Criptografía Cuántica en espacio libre

Verónica Fernández Mármol,
Consejo Superior de Investigaciones Científicas (CSIC),
Instituto de Tecnologías Físicas y de la Información (ITEFI)
C/ Serrano 144, Madrid 28006, Spain

veronica.fernandez@csic.es

Instituto de Tecnologías Físicas y de la Información

CSIC

Amenaza a la seguridad

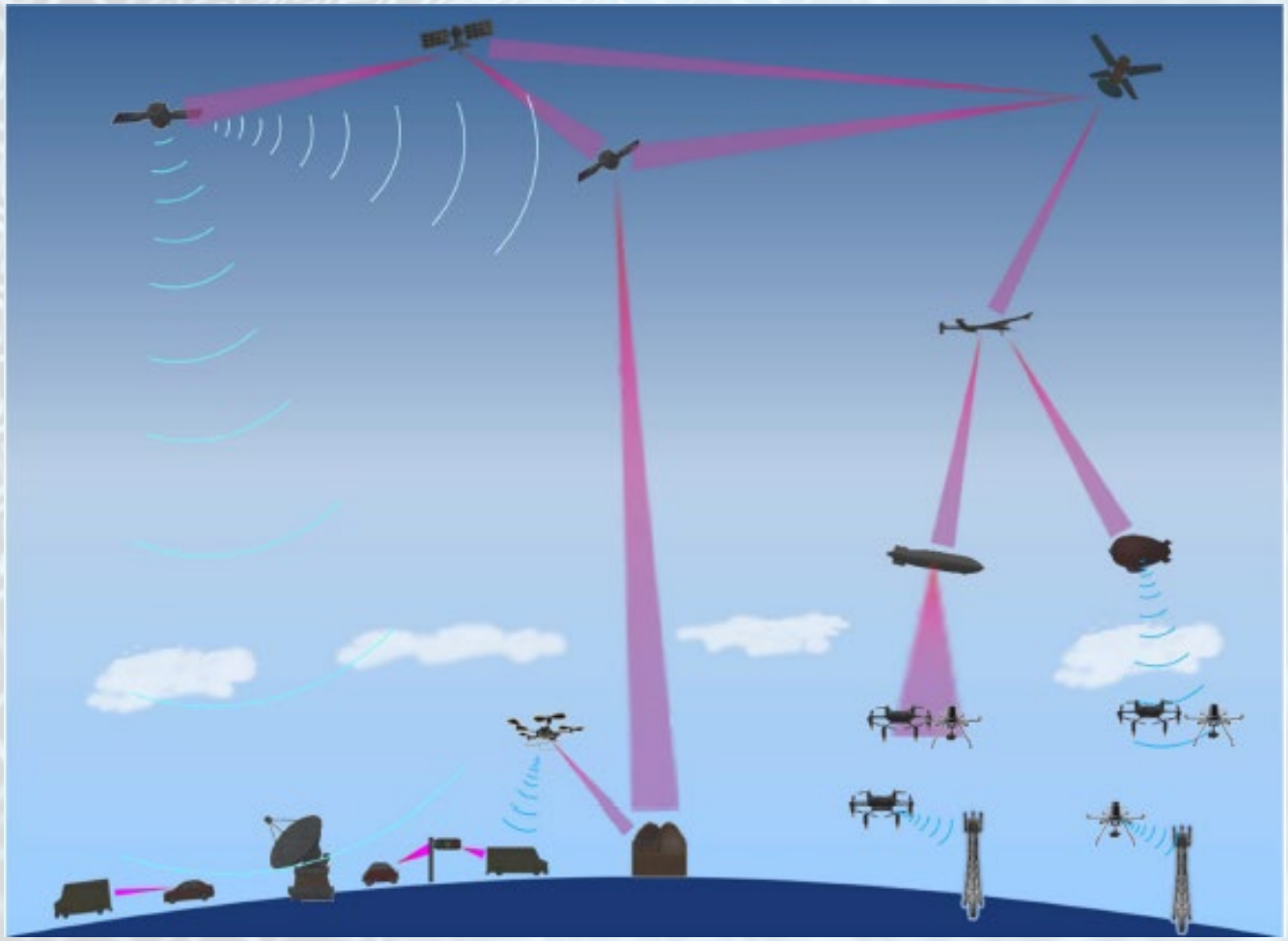
- Todo lo que no esté cifrado con tecnologías *quantum safe* será susceptible de ser descifrado por un ordenador cuántico exponiendo:
  - Información de empresas: secretos industriales
  - Información de gobiernos, agencias de inteligencia y organismos militares: altamente sensible y de seguridad nacional
  - Información de infraestructuras críticas: transporte, energía, etc.
  - Información de los ciudadanos: datos médicos, personales, etc.
- ¿Cuando estará aquí el ordenador cuántico? Organismos como el NIST estiman 10 años…

