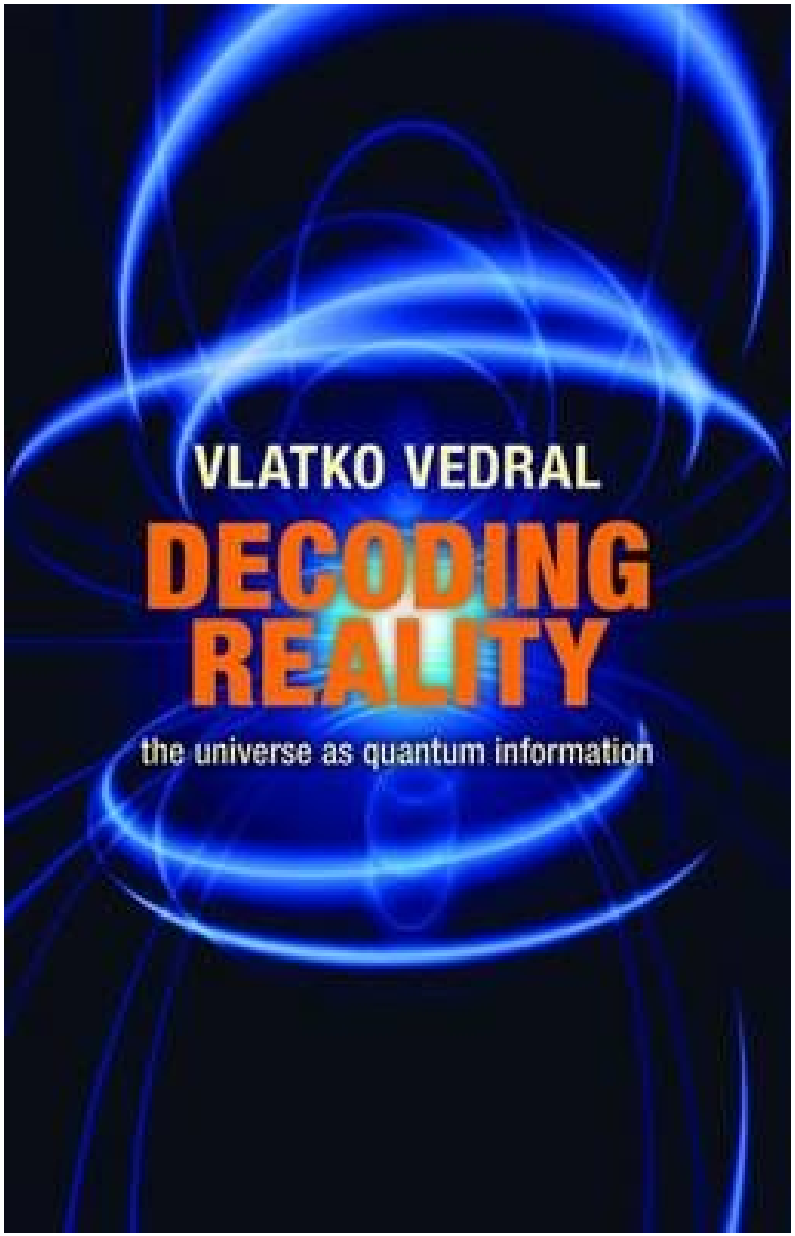
Lecture QI1, QI2

Classical information theory

Information is physical

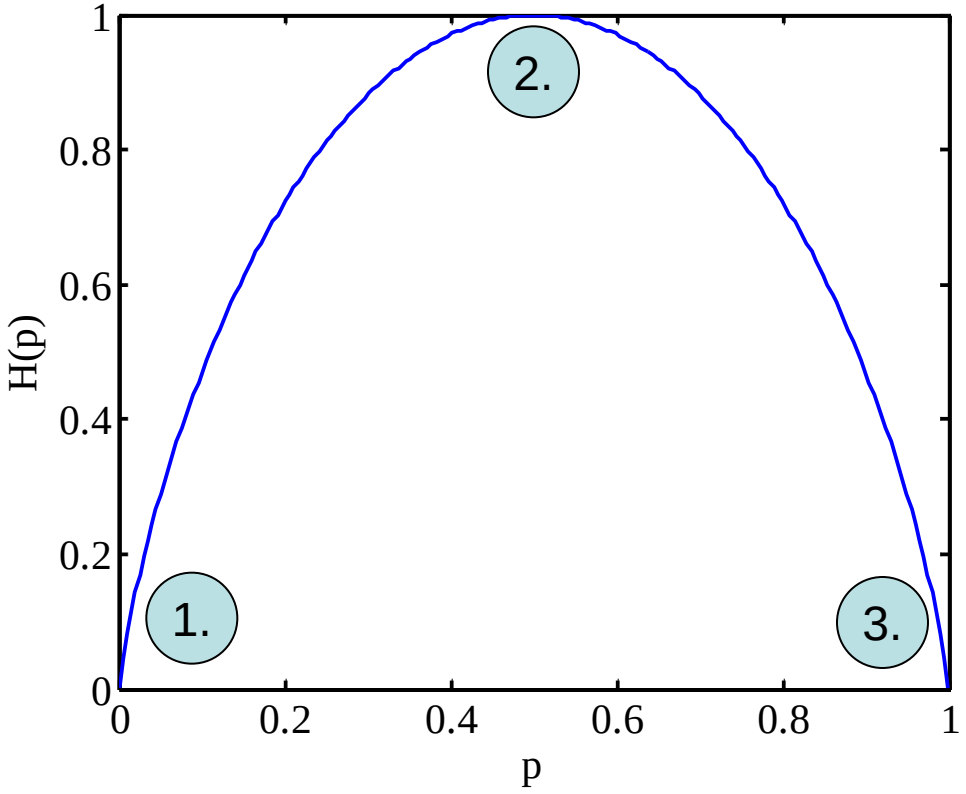
e.g. G Milburn in The Quantum Tamers


VLATKO VEDRAL
DECODING REALITY
the universe as quantum information

Example: two messages

- Alice can send two messages 0 or 1. She chooses 0 with probability p and 1 with probability 1-p. How much information does one of her messages contain?

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$$

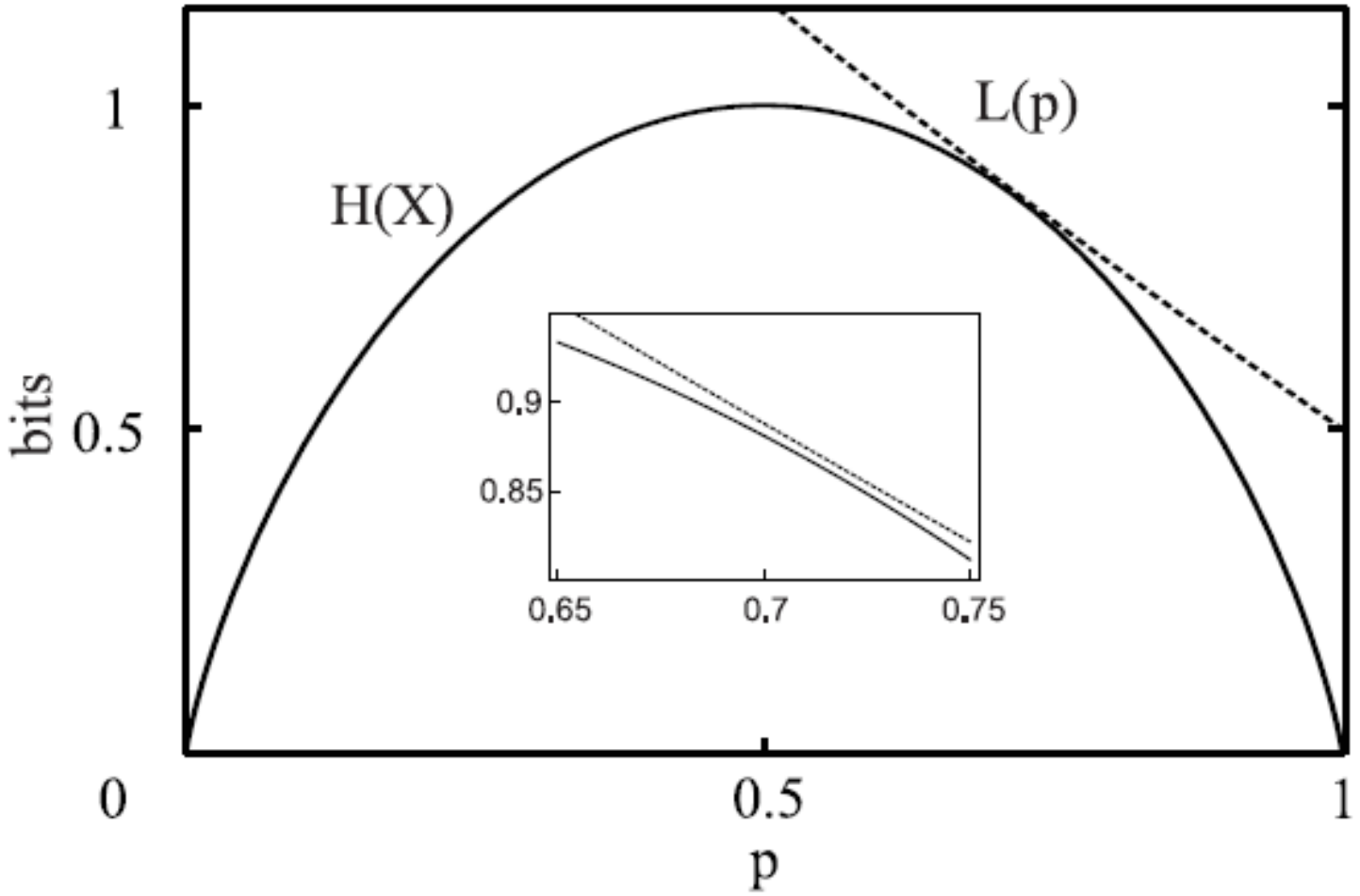


Information contained in the message?

1. There is no information if only 1's may be chosen
2. 1 bit of information is contained if 0's and 1's may be chosen with p=1/2
3. There is no information if only 0's may be chosen

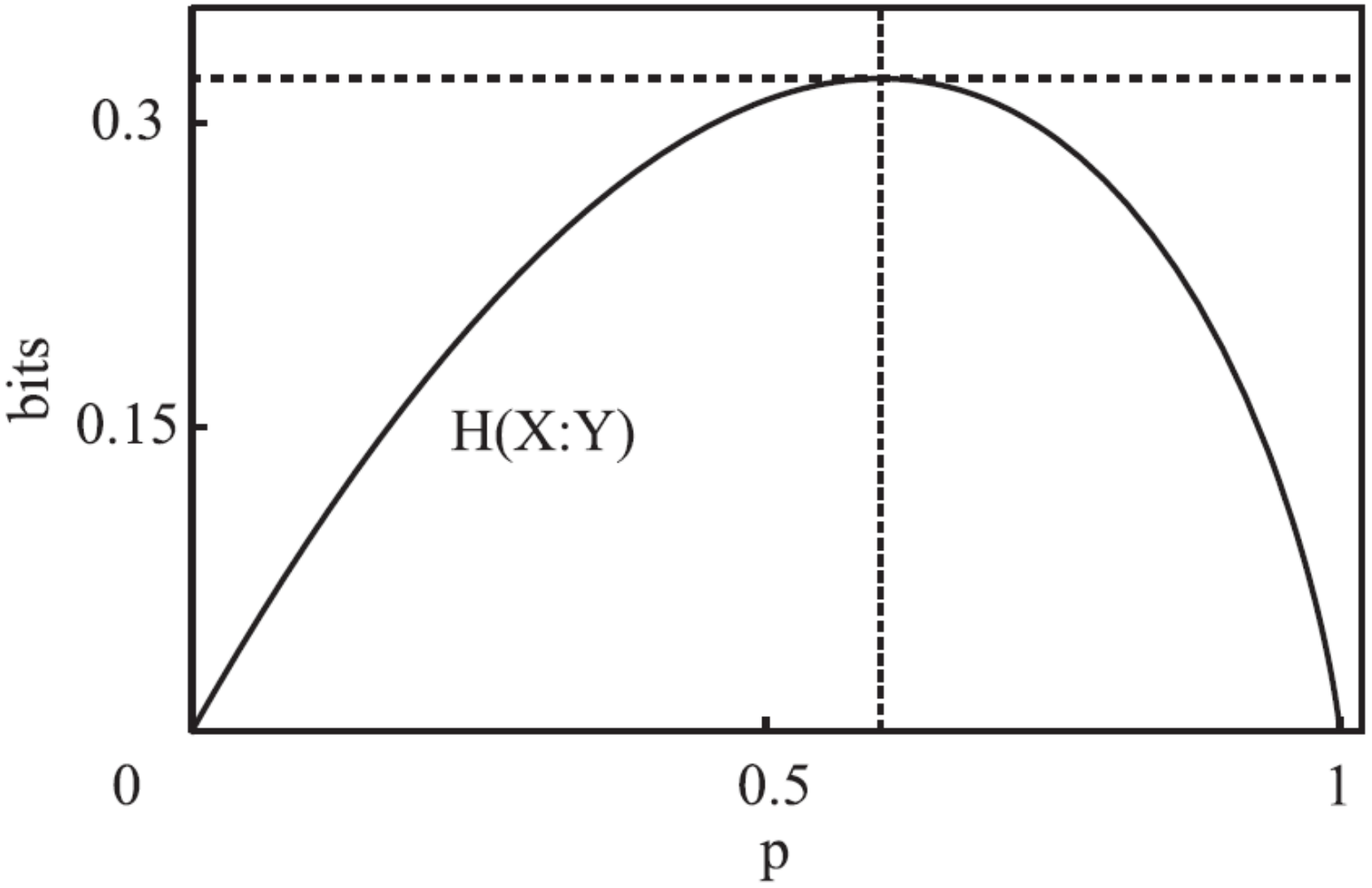
Example: compression

- Imperfect compression encoding for two messages. Message *a* is sent with probability *p* and message *b* is sent with probability *1-p*.



