Quantum Communication

Dieter Jaksch

TT 2009

Clarendon Laboratory
University of Oxford

Contents

1 Introduction

Scientific progress in physics and mathematics has led to the development of efficient technology for communicating and distributing information in the 20^{th} century. This technology forms one of the cornerstones of the information society and our global economy which are highly reliant on secure methods to transfer and distribute information quickly. To satisfy ever increasing demands for speed and security encryption and communication methods are constantly improved and there is an ongoing effort to develop corresponding technology further.

Classical information theory is not usually part of a physics undergraduate degree. It assumes simple classical properties of physical systems and based on those a largely mathematical theory of information is established. The obtained results are mostly independent of the chosen implementation and its physical details. However, one still has to acknowledge that information is physical, i.e. information carriers, senders, and receivers obey the laws of physics. The notion of quantum information comes about since it turns out that the rules of quantum mechanics violate some of the basic physical assumptions of classical information theory. The consequences of this are many, ranging from improved channel capacities, the possibility of physically secure communication protocols to invalidating some assumptions about the security of classical communication protocols. The field of quantum information processing is still at its infancy and is currently closely linked with physics. However, one can expect that quantum information theory will develop into a field of its own if simple quantum physical properties determining the behaviour of quantum information can be identified.

This lecture course starts by introducing the basics of classical information theory and some of the most important quantum counterparts. This is followed by a discussion of photon technologies for realizing quantum communication. The violation of basic classical assumptions by quantum systems is then exemplified by showing how entangled states violate Bell's inequalities and local realism. Finally, schemes for efficient quantum communication based on entangled states and physically secure cryptographic communication methods are introduced.

2 Basics of Information Theory

As already mentioned in the introduction information is physical. It must be embodied in the state of a physical system and processing of information must be accomplished by dynamical evolution of a physical system. Information is thereby defined by the ability to perform a certain task and quantified by how many *resources* are required to perform a specific *task successfully.*

Examples:

E1. How many data CD's (the resources storing the information) are needed to store a map of the UK (the task) which specifies the position of each address (success)?

E2. Which physical resources are required to transmit a state $|\Psi\rangle$ from sender Alice to receiver Bob with entanglement fidelity $F = 0.999$?

As can already be seen from these simple examples numerous different types of resources exist and success can be defined in a number of different ways. It is thus desirable to quantify information in terms which are to a large extent independent of the physical realization.

2.1 Quantifying Classical Information

2.1.1 The setup

We consider the situation where a sender (Alice) communicates with a receiver (Bob) over a communication channel. We do not wish to make assumptions on how the messages are embodied. We assume the following general setup.

- The sender Alice:
  - She can send one out of N messages $x_1 \cdots x_N$ per use of the channel.
  - The probability that Alice chooses message x_j is known and given by p_j. We do not know the physical laws which allow to calculate the message chosen by Alice.
- The communication channel:
  - The channel is capable of transmitting one of Alice's N messages to the receiver in each use.
  - It can introduce noise and be susceptible to eavesdropping by Eve.
  - We consider classical and (later) quantum channels.
- The receiver: Bob
  - The channel provides Bob with one of the messages $y_1 \cdots y_M$.
  - The probability to receive message y_n is denoted by q_n.

To quantify the amount of information transmitted between sender and receiver in this scenario we describe Alice's messages by a random variable X which can take the values $x_1 \cdots x_N$. X takes on the value x_j with probability p_j and the probabilities sum to one

$$\sum_j p_j = 1.$$

The amount of information contained in a message (or in X) is defined as the number of bits which are at least required to store an outcome of a measurement of X. It tells us how much we learn from a perfect measurement of (reading) X. When measuring X the uncertainty about its content is reduced. The information gained about the message is therefore defined as the reduction in information content induced by the measurement. After a perfect measurement of X we know for sure which message was sent and subsequent measurements on this message will not tell us anything new. This process thus reduces the information content to zero and the gained information equals the original information content. For the general case of imperfect measurements the original information content and the gained information do not agree and some residual uncertainty about the message is left. In the following sections we discuss the properties of the sender, receiver and communication channel, respectively.

2.1.2 The Sender and Shannon's Noiseless Coding Theorem

The information content of a message sent out by Alice is given by the *Shannon entropy* $H(X)$ defined as

$$H(X) = -\sum_{j=1}^{N} p_j \log_2(p_j).$$

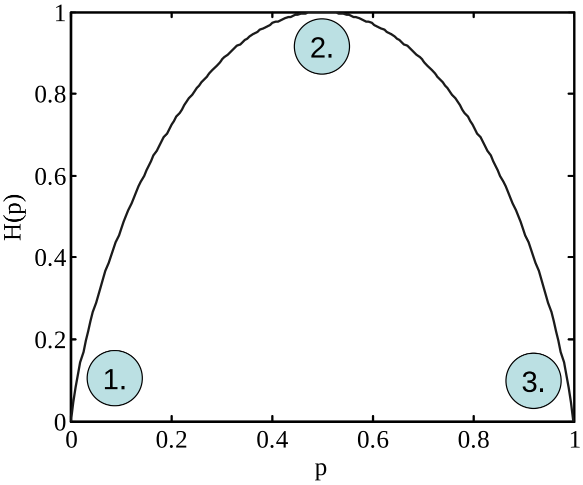


Figure 1: Shannon entropy $H(p)$ as a function of probability p. Message 0 is sent with probability p and message 1 with probability $1-p$. A maximum is reached for $p = 1/2$ at point 2. The information content goes to zero if only one message is ever sent at points 1 and 3.

The Shannon entropy $H(X)$ does not depend on the values x_j of X but just on the probabilities p_j. It is thus applicable to any kind of message if the probability distribution of messages is known. A message which occurs with probability zero does not add to $H(X)$ since $0 \log_2(0) = 0$. We cannot gain any information from messages which are never sent. If only one message appears with certainty it does also not contain any information since $1 \log_2 1 = 0$. Nothing can be learnt from measuring one message only since the outcome can be predicted with certainty. The Shannon entropy is bounded by $0 \leq H(X) \leq \log_2(N)$ with $H(X) = \log_2(N)$ if and only if (iff) $p_j = 1/N \ \forall\, j$.

Example:

E3. Alice can send two messages 0 and 1. She chooses 0 with probability p and 1 with probability $1-p$. How much information does one of her messages contain?

Using the above expression for H we find

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

The maximum information content is reached for

$$\frac{\mathrm{d}H(p)}{\mathrm{d}p} = -\log_2(p) + \log_2(1-p) = 0\,,$$

which yields $p_{\max} = 1/2$ and minima are obtained for $p_{\min,1} = 0$ and for $p_{\min,2} = 1$ since the possible range of values of p is bounded by $0 \leq p \leq 1$. At $p_{\max}$ each message contains one bit of information while at $p_{\min}$ the information content is zero as expected. The shape of $H(p)$ is shown in Fig. 1.

If both messages are sent with equal probability in the above example one bit is necessary to store which message was sent. If Alice always sends the same message nothing needs to be stored to know which message was sent. For all other values of p the information content has to be interpreted as the average number of bits required to store a message if a large number of messages (strictly speaking infinitely many) are sent. That this is indeed the case is the content of *Shannon's noiseless coding theorem* which we state here without proof: A message x_j can on average be compressed to $H(X)$ bits using an optimal code for message compression.

Example:

E4. Alice can send messages X with values a,b,c. The probability for a is $p_a = 1/2$ while b, c have a probability of $p_b = p_c = 1/4$. How much information is contained in one message?

$$H(X) = -p_a \log_2 p_a - p_b \log_2 p_b - p_c \log_2 p_c = \frac{1}{2}(\log_2 2 + \log_2 4) = \frac{3}{2}\,.$$

By encoding a using the bit string 0, b as 10 and c as 11 the average length L of a bit string representing a value of X will be

$$L = 1 \times \frac{1}{2} \times 1 + 2 \times \frac{1}{4} \times 2 = 3/2 = H(X)\,.$$

This code is optimal, the messages cannot be be compressed further without losing information about the original messages. Note that the bit string of optimally encoded messages contains a 0 or a 1 at each position with the same probability 1/2.

Finding the optimal encoding for given message probabilities is a non-trivial task (c.f. the varying performance of data compression software). The following example illustrates the performance of a very simple data compression procedure.

Example:

E5. Alice sends message a with probability p and message b with probability $1-p$. Assuming $p > 1/2$ we choose to encode aa as 0, ab as 10 and b as 11. The message string aa occurs with probability p^2, ab with $p(1-p)$ and b with $(1-p)$. The average number of bits required to store a message L is given by

$$L = \frac{1}{2} \times p^2 + 1 \times p(1-p) + 2 \times (1-p)\,.$$

The comparison of the average length L with the Shannon entropy $H(p)$ shown in Fig. 2 reveals that this encoding is never optimal and gets best for $p \approx 0.774$. This encoding is only better than simply identifying a with 0 and b with 1 if $p > \sqrt{3} - 1$.

The noiseless coding theorem quantifies the amount of information contained in the messages sent out by Alice. It is thus also often called *Shannon's source coding theorem.* When the messages Y are received by Bob they will most often have been subject to noise and thus not be identical to X. Therefore the question arises what Bob learns about the messages X when reading the received messages Y.

2.1.3 The Receiver and Mutual Information

The messages Y transmitted to Bob via the communication channel take on values y_n with probabilities q_n. Bob reads the messages Y and gains information $H(Y)$. To quantify the

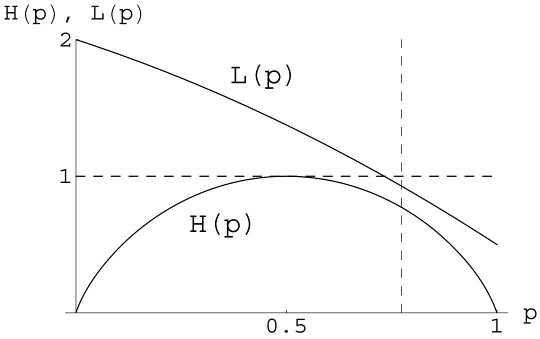


Figure 2: Shannon entropy $H(p)$ and average bit string length $L(p)$ as a function of probability p. The vertical dashed line indicates the value of p where the bit string length is closest to the entropy $H(p)$.

amount of information gained about the original messages X by reading Y we first introduce the joint entropy of the variables X and Y as

$$H(X,Y) = -\sum_{j,n} p(x_j, y_n) \log_2(p(x_j, y_n)) \,,$$

where $p(x_j, y_n)$ is the probability that X takes the value x_j and Y takes the value y_n. This joint entropy is the total information content of variables X and Y. Furthermore we define the entropy of X conditional on knowing Y by

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

$H(X|Y)$ tells us how uncertain we are about the value of X after measuring Y.

If X and Y are uncorrelated, i.e. the probability q_n of Y taking on the value y_n is independent of the value of X, then Bob does not learn anything about X from measuring Y. In this case

$$p(x_j, y_n) = p_j q_n$$

and we have

$$H(X,Y) = H(X) + H(Y) \,,$$

(see class problems for a proof). Thus the information content of X is not decreased by measuring Y. In other words, Bob's uncertainty on the value of X does not decrease when measuring Y, i.e. $H(X|Y) = H(X)$. However, if the value of X is fixed by measuring Y, i.e.[1]

$$p(x_j, y_n) = \left\{ \begin{array}{cl} q_n & \text{for} \quad j = n \\ 0 & \text{otherwise} \end{array} \right. \,,$$

we find that $H(X,Y) = H(Y)$. When Bob measures y_n he knows that X certainly has the value x_n. In this case he learns all he can about X, i.e. $H(X|Y) = 0$. X and Y are perfectly correlated. The measurement reduced the information content $H(X,Y) = H(Y)$ by $H(Y)$ to zero and thus no uncertainty about either X or Y is left after measuring Y.

[1] Here we assume for simplicity that $M = N$ and that the ordering of messages is preserved in the transmission

Based on these two observations we introduce the *mutual information content* of X and Y as

$$H(X:Y) = H(X) + H(Y) - H(X,Y)\,.$$

This can also be written as $H(X:Y) = H(X) - H(X|Y)$. We find that no mutual information is contained in X and Y if they are uncorrelated since then $H(X,Y) = H(X) + H(Y)$. In this case no information is transmitted over the channel. If X and Y are perfectly correlated we have $H(X,Y) = H(Y)$ and the mutual information between X and Y takes its maximal value $H(X:Y) = H(X)$. The information sent by Alice can be completely restored at the receiver side in this case.

2.1.4 The communication channel

We can now quantify the communication channel in terms of its channel capacity. This defines the amount of information which is transmitted by the channel in a single use. Note that it is not important that the messages arrive without being altered. The only criterion is whether Bob can reconstruct Alice's message from the output. For instance, for a channel which maps $1 \to 1$ and $0 \to 0$ we find $H(X:Y) = H(X)$ and a channel with $1 \to 0$ and $0 \to 1$ also has $H(X:Y) = H(X)$. However, a channel with $1 \to 1$ and $0 \to 1$ does not transmit information as can be seen by working out $H(X:Y) = 0$.

A *noiseless channel* $\mathcal{N}$ produces messages Y which are perfectly correlated with the initial messages X and thus $H(X:Y) = H(X)$. In this case Alice can transmit $H(X)$ bits of information with every use of $\mathcal{N}$. By exploiting Shannon's noiseless coding theorem $H(X) = \log_2(N)$ can be achieved. The channel capacity $C(\mathcal{N})$ is therefore given by

$$C(\mathcal{N}) = \log_2(N).$$

If a *noisy channel* is used X and Y will be correlated but not perfectly. The question then is whether by redundant encoding one can ensure arbitrarily good reliability of the channel. *Shannon's noisy channel coding theorem* states that this is possible with a channel capacity of

$$C(\mathcal{N}) = \max_{\{p_j\}}\{H(X:Y)\}\,,$$

where the maximum is taken over all possible input probability distributions p_j of X. We do not give a proof of this theorem.

Remark: Sometimes channel capacity is given in bits/sec which is $C(\mathcal{N})$ times the number of possible channel uses per second (e.g. for internet connections).

2.1.5 Connection to Statistical Physics

The Shannon entropy is a generalization of the equation $S = k_B \ln W$ from statistical physics where k_B is the Boltzmann constant and W the number of microstates accessible to the system. This equation follows from our definition of the Shannon entropy by identifying each microstate with one of the messages and assuming that each of them is occupied with the same probability $1/W$. The Shannon entropy for this type of 'sender' takes on its maximum value and equals S up to an unimportant constant factor. The thermodynamic entropy S is thus a measure of our ignorance of the thermal state assuming that all microstates are equally likely populated.

2.2 Quantifying Quantum Information

It is useful to revise some quantum mechanics before defining quantum information in a quantum setup similar to the classical setup discussed in the previous section.