Comunicaciones Quantum Safe

- Distribución Cuántica de Clave (Quantum Key Distribution, QKD)
  - Seguridad *incondicional* (No puede romperse ni con infinita capacidad computacional)

Redes de comunicaciones ópticas en espacio libre

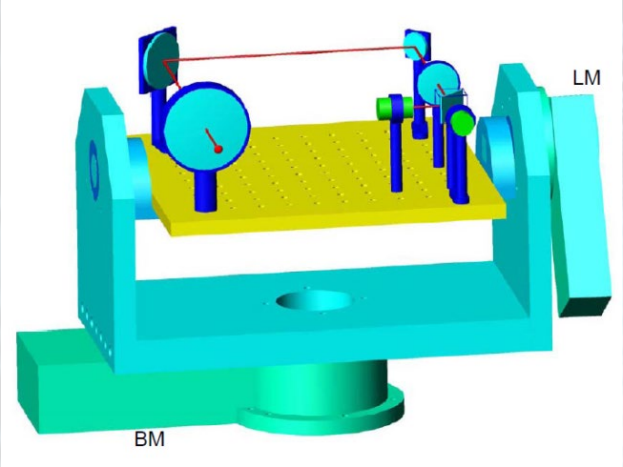
- Plataformas estacionarias:
  - Estaciones base, edificios, etc.
- Plataformas móviles:
  - UAVs, drones,
  - aviones,
  - vehículos autónomos, etc.
- Seguridad QKD
  - Retos:
    - Velocidad
    - Turbulencia



Ref. M. Sasaki, *Quantum Sci. Technol.*, **2**, 020501, 2017

Objetivo:
enlace aéreo de QKD
a alta velocidad
en alta turbulencia

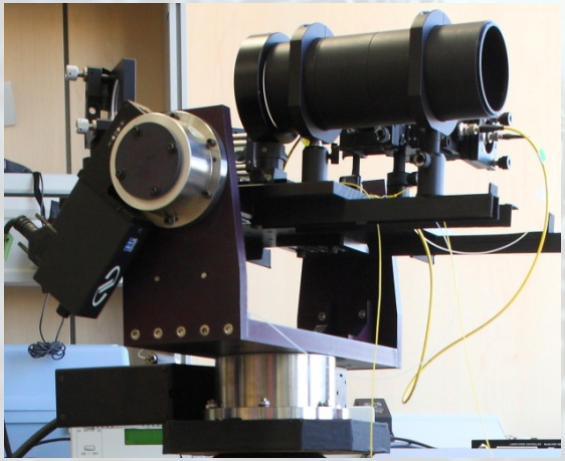
Transmisor: Alice



$\lambda \sim 850$ nm, señal cuántica

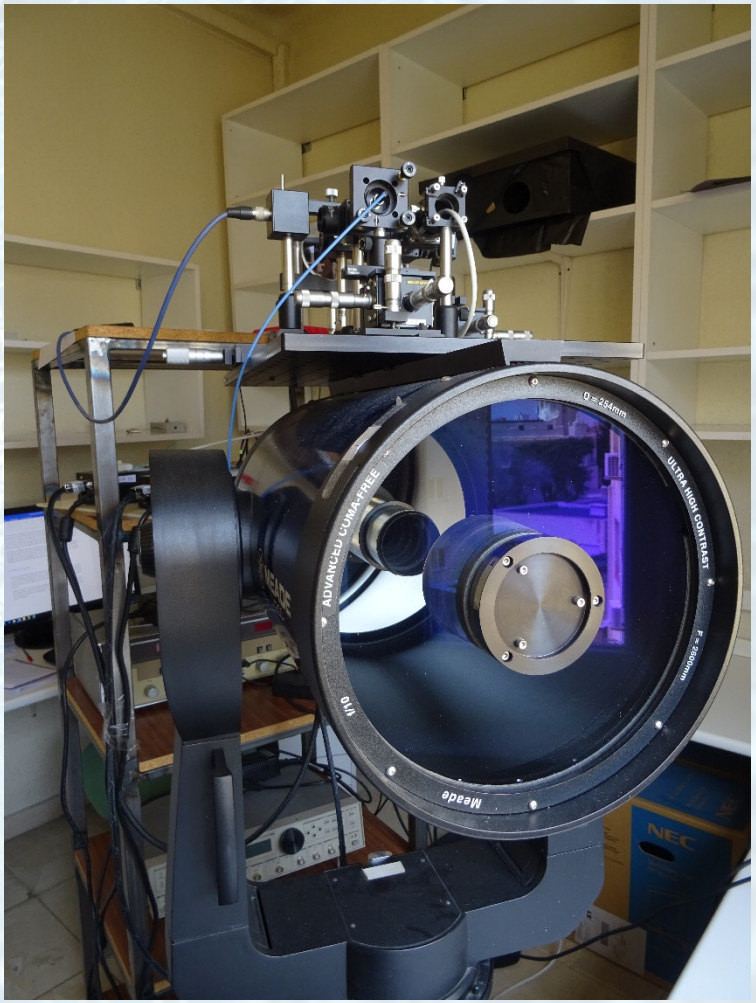
$\lambda \sim 1550$ nm, señal de sincronizado

