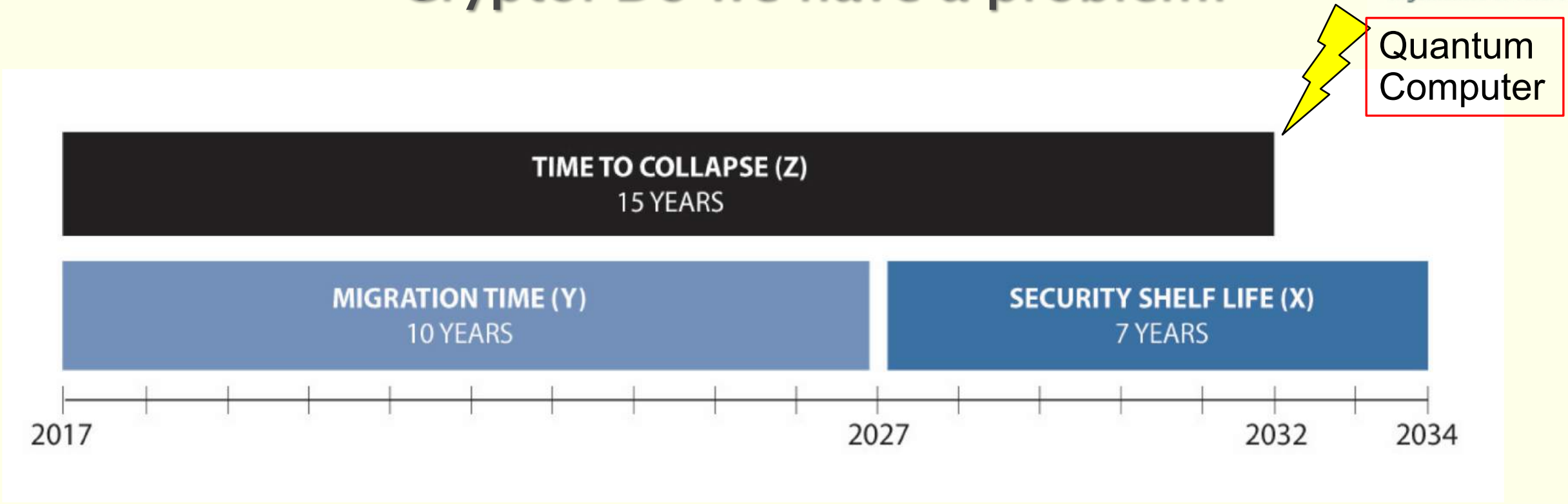
Madrid SDN Quantum Network

SecPho Workshop: Quantum Technologies in Spain. The Future is Now

Madrid, 8 Mayo 2019

Presenter: Vicente Martin
U. Politécnica de Madrid
Vicente@fi.upm.es
gcc.fi.upm.es

Quantum Computing and Quantum Crypto: Do we have a problem?



From : Quantum Computing: Progress & Prospects 2018. A Consensus Report. National Academy of Sciences, Engineering and Medicine (adapted from M. Mosca, 2015)

… write your own answer:

- **Q:** Time to a quantum computer: ?
- **I:** Time to fully change the security infrastructure: Estimate (NIST) 20yrs.
- **S:** Shelf life: 1-50 yrs. (what is your application?)

If I+S > Q… you have problems.

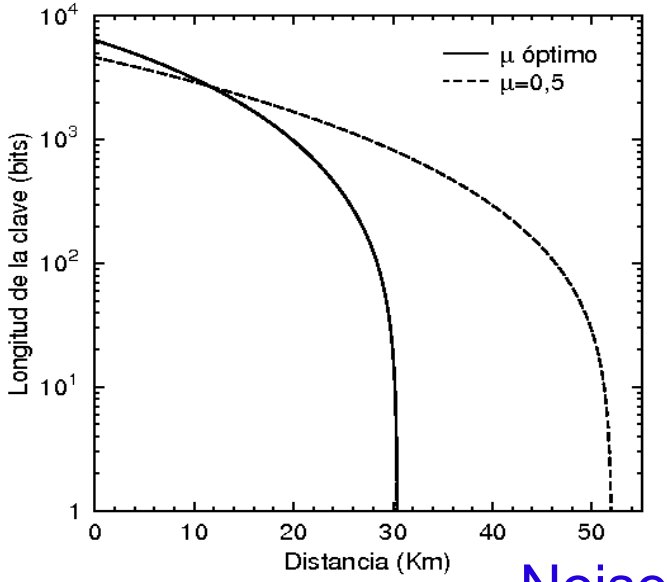
Solutions:

- **Postquantum crypto**: Business as usual.
  - "new" **algorithms** believed to be secure against Quantum Computers.

