The Abdus Salam International Centre for Theoretical Physics

United Nations Educational, Scientific and Cultural Organization

International Atomic Energy Agency

SMR.1738 - 19

WINTER COLLEGE
on
QUANTUM AND CLASSICAL ASPECTS
of
INFORMATION OPTICS

30 January - 10 February 2006

Free Space Quantum Cryptography

J.G. RARITY

Department of Electrical & electronic Engineering
University of Bristol
Bristol
UK

Strada Costiera 11, 34014 Trieste, Italy - Tel. +39 040 2240 111; Fax +39 040 224 163 - sci_info@ictp.it, www.ictp.it

ESA: QIPS

Trieste lecture 2
Free Space Quantum Cryptography

7th Feb 2006

J. G. Rarity
University of Bristol
john.rarity@bristol.ac.uk

LMU Munich
University of Bristol
University of Vienna
QinetiQ
HP labs Bristol

FP6: IP
SECOQC
www.secoqc.net

IP: QAP

University of BRISTOL

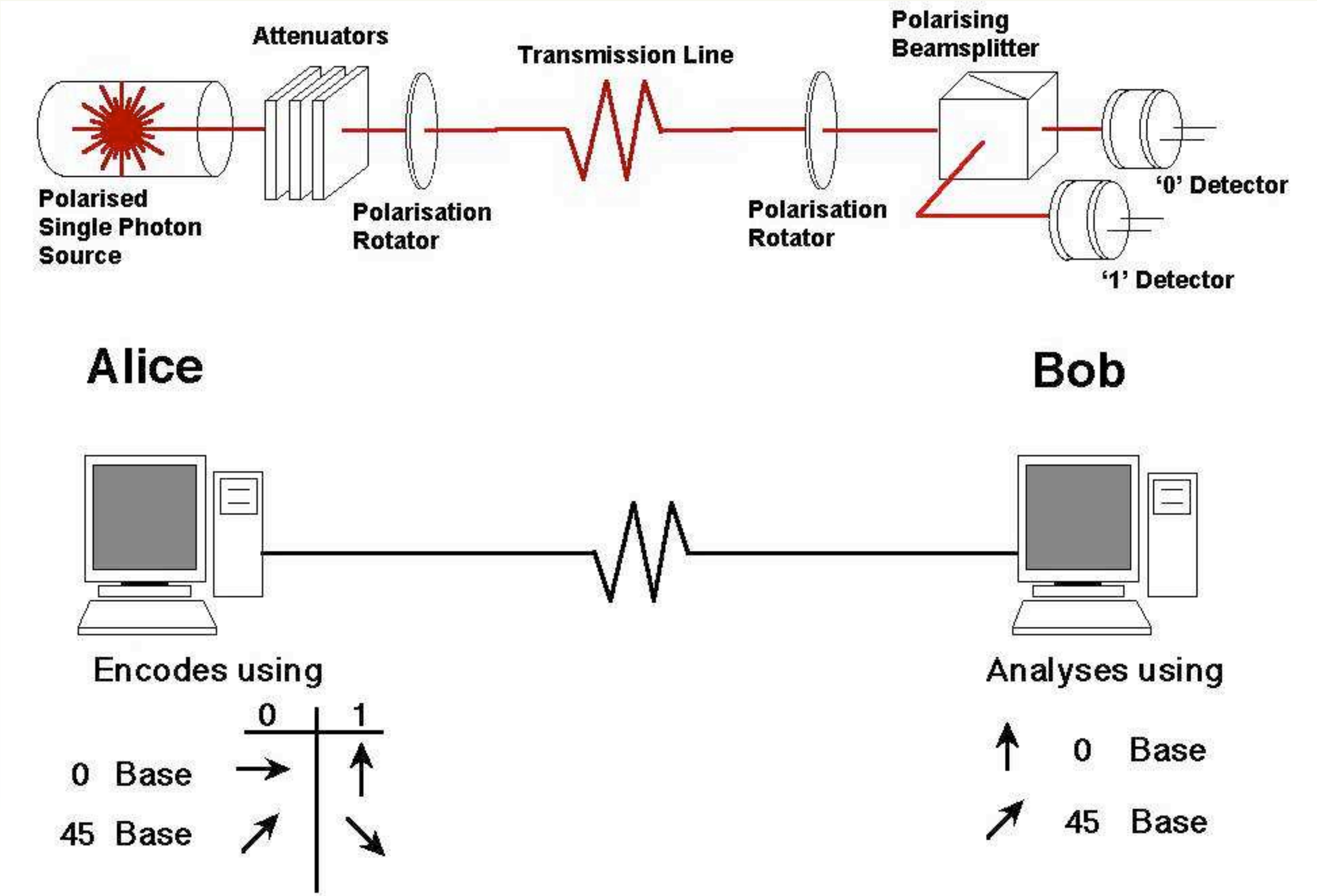
Overview

- Introduction to quantum cryptography
  - Faint pulse
  - Entangled state
- Experiments
  - Faint pulse
  - Heralded entangled photon
- Performance limits
- Future experiments

Bennett and Brassard 1984
Secure key exchange using quantum cryptography

Sends

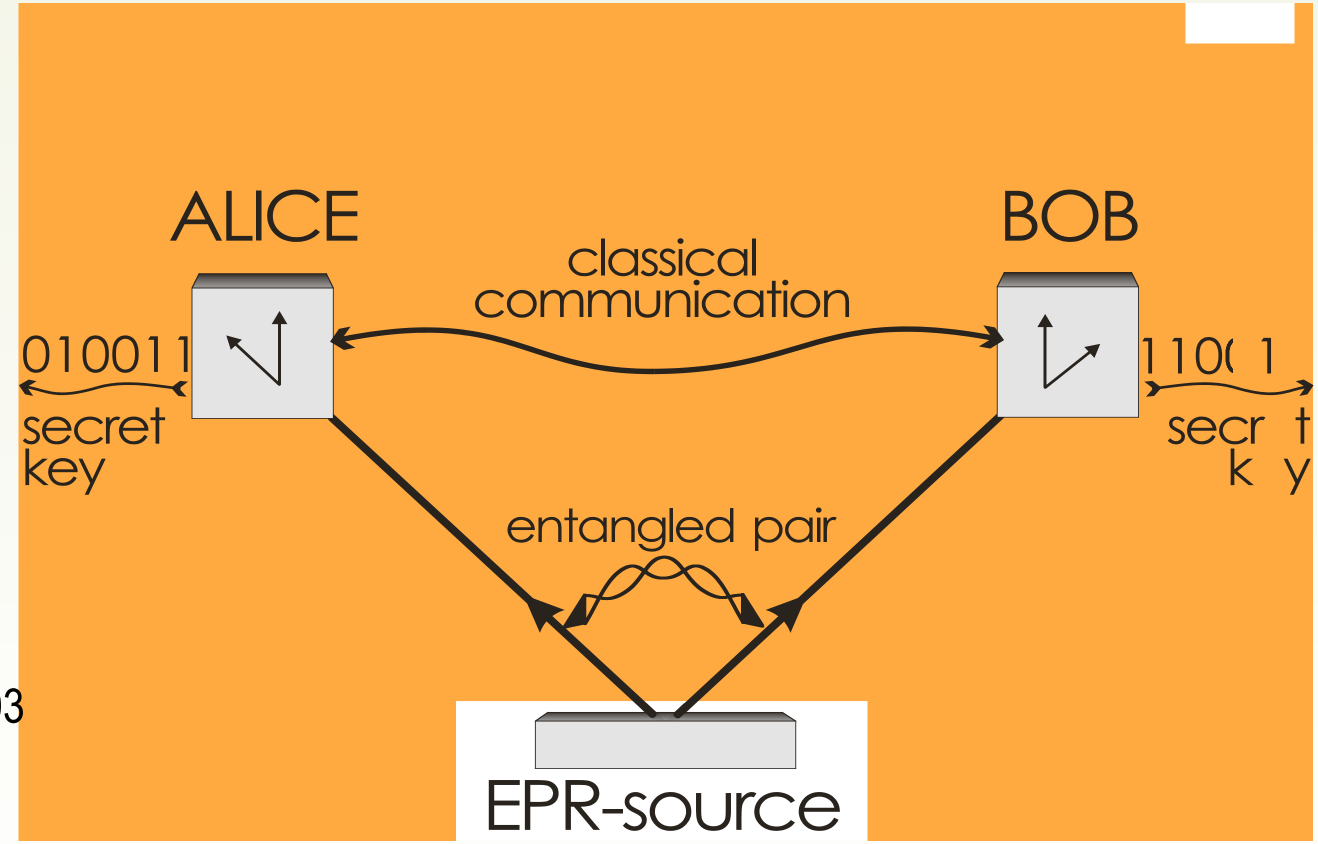
no.	bit	pol.
1	1	45
2	0	45
3	0	0
4	1	45
5	1	0
6	0	45
7	1	45
…		
1004	0	45
1005	1	0
….		
3245	1	45
…		