- Frecuencias de GHz
- Alta precisión temporal



Receptor: Bob

- Telescopio Schmidt-Cassegrain
- Detectores de fotones individuales comerciales de Silicio
- Analizador de intervalos de tiempo de alta precisión
- Filtrado de la radiación solar



Enlace de QKD 300 m

Instituto de Tecnologías Físicas y de la Información (ITEFI)

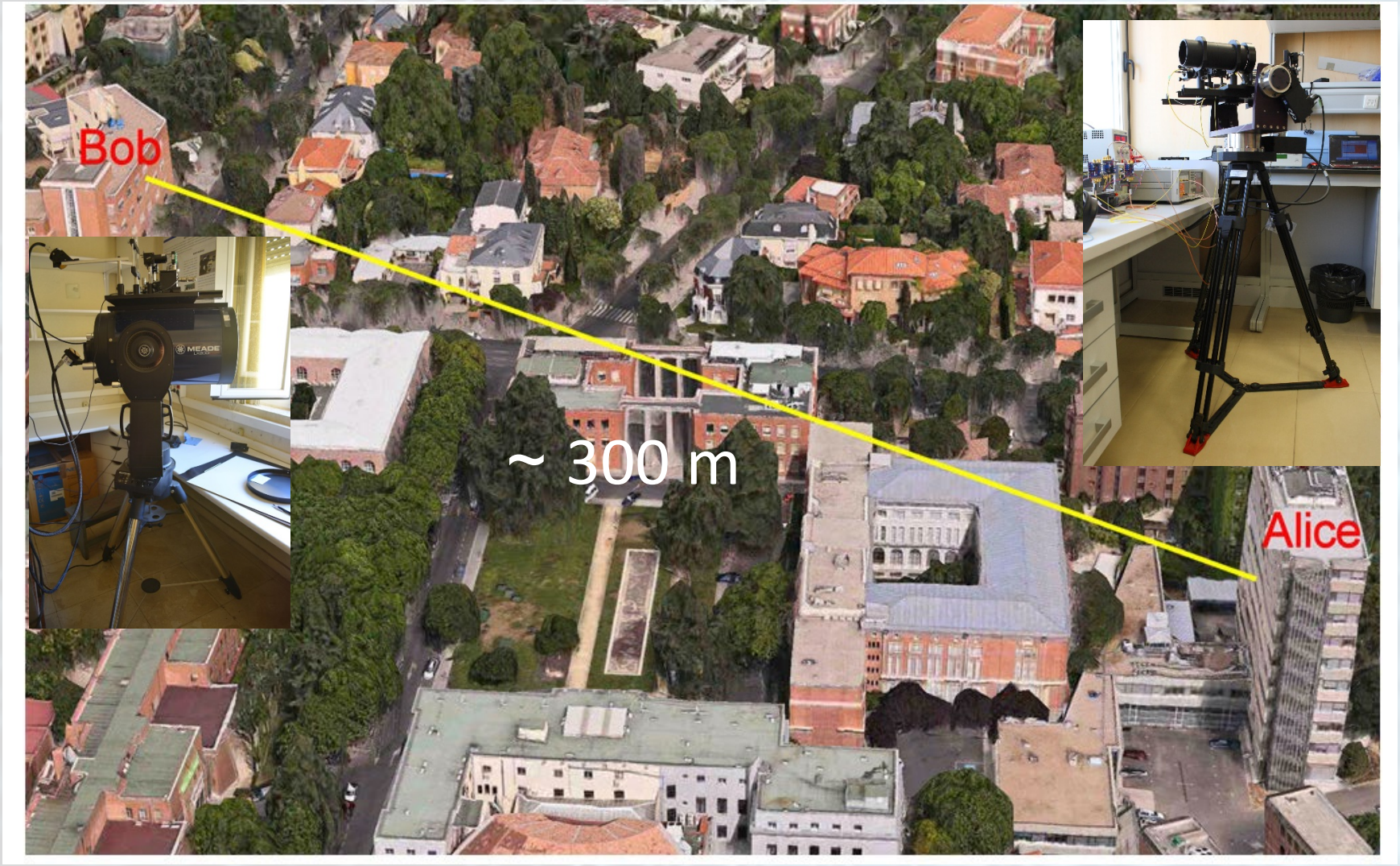
CSIC
Consejo Superior de Investigaciones Científicas