Example: Channel Capacity

- What is the classical channel capacity of a single photon channel where ½ of the photons are lost? Messages: 0 = no photon and 1 = one photon



Summary: classical information

- Shannon entropy (Alice X)

$$H(X) = -\sum_j p(x_j) \log_2 \left(p(x_j) \right)$$

- Joint entropy (Alice X & Bob Y)

$$H(X,Y) = -\sum_{jq} p(x_j, y_q) \log_2 \left(p(x_j, y_q) \right)$$

- Conditional entropy (What Bob Y cannot learn about Alice X)

$$H(X|Y) = H(X,Y) - H(Y)$$

- Mutual information (What Bob Y can learn about Alice X)

$$H(X:Y) = H(X) - H(X|Y)$$

- For two messages 0,1 (a bit when $p_0 = p_1 = 1/2$)

$$0 \leq H(X) \leq 1 \qquad 0 \leq H(X,Y) \leq 2$$

$$0 \leq H(X|Y) \leq 1 \qquad 0 \leq H(X:Y) \leq 1$$

Lecture QI3

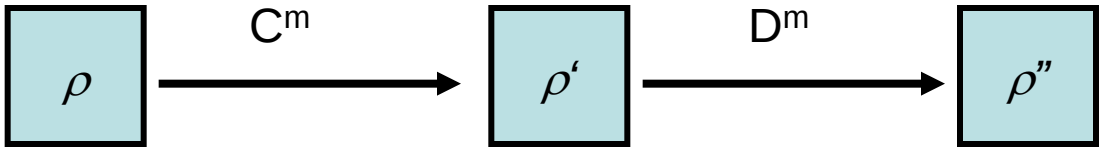
Quantum information

Schumacher's quantum noiseless channel coding theorem

- Schumacher showed that states ρ in a d dimensional Hilbert space H produced by a quantum information source can be compressed. In particular it is possible to reliably compress and decompress ρ to a state in a Hilbert space H_r with dimension

$$\mathrm{d}im(\mathcal{H}_r) \;=\; 2^{S(\rho)}$$

  and can thus be viewed as being represented by $S(\rho)$ qubits.
- Like in classical compression this only works on average, i.e. if the source produces a large number m of quantum messages.
- Reliably in this case means that the entanglement fidelity of the original state ρ^m after compression C^m and decompression D^m tends to 1 for large m. The entanglement fidelity tells us how well the state ρ^m preserves its entanglement with an environment during compression and decompression. We do not define the entanglement fidelity here (see NC page 420).



Lecture QI4

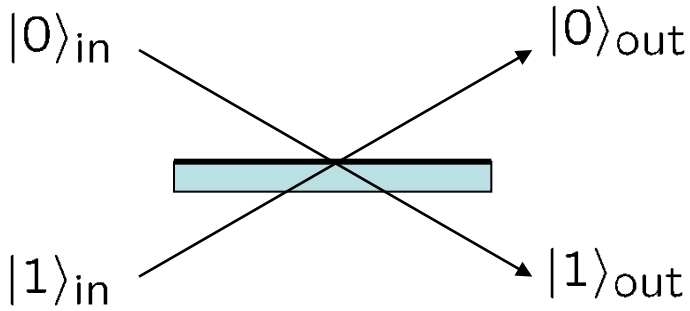
Photon technologies
Quantum communications

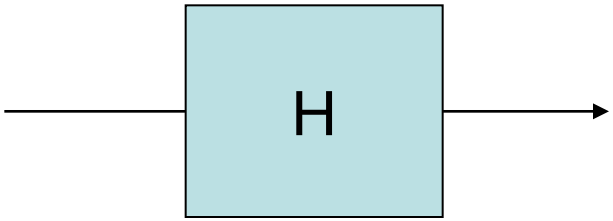
Photons as spatial mode and polarization encoded qubits

- Spatial mode encoding
  - Two spatial modes *a* and *b* (direction, momentum) are chosen to represent the qubit states $|0\rangle$ and $|1\rangle$
  - Single qubit gates are implemented by
    - a phase shifter in one spatial mode → phase gate
    - beam splitter → Hadamard gate
  - Two qubit gates can be realized by Kerr nonlinearities
- Polarization encoding
  - The qubit is encoded in the photon polarization e.g.$|0\rangle = |H\rangle$, $|1\rangle = |V\rangle$
  - Single qubit gates are implemented by
    - polarization rotators and polarization phase shifters
    - polarizing beam splitter → spatially separate $|H\rangle$ and $|V\rangle$ components
  - Two qubit gates e.g. with polarizing beam splitters and Kerr nonlinearities
- Linear optics quantum computing by entanglement creation via measurement
- Photon number encoding: $|0\rangle$→ no photon $|1\rangle$ → 1 photon
- Spatial + polarization encoding allows to store two qubits in one photon
  - This encoding is not easily scalable

A beam splitter (BS) as a single qubit operation

- A simple 50/50 BS for spatial mode encoded qubits





$$|\Psi\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in}$$

$$|\Psi\rangle_{out} = H|\Psi\rangle_{in} = \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}$$

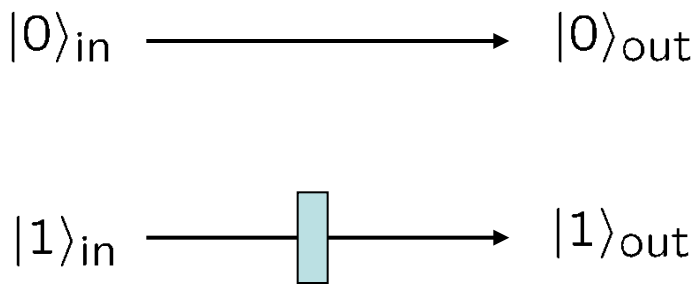
- Matrix representation of the dynamics of a general beam splitter

$$BS(\xi,\varphi) = \begin{pmatrix} \cos(\xi) & e^{i\varphi}\sin(\xi) \\ e^{-i\varphi}\sin(\xi) & -\cos(\xi) \end{pmatrix}$$

This time evolution is unitary. BS(45$^{\pm}$,0)=H is a simple 50/50 beam splitter.

A phase shifter as a phase gate

- A slab of transparent medium put into the path of one mode



A medium of length *L* with refractive index *n* yields a phase shift ϕ

$$\phi = (n - n_0)L\omega/c_0$$

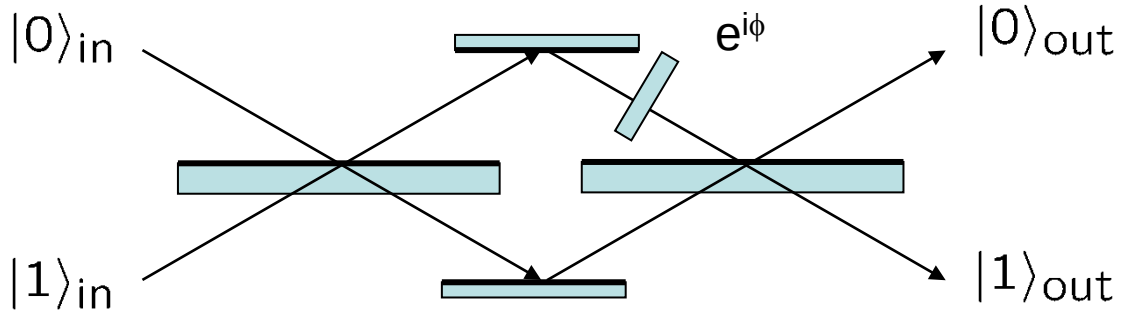
- The resulting quantum gate is a phase gate with the truth table

$$|0\rangle_{out} = |0\rangle_{in} \qquad |1\rangle_{out} = e^{i\phi}|1\rangle_{in}$$

- With beam splitters and phase shifters one can realize every single qubit operation. Kerr nonlinearities χ allow to create a two qubit phase gate where a phase shift is induced if two photons are travelling a distance L in the Kerr medium. The resulting entanglement phase is

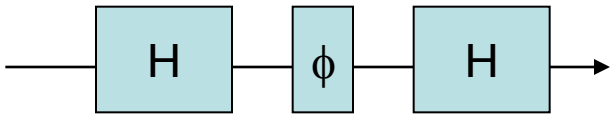
$$\varphi = \chi L$$

Example: A Mach-Zehnder interferometer



- The Mach-Zehnder interferometer evolves the input state $|\Psi i_{in}$ according to

$$|\Psi\rangle_{out} = H\Phi H|\Psi\rangle_{in}$$

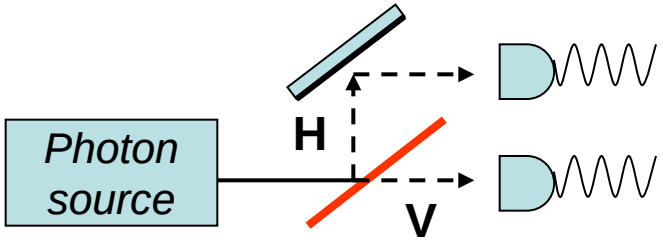


$$|\Psi\rangle_{out} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|\Psi\rangle_{out} = e^{i\phi/2} \begin{pmatrix} \cos(\phi/2)\alpha - i\sin(\phi/2)\beta \\ -i\sin(\phi/2)\alpha + \cos(\phi/2)\beta \end{pmatrix}$$

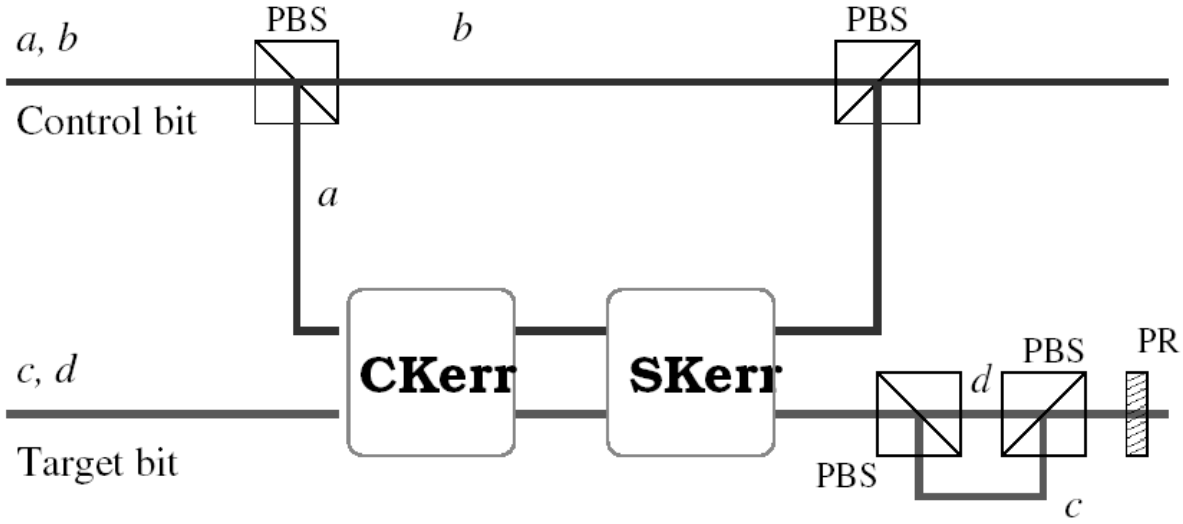
Polarization encoded qubits

- We encode the qubits in their direction of polarization $|0\rangle = |H\rangle$, $|1\rangle = |V\rangle$.
- Single qubit gates are obtained by rotating the direction of polarization.
- A polarizing beam splitter separates the different polarizations in space.
  - This can be used to measure a qubit



Polarizing beam splitter

  - and also to implement a two qubit gate e.g. a CNOT gate

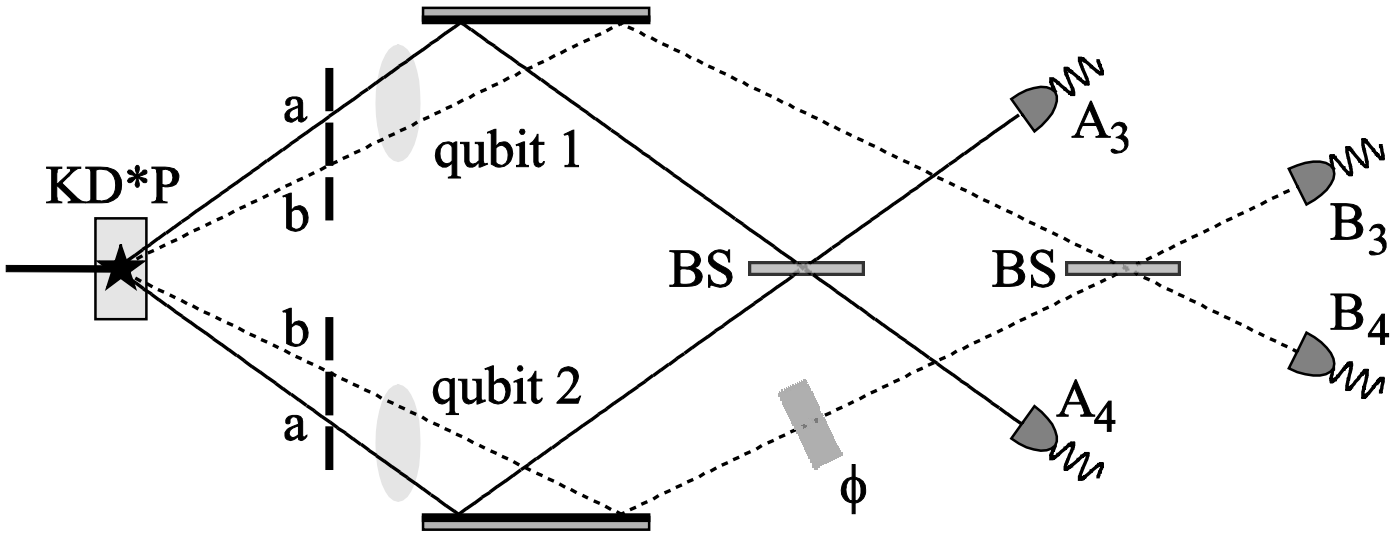


Momentum entanglement

- Using apertures A two individual mode pairs (directions) are selected.
- Each pair consists of one photon with colour a (slightly above) and one with colour b (slightly below halve of the pump frequency).
- Before the beam splitters we thus have the entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|a\rangle_1|b\rangle_2 + |b\rangle_1|a\rangle_2)$$