Receives

no.	Bit	Pol.
246	1	45
1004	0	45
2134	0	0
3245	0	0
4765	1	0
5698	0	45

Entanglement and key exchange



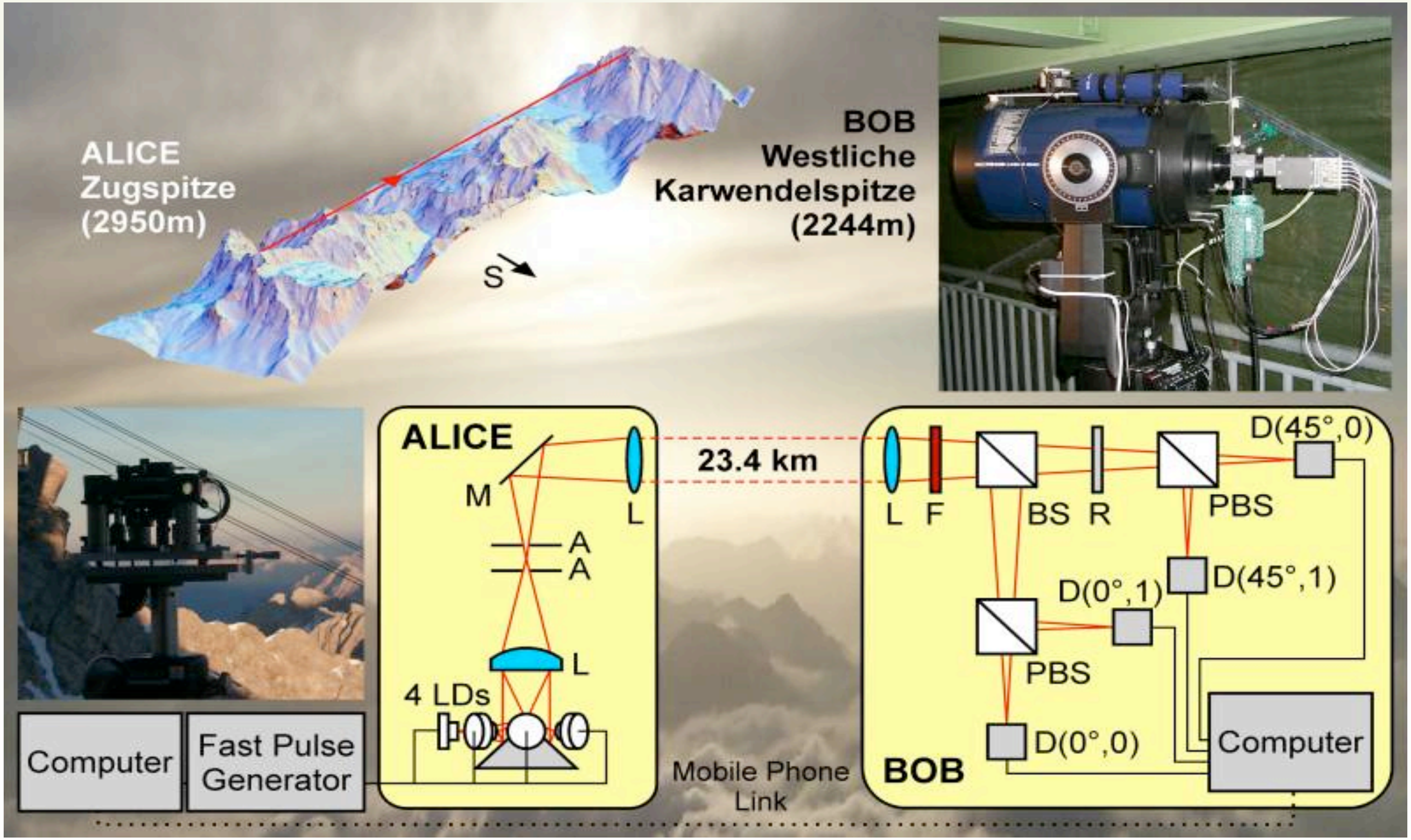
Aspelmeyer et al
Science August 2003

$$|\Psi\rangle = \tfrac{1}{\sqrt{2}}\left(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B\right)$$

$$\equiv \tfrac{1}{\sqrt{2}}\left(|'45'\rangle_A |'45'\rangle_B + |'-45'\rangle_A |'-45'\rangle_B\right)$$