(≈1-2km debido a las pérdidas del telescopio a 850nm extra de -5dB)

Instituto de Ciencias Agrarias

CSIC
Consejo Superior de Investigaciones Científicas

Pruebas a 300 metros



Enlace de QKD a 300m

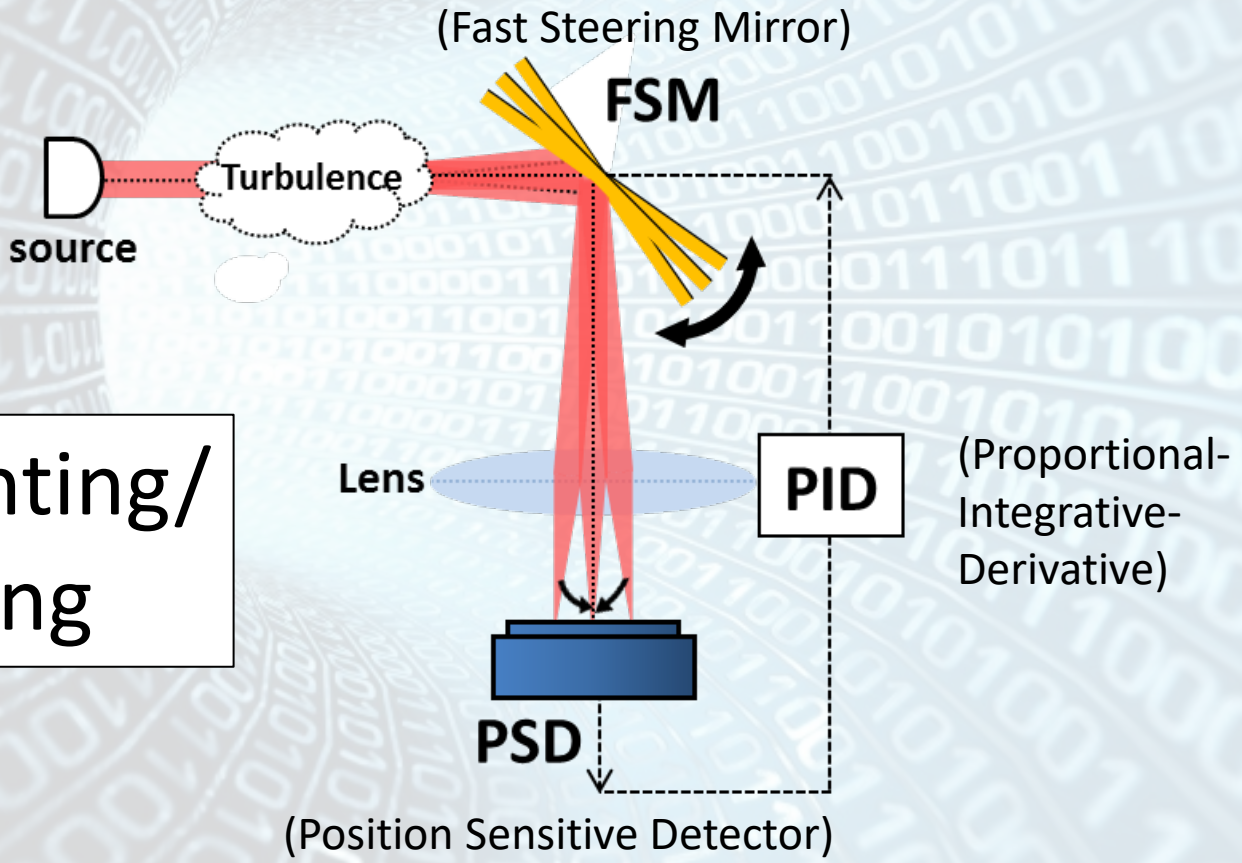
- Tasa de clave segura (considerando ataques PNS+USD)
  - 1Mbps (noche)
  - 700 kbps (día)