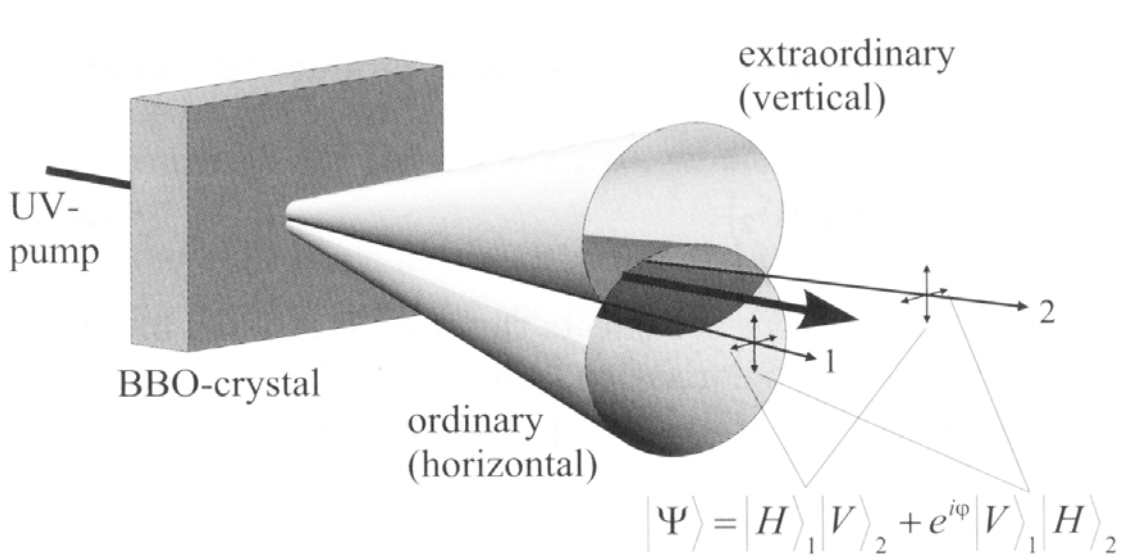
- Behind the BS the two paths cannot be distinguished → interference
- Coincident detections in a and b detectors vary cosinusoidally on changing the phase difference ϕ

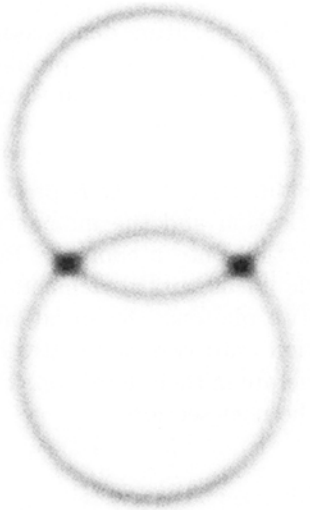


Polarization entanglement

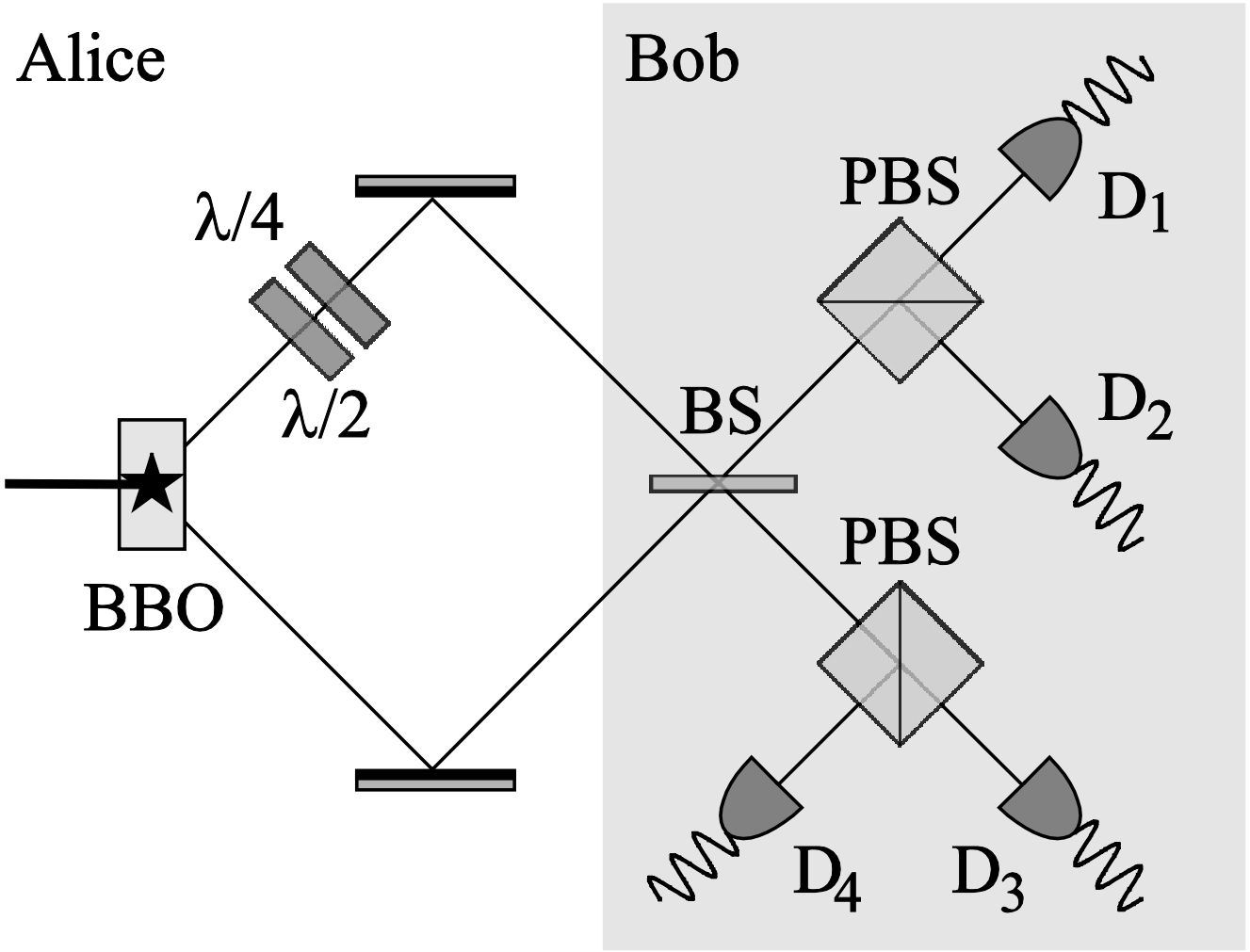
- Non-collinear type-II down-conversion phase matching
- At certain angles with the optical axis such that photons are emitted along cones with no common axis: one cone is ordinarily, the other extraordinarily polarized → they intersect along two directions → unpolarized light
- State created at cone intersections

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|V\rangle_1|H\rangle_2 + |H\rangle_1|V\rangle_2)$$