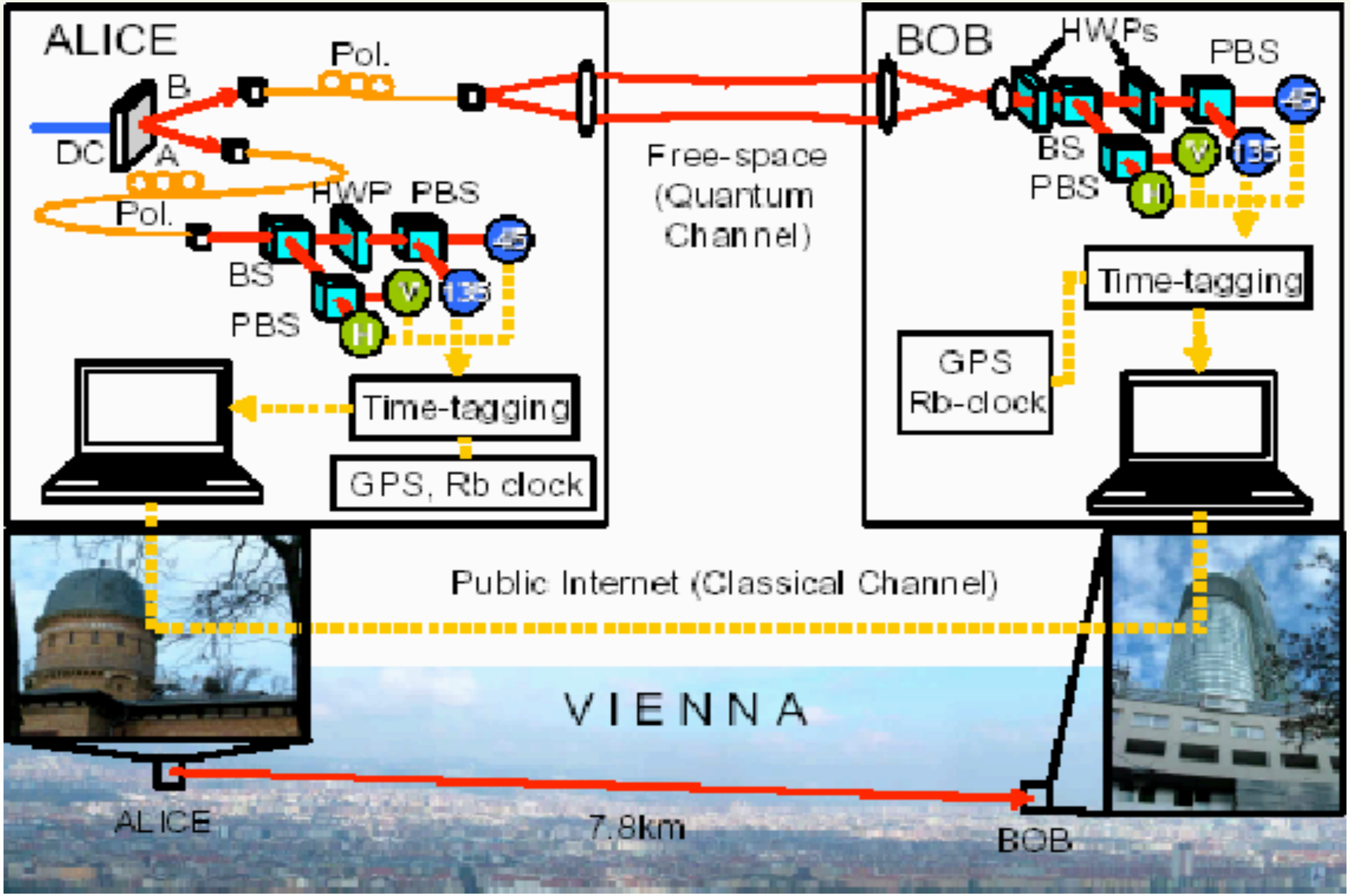
University of BRISTOL

Previous faint pulse free space experiment over 23.4km



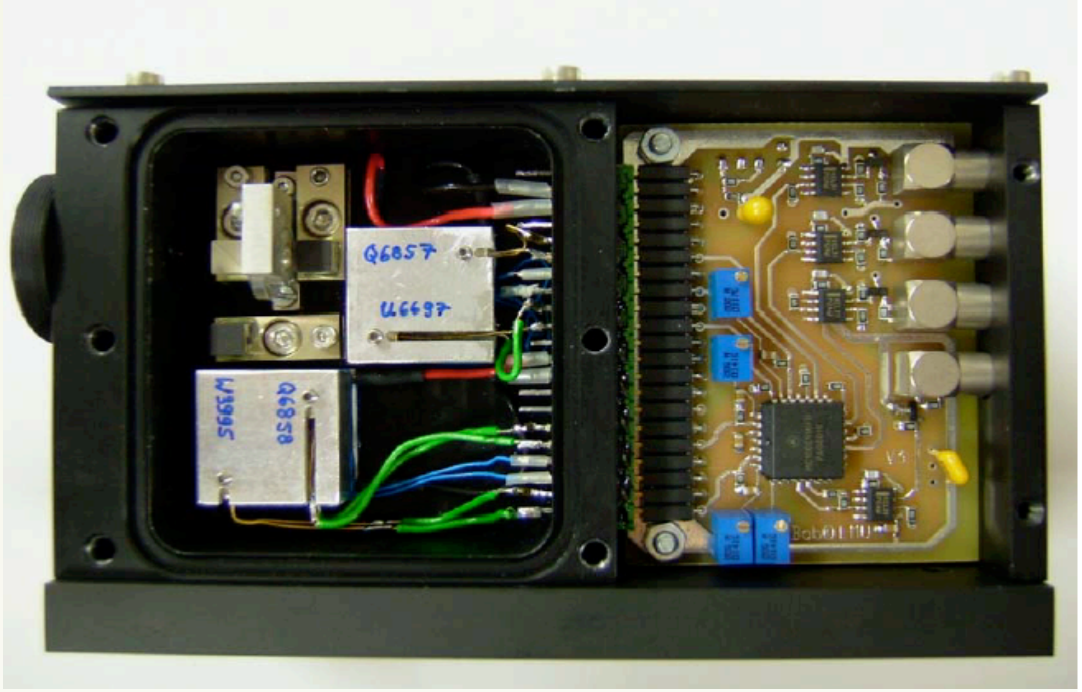
Kurtsiefer et al, (2002), *Nature,* **419**, 450.

Entangled state/heralded single photon system

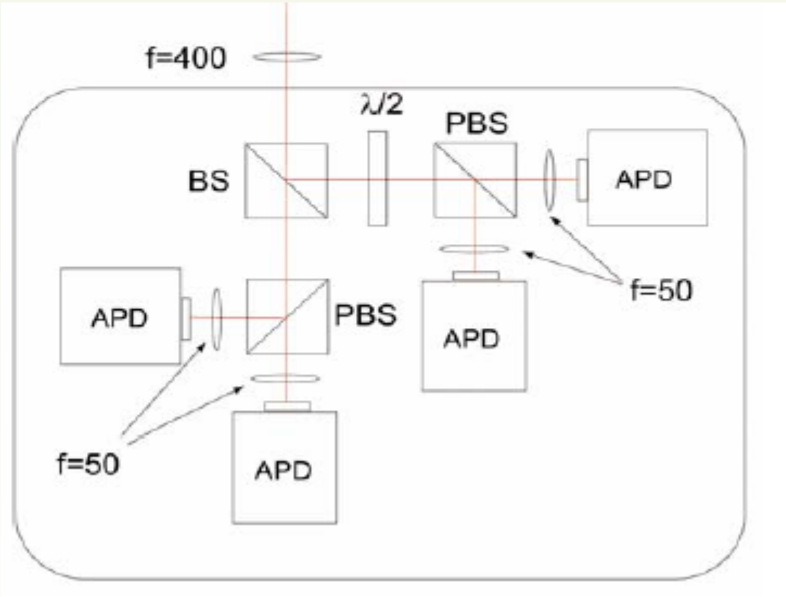


K. J. Resch, Optics Express 13, 202-9 (2005)

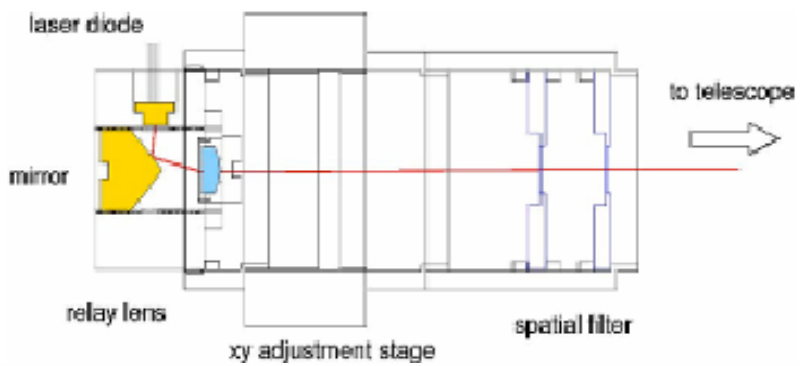
Miniature Bob detector unit:



Medium Bob (F5 optics)



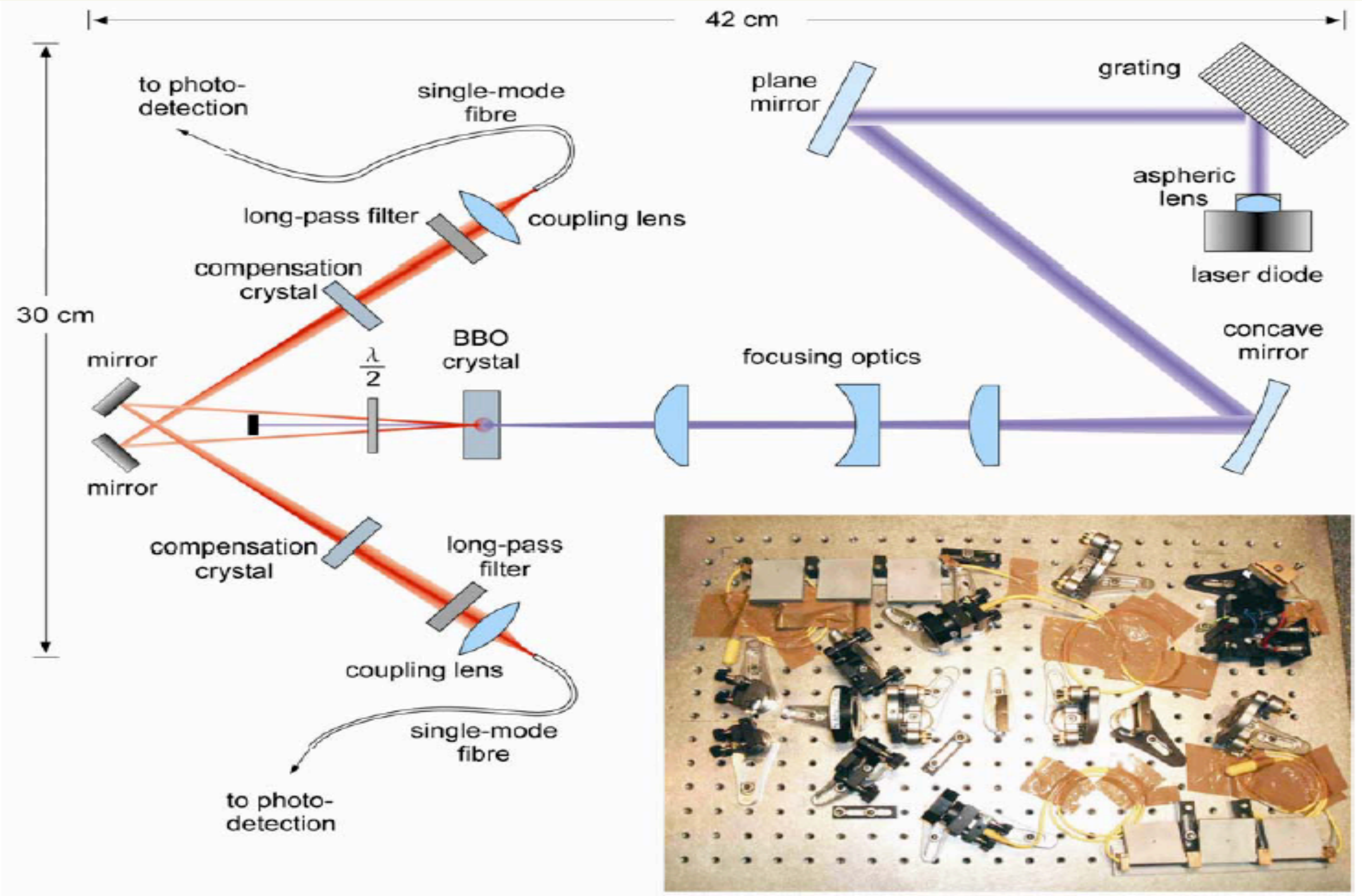
Miniature Alice



Portable Crystal based entangled pair source

150mW diode

70000 detected coincidences/sec



Transmission limitations of any system

Background count error probability per pulse

$P_b = Bt/4$ (half lead to errors)

The photo-count probability

$P_p = \mu T \eta / 2$ (BB84)

μ= photons per bit (0.1 faint pulse, ~0.75 heralded)

T = transmission (variable)

h= efficiency of receiver (20%)

B= background rate (~2000)

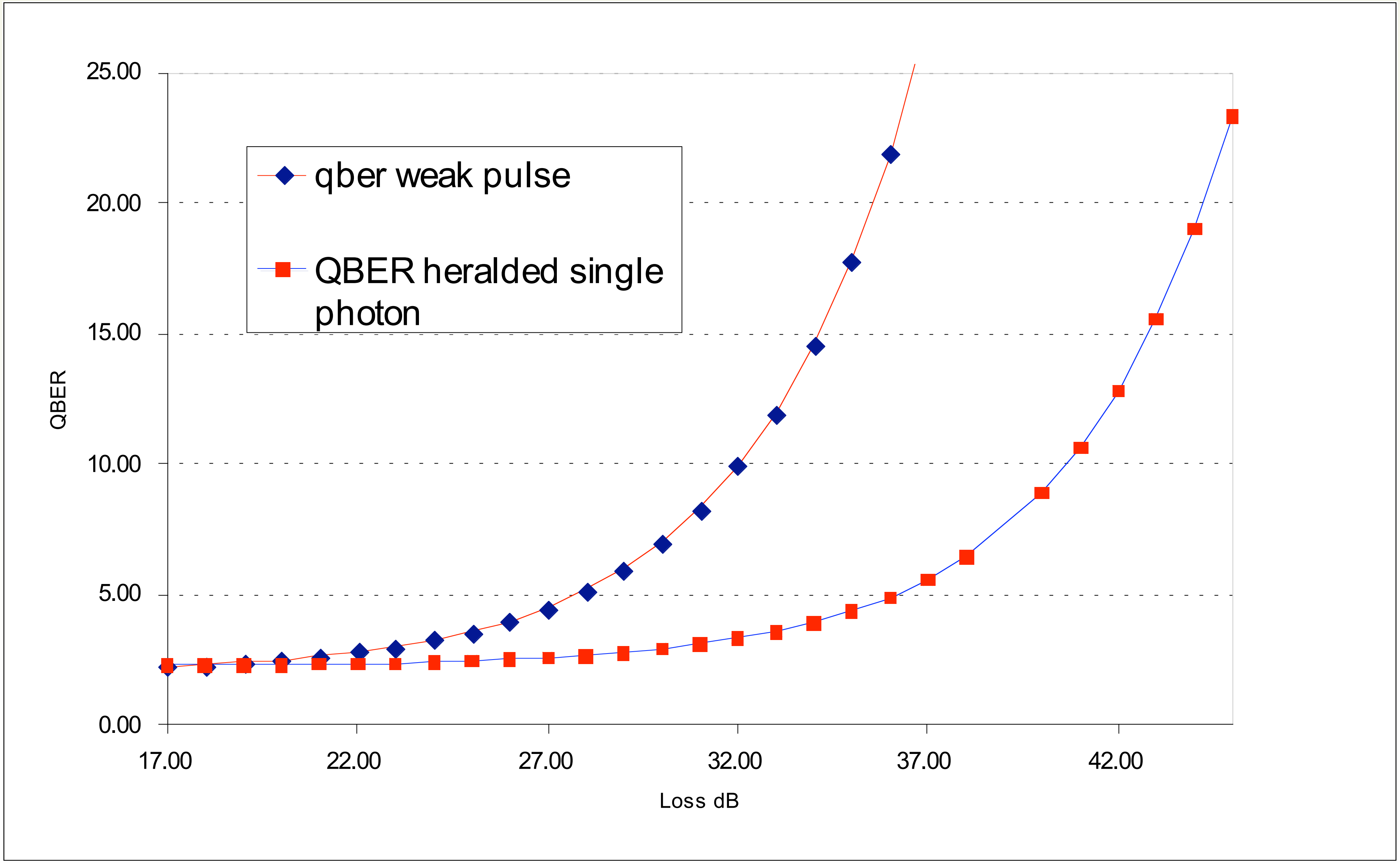
t= gate width (~1ns)