2.2.1 Quantum Mechanics

The trace of an operator In linear algebra the trace of a matrix M is defined as the sum over all diagonal elements

$$\mathrm{Tr}\left\{M\right\} = \sum_n M_{nn}\,.$$

This definition extends to operators in a linear Hilbert space as follows. Given an operator $\hat{M}$ and an orthonormal basis $|\phi_n\rangle$ the operator can be rewritten as a matrix M with matrix elements

$$M_{nm} = \langle\phi_n|\,\hat{M}\,|\phi_m\rangle\ .$$

This matrix represents the operator $\hat{M}$ in basis $|\phi_n\rangle$ and we can write $\hat{M} = \sum_{nm}|\phi_n\rangle\, M_{nm}\,\langle\phi_m|$. The trace of an operator is defined as the sum over all diagonal elements of M

$$\mathrm{Tr}\left\{\hat{M}\right\} = \sum_n M_{nn} = \sum_n \langle\phi_n|\,\hat{M}\,|\phi_n\rangle\ .$$

For this definition to be physically relevant we need to show that it is independent of the chosen basis. Two bases are related by a unitary matrix U according to $|\psi_m\rangle = \sum_n U_{mn}\,|\phi_n\rangle$. Thus in the new basis the trace of $\hat{M}$ is given by the trace of the matrix

$$\mathrm{Tr}\left\{\hat{M}\right\} = \mathrm{Tr}\left\{U^{\dagger}MU\right\}\ .$$

Since the trace does not change under cyclic permutation and U is unitary we have

$$\mathrm{Tr}\left\{\hat{M}\right\} = \mathrm{Tr}\left\{MUU^{\dagger}\right\} = \mathrm{Tr}\left\{M\right\}\ ,$$

and thus the definition of the trace is basis independent.

Analytical function of an operator For working out a function of an operator we first write it in terms of its eigenvalues and eigenvectors $\hat{M} = \sum_m |\phi_m\rangle\, M_m\,\langle\phi_m|$. Any power of this operator can then be written as $\hat{M}^n = \sum_m |\phi_m\rangle\, M_m^n\,\langle\phi_m|$. Any analytical function F of this operator is then well defined as $\mathcal{F}\{\hat{M}\} = \sum_m |\phi_m\rangle\,\mathcal{F}\{M_m\}\,\langle\phi_m|$.

Example:

E6. We calculate the logarithm of the operator $\sigma_x + 3\mathbb{I} = 4\,|+\rangle\,\langle+|+2\,|-\rangle\,\langle-|$ with eigenvalues 2 and 4. We find $\log_2(\sigma_x+3\mathbb{I}) = \log_2(4)\,|+\rangle\,\langle+| + \log_2(2)\,|-\rangle\,\langle-| = 2\,|+\rangle\,\langle+| + |-\rangle\,\langle-|$

The partial trace of an operator The partial trace of an operator is defined as the trace over a subspace of the total Hilbert space. In working it out an operator acting on the total Hilbert space is mapped into one acting on a subspace of the Hilbert space only. In our case we will e.g. be interested in tracing over the part of the Hilbert space pertaining to the sender and will be left with an operator that only acts on the degrees of freedom accessible to the receiver. The total Hilbert space is broken up into two parts $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The basis of $\mathcal{H}$ can be written as $|nm\rangle = |n\rangle_A \otimes |m\rangle_B$ where $|n\rangle_A$ describes degrees of freedom of the sender $\mathcal{H}_A$ and $|m\rangle_B$ those of of the receiver $\mathcal{H}_B$. The partial trace of an operator $\hat{M}$ over subspace $\mathcal{H}_A$ is given by

$$\mathrm{Tr}_A\left\{\hat{M}\right\} = \sum_n {}_A\langle n|\,\hat{M}\,|n\rangle_A = \sum_n |m\rangle_B \left(M_{nm,no}\right)_B\langle o|\ .$$

Here we have used the notation $M_{nm,lo} = \langle nm| \hat{M} |lo\rangle$ and used the rule[2] ${}_A\langle n|\, lo\rangle = \delta_{nl} |o\rangle_B$. The resulting operator contains only basis elements corresponding to degrees of freedom of the receiver. We have thus *traced out* the sender. Note that subsequently tracing over both Hilbert spaces yields the trace of the operator.

The density operator All quantum mechanical expectation values for a system in the pure state $|\psi\rangle$ can be rewritten in terms of a trace

$$\langle \hat{M}\rangle = \langle\psi| \hat{M} |\psi\rangle = \mathrm{Tr}\left\{ |\psi\rangle \langle\psi| \hat{M} \right\}.$$

We can thus define the operator $\rho = |\psi\rangle\langle\psi|$ and use it replace the state vector $|\psi\rangle$. This operator is called the density operator or state of the system. All observable quantities can be worked out from the density operator[3].

Sometimes the state vector of a system is not known but it is known that the system will be in state $|\psi_n\rangle$ with probability p_n. This can e.g. happen if the system preparation is imperfect, after a measurement if the outcome is not revealed, in decoherence processes, when a system is in a thermal state, or when it produces quantum messages $|\psi_n\rangle$ with probability p_n. Then the expectation value of an operator has to be worked out for each possible state and to be weighted with the corresponding probability[4]. This yields

$$\langle \hat{M}\rangle = \sum_n p_n \mathrm{Tr}\left\{ |\psi_n(t)\rangle \langle\psi_n(t)| \hat{M} \right\}.$$

The trace is linear and therefore we can define the (mixed) density operator

$$\rho = \sum_n p_n |\psi_n(t)\rangle \langle\psi_n(t)|,$$

and in general write $\langle \hat{M}\rangle = \mathrm{Tr}\left\{ \hat{M}\rho \right\}$. Using a density operator to describe a system thus allows a compact and efficient way to include classical uncertainty about its wave function into quantum mechanical calculations.

Global measurement In second year quantum mechanics measurement of a hermitian operator $\hat{M}$ with eigenvectors $|\phi_n\rangle$ and non-degenerate eigenvalues a_n is introduced. The average measurement outcome for a system in pure state $|\Psi\rangle$ is given by $\langle \hat{M}\rangle = \langle\Psi| \hat{M} |\Psi\rangle$. In a single measurement the eigenvalue a_n is obtained and the system collapsed into the state $|\phi_n\rangle$ with probability $p_n = |\langle\phi_n|\,\Psi\rangle|^2 = \langle\phi_n|\,\Psi\rangle\langle\Psi|\,\phi_n\rangle$. For a mixed state ρ this extends using identical arguments as above. Outcome a_n is obtained with probability $p_n = \langle\phi_n|\rho|\phi_n\rangle$. If outcome a_n is obtained the mixed state is collapsed into $|\phi_n\rangle\langle\phi_n|\rho|\phi_n\rangle\langle\phi_n|/p_n = |\phi_n\rangle\langle\phi_n|$.

For an operator with degenerate eigenvalues a_n and eigenvectors $|\phi_{n,l}\rangle$, where l enumerates the set of degenerate eigenvectors for eigenvalue a_n, the probability of outcome a_n is given by $p_n = \sum_l \langle\phi_{n,l}|\rho|\phi_{n,l}\rangle$. The mixed state is collapsed into $\sum_l |\phi_{n,l}\rangle\langle\phi_{n,l}|\rho|\phi_{n,l}\rangle\langle\phi_{n,l}|/p_n$. Note that p_n is included here to obtain a normalized state. The observer cannot distinguish states with degenerate eigenvalues. The corresponding degrees of freedom are not accessible in this measurement.

[2] This is not a proper scalar product and slightly sloppy, though widely used, notation.

[3] The unmeasurable global phase is gone.

[4] This is a classical uncertainty of the state and has nothing to do with the quantum uncertainty.

In most cases we will not be concerned with the eigenvalues a_n obtained in a measurement of an operator $\hat{M}$. We instead specify a measurement via a set of orthnormal states $|\phi_n\rangle$ and ask about the probability p_n of projecting the system into state $|\phi_n\rangle$. The corresponding eigenvalues are assumed to be non-degenerate so that these state are distinguishable for the observer. The operator $\hat{M}$ and its eigenvalues a_n are not required to calculate the probabilities p_n. However, a corresponding observable $\hat{M}$ could be constructed as $\hat{M} = \sum_n a_n |\phi_n\rangle \langle\phi_n|$ with arbitrarily chosen real $a_n \neq a_l$ for $n \neq l$.

Local observables and measurement A local observable of the receiver can be written as $\hat{M} = \mathbb{I}_A \otimes \hat{M}_B$ since the receiver cannot directly measure degrees of freedom located at the sender. We work out the expectation value of $\hat{M}$ by first tracing over the sender and find

$$\left\langle \hat{M} \right\rangle = \mathrm{Tr}_B \left\{ \mathrm{Tr}_A \left\{ \hat{M}\rho \right\} \right\} = \mathrm{Tr}_B \left\{ \hat{M}_B \mathrm{Tr}_A \left\{ \mathbb{I}_A \rho \right\} \right\} = \mathrm{Tr}_B \left\{ \hat{M}_B \rho_B \right\}$$

where $\rho_B = \mathrm{Tr}_A \{\rho\}$ is the reduced density operator of the receiver. Thus all information about observables which can be measured locally by the receiver is contained in the reduced density operator ρ_B. The same argument holds for the sender with reduced density operator $\rho_A = \mathrm{Tr}_B \{\rho\}$.

The measurement of a local observable $\hat{M} = \mathbb{I}_A \otimes \hat{M}_B$ can be described as above by specifying the eigenstates of M_B written as $|\phi_m\rangle_B$ and using the reduced density operator ρ_B. The measurement collapses the state of the receiver into $|\phi_m\rangle_B$ and the total system into $\rho_A \otimes |\phi_m\rangle_B \langle\phi_m|$ with probability $p_m = {}_B\langle\phi_m| \rho_B |\phi_m\rangle_B$. The operator $\hat{M}$ has degenerate eigenvalues[5] since the receiver cannot measure degrees of freedom of the sender. Alternatively, we can write the operator as $\hat{M} = \sum_{n,m} |n\rangle_A \langle n| \otimes a_m |\phi_m\rangle_B \langle\phi_m|$ with a_m the (assumed) non-degenerate eigenvalues of M_B and n labeling the degeneracy[6]. Using the above definitions for measuring a global degenerate observable $\hat{M}$ we again find that the system is projected into state $\rho_A \otimes |\phi_m\rangle_B \langle\phi_m|$ with probability p_m. Both approaches are equivalent.

Example:

E7. Alice and Bob share a Bell state $|\psi^-\rangle$. What is the reduced density operator for each of them? What are the probabilities for a local measurement at Alice's site to project the system into the orthogonal states $|\phi_1\rangle_A$ and $|\phi_2\rangle_A$? In this case the Hilbert space is split into $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ and basis states $|nm\rangle = |n\rangle_A \otimes |m\rangle_B$ with $n, m = 0, 1$. The reduced density operator of the receiver Bob is

$$\rho_B = {}_A\langle 0| \psi^-\rangle \langle\psi^-| 0\rangle_A + {}_A\langle 1| \psi^-\rangle \langle\psi^-| 1\rangle_A = \frac{1}{2}\left(|0\rangle_B \langle 0| + |1\rangle_B \langle 1|\right) = \frac{\mathbb{I}_B}{2}.$$

This is the maximally mixed state of a qubit. By symmetry we obtain $\rho_A = |0\rangle_A \langle 0| + |1\rangle_A \langle 1| = \mathbb{I}_A/2$. The probability to project into either of two states in a local measurement is 1/2.

2.2.2 Information content of a density operator

In quantum mechanics the classical messages X are replaced by the density operator. Alice prepares quantum states to be sent to Bob. These encode the messages and are described by a

[5] Except for the trivial case where the sender only consists of a one dimensional Hilbert space

[6] Note that $\sum_n |n\rangle_A \langle n|$ is the identity operator on the sender subspace.

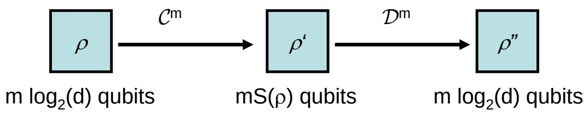


Figure 3: Compression $\mathcal{C}_m$ and decompression $\mathcal{D}_m$ of m copies of a quantum state ρ. The size of the original Hilbert space corresponds to $m\log_2(d)$ qubits which are compressed to $mS(\rho)$ qubits.

density operator ρ. The density operator ρ is hermitian and can thus be written as

$$\rho = \sum_j p_j \left|x_j\right\rangle \left\langle x_j\right| ,$$

where $|x_j\rangle$ are orthogonal normalized eigenvectors (i.e. the quantum messages) and p_j are the probabilities of Alice sending state $|x_j\rangle$ to Bob[7]. The von Neumann entropy of the state ρ is defined by

$$S(\rho) = \text{Tr}\ \{\rho \log_2(\rho)\} = -\sum_j p_j \log_2(p_j)\,.$$

The von Neumann entropy is a measure of our ignorance about the quantum state. It plays a similar role for quantum states as the Shannon entropy does for classical random variables. Using the von Neumann entropy quantum states can almost be treated as if they were information. The von Neumann entropy also plays an important role in quantum statistical mechanics. Up to a constant factor it reduces to the familiar entropy S for thermal states where each accessible microstate (message) is occupied (sent) with the same probability.

Schumacher's quantum noiseless channel coding theorem In analogy to Shannon's noiseless coding theorem Schumacher showed that states ρ in a d dimensional Hilbert space $\mathcal{H}$ produced by a quantum information source can be compressed. In particular it is possible to reliably compress and decompress ρ to a quantum state in a Hilbert space $\mathcal{H}_A$ with dimension

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

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. The procedure is schematically shown in Fig. 3. Reliably in this case means that the entanglement fidelity of the original state $\rho^{\otimes m}$ after compression $\mathcal{C}_m$ and decompression $\mathcal{D}_m$ tends to 1 for large m. The entanglement fidelity tells us how well the state $\rho^{\otimes m}$ preserves its entanglement with an environment during compression and decompression[8].

2.2.3 Joint entropy and mutual information

We define the joint entropy for the quantum state of Alice and Bob ρ_{AB} in analogy to classical information as

$$S(\rho_{AB}) = -\text{Tr}\ \{\rho_{AB} \log_2(\rho_{AB})\}\ .$$

[7] We assume here for simplicity that different messages are orthogonal.

[8] We do not define the entanglement fidelity here (see Nielsen and Chuang, page 420 for details).

The reduced density operators ρ_A for Alice and ρ_B for Bob yield the corresponding information contents $S(\rho_A)$ and $S(\rho_B)$. From those the conditional entropy and mutual information follow as in the classical case

$$S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_B)\,,$$
$$S(\rho_A : \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})\,.$$

These quantities replace those introduced in classical information theory. Note that they do, however, not have the classically expected properties. For instance, the conditional entropy can become negative as we will explicitly work out later for the case of two entangled qubits.

In contrast to the classical case Bob cannot read his messages without affecting the quantum state. The process of measuring the received messages can thus influence the entropy of the state. We study different possibilities by considering measurement on one qubit.

Example:

E8. A qubit is prepared in the pure state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. It is measured in the computational basis and we consider two different scenarios: (i) the outcome of the measurement is $|0\rangle$ and (ii) the outcome of the measurement is not revealed. Case (ii) can e.g. happen in a decoherence process where the measurement is performed by the environment and the outcome is not accessible. How does the information content of the qubit change?