1 orden de magnitud

- Limitación: Turbulencia y ruido solar

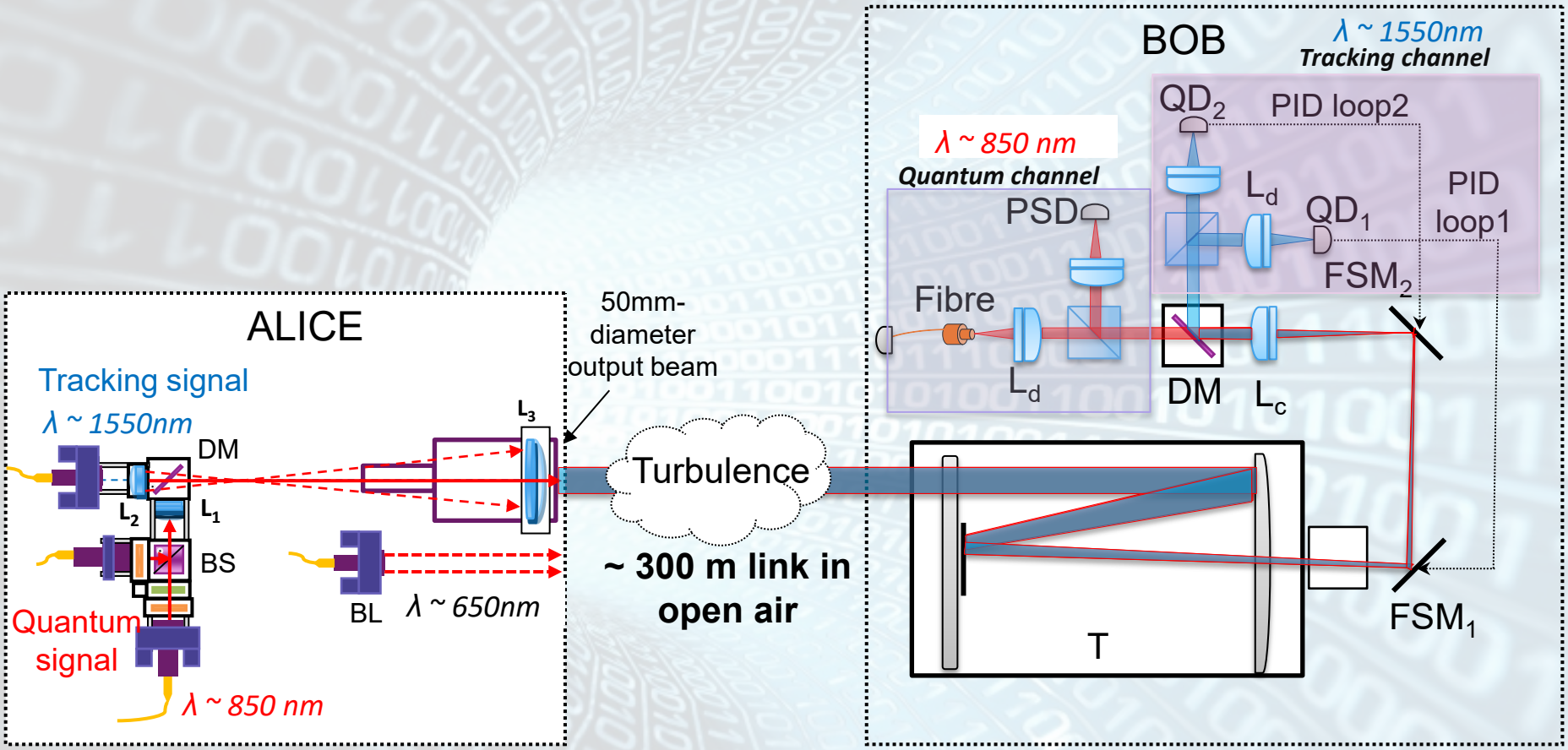
M. J. García-Martínez et al, *Applied Optics,* 52, (14), pp. 3311-3317, (2013)