Error rate (QBER)

$$E = E_0 + Bt / 2\mu T \eta$$

E_0 is the technical error

QBER as a function of loss



University of BRISTOL

Secret bit yields, after error correction and privacy amplification

Raw bit rate

$$K = 10^{-L/10}\mu\eta_B R$$

Number of sifted bits in time *T*

$$n_{rec} = KT/2$$

Number of bits revealed in error correction [1]

$$n_E = n_{rec}(1-E)$$

$$E = \varepsilon\left(7/2 - \log_2(1-\varepsilon)\right)$$

Every error could be a result of eavesdropping

Information leakage [2]:

$$n_{leak} = n_{rec}\left(\log_2\left(1+4\varepsilon-4\varepsilon^2\right)\right)$$

Final key length thus given by:

$$n_{fin} = n_{rec} - n_E - n_{leak} - n_s$$

$$= n_{rec}\left(E - \log_2\left(1+4\varepsilon-4\varepsilon^2\right)\right) - n_s$$

n_s= excess reduction to enhance security

For Poisson sources all multiphoton pulses are insecure

$$n_{fin} = n_{rec}a\left(E - \log_2\left(1+4\frac{\varepsilon}{a}-4\left(\frac{\varepsilon}{a}\right)^2\right)\right) - n_s$$

$$a = \frac{e^{-\mu}.\mu}{1-e^{-\mu}}$$

Is the fraction of pulses containing photons that contain only one

Infinite technology Eve

Multi-photon pulses are split and sent on through a loss free channel to Bob.

$$n_{fin} = n_{rec}b\left(E - \log_2\left(1+4\frac{\varepsilon}{b}-4\left(\frac{\varepsilon}{b}\right)^2\right)\right) - n_s$$

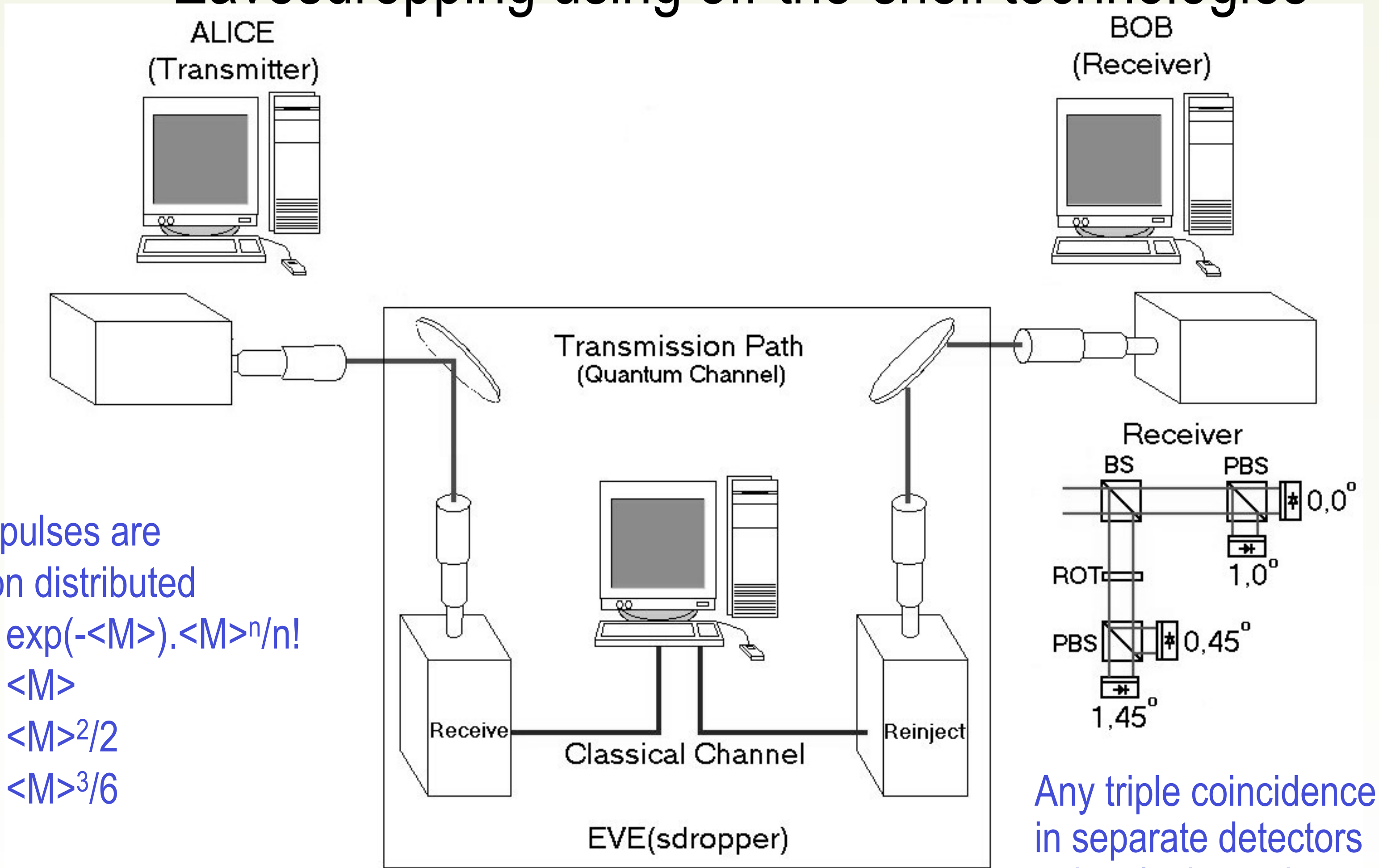
$$b = 1 - \frac{(1-a)}{10^{-L/10}} \quad \mu > 10^{-L/10}, b < 0$$

Eve can only get at >3 photon pulses

$$a' = a(1+M/2) \qquad b = 1 - \frac{(1-a')}{4T}$$

1. L. Tancevski,et al. Proc. SPIE, **3228**, 322-331 (1997).
2. N. Lutkenhaus, Phys. Rev. A 59, 3301–3319 (1999).
3. G. Brassard, et alPhys.Rev.Letts, **85,** pp1330-1333 (2000).

Eavesdropping using off-the-shelf technologies



Weak pulses are Poisson distributed

P(n) = exp(-<M>).<M>^{n}/n!