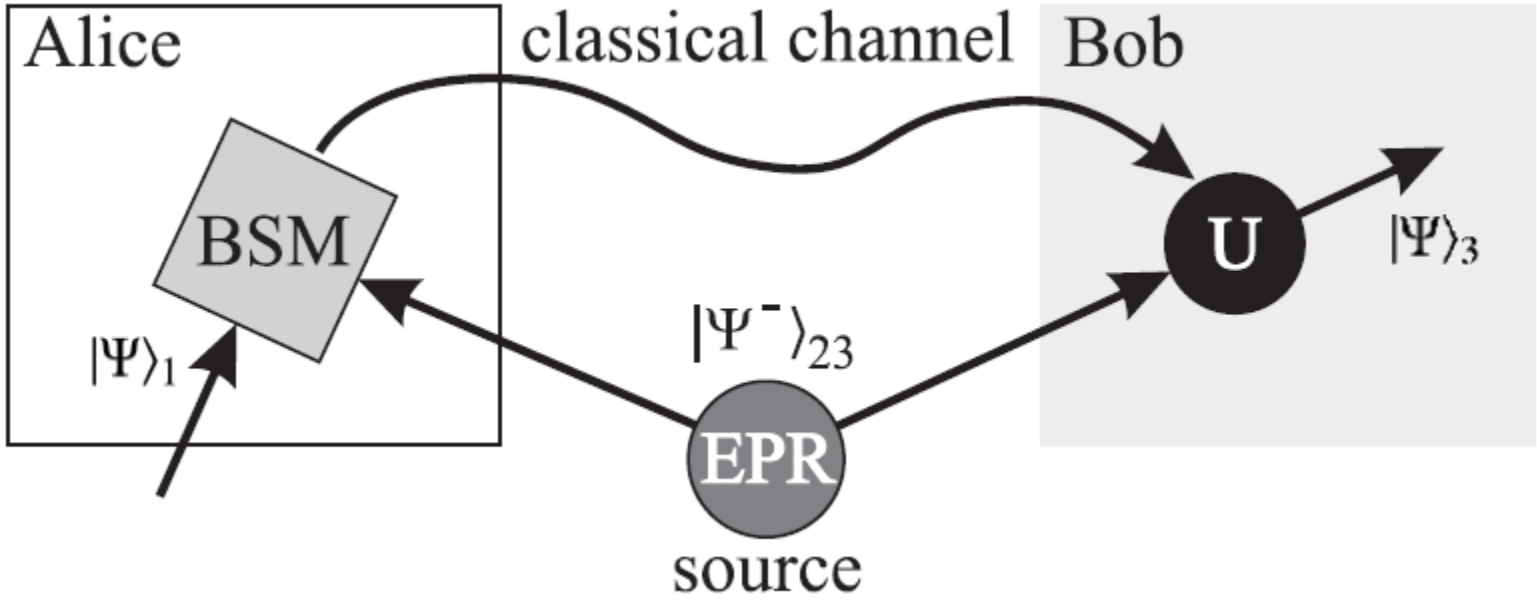


Quantum dense coding – experimental setup



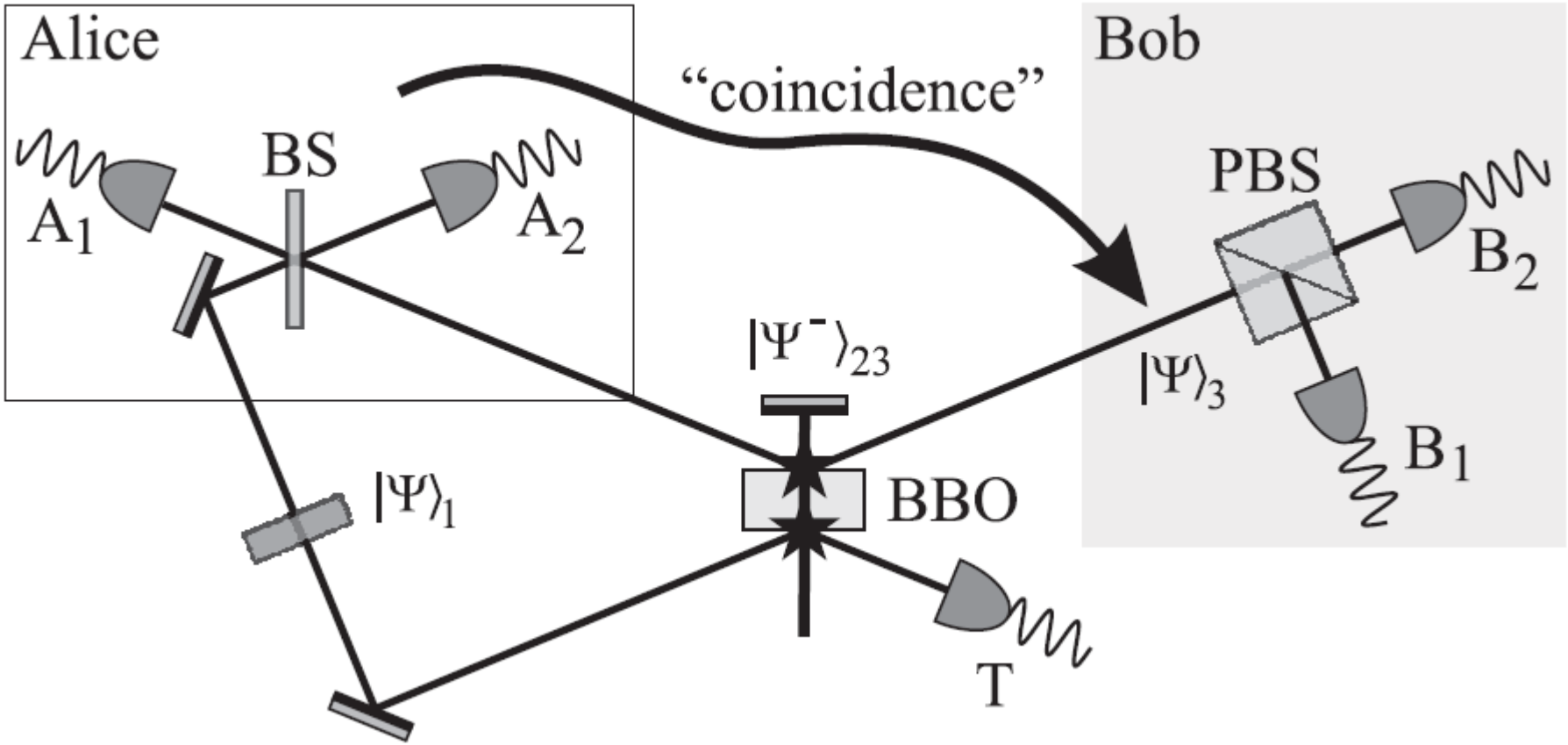
Quantum teleportation

- Schematic



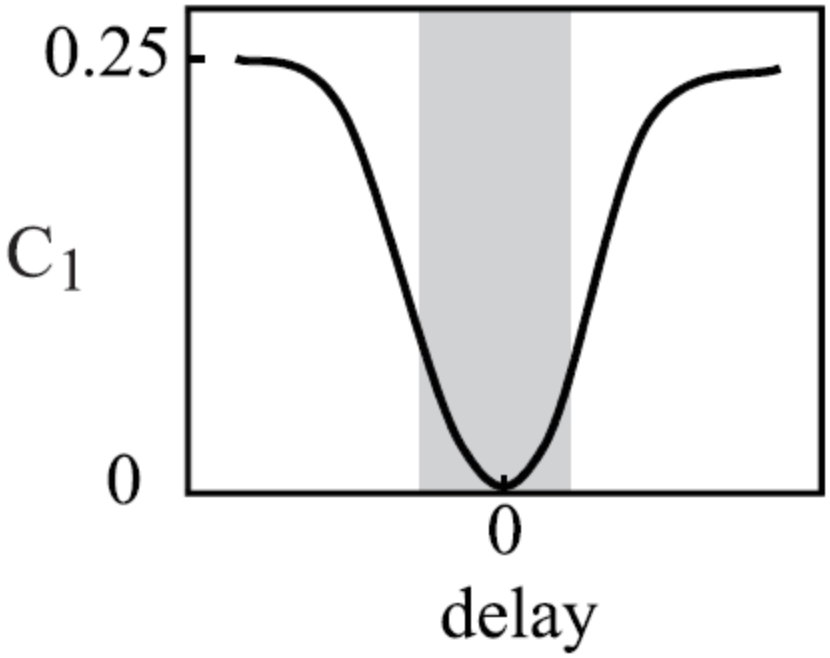
Quantum teleportation

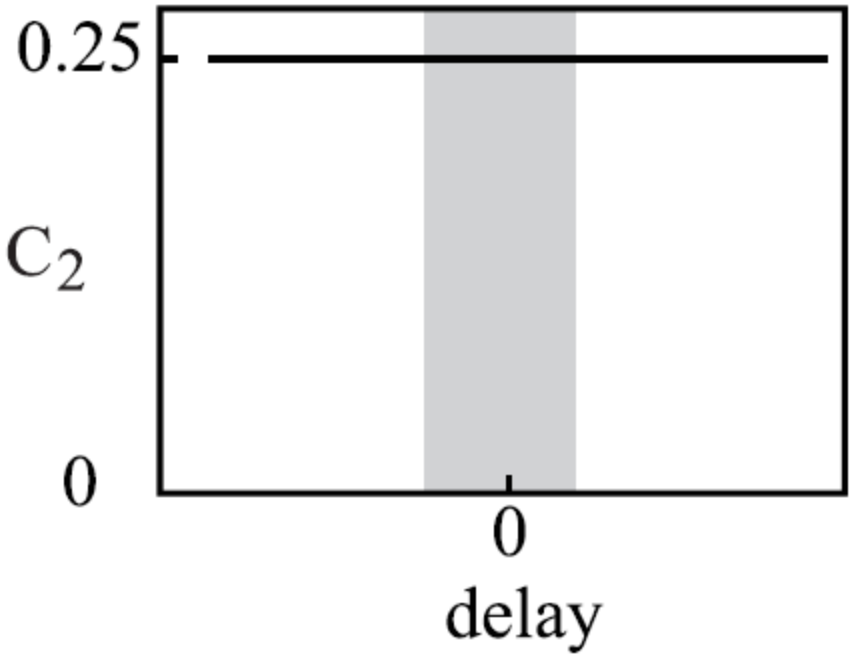
- Experimental setup



Quantum teleportation

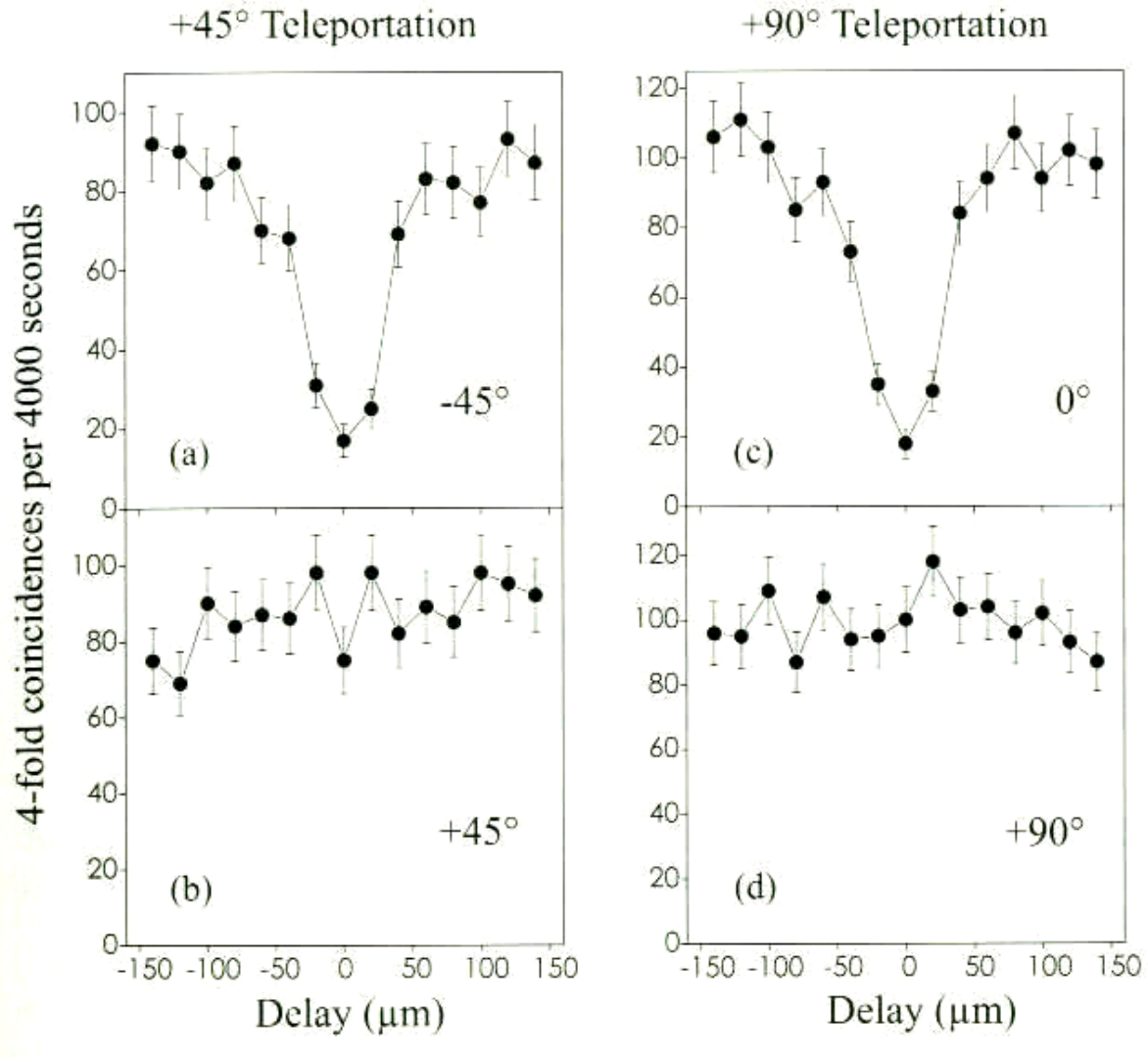
- Expected Result





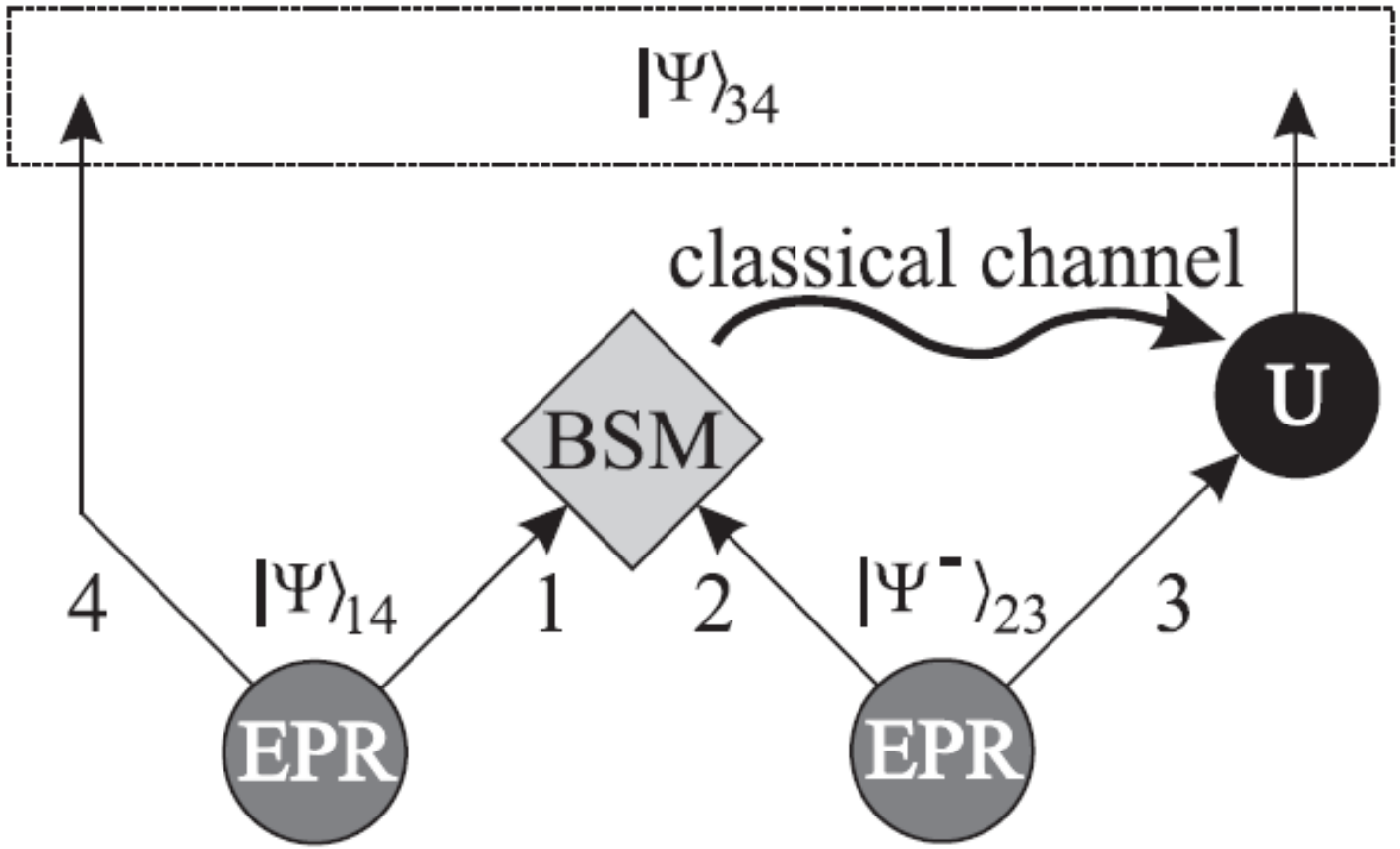
Experimental results

- Experimental results for a 45± and 90± photon state



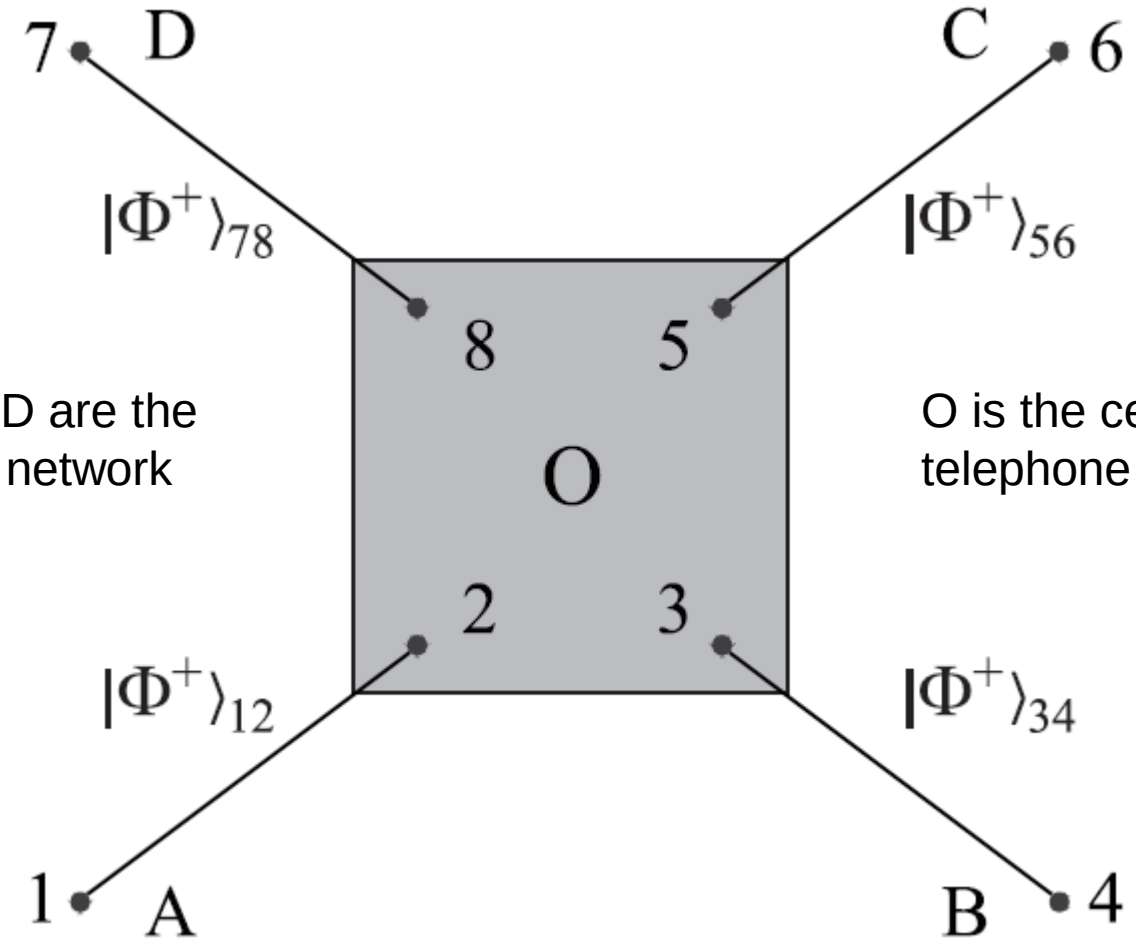
Entanglement swapping

- Schematic Setup



The quantum telephone exchange (I)

- Entanglement swapping can be used to realize a quantum telephone exchange. Imagine there are N users in a communication network. Each user shares a Bell state with a central exchange.