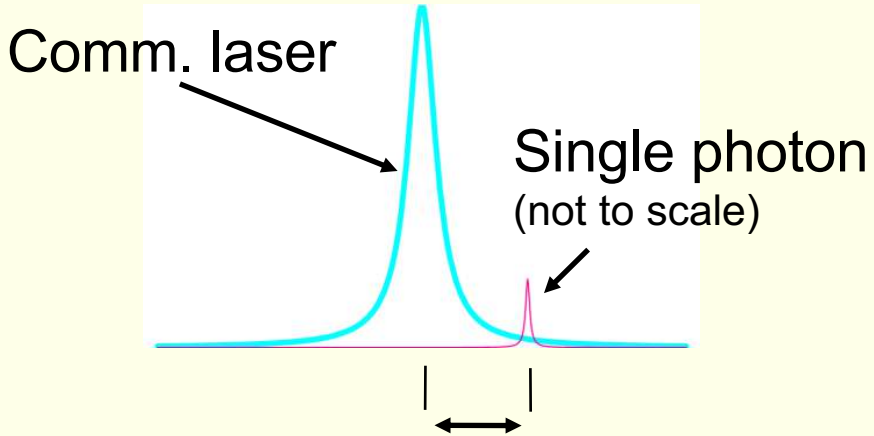
- **Quantum Cryptography**:
  - **Physical** layer security -> Networks
    - You need hardware
    - … and it is not easy
  - Not a complete substitute!

Quantum communications and networks, why is it difficult?

Limited reach, point to point.

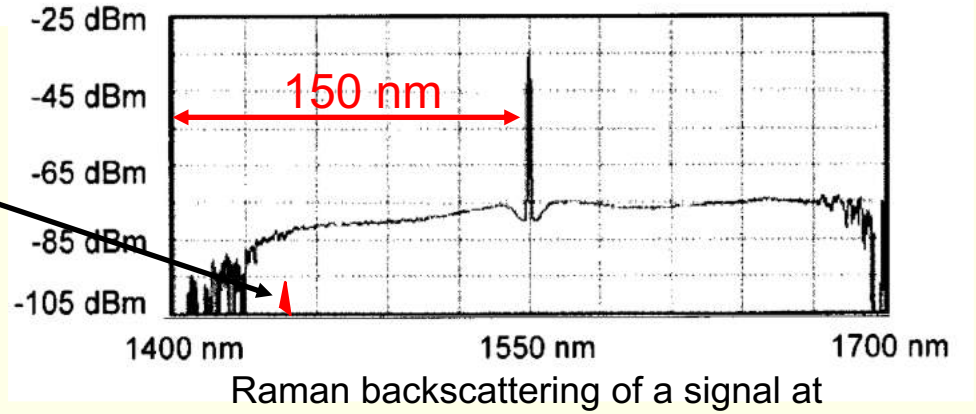


extremely weak signals.



Noise in the fibre: Raman

Single Photon
(approx. scale)