P(1) ~ <M>

P(2) ~ <M>^{2}/2

P(3) ~ <M>^{3}/6

P3)/P(1)=<M>^{2}/6

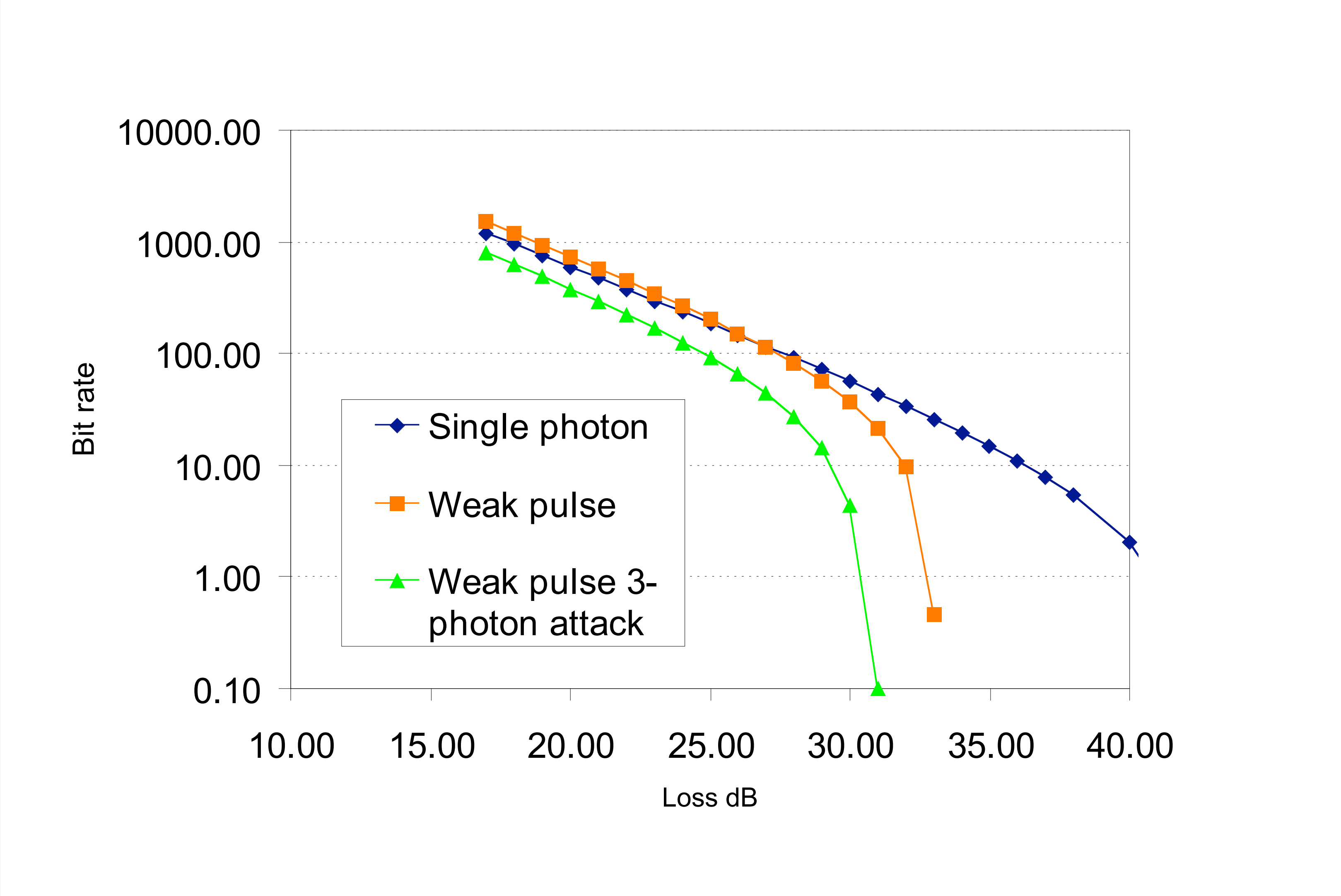
Any triple coincidence in separate detectors uniquely determines the state!!

Safe if M^2<24T

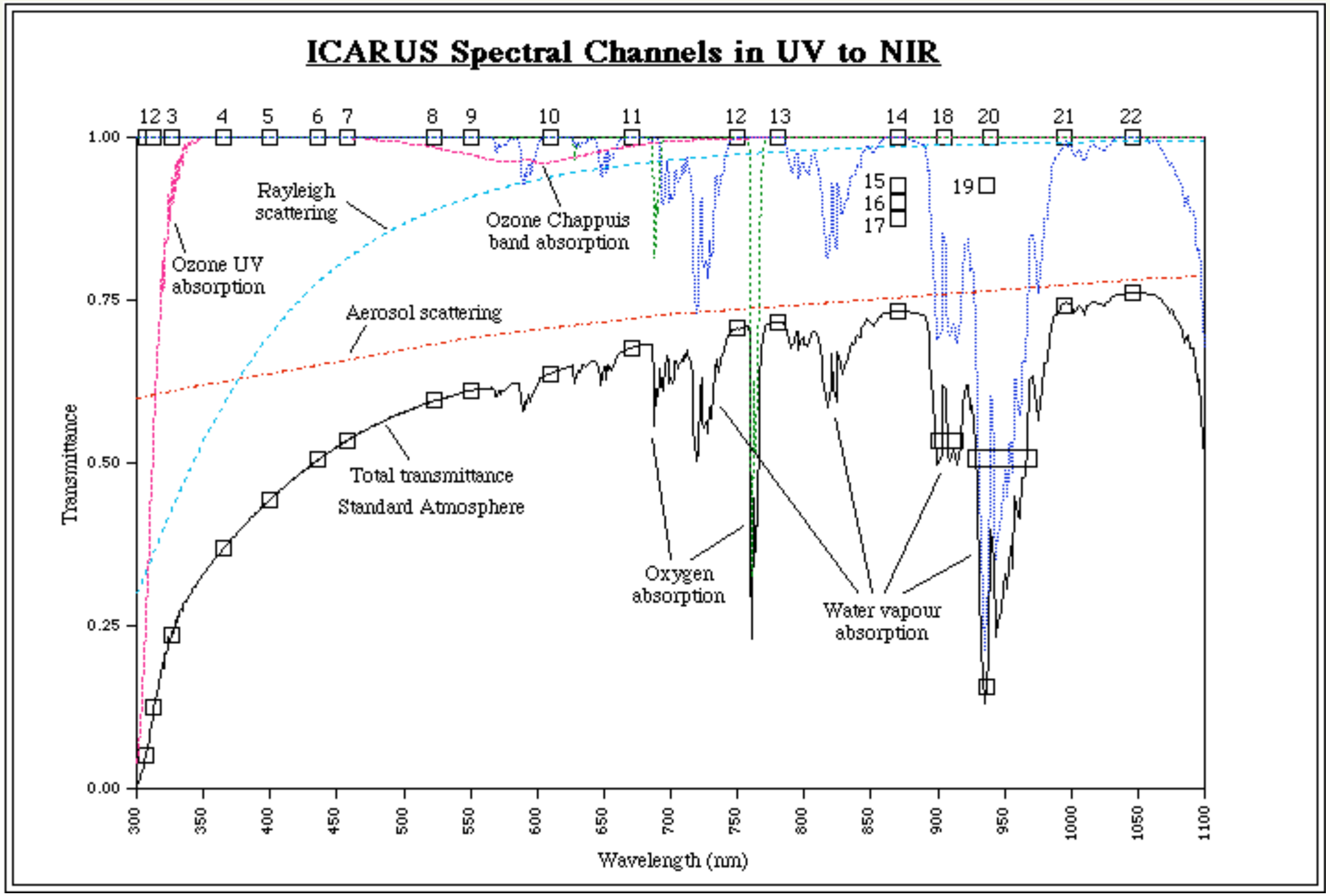
M~0.1 T> -33dB

University of BRISTOL

Expected Secret bit yields as a function of loss after error correction and privacy amplification



Atmospheric Transmission Windows for long range.



