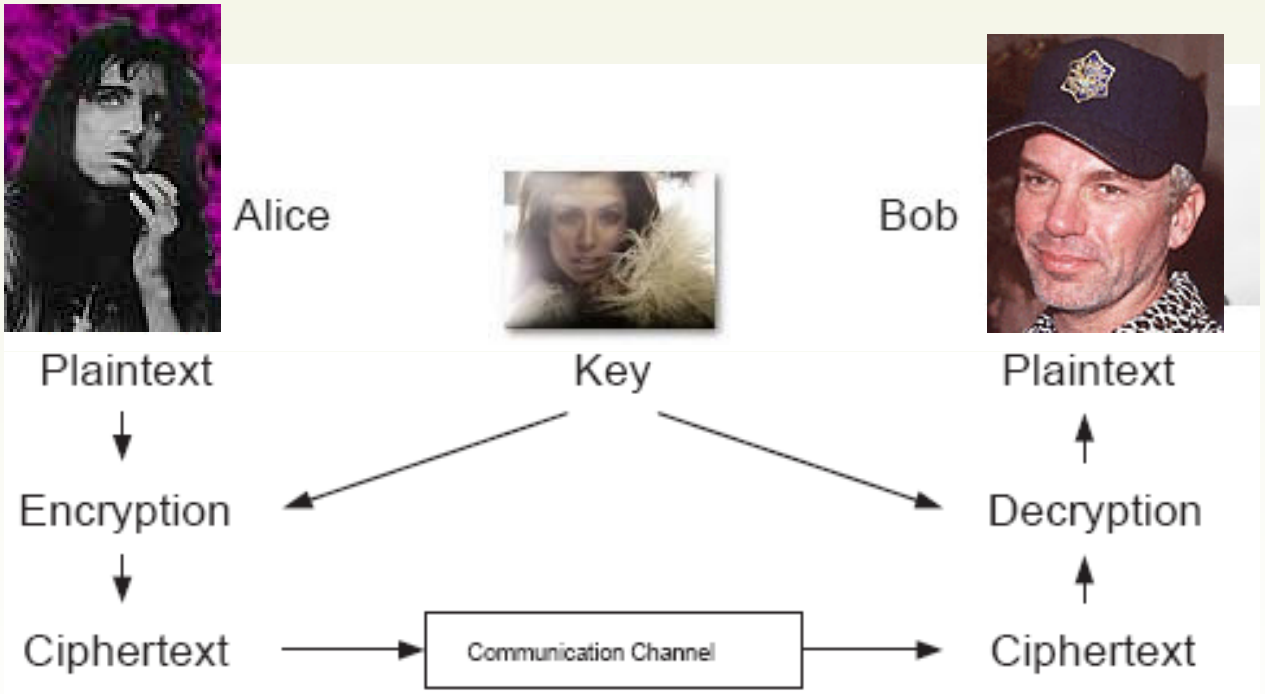
What is quantum cryptography?
Quantum secured key distribution

BCS Meeting, London September 2009

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

University of BRISTOL

Symmetric Cryptosystem



One-time-pad: Provably secure when 1-bit of key XOR 1-bit of plaintext.
AND key never used more than once.
BUT need to distribute the key securely
Without being eavesdropped.

University of BRISTOL

Polarisation encoding using waveplates

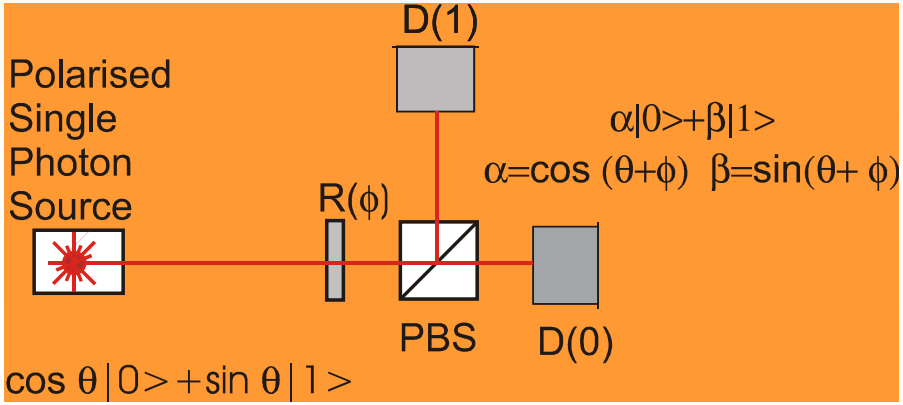
Encoding single photons using two polarisation modes