A, B, C and D are the users of the network

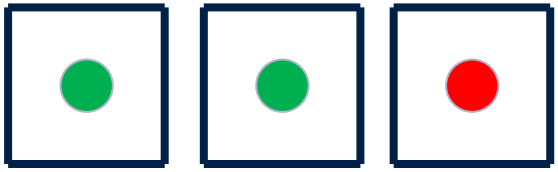
O is the central telephone exchange

Lecture QI5

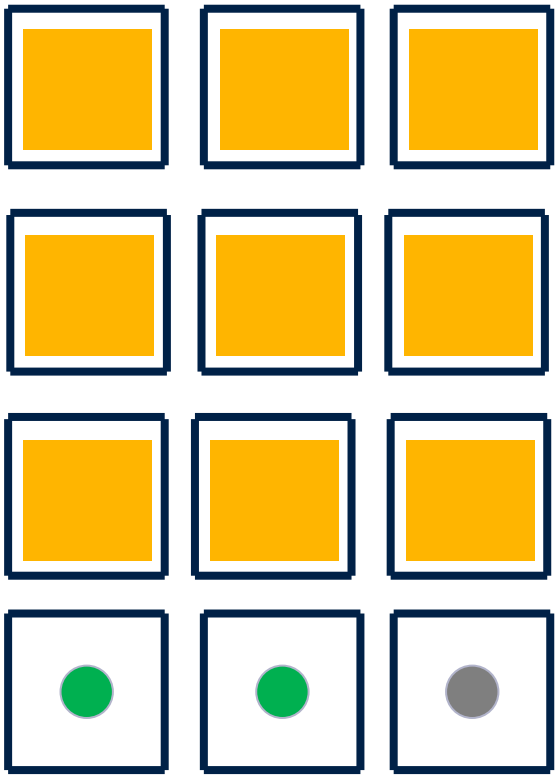
Testing EPR

Local realism limitations

- Flip fair coins



- Locality: measured quantity (red/green) only depends on local state of system
- Realism: quantity (red/green) is well defined independently of measurement



$$p(G,G,:) = p(R,R,:) = \frac{1}{2}$$
$$p(G,R,:) = p(R,G,:) = 0$$

$$p(G,:,G) = p(R,:,R) = \frac{1}{2}$$
$$p(G,:,R) = p(R,:,G) = 0$$

$$p(:,R,G) = p(:,G,R) = \frac{1}{2}$$
$$p(:,R,R) = p(:,G,G) = 0$$

$$p(G,G,R) = ?$$
$$p(G,G,G) = ?$$

p does not exist

Bell function

- Assign colour values $R = 1$ and $G = -1$ and measure colour correlation functions of C_i

$$\mathcal{B} = \langle C_1 C_2 \rangle + \langle C_1 C_3 \rangle - \langle C_2 C_3 \rangle$$

- If we put no restrictions of local realism on the correlations

$$\mathcal{B} = 1 + 1 + 1 = 3$$

- However, local realism (assuming p exists) after the first two correlation measurements gives

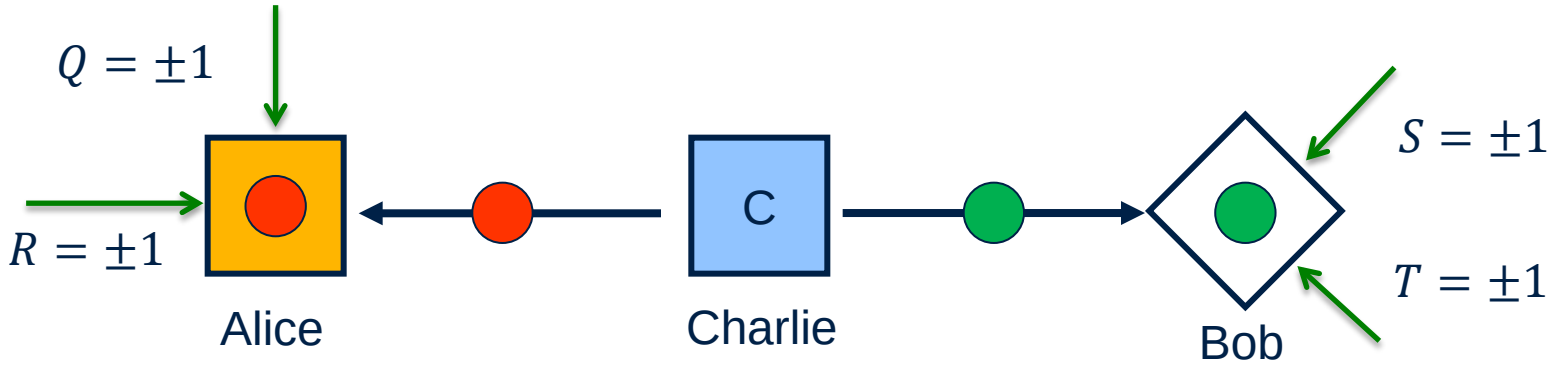
$$p(R,R,R) = p(R,:,R) - p(R,G,R) = \frac{1}{2} - 0 = \frac{1}{2}$$
$$p(G,G,G) = p(G,:,G) - p(G,R,G) = \frac{1}{2} - 0 = \frac{1}{2}$$

- Hence $\langle C_2 C_3 \rangle = 1$ and $\mathcal{B}$ is thus limited to

$$\mathcal{B} = 1 + 1 - 1 = 1$$

Bell inequalities (I)

- A Gedanken experiment (realized by A. Aspect *et al*.)



- (i) Charlie prepares two systems (possibly correlated) and sends one to Alice and the other one to Bob.
  (ii) *After* receiving their respective particles Alice and Bob both *randomly* choose to measure one of two properties of their particle. Then they simultaneously perform their measurement.
  (iii) They repeat this experiment many times and record their outcomes
  (iv) Alice and Bob get together and investigate the correlations between their experimental results. What can they expect to obtain?
- We describe the possible measurements of Alice by random variables Q and R and those Bob by random variables S and T.

Bell inequalities (II)

- We look at the expression

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T = \pm 2$$

as either $Q + R$ or $Q - R$ is zero.

- We now assume that the probability for Q=q, R=r, S=s, T=t *before* the measurement is $p(q, r, s, t)$ and using this probability distribution we find

$$\mathcal{B} = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = \sum_{q,r,s,t} p(q, r, s, t)(QS + RS + RT - QT)$$
$$\leq 2 \sum_{q,r,s,t} p(q, r, s, t) = 2$$

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle \leq 2$$

CHSH inequality

Bell inequalities (III)

- Send a quantum mechanically entangled state (a singlet) and perform spin measurements

$$|\Psi^-\rangle = |\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle$$

- Alice decides between measuring the operators

$$Q = \sigma_z^{(1)} \qquad R = \sigma_x^{(1)}$$

- Bob decides between measuring the operators

$$S = -\frac{\sigma_z^{(2)} + \sigma_x^{(2)}}{\sqrt{2}} \qquad T = \frac{\sigma_z^{(2)} - \sigma_x^{(2)}}{\sqrt{2}}$$

- It is now straightforward to calculate the quantum mechanical expectation values

$$\langle QS\rangle = \frac{1}{\sqrt{2}} \quad \langle RS\rangle = \frac{1}{\sqrt{2}} \quad \langle RT\rangle = \frac{1}{\sqrt{2}} \quad \langle QT\rangle = -\frac{1}{\sqrt{2}}$$

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$$ Violation of the CHSH inequality

Bell inequalities (IV)

- We learn that quantum mechanics is not compatible with *local realism*.
- Entanglement between Alice's and Bob's states yields correlations "stronger" than allowed by local realism.
- Entangled states allow entropy properties which are not possible in classical information theory. For instance if we calculate the entropies of subsystems Alice and Bob from the previous example we find

$$S(\rho_A) = \log_2(2) = 1$$
$$S(\rho_B) = \log_2(2) = 1$$
$$S(\rho_{AB}) = 1\log_2(1) = 0$$

- Therefore the entropy of ρ_A conditional on knowing ρ_B is negative

$$S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_B) = -1$$

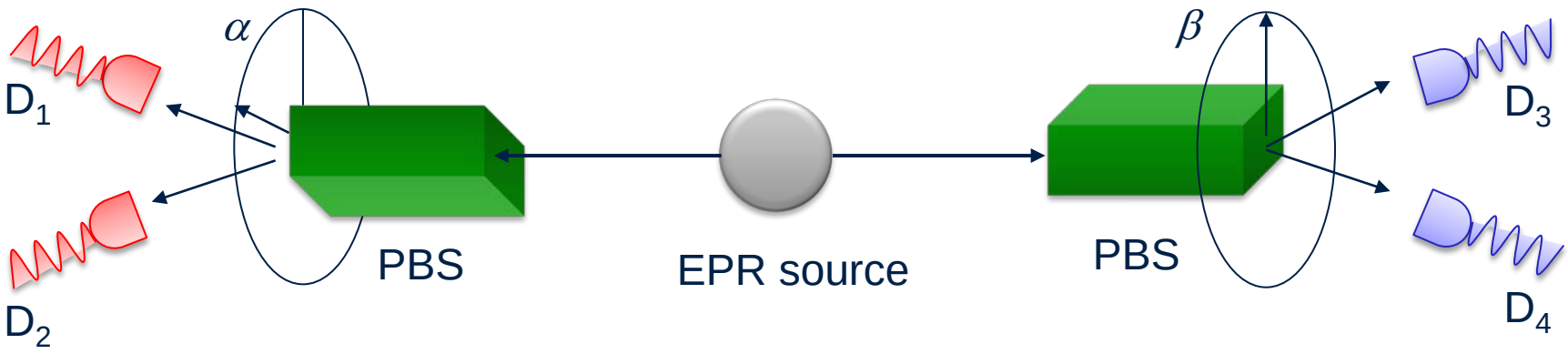
while in the classical case H(X|Y) is *always* larger than zero (see NC p507 for a proof).

- Experiments: A. Aspect *et al.,* Phys. Rev. Lett. **47**, 460 (1981);
  A. Aspect *et al.*, Phys. Rev. Lett. **49**, 91 (1982).

The second experiment tests the *CHSH* inequality

Aspect experiments (I)

- Testing the Bell inequalities with polarization entangled photons



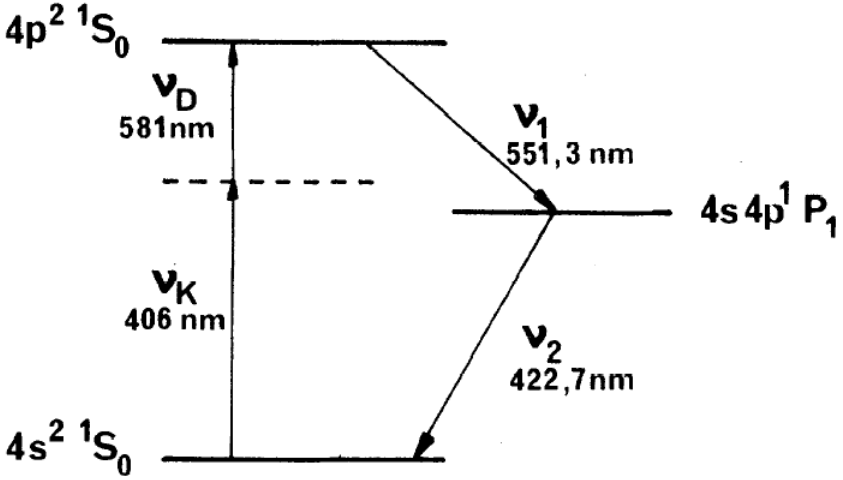
- Setting angels $\alpha = 0$ and $\alpha = \pi/4$ corresponds do measuring $Q = \sigma_z$ and $R = \sigma_x$

- Setting angels $\alpha = \pi/8$ and $\alpha = 3\pi/8$ corresponds do measuring $-S = (\sigma_z + \sigma_x)/\sqrt{2}$ and $-T = (-\sigma_z + \sigma_x)/\sqrt{2}$