(i) The initial state is $\rho_i = |+\rangle\langle+|$. This is a pure state (state $|+\rangle$ is prepared with certainty) and thus has entropy $S(\rho_i) = 0$. After the measurement the state is $\rho_f = |0\rangle\langle 0|$ which is again pure and thus $S(\rho_f) = 0$. While the quantum state changes in this process the qubit remains in a pure quantum state and does not contain information. Still, each of the two possible measurement outcomes occurs with probability 1/2.

(ii) The possible states after the measurement are $|0\rangle$ and $|1\rangle$ each with probability of $p_0 = p_1 = 1/2$. Not knowing the actual outcome we thus have to write

$$\rho_f = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\ .$$

This state has entropy $S(\rho_f) = 1$. Lacking the knowledge of the measurement outcome turns the initial pure state into a mixed state. Its information content (uncertainty about the qubit state) increases.

Finally we consider what happens if a measurement in the computational basis is performed on the state ρ_f and the outcome is $|0\rangle$. In this process the entropy is reduced from 1 to 0. The mixed state is turned into a pure state by the measurement and one bit of information about the original state is gained. This type of measurement is consistent with measuring in a classical system.

2.2.4 Quantum channels

A quantum channel transforms input systems described by a Hilbert space $\mathcal{H}_1$ into output systems described by Hilbert space $\mathcal{H}_2$.[9] It is represented mathematically by a completely positive, unital map T which acts on the density operator ρ as

$$T(\rho) = \sum_{j=1}^{n} E_j \rho E_j^\dagger.$$

[9] $\mathcal{H}_2$ is often assumed to be identical to $\mathcal{H}_1$.

Here F_j are the so-called *Kraus operators* which fulfill $\sum_j E_j^\dagger E_j < \mathbb{I}$. The channel capacity quantifies the number of qubits which can be faithfully transmitted. For an ideal channel we have $T = \mathbb{I}$, the identity operation. The channel capacities of quantum channels are fully understood only for special cases. For instance the Holevo-Schumacher-Westmoreland (HSW) theorem gives the channel capacity if only product input states are used[10]. A detailed discussion of channel capacity is beyond the scope of this lecture course. Instead we consider two simple examples of how noise and decoherence affect the information content of quantum systems.

Examples:

E9. A classical bit is stored in two atomic states $|0\rangle$ and $|1\rangle$. The state $|0\rangle$ is stable while the state $|1\rangle$ is metastable and spontaneously emits photons at a rate γ. How does the mutual information between the state of the atom and the initial bit change with time?

The original bit is in a maximally mixed state $\rho_A = (|1\rangle\langle 1| + |0\rangle\langle 0|)/2$ and contains $S(A) = 1$ bit of information. The joint bit-atom system is initially prepared in state $\rho_{AB} = (|11\rangle\langle 11| + |00\rangle\langle 00|)/2$. If the atom is initially in state $|1\rangle$ the probability p_1 of finding it in state $|1\rangle$ at a later time is determined by the equation $\dot{p}_1 = -\gamma p_1$ and thus we find

$$\rho_{AB} = \frac{\mathrm{e}^{-\gamma t}}{2}|11\rangle\langle 11| + \frac{1-\mathrm{e}^{-\gamma t}}{2}|10\rangle\langle 10| + \frac{1}{2}|00\rangle\langle 00| \,.$$

This state has entropy

$$S(AB) = \frac{\mathrm{e}^{-\gamma t}}{2}(\gamma t \log_2(e) + 1) - \frac{1-\mathrm{e}^{-\gamma t}}{2}\log_2\left(\frac{1-\mathrm{e}^{-\gamma t}}{2}\right) + \frac{1}{2}\,.$$

We find the entropy of the atomic state by tracing out the initial bit obtaining the reduced density operator

$$\rho_B = \frac{\mathrm{e}^{-\gamma t}}{2}|1\rangle\langle 1| + \frac{2-\mathrm{e}^{-\gamma t}}{2}|0\rangle\langle 0|\,.$$

This state has entropy

$$S(B) = \frac{\mathrm{e}^{-\gamma t}}{2}(\gamma t \log_2(e) + 1) - \frac{2-\mathrm{e}^{-\gamma t}}{2}\log_2\left(\frac{2-\mathrm{e}^{-\gamma t}}{2}\right)\,.$$

Both entropies are shown in Fig. 4. Initially the entropy solely arises from the unknown state of the bit. The uncertainty of the atomic state due to spontaneous emission then increases the overall entropy for short times $t \leq 1/\gamma$. For times $t \gg 1/\gamma$ the atom will be in the pure state $|0\rangle$ and the entropy of the system is again solely due to the state of the initial bit. However, in this process the correlation between the state of the atom and the bit is lost as becomes evident by looking at the mutual information $S(A:B) = S(A) + S(B) - S(AB)$ also shown in Fig. 4. Note: This example can equally well be described using classical information theory.

E10. A photonic channel is used to transmit two messages $|0\rangle \equiv$ no photon present and $|1\rangle \equiv$ one photon present. 20% of the photons are lost in the channel. We investigate the following classical and quantum scenarios for using this channel to establish mutual information between sender Alice an receiver Bob.

[10] See Nielsen and Chuang page 555.

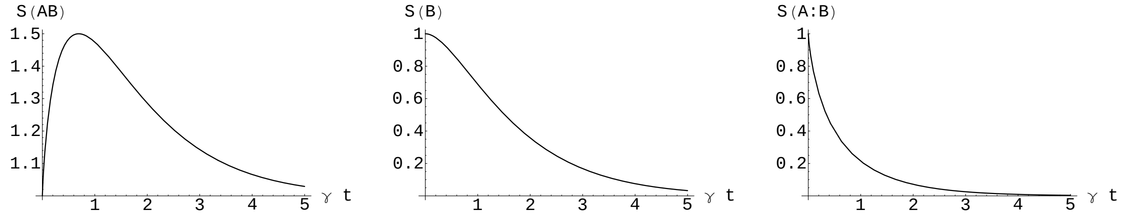


Figure 4: Entropies of an atom B storing a classical bit A. The atom undergoes spontaneous emission.

(i) Classical messages X with values $|0\rangle$ and $|1\rangle$ are sent with probabilities $p_0 = p_1 = 1/2$ and received as messages Y as $|0\rangle$ and $|1\rangle$. How much mutual information is created in one use of the channel?

We find $H(X) = 1$. The joint entropy can be worked out from the probabilities $p(0,0) = 1/2$, $p(0,1) = 0$, $p(1,1) = 4/10$ and $p(1,0) = 1/10$. It is given by $H(X,Y) = 1.361$. The probabilities on the receiver side are $q_0 = 6/10$ and $q_1 = 4/10$ and thus $H(Y) = 0.971$. We therefore find $H(X|Y) = H(X,Y) - H(Y) = 0.39$ and $H(X : Y) = H(X) - H(X|Y) = 0.61$. The noise in the channel (photon loss) significantly reduces the maximally achievable mutual information from 1 bit to 0.61 bits per use of the channel. Note: phase noise leading to $|1\rangle \to -|1\rangle$ does not influence this scheme (it only leads to timing errors and may slightly reduce the maximum possible number of uses of the channel per second).

(ii) Alice creates an entangled state $|\Psi^-\rangle$ and sends one qubit to Bob. The resulting quantum state is

$$\rho = \frac{9}{10}\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{1}{10}|00\rangle\langle 00| .$$

Since the states $|\Psi^-\rangle$ and $|00\rangle$ are orthogonal this density operator has eigenvalues 9/10, 1/10, 0 and 0 giving an entropy of $S(\rho) = 0.469$. The reduced density operator on Alice's side is $\rho_A = (11\,|0\rangle\langle 0| + 9\,|1\rangle\langle 1|)/20$ with entropy $S(\rho_A) = 0.9928$. By symmetry $S(\rho_B) = 0.9928$. We thus find for the conditional entropy $S(\rho_A|\rho_B) = -0.524$ and a mutual information of $S(\rho_A : \rho_B) = 1.517$. If no noise were present the mutual information would increase to 2 bits. Note: This scheme is not resistant against phase noise. It is crucial to keep coherence in the transmission process in order to achieve the increased mutual information compared to the classical case.

As we see from the last example the mutual information established via distributing an entangled state can be larger than in the classical case and negative conditional entropies, which are not possible in classical schemes, may arise. However, there is no (known) scheme on how to solely use this kind of mutual information to transmit messages from Alice to Bob. Alice initially prepares a pure state which does not contain information. Entanglement alone is thus not sufficient for communication (and faster than light communication is not possible). However, by combining entanglement and classical communication improvements over conventional classical communication schemes can be achieved e.g. in quantum dense coding.

2.3 Quantum dense coding

The idea behind quantum dense coding is that Alice can distribute entanglement via the state $|\Psi^-\rangle$ before she has decided which message to send to Bob. The communication scheme thus starts with the state $|\Psi^-\rangle$ shared between Alice and Bob. Alice then sends one of four possible messages 00, 01, 10, 11 by applying a local quantum operation on her qubit of the entangled pair. In detail she applies 00: $\mathbb{I}$, 01: σ_z, 10: σ_x and 11: $\sigma_x\sigma_z$. This operation turns the initial Bell state into the orthogonal Bell states 00: $|\Psi^-\rangle$, 01: $|\Psi^+\rangle$, 10: $|\Phi^-\rangle$ and 11: $|\Phi^+\rangle$. She then sends her qubit to Bob via the quantum channel and Bob measures both bits in the Bell basis. A Bell state analyzer for photon states will be discussed in detail in Sec. 3.1.5. Since the Bell states are orthogonal they can be distinguished having only one copy of the state.

Note: At some point before the communication takes place Alice and Bob need to share the entangled pair. This requires Alice sending a qubit to Bob or sending qubits to Alice and Bob from a source of entangled qubits. The entangled state is independent of the message to be sent in both cases and the distribution can thus be done before Alice decides on which message to send. The initial entangled pair thus acts as a resource for communication between Alice and Bob.

3 Photon techniques

Here we discuss methods for realizing quantum communication and computation with photons. The experimental setups discussed in this section are shown in the appendix.

3.1 Polarization and spatial mode encoding

The wave function of the photon (see optics part of this lecture course) has spatial and polarization degrees of freedom. Both can be used to encode qubits. In spatial mode encoding orthogonal direction/momentum modes a and b are chosen to represent the qubit states $|0\rangle$ and $|1\rangle$. In polarization encoding the qubit is encoded in the photon polarization e.g. $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$. In both cases single qubit gates can be implemented by linear optical elements and two qubit gates via nonlinear media. We will next discuss these conventional 'network' quantum computing techniques. In addition proposals for quantum computing using purely linear optics exist. There entanglement is created by postselection of photons after a measurement is carried out. More recently the creation of highly entangled graph states of photons has attracted a lot of interest. These entanglement of these states serves as resource for carrying quantum information processing. These methods will not be discussed here in more detail.

3.1.1 Spatial encoding

If two spatial paths impinge on a beam splitter (BS) a single qubit gate changing the amplitudes in the two paths is realized. For instance a simple 50/50 BS maps an input state $|\Psi\rangle_{\text{in}} = \alpha|0\rangle_{\text{in}} + \beta|1\rangle_{\text{in}}$ into the output state $|\Psi\rangle_{\text{out}} = H|\Psi\rangle_{\text{in}} = [(\alpha+\beta)|0\rangle_{\text{out}} + (\alpha-\beta)|1\rangle_{\text{out}}]/\sqrt{2}$ which realizes a Hadamard gate. For general beam splitters the transformation is

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

where $\cos^2(\xi)$ and $\sin^2(\xi)$ are the reflectivity and transmitivity of the beam splitter, respectively. The simple 50/50 BS corresponds to $\text{BS}(\pi/4,0) = \text{H}$. The value of ϕ is the phase shift experienced in a transmission through the BS similar to the phase gate discussed next.

A single qubit phase gate Φ is implemented by putting a slab of transparent medium with refractive index n and length L into the path of one spatial mode. This causes a phase shift $\phi = (n - n_0)L\omega/c_0$ with respect to the second arm, which we assume to be in air. Here n_0 and

c_0 are refractive index and speed of light in air, respectively. This maps the qubit wave function according to the truth table $|0\rangle_{\text{out}} \rightarrow |0\rangle_{\text{in}}$ and $|1\rangle_{\text{out}} \rightarrow e^{\mathrm{i}\phi}\,|1\rangle_{\text{in}}$.

These two linear optical elements allow the realization of all necessary single qubit operations. Kerr nonlinearities χ are necessary to create a two qubit phase gate where a phase shift is induced if two photons are traveling a distance L in the Kerr medium (see nonlinear optics part of this course). Since this phase is conditional on both photons being present it is an entanglement phase given by $\varphi = \chi L$ and can be used to realize a controlled two qubit phase gate

$$\begin{array}{lccl} |00\rangle_{\text{in}} & \rightarrow & & |00\rangle_{\text{out}} \\ |01\rangle_{\text{in}} & \rightarrow & \mathrm{e}^{\mathrm{i}\phi} & |01\rangle_{\text{out}} \\ |10\rangle_{\text{in}} & \rightarrow & \mathrm{e}^{\mathrm{i}\phi} & |10\rangle_{\text{out}} \\ |11\rangle_{\text{in}} & \rightarrow & \mathrm{e}^{\mathrm{i}(\varphi+2\phi)} & |11\rangle_{\text{out}}\ , \end{array}$$

where the phase ϕ is caused by the linear refractive index of the Kerr medium. Together these gates form a universal set of gates for quantum computing.

Example:

E11. We can now interpret the familiar setup of a Mach-Zehnder interferometer in terms of single qubit gates. The setup consists of a 50/50 BS followed by a phase shifter Φ in one arm and then a second 50/50 BS. This maps the input state $|\Psi\rangle_{\text{in}}$ according to $|\Psi\rangle_{\text{out}} = \mathrm{H}\Phi\mathrm{H}|\Psi\rangle_{\text{in}}$ which in matrix form is given by

$$|\Psi\rangle_{\text{out}} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

and gives

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

Note that the phase shifter can be written as $\Phi = \mathrm{e}^{\mathrm{i}\phi/2}(\cos(\phi/2)\mathbb{I} - \mathrm{i}\sin(\phi/2)\sigma_z)$ and thus $\mathrm{H}\Phi\mathrm{H}= \mathrm{e}^{\mathrm{i}\phi/2}(\cos(\phi/2)\mathbb{I} - \mathrm{i}\sin(\phi/2)\sigma_x)$, using $\mathrm{H}\sigma_z\mathrm{H}= \sigma_x$.

3.1.2 Polarization encoding

Single qubit gates are implemented by polarization rotators and polarization phase shifters acting on the polarization degrees of freedom instead of the spatial degrees of freedom discussed in the previous section. For realizing two qubit gates polarizing beam splitter (PBS) can be used to first spatially separate $|H\rangle$ and $|V\rangle$ components. The spatially separated paths are then used to realize a phase gate as before. After a PBS the qubit state can be measured by two spatially separated photo detectors.