Chosen trial site:

1 - The Observatorio del Roque de los Muchachos (Island of La Palma)

http://www.iac.es/gabinete/orm/indice.html

2 - The Observatorio del Teide (Island of Tenerife)

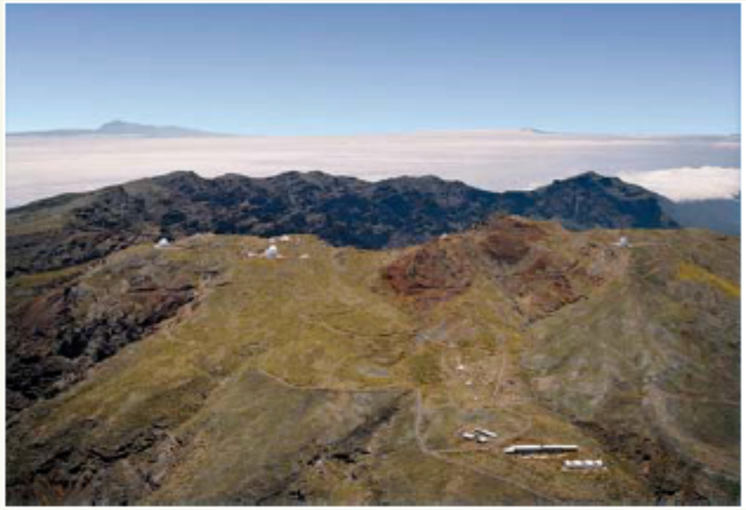
http://www.iac.es/ot/indice.html

The design and loss budget

- 10 MHz pulse rate, 0.1 photons/pulse
- Entangled source with >5.10^6 pairs/sec (>100000/s locally)
- 700/810/850nm wavelength
- <20 μR beam divergence
- Diffraction spot <3 m diameter after 144 km
- Expect ~40 μR from turbulence + ~10 dB absorption/scatter
- Collection and atmospheric transmission, 25-35dB loss
- Aim for background counts <2000 cps/detector through 10nm filter at night

University of BRISTOL

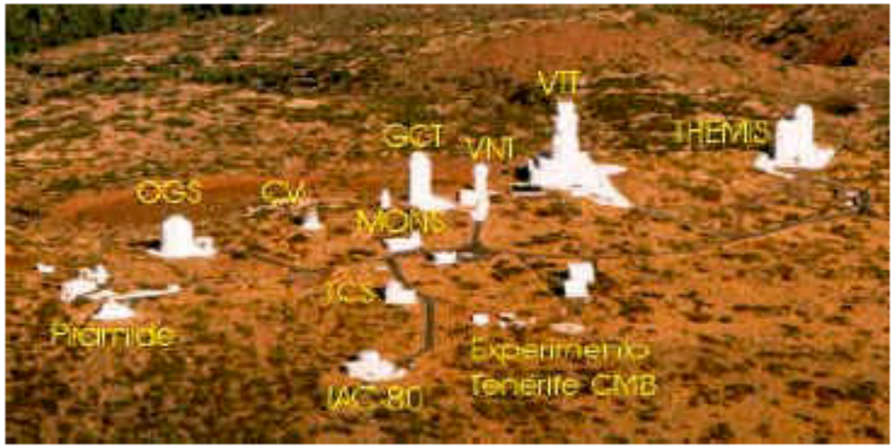
La Palma: Roque de los Muchachos



Overview of Roque with Tenerife in background

La Palma from Tenerife

Optical ground station Tenerife



Overview of Izana (Tenerife) site

OGS with mount Tiede in background

University of BRISTOL

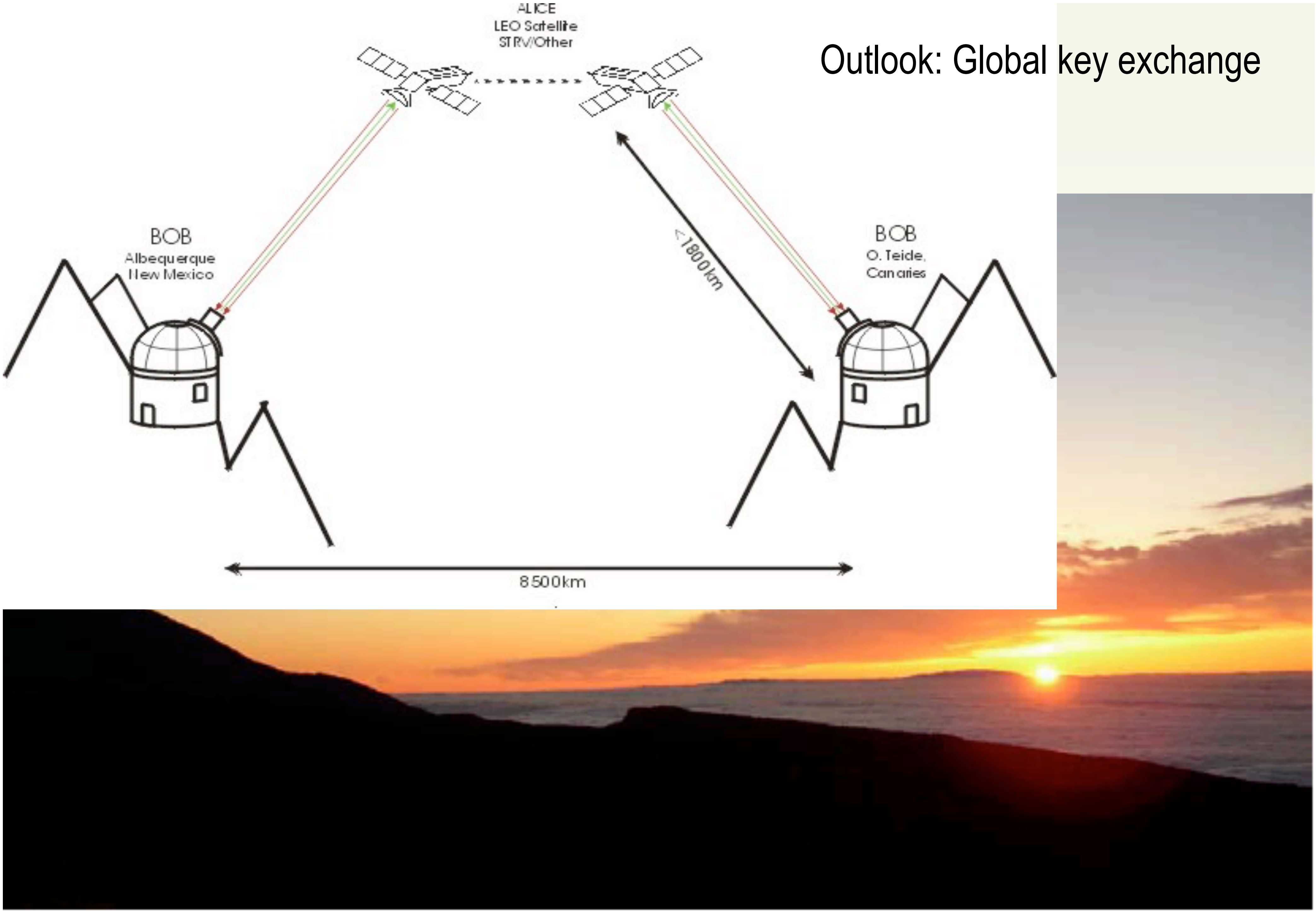
ESA OGS 1 metre telescope (Bob)

Metrology:

- Cartesian distance OGS - NOT : 143.630 km
- in position angle (North trough West) : 251°.
- Angle TNG-NOT-Teide: 123°.7 (vertex at NOT).