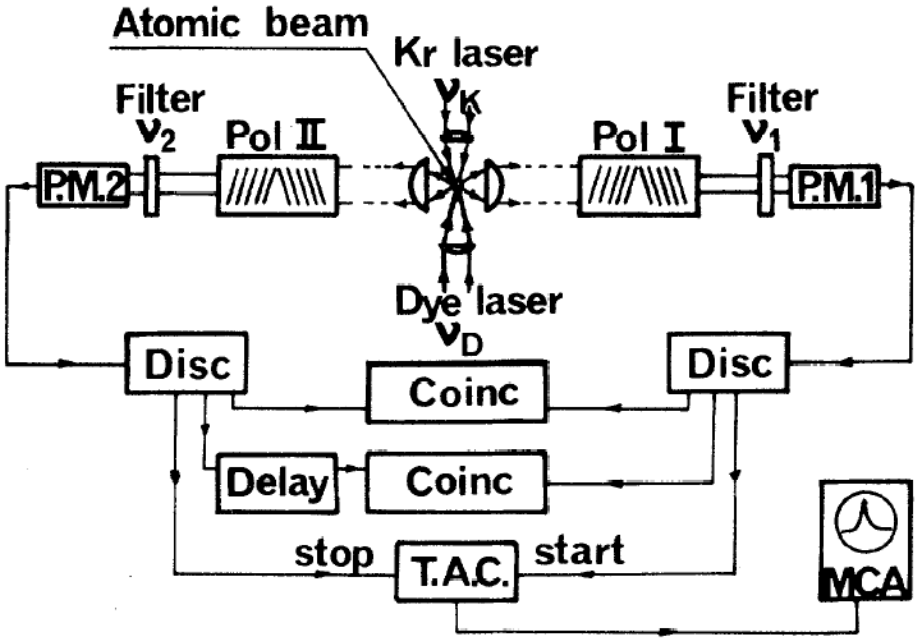
The Aspect experiments (II)

- Aspect used photons entangled in their polarization degree of freedom. By correlating the different measurement results he could violate Bell's inequalities.
- The polarizer setting determines which observable is measured

- Atomic cascade



Basic experimental setup



Aspect experiments (III)

- This result can be viewed as evidence for non-locality but this is not the only explanation. Various experiments had several loopholes:
  a) fair sampling assumption (CHSH probabilities as fraction of coincidences)
  b) efficiency of photo detectors is rather small
  c) accidental coincidences
  d) polarizers are set up (not randomly) before photons are created
  e) strict Einstein locality of the measurements
  f) the quantum system is not truly a bipartite system atom + two photons
- Addressing these loopholes
  a) b) 100% detection efficiency in ion trap experiments (only 3μm distance)
  c) keeping the accidental coincidences in the data
  d) e) adjusting the polarizers randomly after the photons are created
    – a random quantum process can be used to set up the measurement
    – the measurements are then performed in strict Einstein locality
    – perform measurements in different moving frames
- There are also other ways to test local realism against QM using GHZ states

Local Realism vs. Quantum mechanics

Disproofs of Bell, GHZ, and Hardy Type Theorems and the Illusion of Entanglement

Joy Christian*

Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom

An elementary topological error in Bell's representation of the EPR elements of reality is identified. Once recognized, it leads to a topologically correct local-realistic framework that provides exact, deterministic, and local underpinning of at least the Bell, GHZ-3, GHZ-4, and Hardy states. The correlations exhibited by these states are shown to be exactly the classical correlations among the points of a 3 or 7-sphere, both of which are closed under multiplication, and hence preserve the locality condition of Bell. The alleged non-localities of these states are thus shown to result from misidentified topologies of the EPR elements of reality. When topologies are correctly identified, local-realistic completion of any arbitrary entangled state is always guaranteed in our framework. This vindicates EPR, and entails that quantum entanglement is best understood as an illusion.

Preprint server 28/04/2009

Local Realism vs. Quantum mechanics

Characterization of Multipartite Entanglement for One Photon Shared Among Four Optical Modes

Scott B. Papp,[1]* Kyung Soo Choi,[1]* Hui Deng,[2] Pavel Lougovski,[3] S. J. van Enk,[3] H. J. Kimble[1]†

Access to genuine multipartite entanglement of quantum states enables advances in quantum information science and also contributes to the understanding of strongly correlated quantum systems. We report the detection and characterization of heralded entanglement in a multipartite quantum state composed of four spatially distinct optical modes that share one photon, a so-called *W* state. By randomizing the relative phase between bipartite components of the *W* state, we observed the transitions from four- to three- to two-mode entanglement with increasing phase noise. These observations are possible for our system because our entanglement verification protocol makes use of quantum uncertainty relations to detect the entangled states that span the Hilbert space of interest.

Science, 8/05/2009

GHZ states

- A GHZ state is a three particle entangled state. These states can be used to test quantum mechanics against local realism. In this setup no inequalities are needed for these tests as quantum mechanics makes definite predictions rather than statistical ones. We look at the three qubit state of polarization entangled photons:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle)$$

- $|H\rangle$ and $|V\rangle$ are eigenstates of σ_z. The polarizations rotated through 45± with respect to H and V denoted by $|H'\rangle$ and $|V'\rangle$ are eigenstates of σ_x. Left handed $|L\rangle$ and right handed $|R\rangle$ circular polarizations are eigenstates of σ_y. Rewriting the state |GHZi in the YYX basis we find

$$|GHZ\rangle = \frac{1}{2}(|RLH'\rangle + |LRH'\rangle + |RRV'\rangle + |LLV'\rangle)$$

- Thus if measuring in the YYX basis we know with certainty the outcome of the third measurement after determining the state of the first two qubits!
- By cyclic permutation one finds analogous expressions for measuring any two photons in circular polarization and the remaining one in 45± basis

GHZ state and local realism

- From a local realism point of view these perfect correlations can only be explained by assuming that each photon carries elements of reality which determine the outcome for all measurements considered.
- Let us consider a measurement in the XXX basis. Which outcomes are possible if the elements of reality exist? The permutations of $|GHZ\rangle$ imply that if H' (V') is obtained for one photon the other two have to have opposite (identical) circular polarizations.
- Imagine we find V' and V' for photons 2 and 3. Since 3 is V', 1 and 2 have to have identical circular polarization. Also, since 2 is V', 1 and 3 have to have identical circular polarization. If all of these are elements of reality then all photons have identical circular polarization. Thus photon 1 needs to carry polarization V'. We conclude that $|V'V'V'\rangle$ is a possible outcome. Similarly one can verify that the only four possible outcomes are

$$|V'V'V'\rangle, \qquad |H'H'V'\rangle, \qquad |H'V'H'\rangle, \qquad |V'H'H'\rangle.$$

- However, in the XXX basis the |GHZi reads

$$|GHZ\rangle = \frac{1}{2}(|H'H'H'\rangle + |H'V'V'\rangle + |V'H'V'\rangle + |V'V'H'\rangle)$$

- Local realism and quantum mechanics predict opposite results in all cases!

A source for three-photon GHZ states

- Polarization entangled pairs of photons are created in the BBO crystal such that

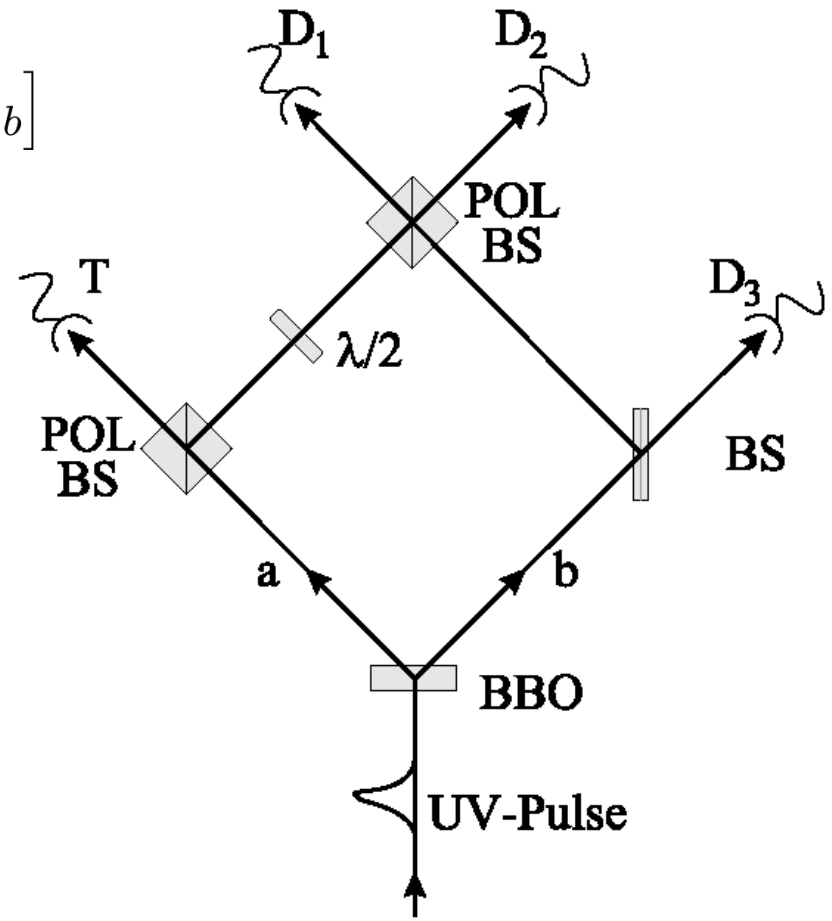
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle_a|V\rangle_b + e^{i\phi}|V\rangle_a|H\rangle_b\right]$$

- In the rare event that two pairs are created with one UV pulse the four fold coincidence corresponds to the observation of the state

$$|\mathrm{GHZ}'\rangle = \frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle)$$

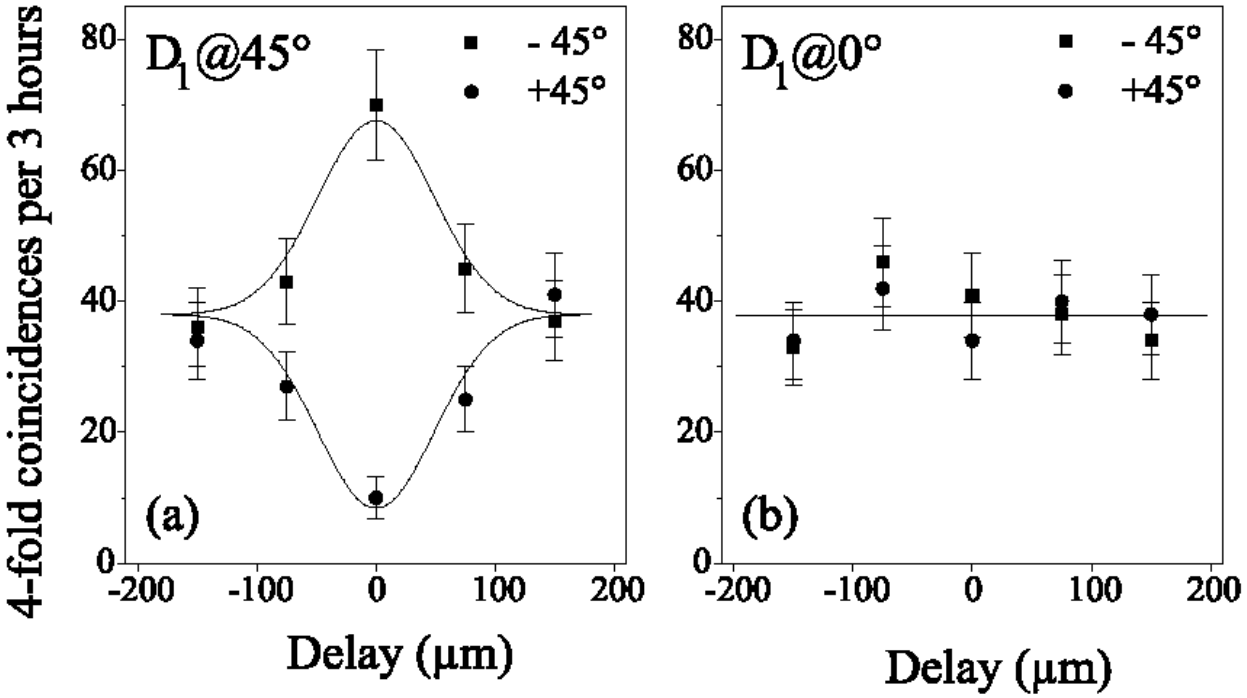
at the detectors D1, D2, D3.

- The detection of a photon at detector T acts as the trigger
- Note: The coherence of the photons nee to be substantially longer than the length the UV pulse so that the two pairs are not distinguishable



Experimental proof of GHZ entanglement

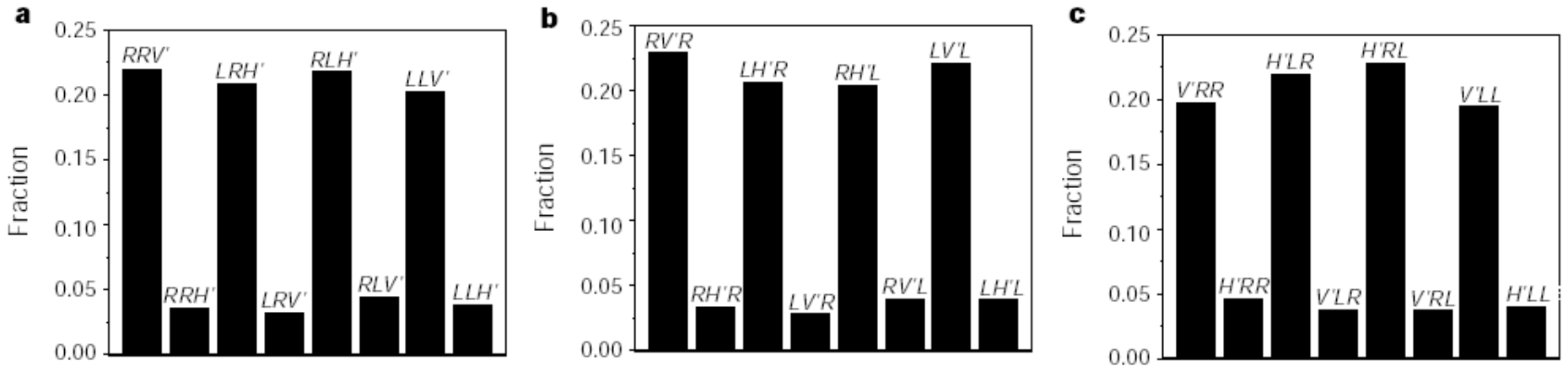
- As a first step $|GHZ\rangle$ entanglement has to be confirmed experimentally. Four fold coincidences are detected for variable delays in path a