Example:

E12. A quarter-wave plate with its fast axis at an angle of $\pi/4$ to the vertical and horizontal directions of polarization is placed into the path of a polarization encoded photon. Which gate does this wave plate implement? What happens for a half-wave plate placed at an angle of ϕ to the vertical axis?

The fast axes is $(|V\rangle + |H\rangle)/\sqrt{2}$ and the slow axis is $(|V\rangle - |H\rangle)/\sqrt{2}$. The fast axis will pick up a phase of $e^{-\mathrm{i}\pi/2}$ relative to the slow axis. An initially vertically polarized photon will end up in state $|V\rangle \to (|V\rangle - \mathrm{i}\,|H\rangle)/\sqrt{2}$ while a horizontally polarized photon is turned into $|H\rangle \to (|V\rangle + \mathrm{i}\,|H\rangle)/\sqrt{2}$ (up to global phases). For a half-wave plate a phase of $e^{\mathrm{i}\pi} = -1$ is picked up. Up to global phases this leads to a rotation of the polarization angle by 2ϕ, i.e. $|V\rangle \to \cos(2\phi)\,|V\rangle + \sin(2\phi)\,|H\rangle$ and $|H\rangle \to -\cos(2\phi)\,|H\rangle + \sin(2\phi)\,|V\rangle$. This is a σ_x or NOT gate for $\phi = \pi/4$ and a Hadamard gate for $\phi = \pi/8$.

3.1.3 Parametric down conversion

In nonlinear optical media a single photon can be converted into a pair of photons as discussed in the nonlinear optics part of this lecture course. Energy, momentum and angular momentum conservation rules obeyed in this process determine the correlations between the two created photons. Experimental setups can be designed to create the following types of entangled states.

Time entanglement This only relies on the fact that the two photons in a pair are created simultaneously and satisfy energy conservation laws. The time entangled states can be measured in a Franson type interferometer with two short $|S\rangle_{1,2}$ and two long arms $|L\rangle_{1,2}$. The created state is given by

$$|\psi\rangle = \frac{1}{2}\left[|S\rangle_1|S\rangle_2 + e^{i(\phi_1+\phi_2)}|L\rangle_1|L\rangle_2 + e^{i\phi_2}|S\rangle_1|L\rangle_2 + e^{i\phi_1}|L\rangle_1|S\rangle_2\right].$$

Here $\phi_{1,2}$ is a phase introduced in the long arms of the interferometer. The path difference between the L and the S arms is much longer than the coherence length of the photons and thus no interference fringes are observed inside the two interferometers. While the overall state is a product state appropriate time gating can be used to detect only the first two terms of the state and discard the SL and LS terms. The LL and SS terms are truly coincident and indistinguishable because the time of creation of the photon pair is not known. These two parts of the wavefunction will thus interfere and show fringes as a function of the phase $\phi_1 + \phi_2$. This interference indicates time entanglement and can be observed by measuring coincidences in the outputs of the two interferometers.

Momentum entanglement This can be created in non-collinear down-conversion and fulfilling the phase matching conditions. The state created in this process is given by

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[e^{i\phi_b}|a\rangle_1|b\rangle_2 + e^{i\phi_a}|a\rangle_2|b\rangle_1\right],$$

where $|a\rangle_{1,2}$ and $|b\rangle_{1,2}$ are different photon paths. Combining these paths with BSs interference fringes are detected as a function of $\phi_{a,b}$ indicating entanglement.

Polarization entanglement Non-collinear type-II down-conversion phase matching can be used to achieve photons entangled in polarization. Photons at certain angles with the optical axis such that they are emitted along cones with no common axis are used. One cone is ordinarily, the other extraordinarily polarized. They intersect along two directions where the light is unpolarized. At this intersection the state of two photons is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|V\rangle_1|H\rangle_2 + e^{i\phi}|H\rangle_1|V\rangle_2\right].$$

The phase ϕ can be controlled by a compensator crystal.

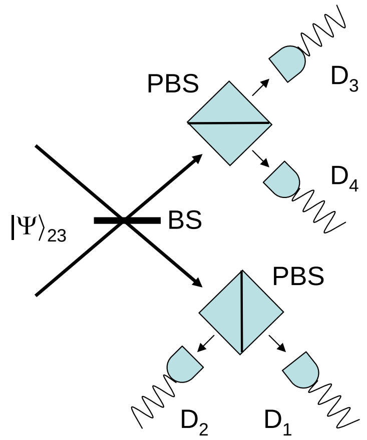


Figure 5: A partial Bell state analyzer identifying the polarization encoded Bell states $|\Psi^+\rangle$ and $|\Psi^-\rangle$.

3.1.4 Single photon sources and single photon detectors

The simplest way to achieve a single photon source is to use laser light which is a superposition $|\alpha\rangle$ (a coherent state) of different photon number states $|n\rangle$ given by

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \, .$$

The first few terms in this sum are

$$|\alpha\rangle \propto |0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle + \frac{\alpha^3}{\sqrt{6}}|3\rangle \, .$$

By attenuating this beam the laser intensity and thus the parameter $|\alpha|^2$ goes down. Then the dominant contributions to the state of the laser are vacuum $|0\rangle$ and the single photon state $|1\rangle$ while all higher order terms decrease with higher powers of α. For instance for $\alpha = \sqrt{0.1}$ if light ever makes it through the attenuator it is a single photon with 95% probability. The drawback of this simple method is that the source does not indicate whether a photon is present or not. Instead, in parametric down conversion measuring one photon indicates the presence of the other. More sophisticated schemes are currently developed which allow the on demand generation of a photon with well defined polarization, wave length and direction. Such single photon sources are important for improved implementations of quantum communication schemes.

Single photon detectors required in quantum communication should posses a high quantum efficiency, detect photons over a broad frequency range (100nm to 2000nm), have low dark count rates (NO false counts, NO afterpulsing). They should recover quickly after detecting a photon and have fast rise/pulse pair resolution. Single photon detectors are further separated into photon number resolving and photon counting devices.

3.1.5 Quantum dense coding: Experimental setup

Parametric down conversion is used to create a pair of polarization entangled photons realizing two qubits in a Bell state. One qubit is sent to the receiver and the other is manipulated by the sender before being submitted to the receiver: A $\lambda/4$ and $\lambda/2$ plate are used to realize σ_x and σ_z operations on this qubit. When both qubits have arrived at the receiver side a Bell state measurement needs to be carried out.

A setup for partially achieving a Bell state measurement is shown in Fig. 5. Two polarization entangled photons are incident onto the BS. The overall wave function of the two photons (polarization + spatial wave function) has to be symmetric since the photons are bosons. Therefore, if the polarization part of the state is (anti)symmetric the spatial part also has to be (anti)symmetric. For Bell state $|\Psi^-\rangle$ with antisymmetric polarization part one photon has to follow the upper arm and the other photon the lower arm after the BS. Thus a coincidence between D3 and D2 or D4 and D1 is registered. For $|\Psi^+\rangle$ both photons follow the same arm and thus a coincidence between D1 and D2 or between D3 and D4 is registered. In the other two cases $|\Phi^+\rangle$, $|\Phi^-\rangle$ two photons are detected in the same detector and they cannot be distinguished. This analyzer therefore identifies two of the four Bell states and distinguishes them from the other two Bell states. It does not allow to identify all four of them. Once can show that using only linear optics it is not possible to distinguish all four Bell states.

Example:

E13. Two identical photons impinge on a 50/50 BS one arriving at the upper arm $|u\rangle$ and the other at the lower arm $|l\rangle$. The photons have a symmetric polarization wave function. Which path will the photons take after the BS?

The initial symmetric wave function is $(|ul\rangle + |lu\rangle)/\sqrt{2}$. Each photon undergoes a Hadamard gate. This turns the wave function into

$$\frac{(|u\rangle + |l\rangle)(|u\rangle - |l\rangle) + (|u\rangle - |l\rangle)(|u\rangle + |l\rangle)}{\sqrt{8}} = \frac{|uu\rangle - |ll\rangle}{\sqrt{2}} .$$

Therefore both photons follow the upper or lower arm after the BS. Because of interference the $|ul\rangle$ and $|lu\rangle$ terms cancel and thus the two photons will never follow different paths.

4 Testing EPR

We discuss violations of local realistic assumptions by quantum mechanics as first predicted by Einstein Podolsky and Rosen (EPR). We consider the two most prominent examples of violating Bell inequalities and measurements on Greenberger-Horne-Zeilinger (GHZ) states. The experimental setups discussed in this section are shown in the appendix.

4.1 Bell inequalities

Violations of Bell inequalities can be used to demonstrate non-classical properties of entangled states and test quantum mechanics. Systems which follow classical common sense are described by a local and realistic theory and can be shown to obey inequalities for the maximum strengths of correlations between their constituents. We will show that these inequalities are violated by quantum mechanics and discuss experiments demonstrating such violations.

4.1.1 The CHSH inequality

We derive a Bell-type inequality (the so called CHSH inequality) by analyzing the Gendankenexperiment shown in Fig. 6 using common sense (not quantum theory). We assume

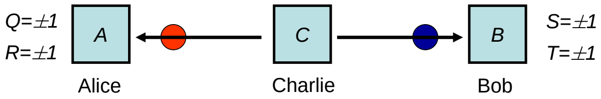


Figure 6: Schematic experimental setup to detect violations of the CHSH inequality

- Charlie prepares two systems (possibly correlated) and sends one to Alice and the other one to Bob.
- 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.
- They repeat this experiment many times and record their outcomes
- Alice and Bob meet and investigate the correlations between their experimental results.

What can they expect to obtain? For simplicity we assume that each measurement can only yield a value of ±1. We describe the possible measurements of Alice by random variables Q and R and those of Bob by random variables S and T. By common sense we assume that the measurement values of Q, R, S, and T exist independent of observation. This is the assumption of *realism.* Furthermore, Alice's measurement does not influence the outcome of Bob's measurement. They are performed in a causally disconnected manner, so it is reasonable to assume this. This is the assumption of *locality.* We investigate the expression

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

since either $Q + R$ or $Q - R$ is zero. We assume that the probability for measurement values $Q = q$, $R = r$, $S = s$, $T = t$ before the measurement is $p(q, r, s, t)$ and using this probability distribution we find the expectation value

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t} p(q, r, s, t)(QS + RS + RT - QT) \leq 2 \sum_{q,r,s,t} p(q, r, s, t) = 2\,.$$

This yields the CHSH inequality obeyed if the assumptions of local realism hold for the measurements carried out by Alice and Bob

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2\,.$$

We now analyze the same experiment using quantum mechanics for the case where Charlie generates an entangled Bell state $|\Psi^-\rangle$. He sends one qubit to Alice and the other to Bob. Alice chooses between measuring the operators $Q = \sigma_z$ and $R = \sigma_x$ on her qubit. Bob measures one of the operators $S = -(\sigma_z + \sigma_x)/\sqrt{2}$ and $T = (\sigma_z - \sigma_x)/\sqrt{2}$. We find the quantum mechanical expectation values $\langle QS\rangle = 1/\sqrt{2}$, $\langle RS\rangle = 1/\sqrt{2}$, $\langle RT\rangle = 1/\sqrt{2}$, and $\langle QT\rangle = -1/\sqrt{2}$ and therefore

$$E(QS) + E(RS) + E(RT) - E(QT) = 2\sqrt{2} > 2\,.$$

The experiment violates the CHSH inequality and the assumptions of local realism. Entanglement between Alice's and Bob's states yields correlations stronger than allowed by local realism.

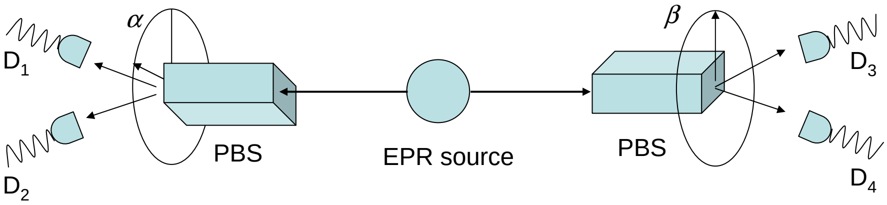


Figure 7: Schematic experimental setup of the Aspect experiments

4.1.2 The Aspect experiments

The first experiments demonstrating the violation of Bell inequalities were carried out by A. Aspect and co-workers[11]. A schematic setup of the experiment is shown in Fig. 7. The measurements were carried out on polarization entangled photons in state $|\Phi^+\rangle$. One photon was detected after a polarizing beam splitter (PBS) at angle α or β, the other after a PBS either at angle β or γ. Assuming local realism one can show that the number of coincidences N to obtain one photon at output port 0 or 1 (i.e. at detector D1 or D2 on Alice's side and at detector D3 or D4 on Bob's side) obeys the inequality

$$N(1_\alpha, 1_\beta) \leq N(1_\alpha, 1_\gamma) + N(1_\beta, 0_\gamma)\,.$$

Here $N(1_\alpha, 1_\beta)$ is the probability for Alice to obtain a click in D1 when setting her PBS at angle α and Bob to obtain a click in D3 when setting his PBS at angle β. This inequality is violated if the two photons are prepared in the entangled state $|\Phi^+\rangle$ when setting $\alpha - \beta = \beta - \gamma = 30^\circ$ since $N(1_\alpha, 1_\beta) \propto \cos^2(\alpha - \beta)$. By correlating different measurement results the Aspect experiments managed to violate the above Bell inequality.

4.1.3 Loopholes

The results of the Aspect experiments (and several experiments which followed them) can be viewed as evidence for the violation of local realism but this is not the only explanation. Various experiments had several loopholes: a) fair sampling assumption which presumes that the measured values are a fair reflection of all possible outcomes; b) rather small efficiency of photo detectors; c) accidental coincidences were removed in the experiment; d) polarizers were set up (not randomly) before the photons were created; e) strict Einstein locality of the measurements was not obeyed; f) the quantum system was not truly a bipartite system since it e.g. consisted of an atom and two photons. Addressing these loopholes requires a)b) 100% detection efficiency (e.g. achieved in ion trap experiments but only at 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. Measurements can be performed in strict Einstein locality and in different moving frames; f) measuring additional particles in the system and showing that they are not correlated with the two photons.

4.2 GHZ states

Bell inequalities are formulated in terms of expectation values. In principle the measurement of these expectation values requires infinitely many runs of the experiment. Local realism is only

[11] A. Aspect et al.,Phys. Rev. Lett. **47**, 460 (1981); A. Aspect et al., Phys. Rev. Lett. **49**, 91 (1982).

violated on average and not in any single run of an experiment. In contrast quantum mechanics predicts the violation of local realism with certainty for some entangled states of three particles, e.g. GHZ states. In these experiments measurement outcomes which are not allowed according to local realism will be found with certainty using quantum theory. Since we can make definite predictions rather than statistical ones no inequalities are needed in this setup.