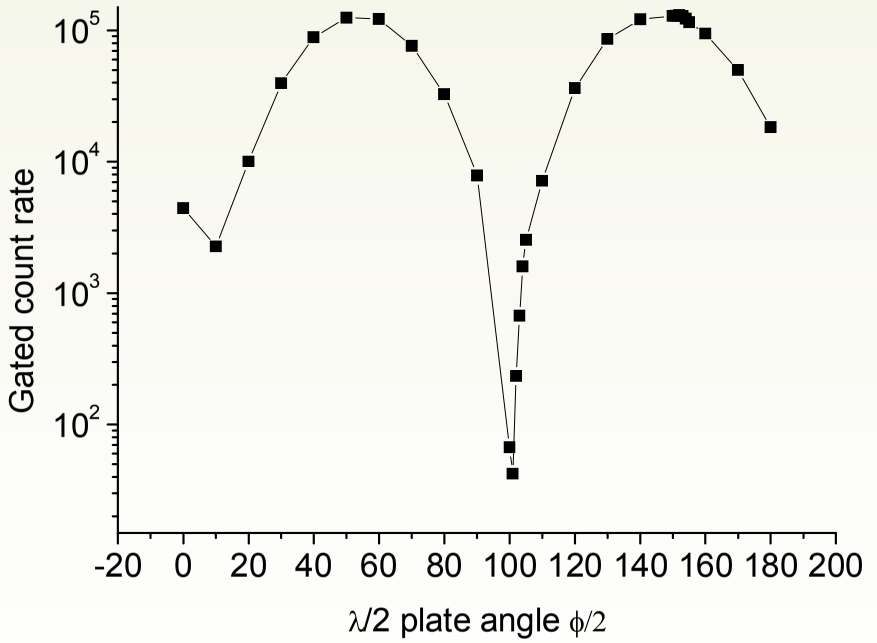
Superposition states of '1' and '0'

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Probability amplitudes α , β

Detection Probability: $|\alpha|^2$





Single photon encoding showing QBER<5.10^{-4}
(99.95% visibility)

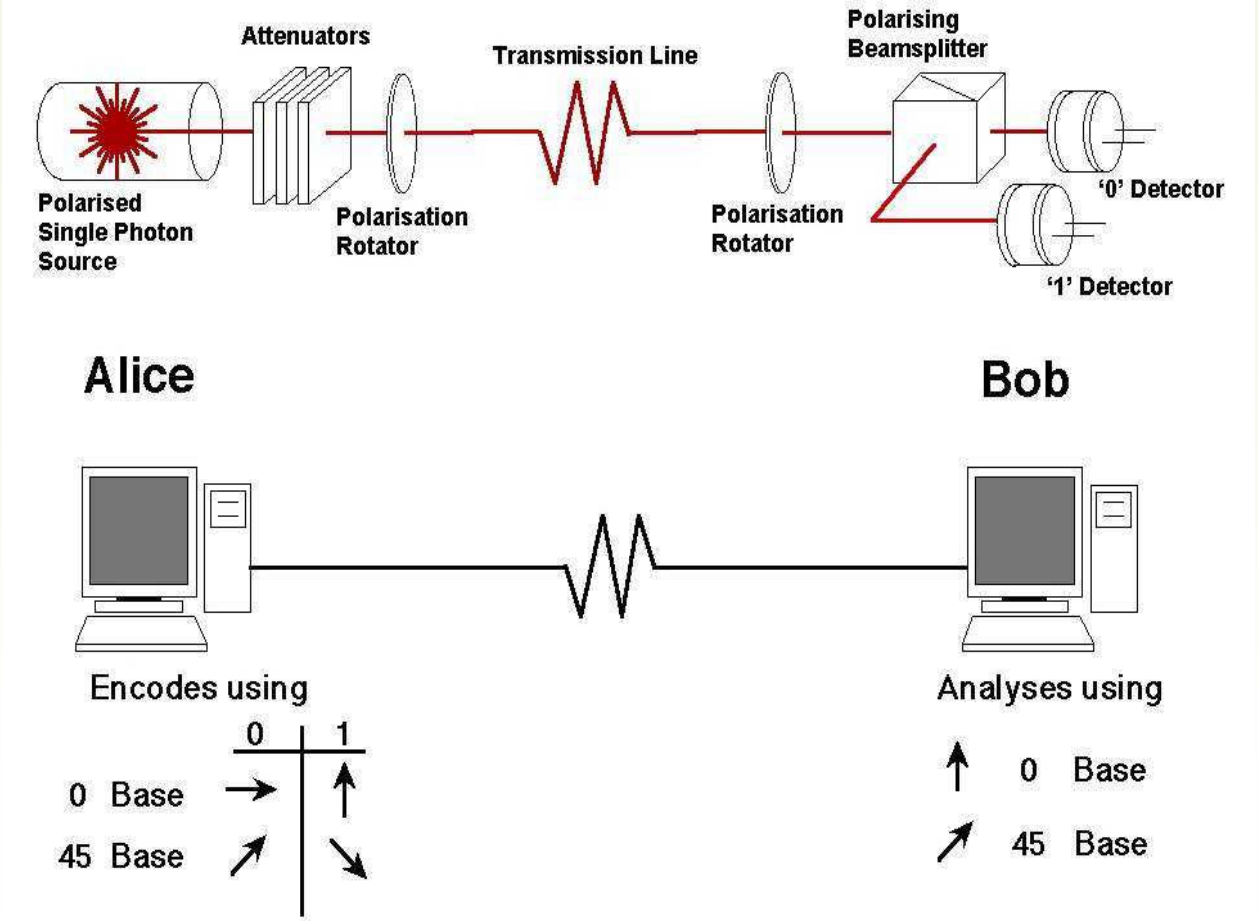
NOTE: in a 50:50 beamsplitter we get purely random clicks in 1 and 0 detectors
RANDOM NUMBER GENERATOR