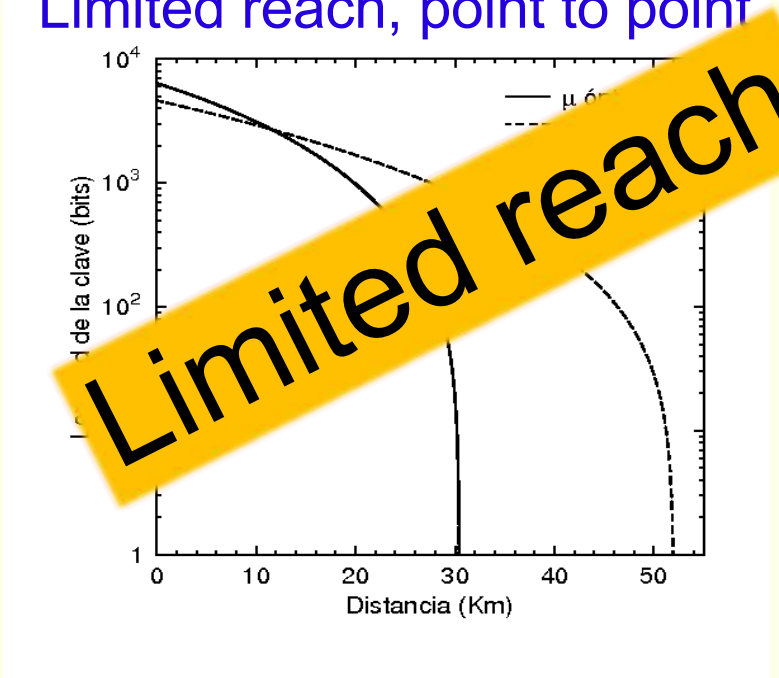


Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

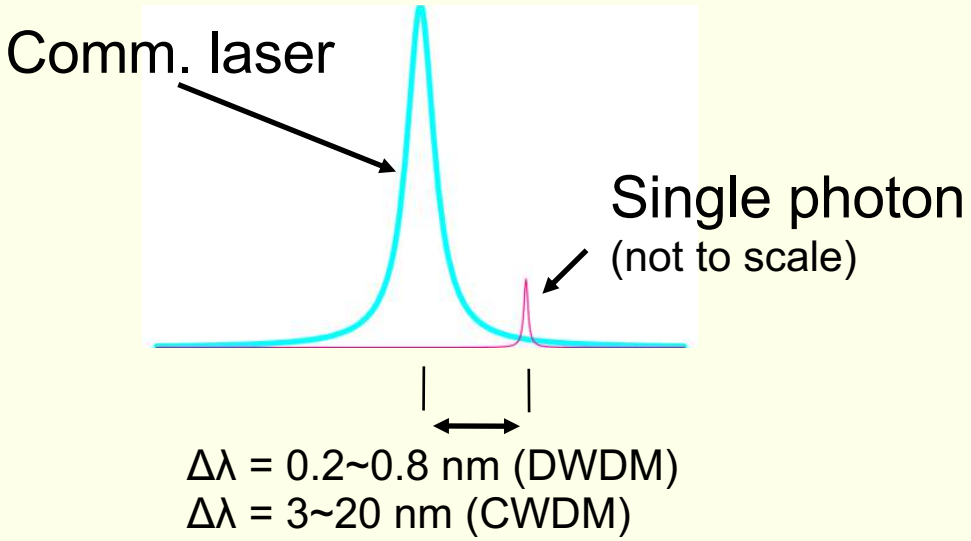
- Difficult to detect.
- Absorpions
- Masked by the noise

Quantum communications and networks, why is it difficult?

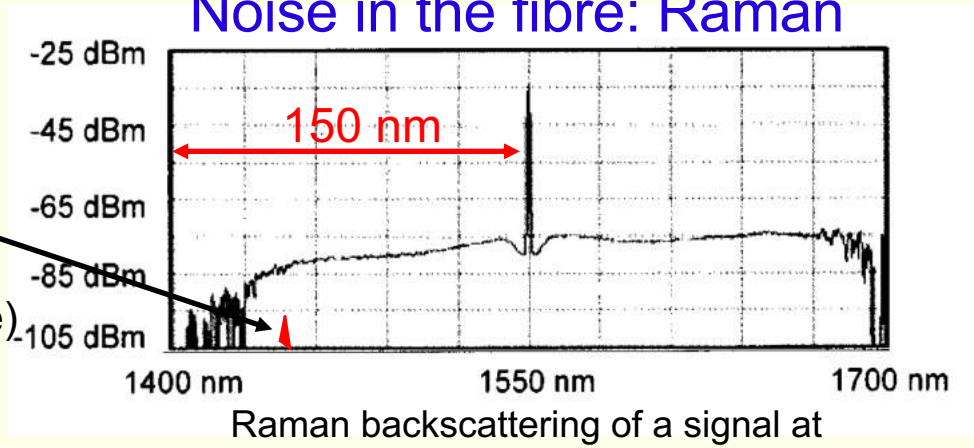
Limited reach, point to point



extremely weak signals.