Corrección activa de turbulencia atmosférica



Fine pointing/ tracking

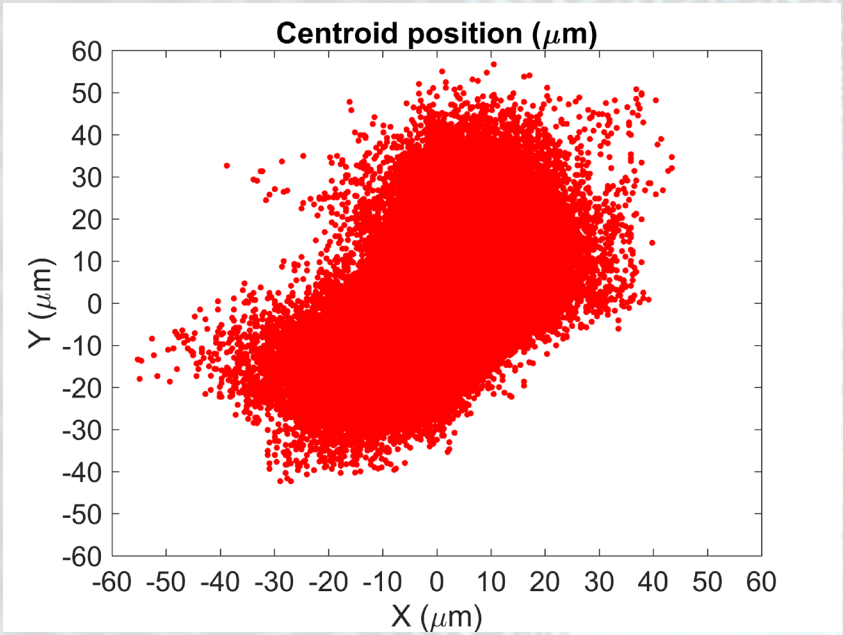
Pruebas a 300 metros

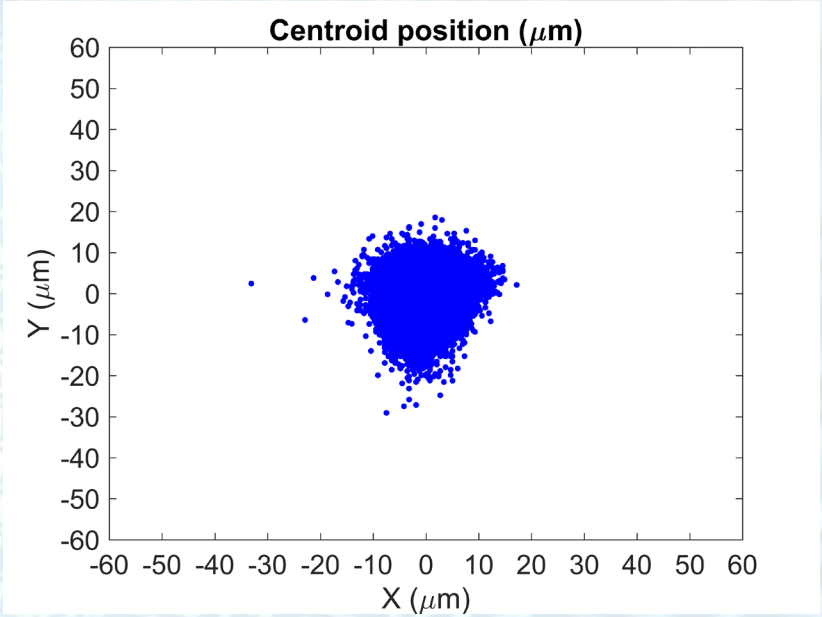


A. Carrasco-Casado, N. Denisenko and V. Fernandez, Optical Engineering, 53 (8), 084112 (2014)

V Fernandez et al, IEEE Access, Vol 6, Issue1, pp. 3336-3345 (2018)

Reducción del ruido después de corregir





hasta 3 veces menor área en el plano focal del receptor

Reducción de hasta 90% en error cuántico QBER en condiciones de alta turbulencia
Aumento tasa de clave segura

Trabajo actual

- Desarrollo de otros protocolos de QKD basado en variables continuas, inmunes a la radiación solar y canal aéreo o fibra
- Adaptación a plataformas móviles

¿Cómo colaborar?

- A través de los dos tipos de contratos que tiene el CSIC o a través de proyectos del CDTI o europeos
- Proyectos de desarrollo para pasar de TRLs medios a altos y transferibles a la industria y a la sociedad (organismos dispuestos a llevar a cabo parte de las tareas)
- Proyectos de investigación en los que los organismos interesados inviertan en la investigación realizada del CSIC


Gracias
veronica.fernandez@csic.es