Graph (a) polarization analysis at D3 (two curves § 45±), conditioned on T, and the detection of one photon at D1 polarized at 45± and one photon at detector D2 polarized at -45±. In (b) no such intensity difference is predicted if the polarizer in front of detector D1 is set at 0±

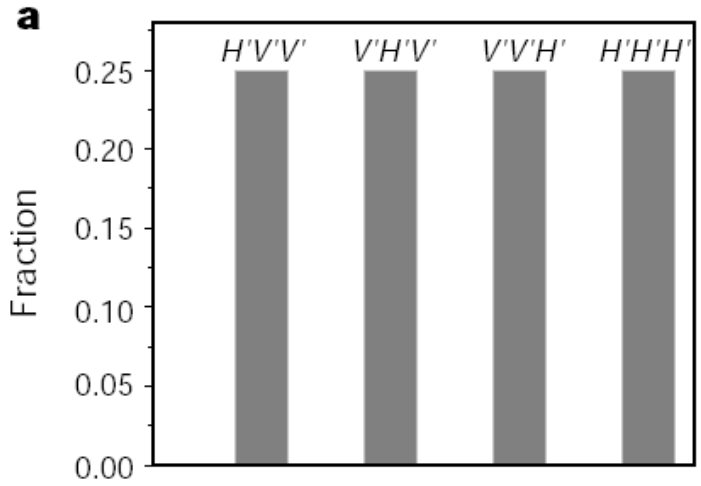
Measurements in different bases

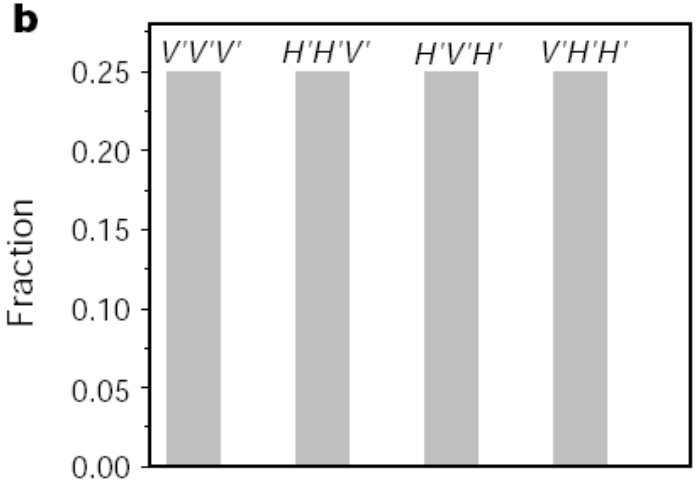
- Performing the measurements in the YYX (a), YXY (b), and XYY (c) basis confirms the entanglement properties of the $|GHZ\rangle$ state
- The experiment yields a visibility of 71%.
- Based on these results one can identify the terms which are supposed to be absent and those which should be present.
- Thus one can compare the quantum mechanical and local realistic results for measurements in the XXX basis.

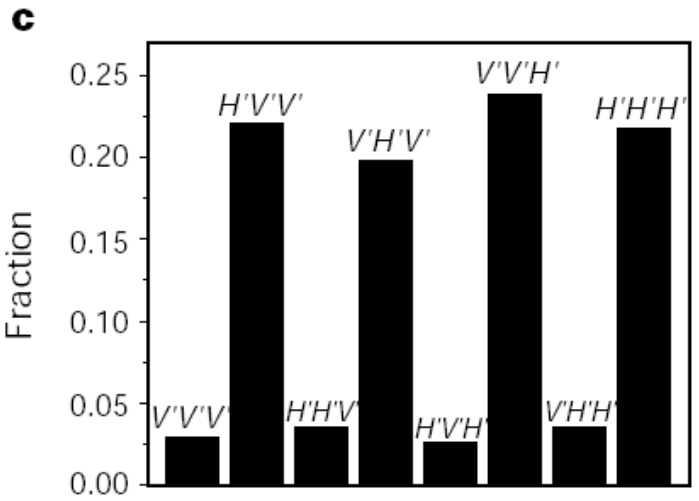


Local realism vs. quantum mechanics

- The measurements in the XXX basis yield the following results: (a) XXX quantum mechanics; (b) XXX local realism; (c) XXX experimental results:





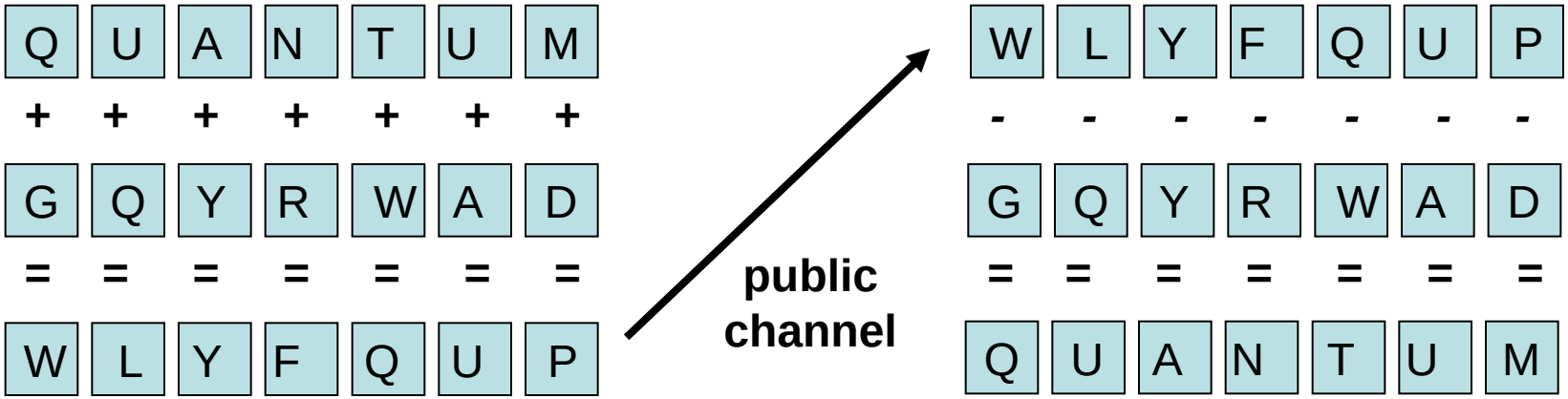


Lecture QI7

Quantum Cryptography

One time pads

- Cryptographic protocol which allows the encryption and decryption protocol to be publicly known. The security of the protocol relies entirely on the key which is private and not publicly known.
- A simple, very secure cryptosystem is the *Vernam cipher* or *one time pad.*
- Alice and Bob share identical *n*-bit secret key strings. Alice encodes her message by adding message and key (XOR). Bob decodes by subtracting the key again.
- As long as the key is secure the one time pad is provably secure, i.e. Eve's mutual information with the message can be made arbitrarily small.
- In contrast public key distribution relies on the unproven difficulty of solving certain mathematical problems like factoring.



Quantum key distribution and no-cloning

- Transmission of single or entangled quanta (qubits) between Alice and Bob.
- The security is guaranteed by encoding the key in non-orthogonal quantum states (we will discuss BB84) or in entangled pairs of qubits (EPR cryptography).
- The No-Cloning Theorem guarantees that non-orthogonal states cannot be copied (this property of quantum states could also be used for quantum money which cannot be forged). To see this we consider normalised states |ai and |bi which are not orthogonal i.e. $\langle a|b\rangle \neq 0$. A cloning machine described by the state |machinei would have to operate

$$|a\rangle|\text{blank}\rangle|\text{machine}\rangle \rightarrow |a\rangle|a\rangle|\text{machine}_\text{a}\rangle$$
$$|b\rangle|\text{blank}\rangle|\text{machine}\rangle \rightarrow |b\rangle|b\rangle|\text{machine}_\text{b}\rangle$$

- The unitary operation of the machine has to preserve the inner product

$$\langle a|b\rangle\langle\text{machine}|\text{machine}\rangle \rightarrow \langle a|b\rangle\langle a|b\rangle\langle\text{machine}_\text{a}|\text{machine}_\text{b}\rangle$$

- This is only possible if $\langle a|b\rangle = 0$ or $\langle a|b\rangle = 1$. Note: classical information is encoded in orthogonal quantum states and can thus be copied.

The BB84 protocol (I)

- Alice begins with two strings A and B each consisting of $(4+\delta)n$ qubits. She encodes these strings as a block of $(4+\delta)n$ qubits

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k,b_k}\rangle$$

where a_k is the k^{th} bit of A and b_k is the k^{th} bit of B. Each qubit is in one of the four states

$$\begin{aligned} |\psi_{00}\rangle &= |0\rangle \\ |\psi_{10}\rangle &= |1\rangle \\ |\psi_{01}\rangle &= (|0\rangle + |1\rangle)/\sqrt{2} \\ |\psi_{11}\rangle &= (|0\rangle - |1\rangle)/\sqrt{2} \end{aligned}$$

- The bits in A are encoded in the basis X or Z determined by B.
- These four states are not mutually orthogonal and cannot be distinguished with certainty

The BB84 protocol (II)

Transmission

- Alice sends $4(n+\delta)$ encoded message qubits to Bob
- Bob publicly announces receipt of the qubits

Measurement

- Bob measures in random bases B' to get his bit string A'
- Then the bases B and B' are announced publicly

Verification

- Alice and Bob keep $2n$ key bits a_K, a'_k where encoding $b_k = b'_k$
- They compare n of these bits to check for an eavesdropper
- If sufficiently few of these disagree: success

Secure key

- The remaining bits provide a random secure key
- This can be used for the provably secure classical Vernam cipher.

Intercept - Resend Attack (I)

Alice	Eve	$p(E\|A)$	Bob	$p(B\|EA)$
0X	0X	1/2	0X	1/4
			0Z	1/8
			1Z	1/8
	1Z	1/4	1Z	1/8
			0X	1/16
			1X	1/16
	0Z	1/4	0Z	1/8
			0X	1/16
			1X	1/16

Intercept - Resend Attack (II)

- Eve guesses the correct value of the bit with 75% probability.
- If Alice and Bob measure in the same basis then their results will disagree with a probability of 1/4. Therefore (for a perfect noiseless channel) the probability for Alice and Bob to find disagreement and thus identifying Eve when comparing *n* of their key bits is given by

$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

- Thus the number of bits *n* that need to be compared for detecting an eavesdropper with a probability P_d is:

$$n = \frac{\log_2(1 - P_d)}{\log_2(3/4)}$$

- Thus in comparison to trusting the transmission (and not comparing any key bits) Alice and Bob need at least to sacrifice *n* bits from their key for detecting Eve with probability P_d.

The Ekert 91 protocol using EPR pairs

- Alice and Bob measure at angles ϕ_A and ϕ_B
- Expectation value

$$E(\phi_A, \phi_B) = \langle \Psi^- | \sigma_{\phi_A} \sigma_{\phi_B} | \Psi^- \rangle = -\cos(2(\phi_A - \phi_B))$$

- The correlations for ± 1 outcomes are

$$P_{\pm\pm} = \left| \langle \phi_A^{\pm} \phi_B^{\pm} | \psi^- \rangle \right|^2$$

The Ekert 91 protocol using EPR pairs

Alice and Bob set measurement angles randomly

$\phi_{A1} = 0, \phi_{A2} = \frac{\pi}{4}, \phi_{A3} = \frac{\pi}{8}$ $\phi_{B1} = 0, \phi_{B2} = \frac{3\pi}{8}, \phi_{B3} = \frac{\pi}{8}$

Alice and Bob announce their measurement angels and results

Alice and Bob announce their results when the angels are different

They work out the Bell function $\mathcal{B}$ from the CHSH inequality, detect eavesdropper if $\mathcal{B} \leq 2\sqrt{2}$