Noise in the fibre: Raman



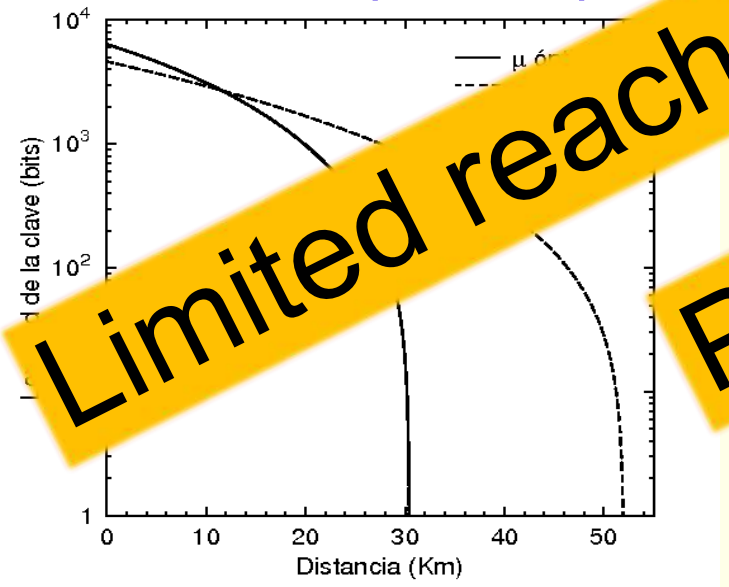
Single Photon (approx. scale)

Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

- Difficult to detect.
- Absorpions
- Masked by the noise

Quantum communications and networks, why is it difficult?

Limited reach, point to point

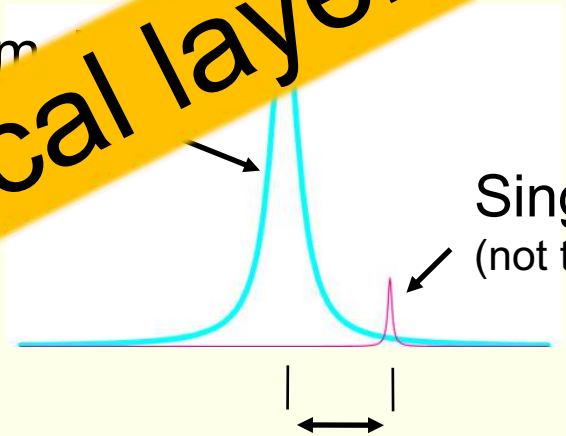


Limited reach

Physical layer

extremely … nals.

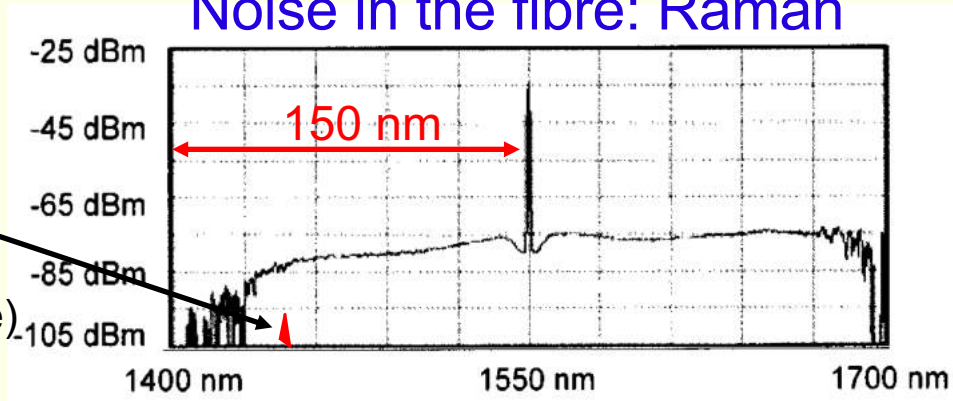
Comm…



Single photon
(not to scale)