4.2.1 Violations of local realism

A GHZ state is a three qubit entangled state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right) = \frac{1}{\sqrt{2}} \left(|VVV\rangle + |HHH\rangle\right) .$$

We analyze the state using notation commonly employed for polarization encoded qubits $|0\rangle \equiv |V\rangle$ and $|1\rangle \equiv |H\rangle$ which are eigenstates of σ_z. The polarizations rotated through 45° with respect to $|H\rangle$ and $|V\rangle$ are denoted by $|H'\rangle$ and $|V'\rangle$ and are eigenstates of σ_x. Left handed $|L\rangle$ and right handed $|R\rangle$ circular polarizations are eigenstates of σ_y. Rewriting the state $|\mathrm{GHZ}\rangle$ in the YYX basis we find

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

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 we find analogous expressions for measuring any two photons in circular polarization and the remaining one in 45° basis.

Local realistic analysis From a local realistic 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 investigate a measurement in the XXX basis. Which outcomes are possible if these elements of reality exist? The permutations of $|\mathrm{GHZ}\rangle$ 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. All of these polarizations are elements of reality so 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. Using similar arguments one can verify that the only four possible outcomes are

$$\left|V'V'V'\right\rangle \qquad \left|H'H'V'\right\rangle \qquad \left|H'V'H'\right\rangle \qquad \left|V'H'H'\right\rangle .$$

Quantum theoretical analysis In the XXX basis the state $|\mathrm{GHZ}\rangle$ reads

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

Local realism and quantum theory predict opposite results in all cases!

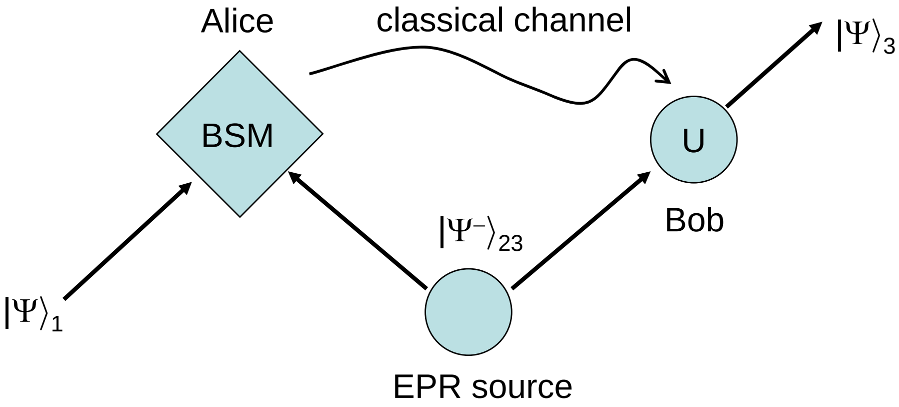


Figure 8: Quantum teleportation setup.

4.2.2 Experimental realization

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

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle + \mathrm{e}^{\mathrm{i}\phi}\,|VH\rangle\right) .$$

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

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

at three detectors D1, D2, D3 and the detection of the fourth photon at a detector T acts as the trigger. Note that in this experiment the coherence of the photons needs to be substantially longer than the length of the UV pulse so that the two pairs created in the downconversion processes are not distinguishable. See the classes for a detailed analysis of the experimental setup. Experimental results obtained from this setup agree with the quantum mechanical predictions and violate the local realistic predictions.

5 Quantum communication

We have already discussed quantum dense coding and seen that entanglement can serve as a resource for communication between Alice and Bob when combined with classical communication. In quantum dense coding two bits of information are transmitted via a shared pair of qubits and transmission of one qubit between sender and receiver. We will now consider more sophisticated quantum communication schemes. The experimental setups discussed in this section are shown in the appendix.

5.1 Quantum teleportation

The aim of quantum teleportation is to send an unknown quantum state of qubit 1 from Alice to Bob using classical communication and an entangled pair of qubits as shown in Fig. 8. The sender Alice receives qubit 1 in an unknown state $|\Psi\rangle_1 = \alpha\,|0\rangle + \beta\,|1\rangle$ and qubit 2 which is part of an entangled Bell state $|\Psi^-\rangle_{23}$ with qubit 3. The state of the three qubits is $|\Psi\rangle_{123} = [\alpha(|001\rangle - |010\rangle) + \beta(|101\rangle - |110\rangle)]$. Alice performs a Bell state measurement (BSM) on her two qubits and tells Bob the result. The measurement projects qubits 1 and 2 onto one of the four Bell states. The quantum state is projected according to the measurement outcome:

Outcome:	Quantum state:
$\|\Psi^-\rangle_{12}$	$\|\Psi^-\rangle_{12}\,(\alpha\,\|0\rangle + \beta\,\|1\rangle)_3$
$\|\Psi^+\rangle_{12}$	$\|\Psi^+\rangle_{12}\,(\alpha\,\|0\rangle - \beta\,\|1\rangle)_3$.
$\|\Phi^-\rangle_{12}$	$\|\Phi^-\rangle_{12}\,(\alpha\,\|1\rangle + \beta\,\|0\rangle)_3$
$\|\Phi^+\rangle_{12}$	$\|\Phi^+\rangle_{12}\,(\alpha\,\|1\rangle - \beta\,\|0\rangle)_3$

Note that qubit 3 is never entangled with qubits 1 and 2 after the measurement.

Bob receives qubit 3 and the measurement result from Alice. He applies a unitary U to particle 3 conditional on the measurement result as follows.

Outcome:	Quantum operation:
$\|\Psi^-\rangle_{12}$	$U = \mathbb{I}$
$\|\Psi^+\rangle_{12}$	$U = \sigma_z$.
$\|\Phi^-\rangle_{12}$	$U = \sigma_x$
$\|\Phi^+\rangle_{12}$	$U = \sigma_x \sigma_z$

For any measurement outcome the operation U turns the state of qubit 3 into the original state of qubit 1 yielding $|\Psi\rangle_3 = \alpha\,|0\rangle + \beta\,|1\rangle$ up to a irrelevant global phase.

We remark that the quantum state of all three qubits before Alice's measurement can be written as

$$\begin{aligned} |\Psi\rangle_{123} &= \frac{1}{2}\left(\left|\Psi^-\right\rangle_{12}(\alpha\,|0\rangle + \beta\,|1\rangle)_3 + \left|\Psi^+\right\rangle_{12}(\alpha\,|0\rangle - \beta\,|1\rangle)_3 + \left|\Phi^-\right\rangle_{12}(\alpha\,|1\rangle + \beta\,|0\rangle)_3 \right. \\ &\quad \left. + \left|\Phi^+\right\rangle_{12}(\alpha\,|1\rangle - \beta\,|0\rangle)_3\right) . \end{aligned}$$

Thus each of the four Bell states will be found with probability 1/4 in Alice's measurement. If the outcome is not revealed the measurement turns the state into a mixed state given by

$$\begin{aligned} \rho_{123} &= \left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right|(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\,\langle 0| + \beta^*\,\langle 1|) + \left|\Psi^+\right\rangle\left\langle\Psi^+\right|(\alpha\,|0\rangle - \beta\,|1\rangle)(\alpha^*\,\langle 0| - \beta^*\,\langle 1|) + \right. \\ &\quad \left. \left|\Phi^-\right\rangle\left\langle\Phi^-\right|(\alpha\,|1\rangle + \beta\,|0\rangle)(\alpha^*\,\langle 1| + \beta^*\,\langle 0|) + \left|\Phi^+\right\rangle\left\langle\Phi^+\right|(\alpha\,|1\rangle - \beta\,|0\rangle)(\alpha^*\,\langle 1| - \beta^*\,\langle 0|)\right)\frac{1}{4} . \end{aligned}$$

At this stage the reduced density operator of Bob's particle is given by

$$\rho_3 = \frac{1}{2}\left(|0\rangle\,\langle 0| + |1\rangle\,\langle 1|\right) .$$

This is the maximally mixed state and has no correlations with the initial state of particle 1. Once the measurement outcome has been communicated from Alice to Bob he applies the conditional unitary operation U. We analyze its effect by studying what happens to the different parts of ρ_{123} and find

$$\begin{aligned} \rho'_{123} &= \frac{1}{4}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right)(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\,\langle 0| + \beta^*\,\langle 1|) \\ &= \frac{\mathbb{I}}{4}(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\,\langle 0| + \beta^*\,\langle 1|) . \end{aligned}$$

Alice now possesses a maximally mixed state which is not correlated with Bob's particle. Bob is in possession of the state to be teleported. The teleportation of 1 qubit starts with an entangled

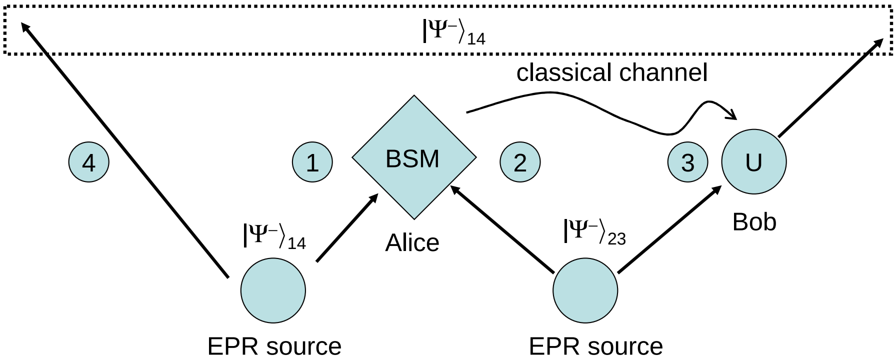


Figure 9: Schematic entanglement swapping setup.

state of negative conditional entropy $S(\rho_A|\rho_B) = -1$ which is independent of the qubit state to be sent. The transmission of 2 bits of classical information from Alice to Bob via a classical channel is required to complete the protocol. Classical communication and entanglement are both essential resources for teleportation but none of them is sufficient on its own to teleport $|\Psi\rangle_1$ from Alice to Bob.

5.2 Entanglement swapping

The state of qubit 1 is teleported with all its quantum properties using the setup described in the previous section. In particular any entanglement of qubit 1 with another system is preserved. We can see this by assuming α and β being state vectors instead of just c-numbers. This fact can be used to extend the teleportation setup to teleport entanglement. In this case the state of qubit 1 is not well defined (e.g. qubit 1 is in a Bell state with another qubit 4). The initial state of the system can thus be written as $|\Psi\rangle = (|\alpha\rangle_4 |0\rangle_1 + |\beta\rangle_4 |1\rangle_1) |\Psi^-\rangle_{23}$. The experimental setup for entanglement swapping is shown in Fig. 9. The analysis of this setup using the same method as in the teleportation protocol is left as an exercise. Also, the same entanglement and information resources as for teleportation are necessary.

6 Quantum cryptography

Cryptographic protocols can be classified by the type of security against eavesdropping. There exist mathematically secure schemes (like public key RSA encryption) whose security relies on assumptions[12] about the mathematical complexity of decrypting the cipher text without possessing the correct key. The majority of nowadays secure public internet connections relies on such schemes. Alternatively a cryptographic setup may provide a physically secure method for communicating. In such setups the security is provided by the physical laws[13] governing the communication protocol. Here we first discuss a provably secure classical communication protocol and then quantum methods for distributing the necessary keys. The experimental setups discussed in this section are shown in the appendix.

[12] These assumptions are sometimes unproven.

[13] Physical laws are not provably correct.

6.1 One time pads and the Vernam cipher

The Vernam cipher is a 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. Alice and Bob share identical n-bit secret key strings (the one time pad). Alice encodes her message by adding message and key using a classical XOR gate on each pair of bits. Bob decodes by subtracting the key again, i.e. by applying another XOR operation with his key bit. As long as the key is of the same length as the message and can be securely distributed to Alice and Bob the Vernam cipher is provably secure and Eve's mutual information with the sent message can be made arbitrarily small. This means that one needs a secure method for distributing a large number of key bits. Key bits must be delivered in advance of the message. Otherwise one could deliver the message itself by secure means. Furthermore the key bits must be guarded until they are used and the key must be destroyed after the bits were used. These difficulties in key distribution make the Vernam cipher impractical for general use. However, it is used e.g. in military applications.

We note as an aside that the problem of key distribution is circumvented in public key cryptography. The public key can easily be used to encrypt a message (like a box can be locked using a padlock without possessing the key). To decrypt the message a private key (corresponding to the key for the padlock) needs to be used. In public key cryptography Alice sends out public keys to everyone and whoever wants to securely communicate with Alice may use her key. The security of this protocol relies on the assumption that decrypting the message without possessing the private key is difficult.

6.2 The BB84 protocol

The BB84 protocol (see also the short option Quantum ideas for a qualitative description) is a physically secure way to distribute a secret key. It also allows to detect the presence of an eavesdropper Eve. Alice begins with two strings A and B each consisting of $(4+\delta)n$ bits. 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

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

The bits in A are encoded in the basis X or Z as determined by B. These four states are not mutually orthogonal and cannot be distinguished with certainty. Bob receives $\mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ describes the action of the channel and an eventual eavesdropper. He publicly announces the fact that he has received the state. At this point Alice, Bob and a possibly present Eve have their own states each with separate density matrices. Note that Alice has not revealed B thus Eve has no knowledge on which basis she should have used when trying to eavesdrop the communication by measuring qubits. At best she can guess and if her guess is wrong she will disturb the states received by Bob. Note that noise in the channel also contributes to $\mathcal{E}$. Bob now measures each qubit in basis X or Z depending on a random $(4+\delta)n$ bit string B'

which he creates on his own. We call Bob's measurement results A'. After this Alice announces B over a public channel and Bob and Alice discard all bits in $\{A, A'\}$ except for those where the bits in B and B' are equal. We assume that δ is sufficiently big so that they can keep $2n$ bits. It is important that Alice does not publish B before Bob has received the message to ensure security of the scheme! To check for noise and eavesdropping Alice now selects n bits and publicly announces the selection. Alice and Bob publicly compare these n bits and if more than t bits disagree they abort and retry the protocol. t is selected so that they can apply information reconciliation and privacy amplification (see Sec. 6.5.3) to obtain $m < n$ acceptably secret shared key bits. This protocol can be generalized to other states and bases. For instance the B92 protocol only uses two non-orthogonal states $|0\rangle$ and $|+\rangle$ for the communication.

For the BB84 protocol qubits need to be sent via a quantum channel and also classical bits are transmitted from Alice to Bob. However, it does not require any entanglement. The protocol relies on the fact that non-orthogonal quantum states cannot be perfectly distinguished by an eavesdropper whose actions will necessarily affect some of the states received by Bob. This reduces the mutual information between Alice and Bob for those cases where they have measured in the same basis. By detecting this reduction in mutual information they can identify Eve as we will now investigate for a simple eavesdropping strategy.

6.2.1 Intercept - resend strategy

The security of the BB84 protocol relies on the impossibility for any eavesdropper to distinguish between Alice's states without disrupting the correlations between the bits in A and A'. We investigate one particular eavesdropping strategy where Eve intercepts the sent qubits, measures them and the resends them. This is called the intercept/resend strategy and we will see how Alice and Bob can detect Eve in this case and abort their communication.