A secret key is established from those cases where the angels agree

$E(\phi_{A1}, \phi_{B1}) = -1$ $E(\phi_{A3}, \phi_{B3}) = -1$

Free space cryptograph: Alice – the sender

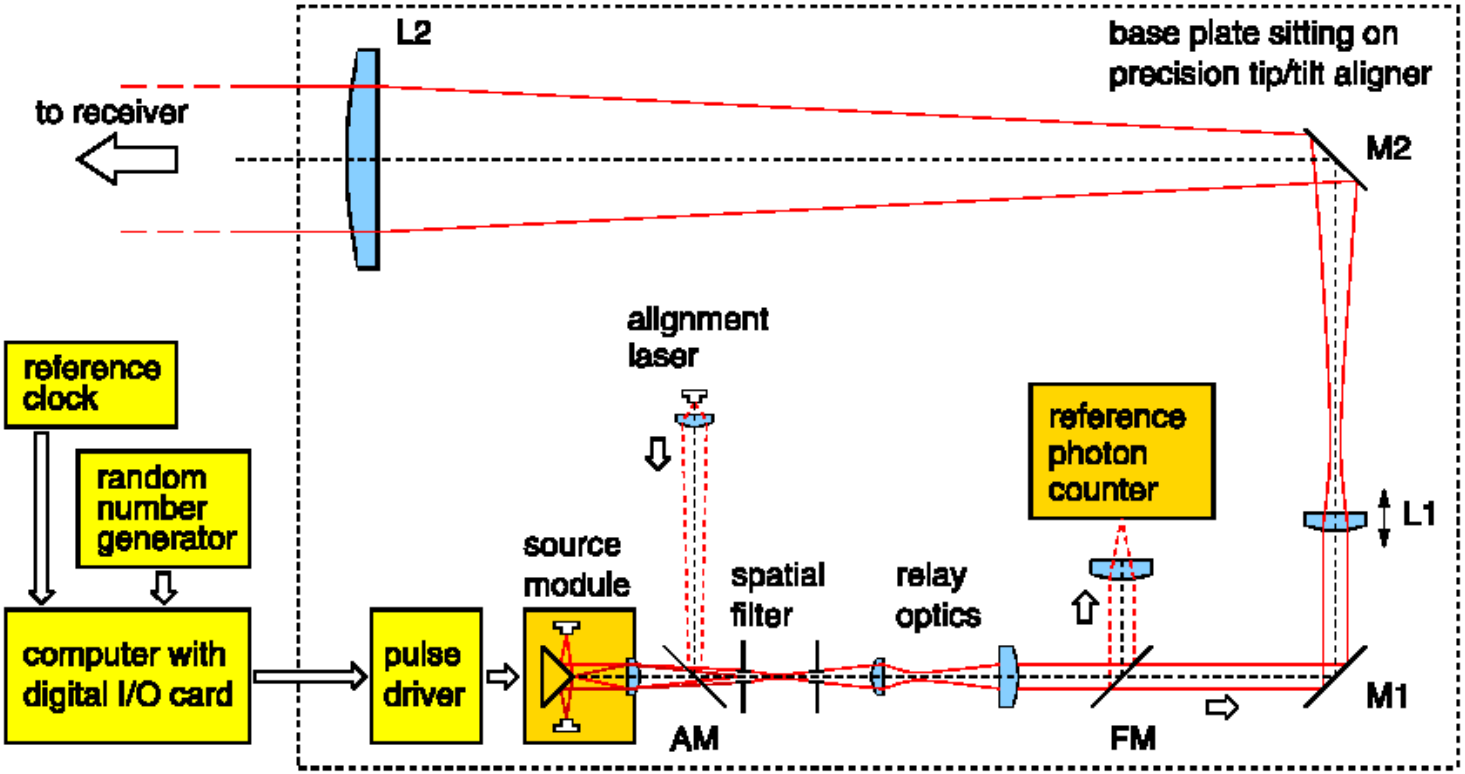


Figure 1: The Alice compact breadboard transmitter. The digital I/O card delivers a random 2-bit signal at 10 MHz synchronised to the reference clock. This signal is used in the pulse driver for randomly firing one of four lasers in the miniature source module. The four lasers are combined in a spatial filter using a conical mirror and relay lens. This system produces pulses with 0.05-0.5 photons per pulse. The output of the spatial filter is then transformed to a collimated beam with 2 mm FWHM and further expanded in a x20 telescope (L1 and L2) to produce a near diffraction-limited 40mm beam. A precision translator with lens L1 allows for the fine focus adjustment. A bright CW laser beam can be injected with an auxiliary mirror AM for alignment purposes into the the same spatial filter as the faint pulses, while a calibration of the number of photons per bit can be made by inserting mirror FM and measuring a reference photo-count. Mirrors AM, FM M1 and M2 are gold coated for high reflectivity in the infra-red.

Free space cryptograph: Bob – the receiver

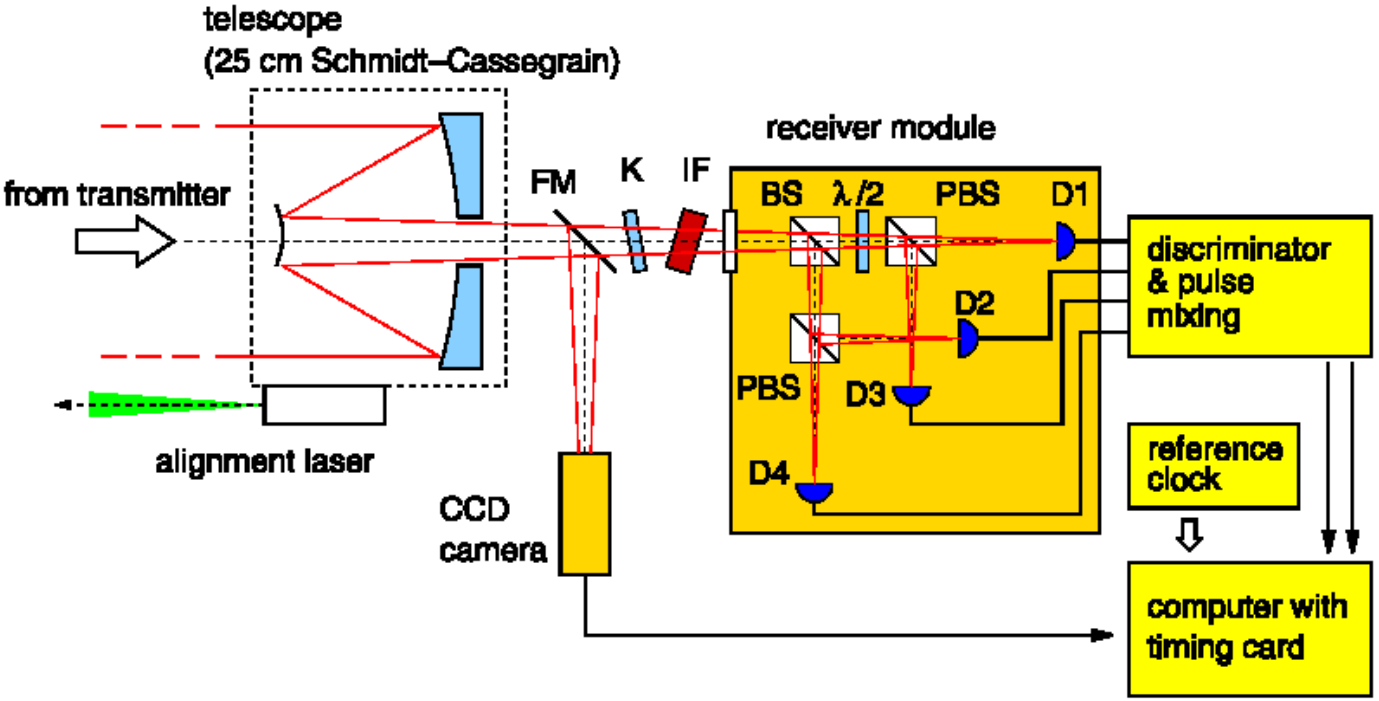
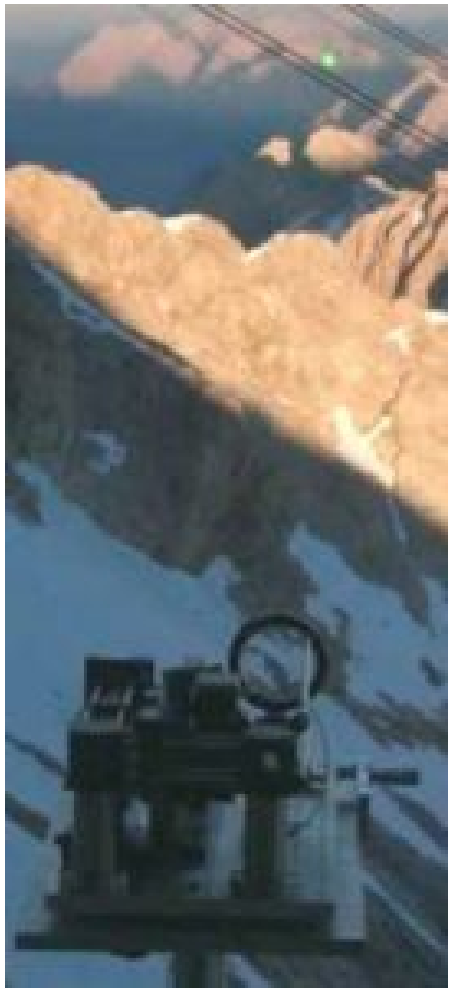
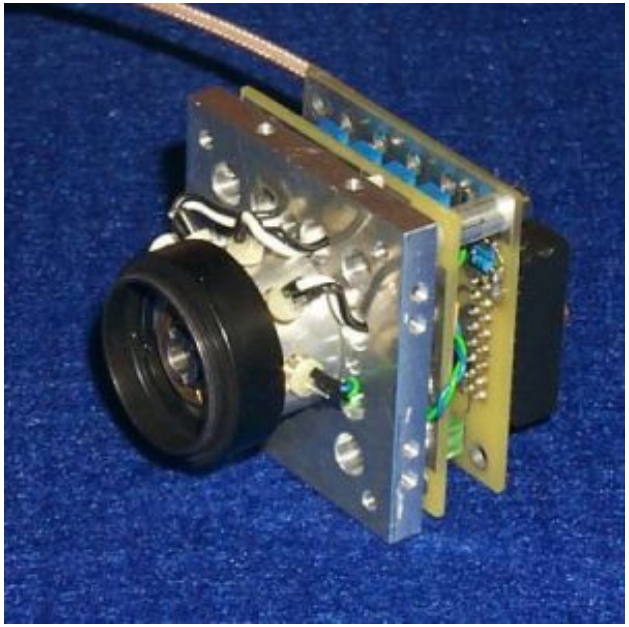


Figure 2 The receiver (Bob) consists of a 25 cm aperture Schmidt-Cassegrainian telescope. The miniature detector module is attached to the rear mounting of the telescope. It consists of a non-polarising beamsplitter (BS) followed by two polarising beamsplitters (PBS). Single photon detectors (D1-4) receive the output of the polarisers. In the D1/D3 arm, a half wave plate rotates the analysed polarisation to the 45° basis. The module incorporated high voltage supplies and discriminator circuitry to produce standard NIM pulses at the output. The detector outputs D3, D4 are combined with the D1, D2 outputs with a delay of 5 ns and input into the two channel timing card in the PC. A flip mirror allows a CCD camera to view the incoming light for alignment purposes.

Free space cryptography – real experiment



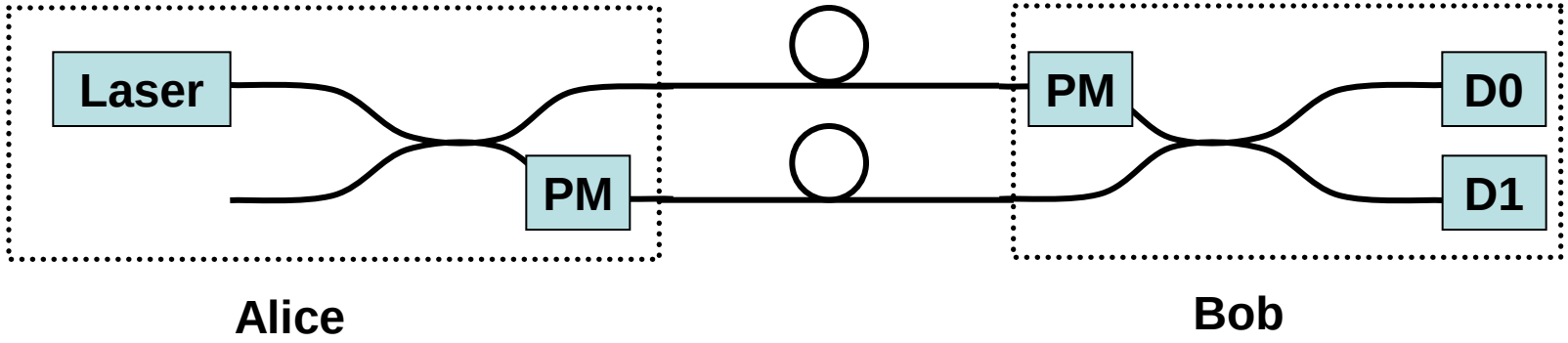
Alice:



Bob:

Phase encoded systems in fibres (I)

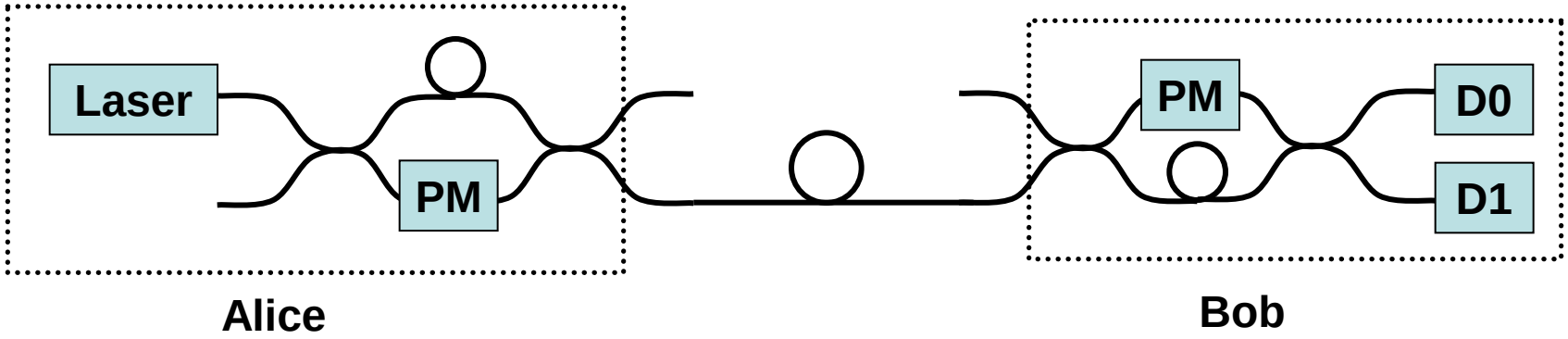
- Optical fibres do not conserve the polarization
  - depolarization (suppressed by very coherent source)
  - randomly fluctuating birefringence (1 hour timescale)
  - Polarization tracking is possible but makes the scheme cumbersome
- An extended Mach-Zehnder setup is used for phase encoding



- Alice uses her phase modulator (PM) to encode 0, 1 in phases 0 and π or in phases $\pi/2$ and $3\pi/2$.
- Bob also chooses between 0 phase shift and $\pi/2$ phase shift for his measurements → This scheme is equivalent to polarization encoding.
- However, keeping the phase constant over large distances is very difficult.

Phase encoded systems in fibres (II)

- A better practical setup is to collapse the interferometer



- Two pulses are propagating down the single fibre. They are denoted by S (short path) and L (long path). After travelling through Bob's part of the Mach-Zehnder they create three different outputs: SS and LL are not relevant as they show no interference effects.
- SL and LS are indistinguishable and thus interfere. The choice of phase shifts by Alice and Bob gives the encoding-decoding exactly as in the previous scheme.
- Setup much more stable since the pulses follow the same path for most of the interferometer.
- Drawback: Half of the signal is lost in the SS and LL path.