$\Delta\lambda$ = 0.2~0.8 nm (DWDM)
$\Delta\lambda$ = 3~20 nm (CWDM)

Noise in the fibre: Raman



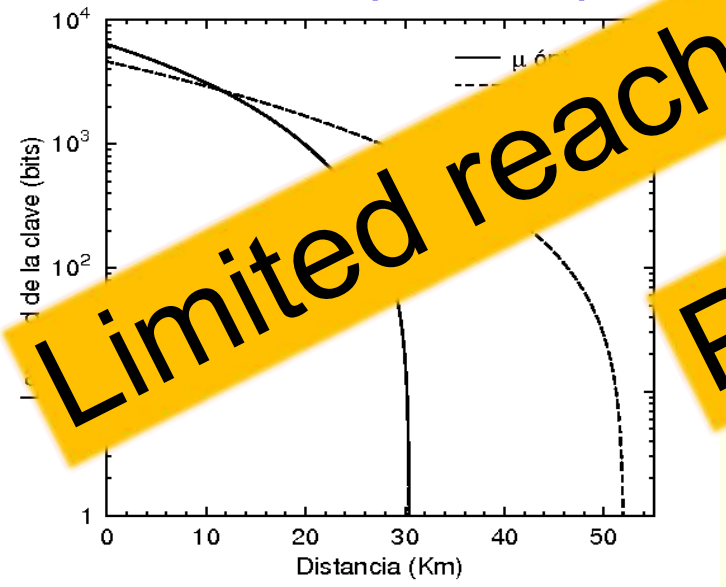
Single Photon
(approx. scale)

Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

- Difficult to detect.
- Absorpions
- Masked by the noise

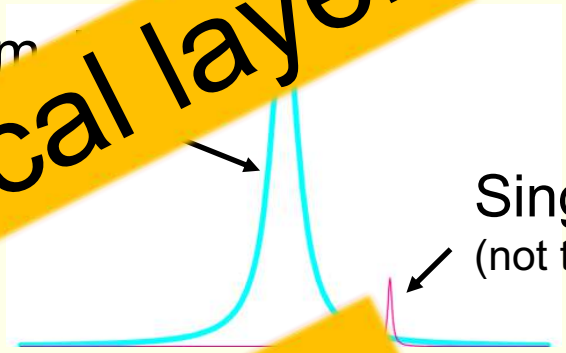
Quantum communications and networks, why is it difficult?

Limited reach, point to point



extremely ... nals.

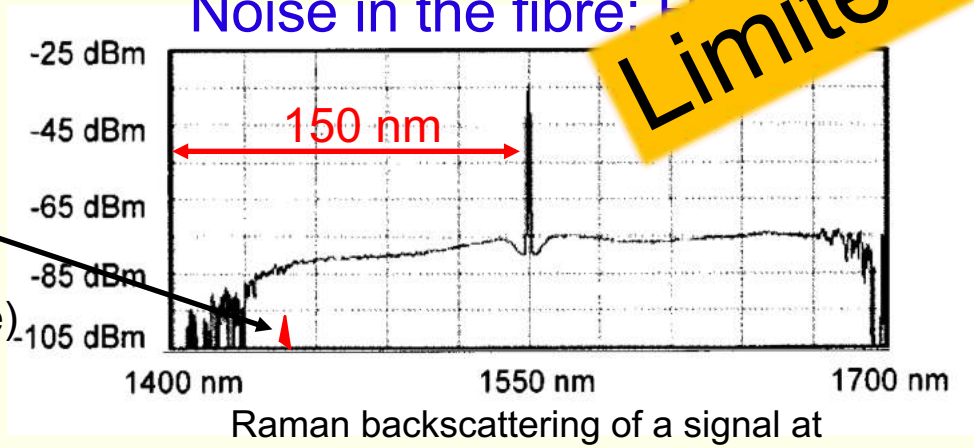
Comm...