Let us assume that Eve intercepts each qubit. She chooses the X or Z basis at random to measure the qubit. Then she prepares a qubit in the state she had measured and sends it to Bob. With 50% probability Eve will choose the wrong basis. Each time Eve's basis is wrong she will get a result which is completely uncorrelated with the bit that Alice has sent. If the channel is otherwise perfect this leads to the following outcomes and probabilities provided that Alice sent message 0 in basis X

Alice	Eve	probability	Bob	probability
$0X$	$0X$	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

The cases where Alice sends 1X, 0Z, or 1Z can be worked out in the same way. 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. For a perfect noiseless channel the mutual information between Alice's and Bob's messages obtained when measuring in the same basis has thus been reduced from $H(X : Y) = 1$ to $H(X : Y) = 0.456$ by Eve. 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

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

By sacrificing n bits from their key Alice and Bob detect Eve with probability P_d.

6.3 Quantum key distribution using EPR pairs

A quantum channel emits pairs of photons in the singlet state of polarizations

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|V\rangle_1|H\rangle_2 - |H\rangle_1|V\rangle_2\right] .$$

The two photons fly along the z-axis to Alice and Bob, respectively. They perform measurements and register the outcome in one of three bases, obtained by rotating around the z-axis by angles $\phi_1^a = 0$, $\phi_2^a = \pi/4$, $\phi_3^a = \pi/8$ for Alice and by $\phi_1^b = 0$, $\phi_2^b = -\pi/8$, $\phi_3^b = \pi/8$ for Bob. These angles are chosen independently and randomly for each pair. The outcomes can be ±1 depending on which polarization is measured. The correlation coefficient of the measurements is given by

$$E(\phi_i^a, \phi_j^b) = P_{++}(\phi_i^a, \phi_j^b) + P_{--}(\phi_i^a, \phi_j^b) - P_{+-}(\phi_i^a, \phi_j^b) - P_{-+}(\phi_i^a, \phi_j^b) ,$$

and quantum mechanics predicts $E(\phi_i^a, \phi_j^b) = -\cos[2(\phi_i^a - \phi_j^b)]$, where the P's are the probabilities that ±1 is obtained in the respective bases. For the two pairs of bases 1 and 3 quantum mechanics predicts perfect anti-correlations $E(\phi_1^a, \phi_1^b) = E(\phi_3^a, \phi_3^b) = -1$. Alice and Bob now define S as

$$S = E(\phi_1^a, \phi_3^b) + E(\phi_1^a, \phi_2^b) + E(\phi_2^a, \phi_3^b) - E(\phi_2^a, \phi_2^b) ,$$

which should be (see CHSH inequality) $S = -2\sqrt{2}$. They discard measurements in which either or both failed to register a qubit. Alice and Bob can now publicly announce the orientations of the analyzers. Then they announce all results for which their orientations were different. This allows them to establish the result for S which will only be $S = -2\sqrt{2}$ if the particles were not disturbed. This ensures that the remaining measurements are perfectly anti-correlated and use them to establish a secret key. Eve cannot elicit any information from the particles while in transit from the source to the legitimate user since no information is encoded there. The information 'comes into being' after the legitimate users perform the measurements and communicate in public afterwards. In each case an eavesdropper will introduce elements of physical reality to the particles and will lower S below its quantum limit. Thus the Bell theorem can expose an eavesdropper.

In this scheme classical communication is only necessary to expose and eavesdropper but not for establishing the secret key. If no eavesdropper could be present all measurements could be carried out in the same basis. Before the measurement an entangled state with negative conditional entropy $S(\rho_A|\rho_B) = -1$ is created. The classical information gained from the measurements is perfectly correlated with $H(X:Y) = 1$. However, neither Alice nor Bob have the ability to engineer their measurement outcome and choose which message to send. Quantum mechanics does not tell us how to influence a measurement outcome and we do not have a more advanced theory to do this. Thus, while correlated classical information comes into being during the measurement process, it cannot be used to transmit messages between Alice and Bob. However, the random bits generated in this scheme are very useful as a secret key.

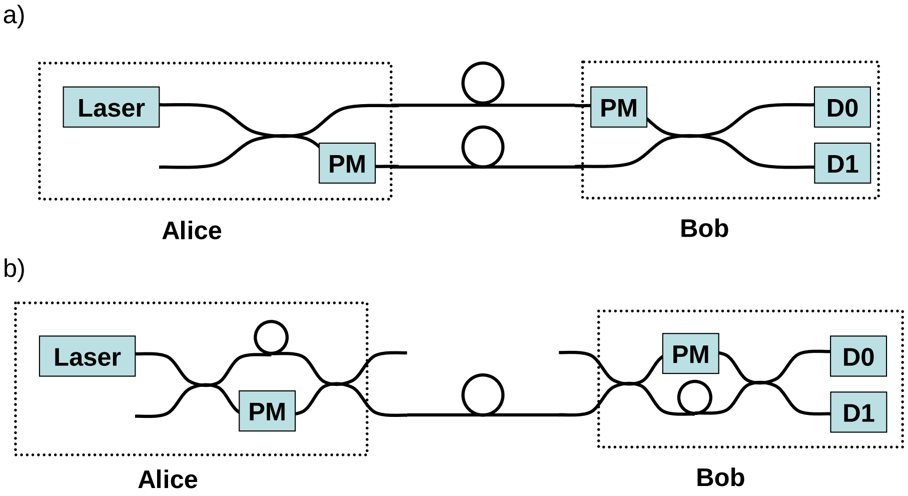


Figure 10: BB84 using phase encoding in optical fibres setups. a) Extended Mach-Zehnder setup. b) Collapsed Mach-Zehnder setup. The circles denote delay loops of Δ.

6.4 Experimental setups

We can distinguish between free space cryptography where polarization encoded qubits are used and fibre systems. Free space experiments require robust optical setups at the sender and receiver side. Recent developments include the realization of small and highly efficient devices which achieved distances of up to 23.4km. The predicted maximum distance is $\approx$ 1000km so that connections to satellites are in principle possible. Here we consider in more detail two fibre setups to realize the BB84 protocol.

6.4.1 Phase encoded fibre systems

Optical fibres do not conserve the polarization because of randomly fluctuating birefringence (1 hour timescale). Polarization tracking is possible but would make a polarization scheme cumbersome. Instead we consider an extended Mach-Zehnder setup used for phase encoding and shown in Fig. 10a). 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 but replaces the polarization with a relative phase in the wave function. The drawback is that keeping the phase constant over large distances is very difficult due to temperature variations and other imperfections induced by the environment.

Example:

E14. We analyze the setup shown in Fig. 10a). Alice produces the state $|0\rangle$, which is turned into $|+\rangle$ by the BS and the PM induces a relative phase ϕ_A so that the state which leaves the sender is $(|0\rangle + \mathrm{e}^{i\phi_A}|1\rangle)/\sqrt{2}$. In the ideal case the delay Δ accumulated between Alice and Bob acts equally on both arms and gives $|0\rangle \to |0, \Delta\rangle$, and $|1\rangle \to |1, \Delta\rangle$. Since both arms are equally affected we leave Δ out in the following. Bob's PM introduces another relative phase ϕ_B so that the state turns into $(\mathrm{e}^{i\phi_B}|0\rangle + \mathrm{e}^{i\phi_A}|1\rangle)/\sqrt{2}$. The BS turns this state into $[(\mathrm{e}^{i\phi_B} + \mathrm{e}^{i\phi_A})|0\rangle + (\mathrm{e}^{i\phi_B} - \mathrm{e}^{i\phi_A})|1\rangle]/2$. If Alice chooses $\phi_A = 0$ ($\phi_A = \pi$) and

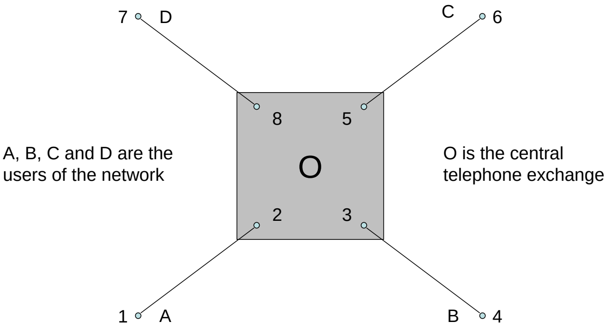

7
D
C
6
8
5
A, B, C and D are the users of the network
O
O is the central telephone exchange
2
3
1
A
B
4

Figure 11: A quantum telephone exchange.

Bob chooses $\phi_B = 0$ he will get a click in D_0 (D_1) with certainty. If he chooses $\phi_B = \pi/2$ a click in each detector is equally likely. If Alice chooses phases $\phi_A = \pi/2$ ($\phi_A = 3\pi/2$) and Bob selects $\phi_B = \pi/2$ D_0 (D_1) will click with certainty. Otherwise he will get equal probability for a click in one of the detectors. Thus Alice encodes 0 and 1 in the two bases by choosing phases 0 and π or $\pi/2$ and $3\pi/2$ to use this setup for realizing the BB84 protocol.

A more practical scheme is realized by collapsing the interferometer as shown in Fig. 10b). Two pulses are propagating down the single fibre. They are denoted by S (short path, no delay at the sender side) and L (long path, delay Δ at the sender side). The delay Δ is assumed to be much longer than the duration of the photon wave packet. After traveling through Bob's part of the Mach-Zehnder they create three different outputs: SS (which only experiences the delay between sender and receiver station) and LL (going through the delay lines at sender and receiver side in addition to the delay of the connecting fibre) are not relevant as they show no interference effects. SL and LS (going through exactly one of the delay lines at sender and receiver in addition to the delay of the fibre) are indistinguishable and thus interfere. Experimentally they can be selected by time gating. The choice of phase shifts by Alice and Bob gives the encoding-decoding in the SL and LS components exactly as in the previous scheme. This setup is much more stable since the pulses follow the same path for most of the setup. Any phase fluctuations which happen on time scales much longer than the delay Δ will only affect the global phase of the wave function which is irrelevant. The major drawback of the scheme is that half of the signal is lost in the SS and LL path. The analysis of this scheme is similar to the analysis presented for the above setup and left as an exercise. Note that the delay loops Δ at sender and receiver are present in one arm only. Their action can thus not be ignored in the analysis.

6.5 More about communication schemes

The setups discussed in this section are included for completeness and will only be discussed in the lectures if there is sufficient time left.

6.5.1 The quantum telephone exchange

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 as shown in Fig. 11. Projecting the particles at the exchange O into an entangled multi-particle

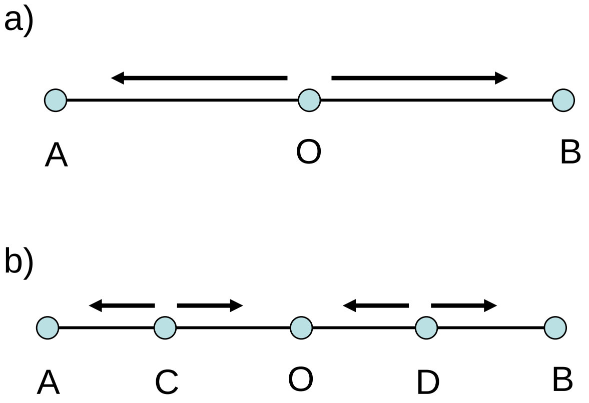


Figure 12: Speeding up entanglement distribution. a) Entanglement distribution without entanglement swapping. b) Entanglement distribution using an entanglement swapping station.

state by doing a measurement will immediately project their partner particles at the users site into the same type of entangled state.

Example:

E15. Imagine that all the Bell states are of the type $|\Phi^+\rangle$. A, B and C would like to share a $|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ for further quantum communication. If the exchange O projects the particles 2, 3 and 5 into the GHZ state then we find

$$_{235}\langle\mathrm{GHZ}|\left(\left|\Phi^+\right\rangle_{12}\left|\Phi^+\right\rangle_{34}\left|\Phi^+\right\rangle_{56}\right) = (|000\rangle_{146} + |111\rangle_{146})/\sqrt{2}\,.$$

In this process the quantum telephone exchange provides the communicating parties with an entangled state and becomes disentangled from all of them. The advantages of this scheme are that pure Bell states between the users and O can be created by state purification protocols i.e. using a large number of not maximally entangled state to distil fewer better entangled states. The preparation of the shared Bell pairs between users and O is independent of the states to be shared later between the users. The telephone exchange becomes disentangled from the users and cannot eavesdrop in later communication. The drawback is that the operations to be carried out by the telephone exchange are difficult to realize.

6.5.2 Speeding up distribution of entanglement

Entanglement swapping can save a significant amount of time in providing distant parties A and B with entangled pairs of particles. For this several Bell state producing and Bell state measuring substations are put into the route between them as shown in Fig. 12b). In Fig. 12a) it takes a time $t_a = L/2v$ with $v < c$ the speed of the entangled particles and L the distance between A and B. Case Fig. 12b) uses entanglement swapping at O which is an entanglement measuring station. At $t = 0$ C and D send off Bell pairs. The particles arrive at time $t = L/4v$. The Bell measurement at O takes a time t_m. Thus it takes a time $t_b = L/4v + t_m$ to distribute the Bell pair. Note that one has to add the time needed to classically communicate the measurement result at O to A and B and therefore there is no advantage when the distributed qubits are photons.

6.5.3 Privacy amplification

Privacy amplification is a purely classical technique to reduce the amount of mutual information an eavesdropper can gain when distributing an encryption key. It also reduces the number of message which Alice and Bob can send. The amplification process starts once Alice and Bob share with high probability an identical reconciled key of length n and know the error rate ϵ of the transmission. They assume that all the errors are due to an eavesdropper Eve. Then they deduce t, the number of bits by which the key has to be shortened for privacy. Alice picks a random $(n-t) \times n$ binary matrix K and publicly transmits K to Bob. Using K Alice and Bob obtain the final private key as

$$\mathbf{k}_{\text{final}} = K \cdot \mathbf{k}_{\text{reconciled}}$$

.

While implementing privacy amplification is simple, finding t and proving security is very difficult. In general one distinguishes between different types of eavesdropping attacks:

- Incoherent attacks: Eve entangles quantum probes with one photon at a time. She then stores (quantum memory) and measures her probes after Alice and Bob have made their public announcements.
- Collective attacks: Eve only entangles her probes with one photon but has a quantum computer to further process her states after the public communication.
- Coherent attacks: Eve can entangle her probe with any dimension of the whole state in the transmission. She has a quantum computer to process the resulting states at any time she wishes to do so.

Answers have been provided for more and more powerful attacks but there are still open questions about the security of quantum communication.

7 Further reading

A comprehensive introduction to quantum computing can be found in [14]. For further details on quantum communication schemes and Bell inequalities discussed in this manuscript see [15].

[14] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)

[15] D. Bouwmeester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information*, Springer (Berlin) (2000); R.A. Bertlmann and A. Zeilinger, *Quantum [Un]speakables*, Springer (Berlin) (2002).