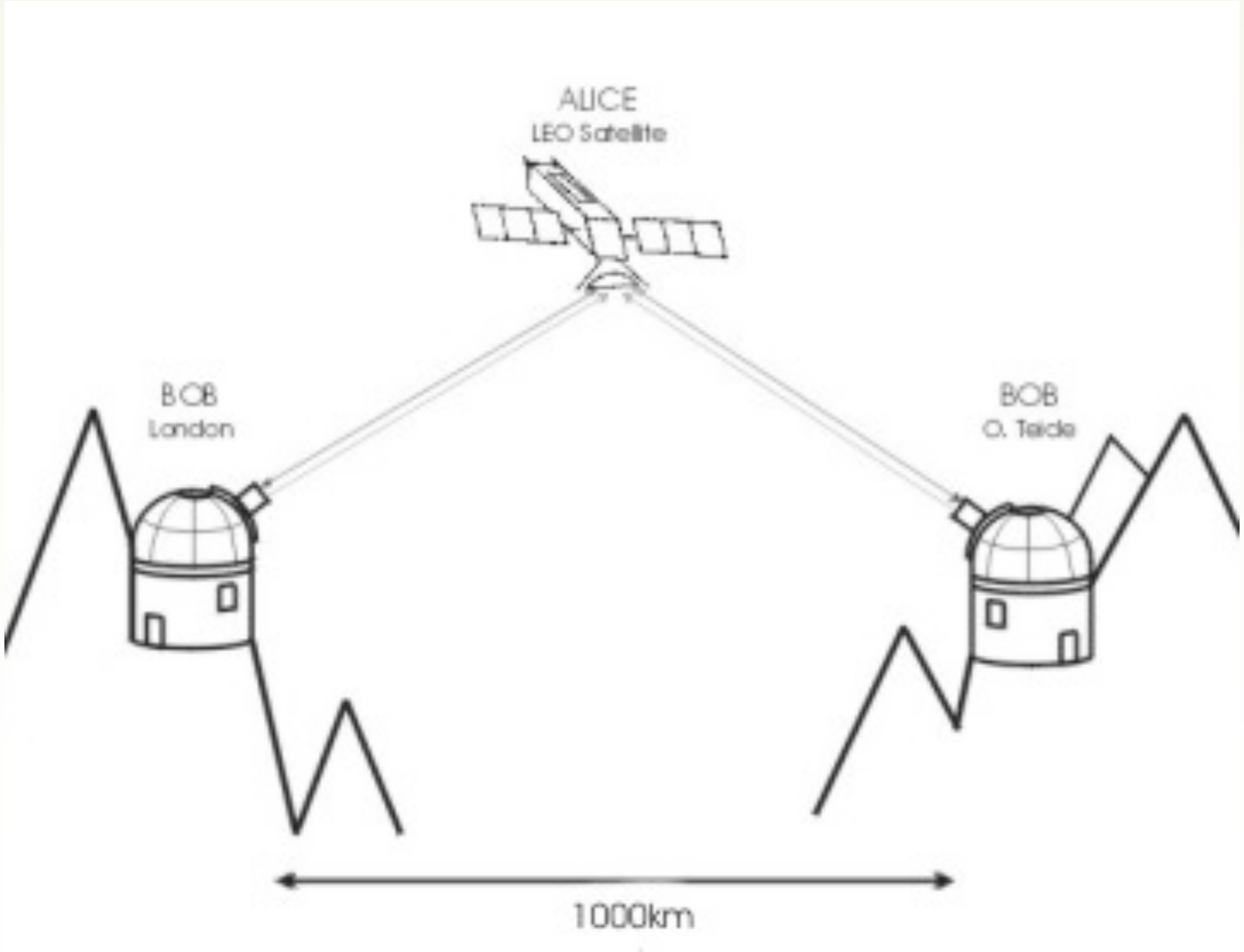
- Also possible Teide-OGS-La Palma (see TN4)

Outlook: Global key exchange

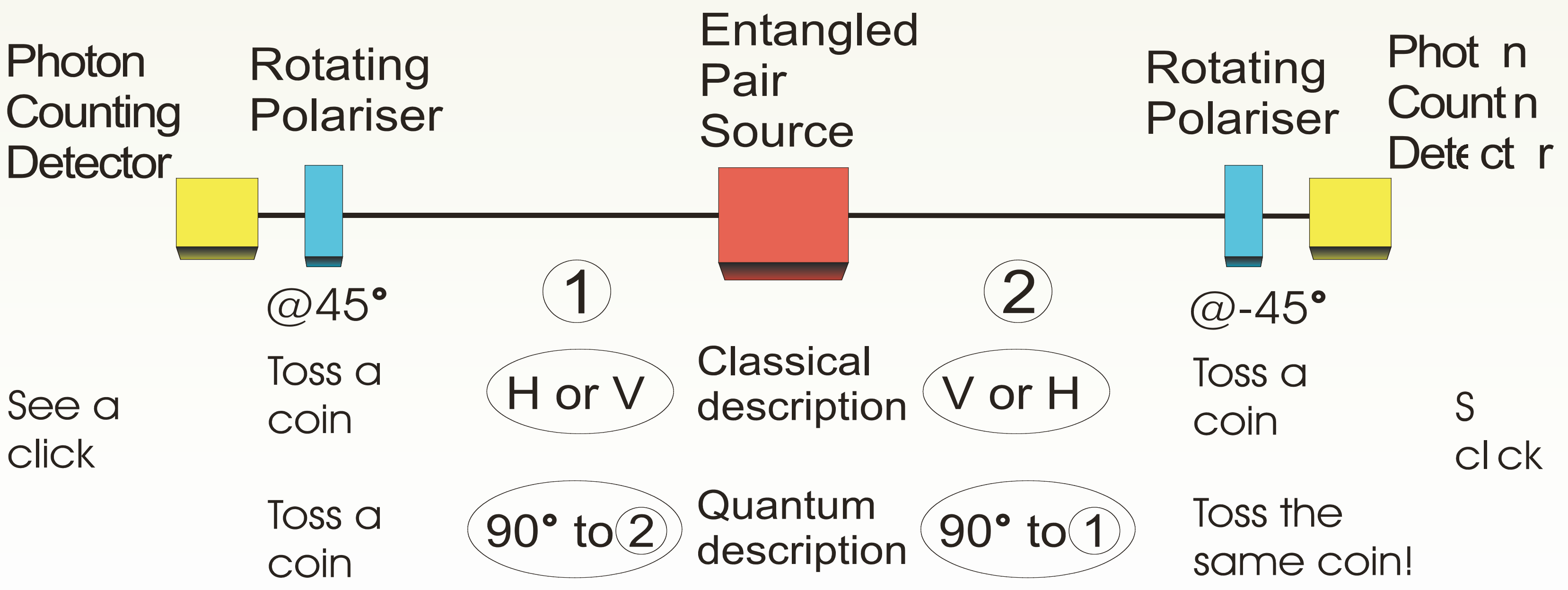


University of BRISTOL

Coincident key generation at 1000km separations using satellite, also tests the non-locality of QM



Philosophical questions
Non-locality of entangled photon pairs



Rarity: Science Perspective August 2003