Single photon
(not to scale)

...nm (DWDM)
...0 nm (CWDM)

Noise in the fibre: R...



Single Photon
(approx. scale)

Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

Limited reach

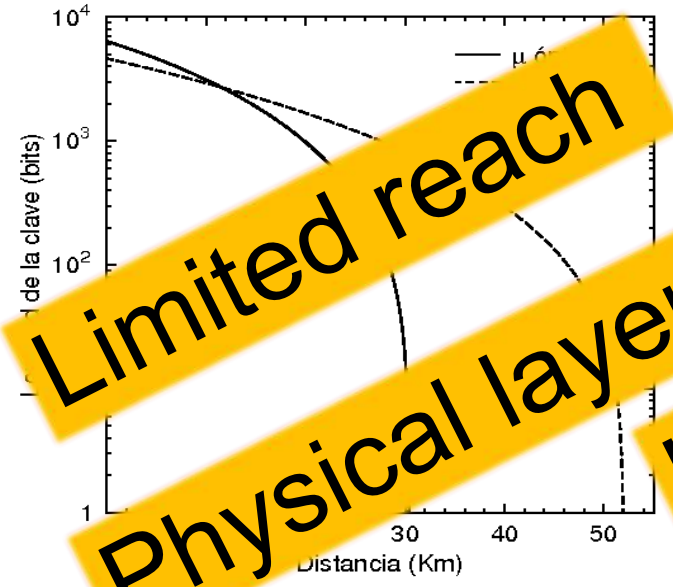
Physical layer

Limited crypto

- Difficult to detect.
- Absorpions
- Masked by the noise

Quantum communications and networks, why is it difficult?

Limited reach, point to point.



extremely weak signals.

Comm. laser

ton

M)

DM)