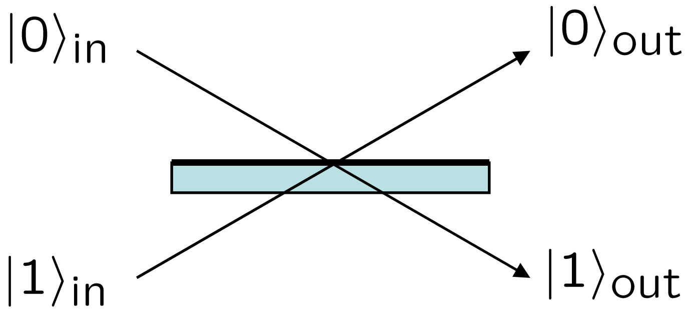
Appendix

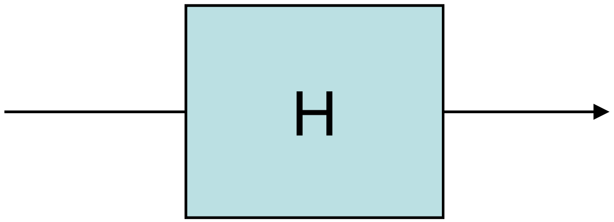
Schematics and Experimental setups

3. Photon techniques

3.1.1 Spatial encoding: Beam splitter

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





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

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

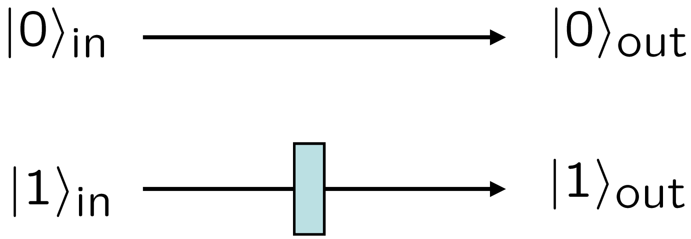
- Matrix representation of the dynamics of a general beam splitter

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

This time evolution is unitary. BS(45°,0)=H is a simple 50/50 beam splitter.

3.1.1 Spatial encoding: phase gate

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



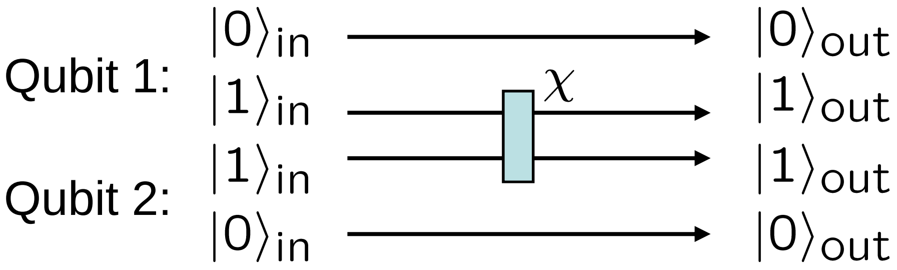
A medium of length *L* with refractive index *n* yields a phase shift ϕ

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

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

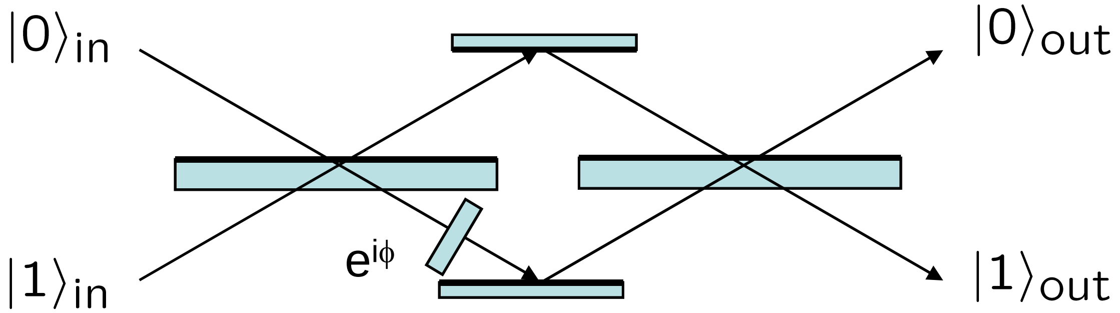
$$|0\rangle_{\text{out}} = |0\rangle_{\text{in}} \qquad |1\rangle_{\text{out}} = e^{i\phi}|1\rangle_{\text{in}}$$

- 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 $\varphi = \chi L$



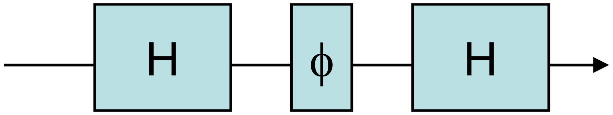
$$|00\rangle_{\text{out}} = |00\rangle_{\text{in}}$$
$$|01\rangle_{\text{out}} = \mathrm{e}^{\mathrm{i}\phi}|01\rangle_{\text{in}}$$
$$|10\rangle_{\text{out}} = \mathrm{e}^{\mathrm{i}\phi}|10\rangle_{\text{in}}$$
$$|11\rangle_{\text{out}} = \mathrm{e}^{\mathrm{i}(2\phi+\varphi)}|11\rangle_{\text{in}}$$

3.1.1 Mach-Zehnder interferometer



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

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

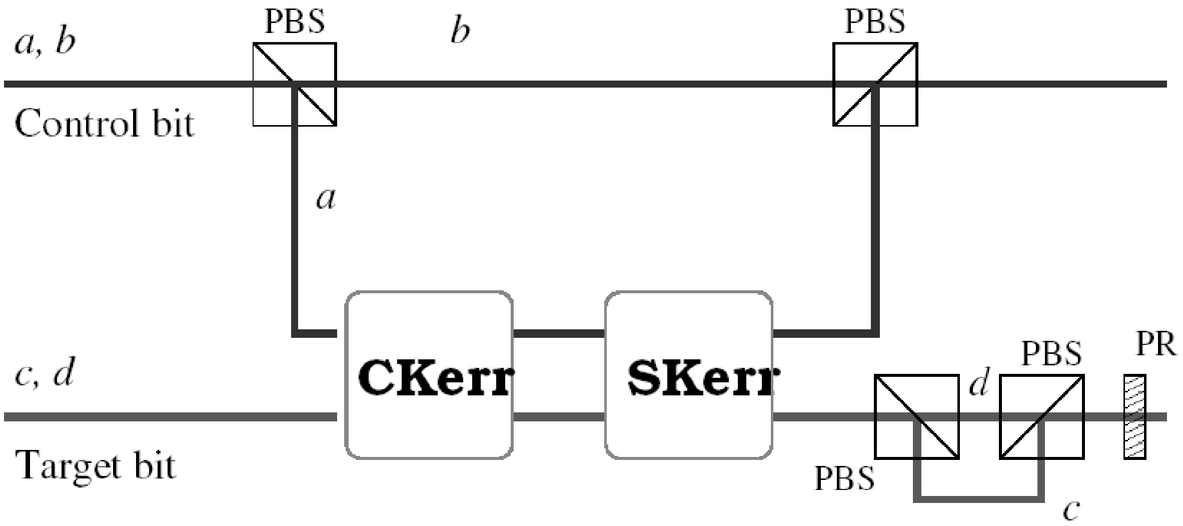


$$|\Psi\rangle_{\text{out}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

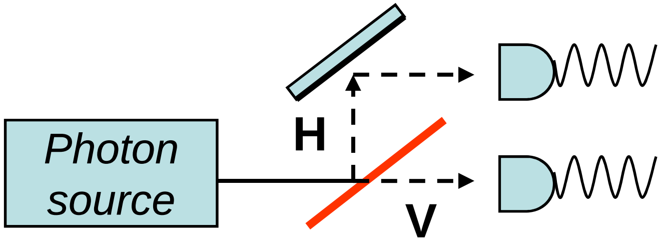
$$|\Psi\rangle_{\text{out}} = e^{i\phi/2} \begin{pmatrix} \cos(\phi/2)\alpha - i\sin(\phi/2)\beta \\ -i\sin(\phi/2)\alpha + \cos(\phi/2)\beta \end{pmatrix}$$

3.1.2 Polarization encoding

- Implement a two qubit gate e.g. a CNOT gate



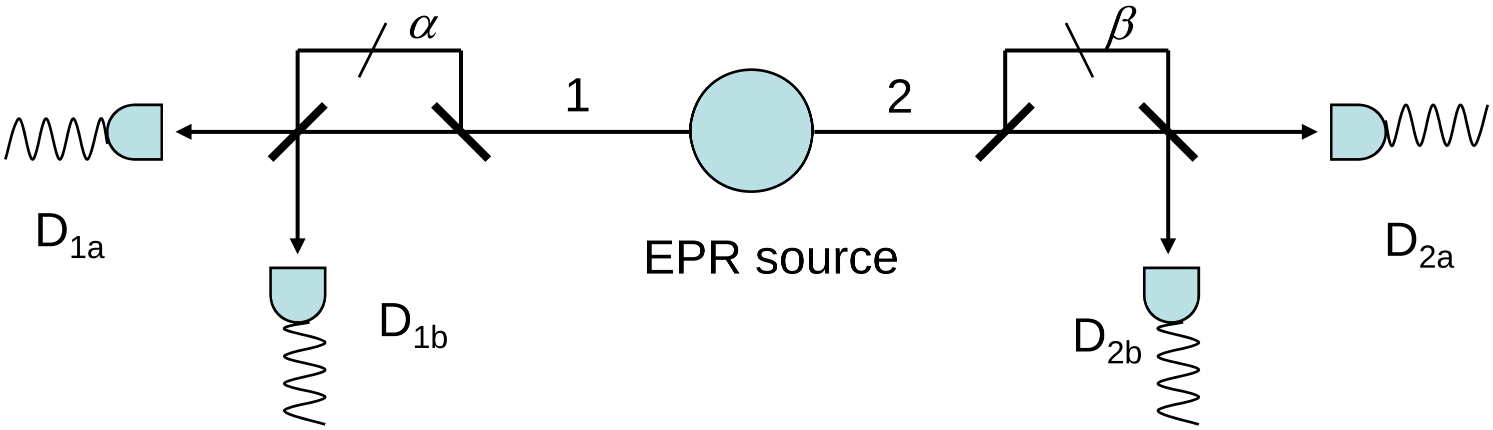
- Measure a qubit



Polarizing beam splitter

3.1.3 Parametric down conversion: Time entanglement

- The emission time is uncertain within the coherence time of the pump laser.
- The photons are simultaneous since they are broadband with coherence times of order 100fs.
- Two-photon Franson-interferometry



- Inside the interferometer

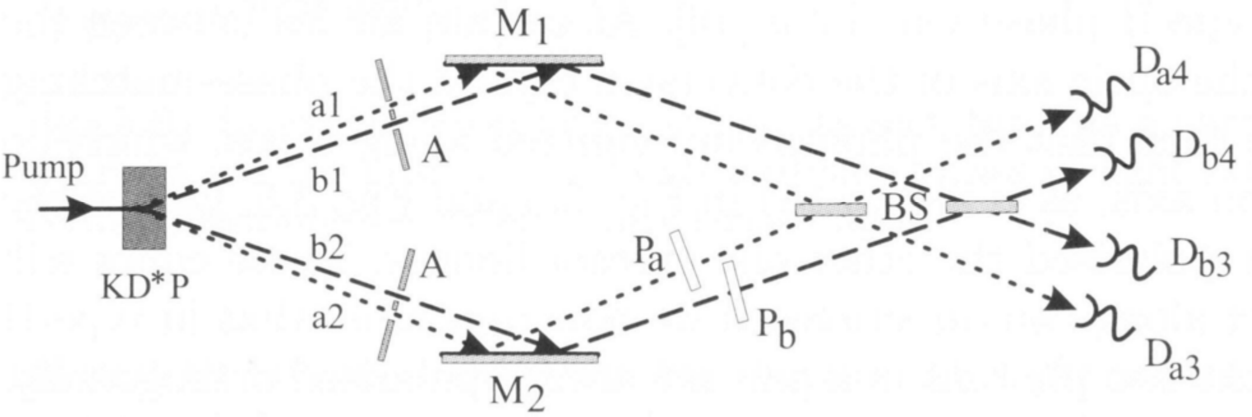
$$|\psi\rangle = \frac{1}{2}\Big[|S\rangle_1|S\rangle_2 + e^{i(\phi_1+\phi_2)}|L\rangle_1|L\rangle_2 + e^{i\phi_2}|S\rangle_1|L\rangle_2 + e^{i\phi_1}|L\rangle_1|S\rangle_2\Big]$$

3.1.3 Parametric down conversion: Momentum entanglement

- The pairs are emitted in either modes a1, b2 or in modes a2, b1.
- Before the beam splitters we thus have the entangled state

$$|\Psi\rangle \ = \ \frac{1}{\sqrt{2}}\left[e^{i\phi_b}|a\rangle_1|b\rangle_2 + e^{i\phi_a}|a\rangle_2|b\rangle_1\right]$$

- Behind the BSs the two paths cannot be distinguished → interference
- Coincident detections in a and b detectors vary cosinusoidally on changing the phase difference $\phi = \phi_a - \phi_b$

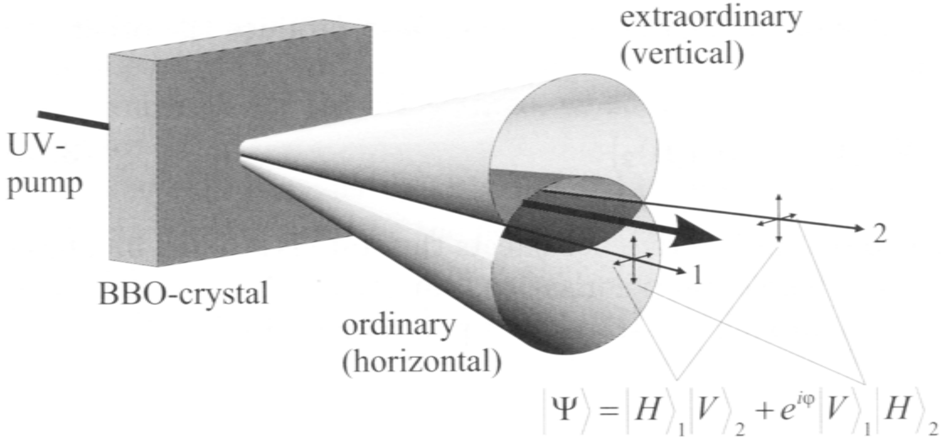


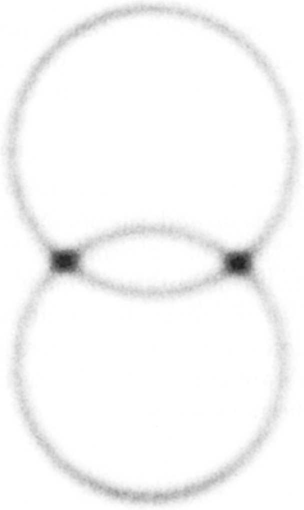
3.1.3 Parametric down conversion: Polarization entanglement

- Different light speed of ordinary and extraordinary beam → distinguishable photons → compensation by inserting crystals of half the thickness at 90◦

$$|\Psi\rangle \;=\; \frac{1}{\sqrt{2}}\left[|V\rangle_1|H\rangle_2 + e^{i\phi}|H\rangle_1|V\rangle_2\right]$$