University of BRISTOL

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
…		

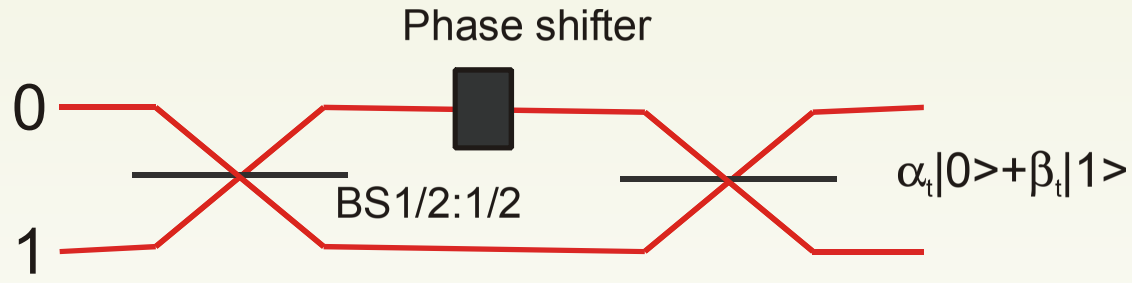


Receives

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

University of BRISTOL

Path encoding with single photons

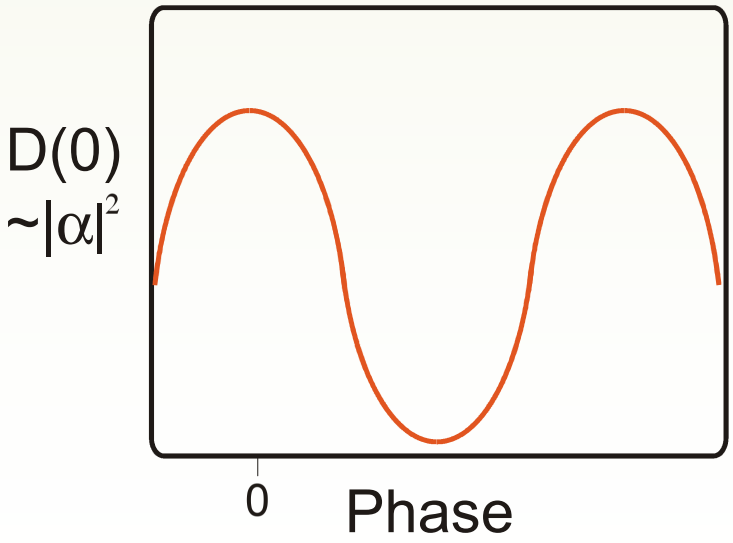


Single photon can only be detected in one detector

BUT interference pattern built up from many individual counts

Equal superposition leads to randomness when at half height