- Difficult to detect.
- Absorpions
- Masked by the noise

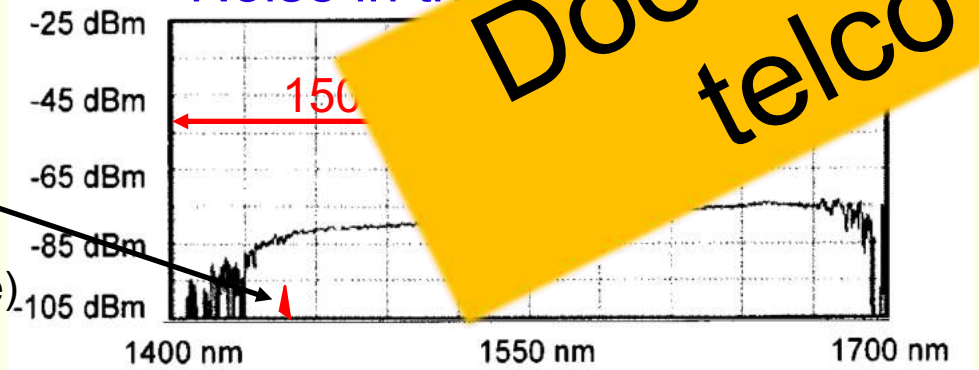
Limited reach

Physical layer

Limited crypto

Does not play well in telco networks

Noise in the

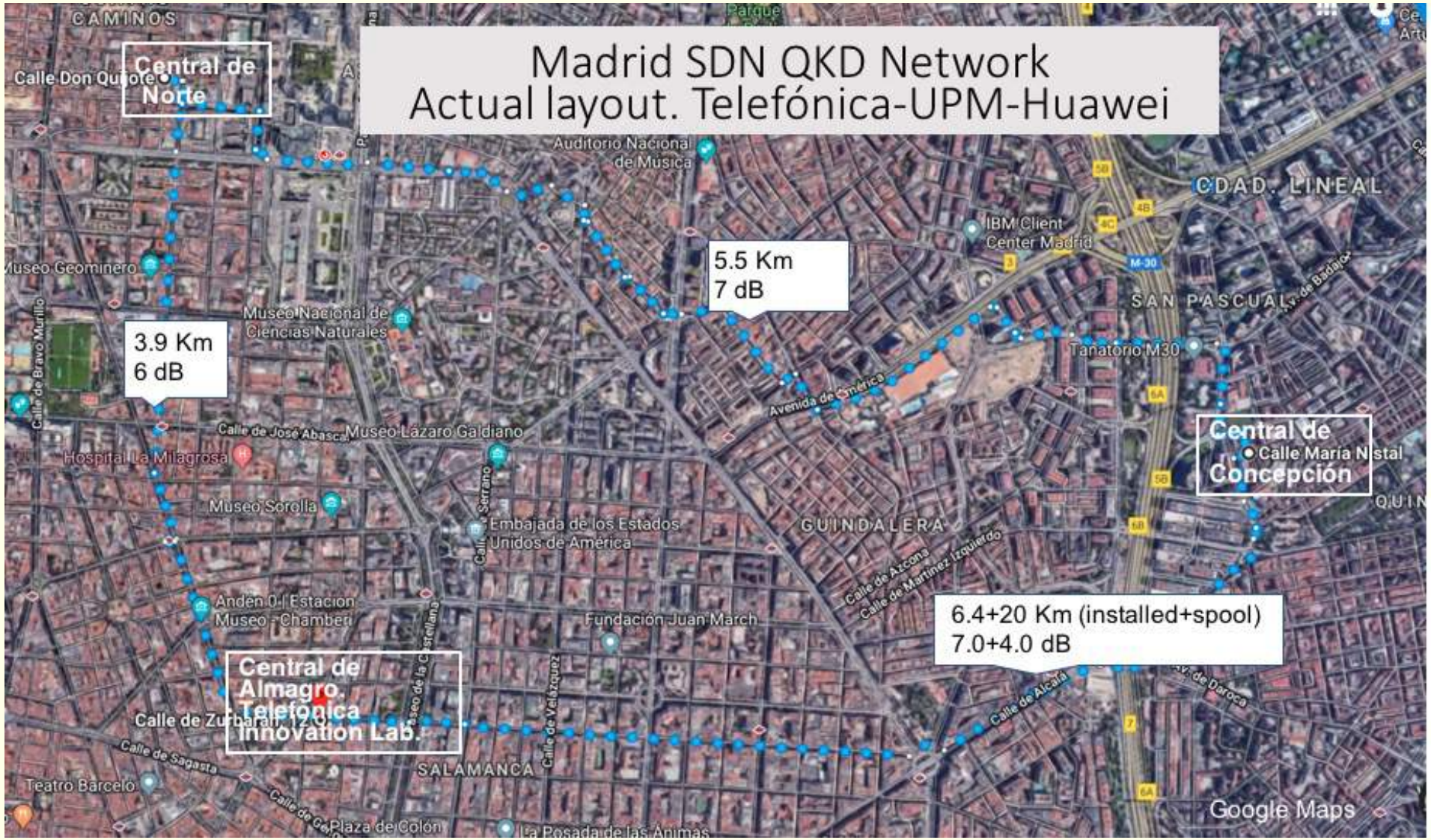


Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

Single Photon (approx. scale)

R. Doisneau

Does not play well in telco networks?



It does…

First Quantum SDN Network in the world.

Installed in Telefónica Spain **production facilities**.

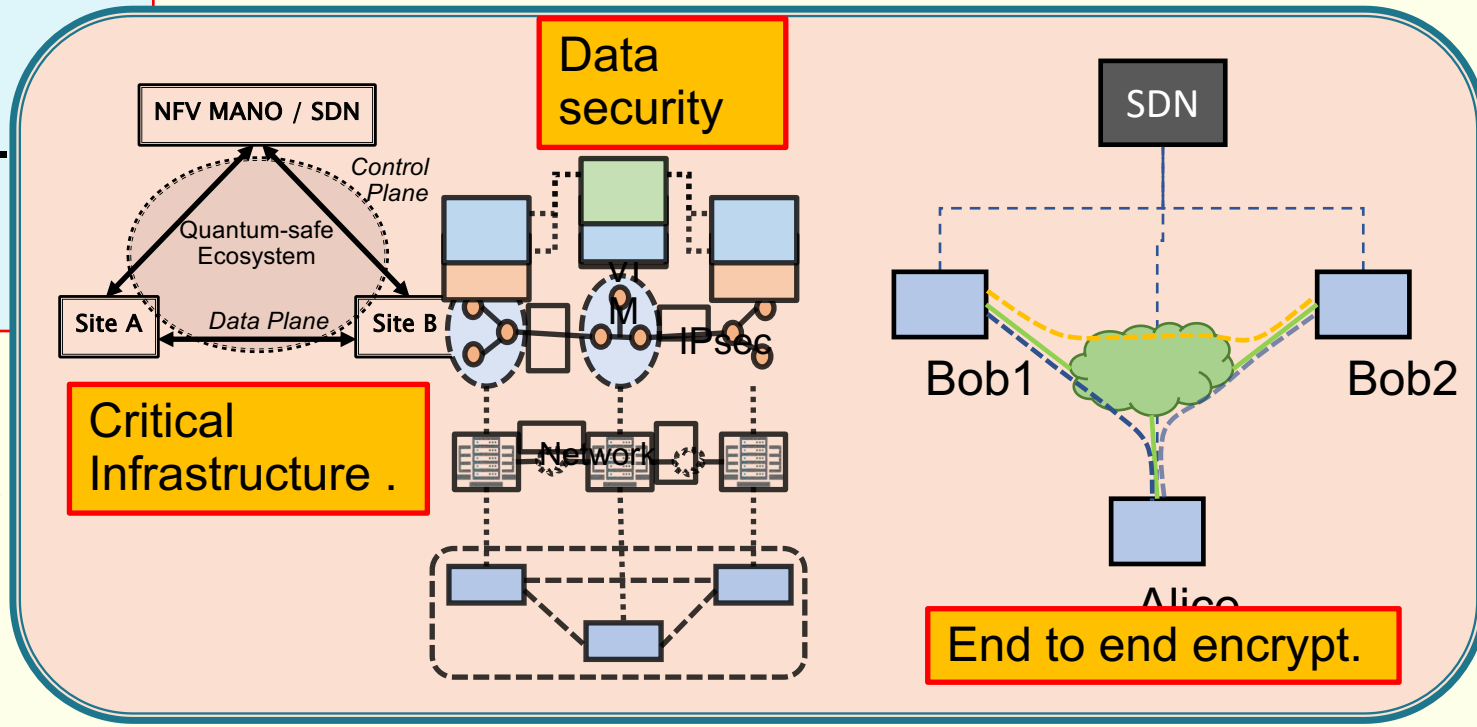
Madrid Quantum Network: First SDN-QKD network in the world

Use the correct technology

- **SDN** – Software Defined Networking
  - Network Flexibility
- **CV-QKD** technology:
  - Better tolerance to noise: quantum/classical copropagation.
  - Prospective industrialization path

EU H2020
Grant 820466

Real world use cases:



Future

- Evolution of the Madrid Quantum Network.
  - RedIMadrid.
  - EU H2020 Project in negotiation phase.
  - Beyond QKD

EU H2020
Grant 820466

EU H2020
Grant 820466

Madrid Quantum Network

Comunidad de Madrid
S2018/TCS-4342

CvQuCo - MINECO/FEDER TEC2015-70406-R

A. Aguado[1], P. Salas[1],
A.L. Sanz[1], J.P. Brito[1],
D. R. Lopez[2], V. Lopez[2],
A. Pastor[2], J. Folgueira[2],
F. de la Iglesia[2] , H.H. Brunner[3],
S. Bettelli[3], F. Fung[3],
D. Hillerkuss[3], L. C. Comandar[3],
D. Wang[3], A. Poppe[3] ,
M. Peev[3] and V. Martin[1],

[1]Center for Computational Simulation and ETSI Informáticos, Universidad Politécnica de Madrid 28660 Madrid, Spain
[2]Telefónica Investigacion y Desarrollo, Ronda de la Comunicacion s/n 28050 Madrid. Spain
[3]Huawei Technologies Duesseldorf GmbH, Riesstrasse 25, 80992 München. Germany

Thanks!...
Questions/comments?

Vicente Martin
U. Politécnica de Madrid
Vicente@fi.upm.es
gcc.fi.upm.es