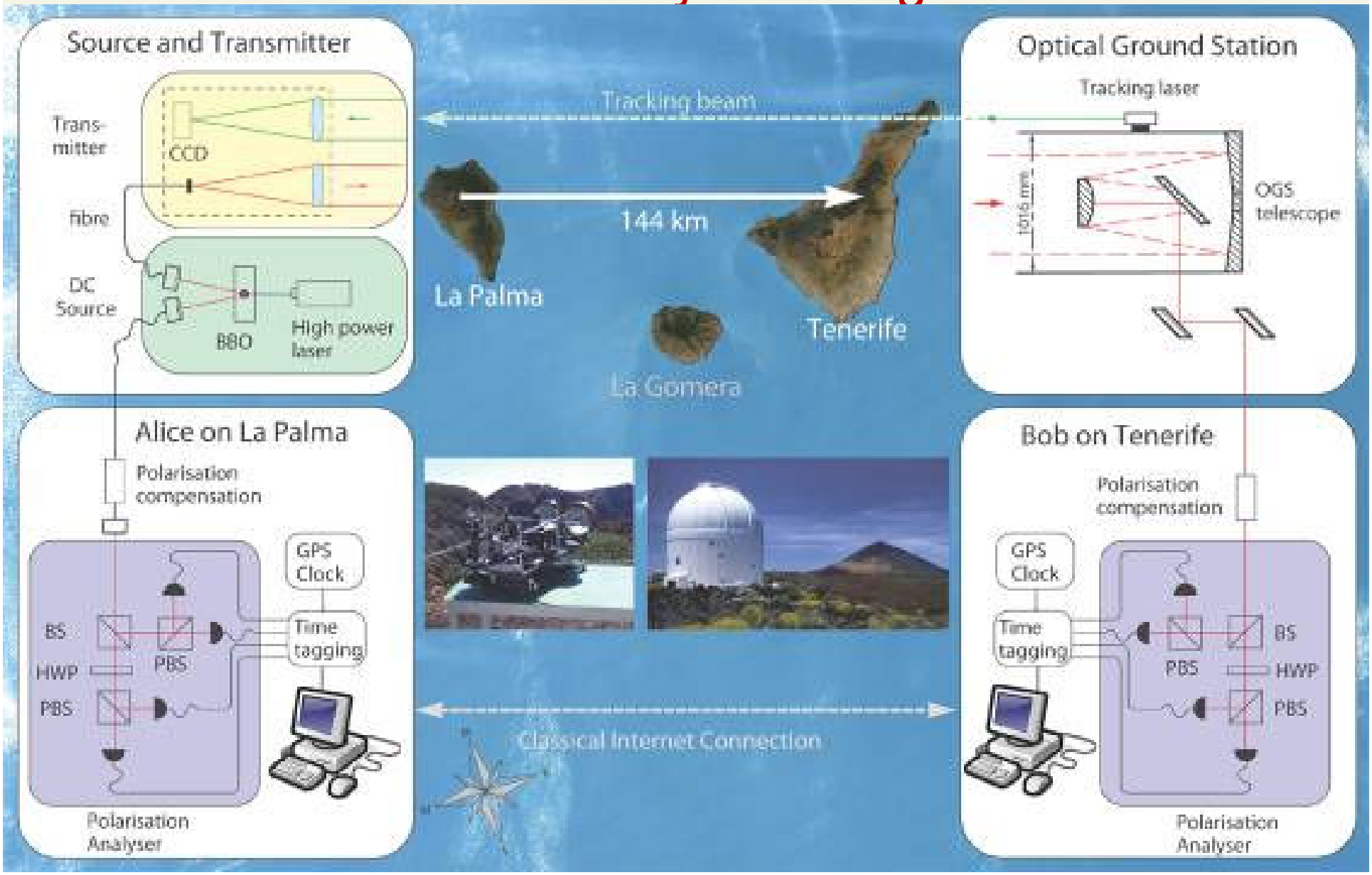
P. Grangier et al, Europhys Letts 1986



University of BRISTOL

Entanglement based quantum communication over 144km.
R. Ursin, et al quant-ph/0607182, Nature Physics **3** 481, 2007

144km key exchange



University of BRISTOL

Quantum key growing used for secure banking

Key exchange at ATM allows user to ‘top-up’ a personal one-time-pad.
Protects against ‘skimming’
One time pad encoding of PIN protects online transactions