- Phase ϕ can be controlled by compensator crystal, additional half wave plate for creating the other two Bell states


extraordinary
(vertical)
UV-
pump
BBO-crystal
ordinary
(horizontal)
2
1
$|\Psi\rangle = |H\rangle_1 |V\rangle_2 + e^{i\varphi} |V\rangle_1 |H\rangle_2$



3.1.4 Single photon source

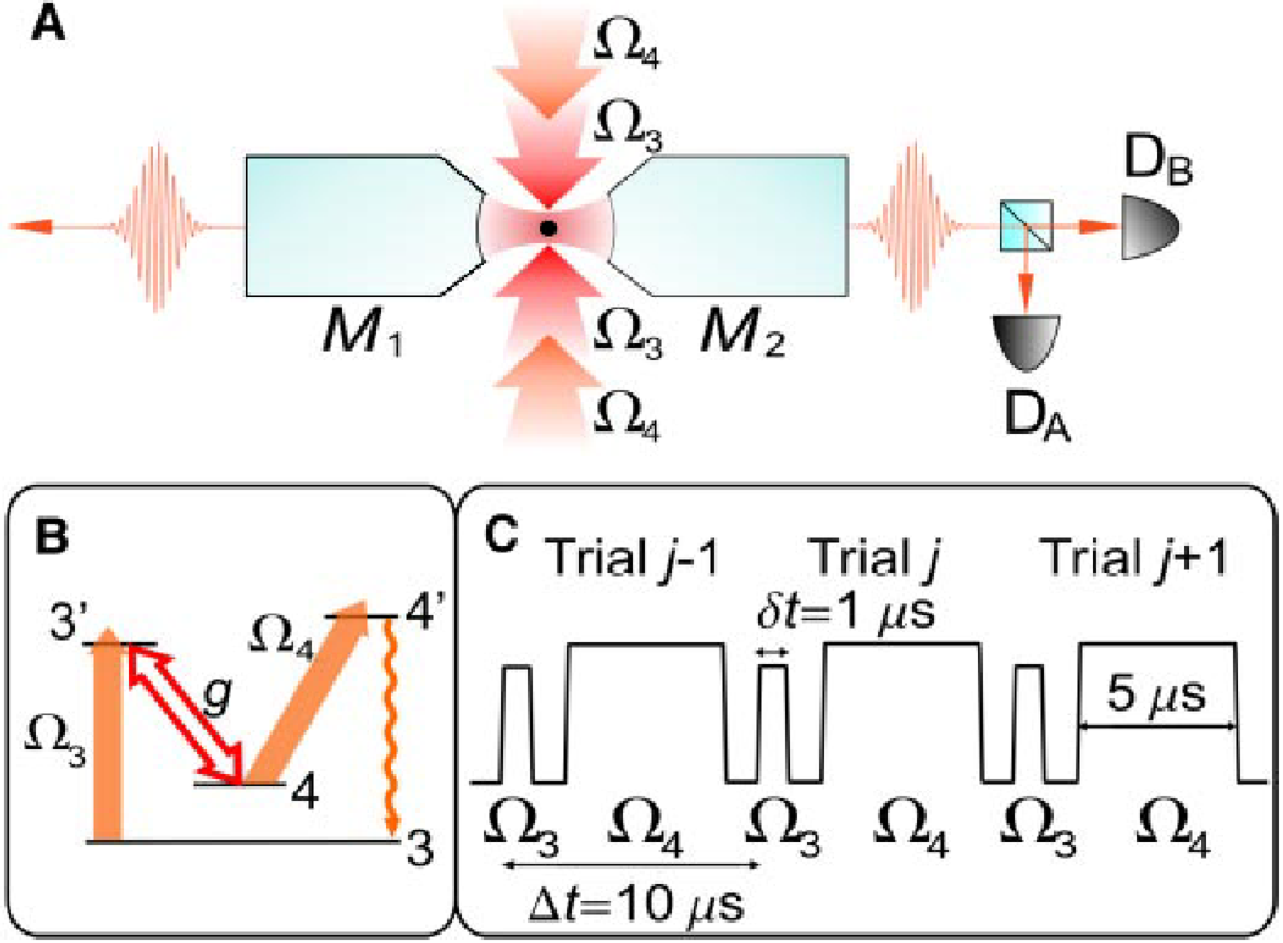
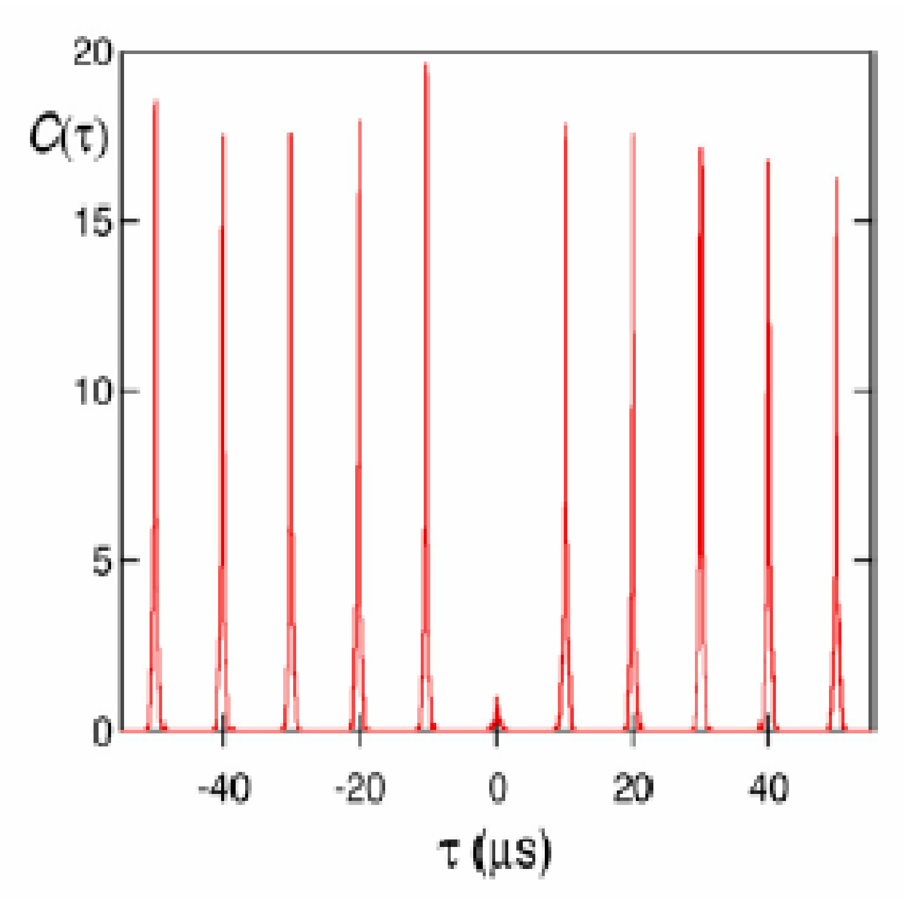


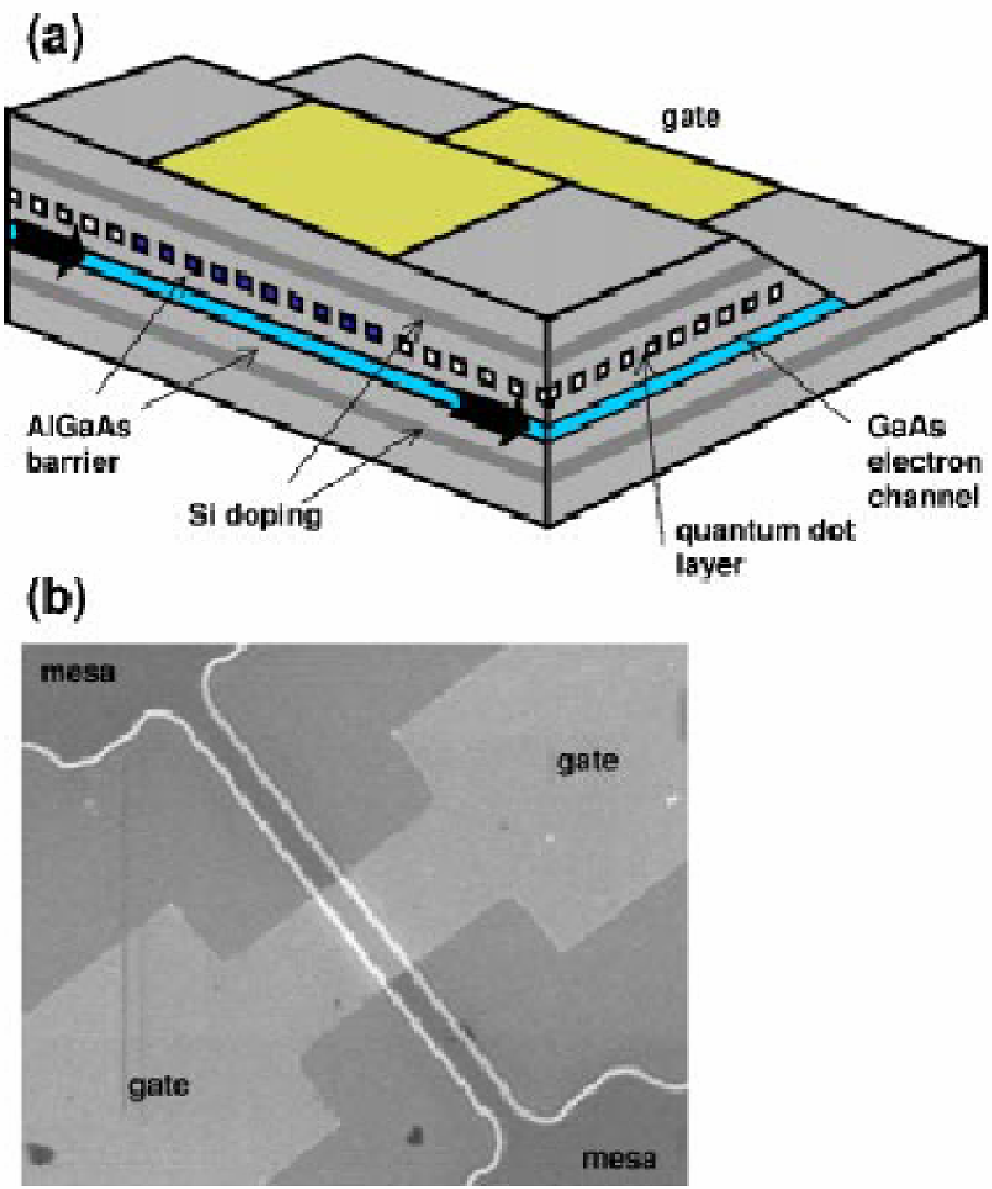
Fig. 1. Illustration of the generation of single photons by one atom trapped in an optical cavity. (**A**) A single Cs atom is trapped in a cavity formed by the reflective surfaces of mirrors (M_1, M_2) and is pumped by the external fields (Ω_3, Ω_4) (25). (**B**) The relevant atomic levels of the Cs D_2 line at 852.4 nm. Strong coupling at rate g is achieved for the transition $F' = 3' \rightarrow F = 4$ near a cavity resonance, where $g = 2\pi \times 16$ MHz. Atom and cavity decay rates $(\gamma,\kappa)/2\pi$ = (2.6 MHz, 4.2 MHz). (**C**) The timing sequence for the generation of successive single photons by way of the $\Omega_{3,4}$ fields.

3.1.4 Single photon source

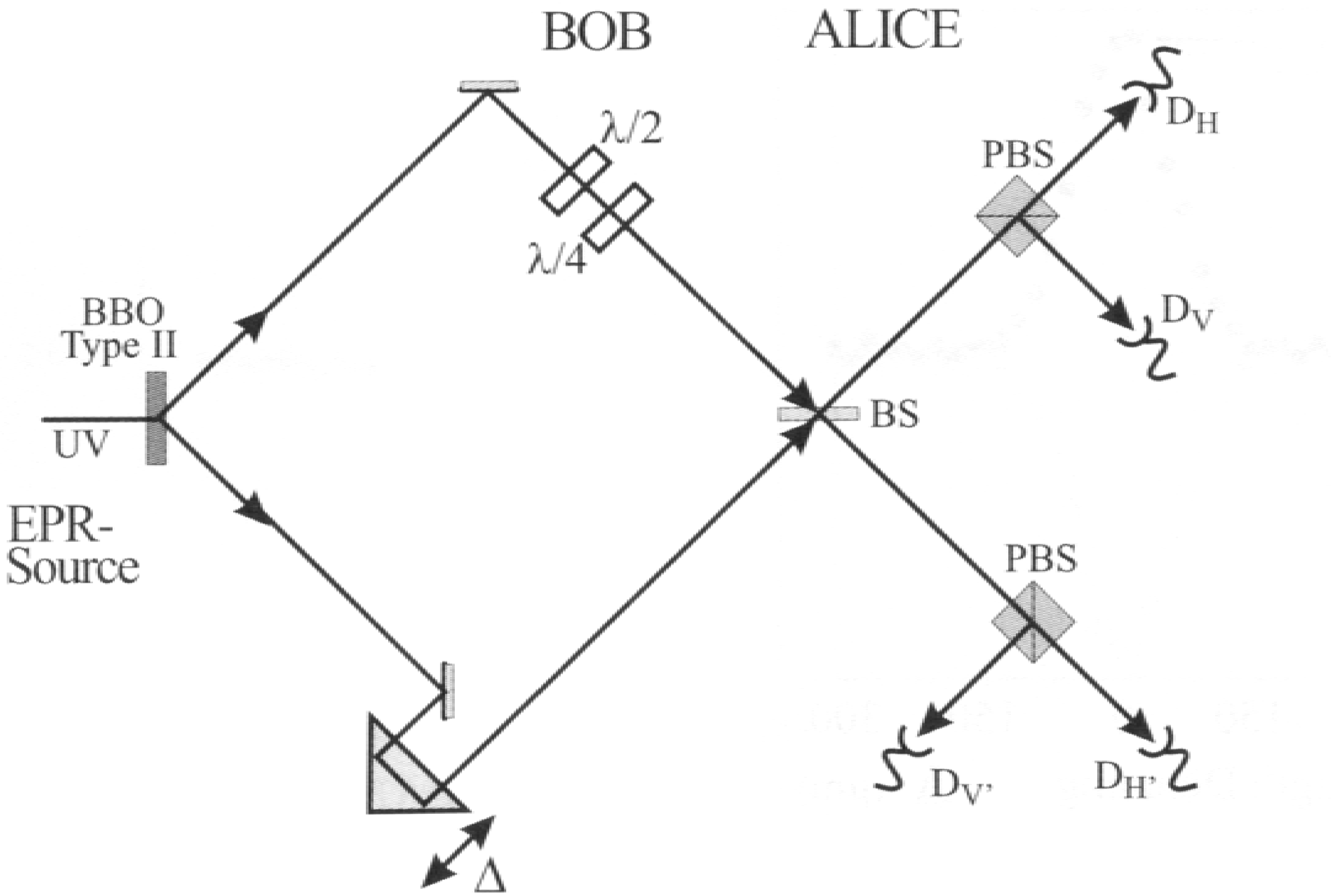


coincidence detection
at D_A and D_B

3.1.4 Single photon detectors



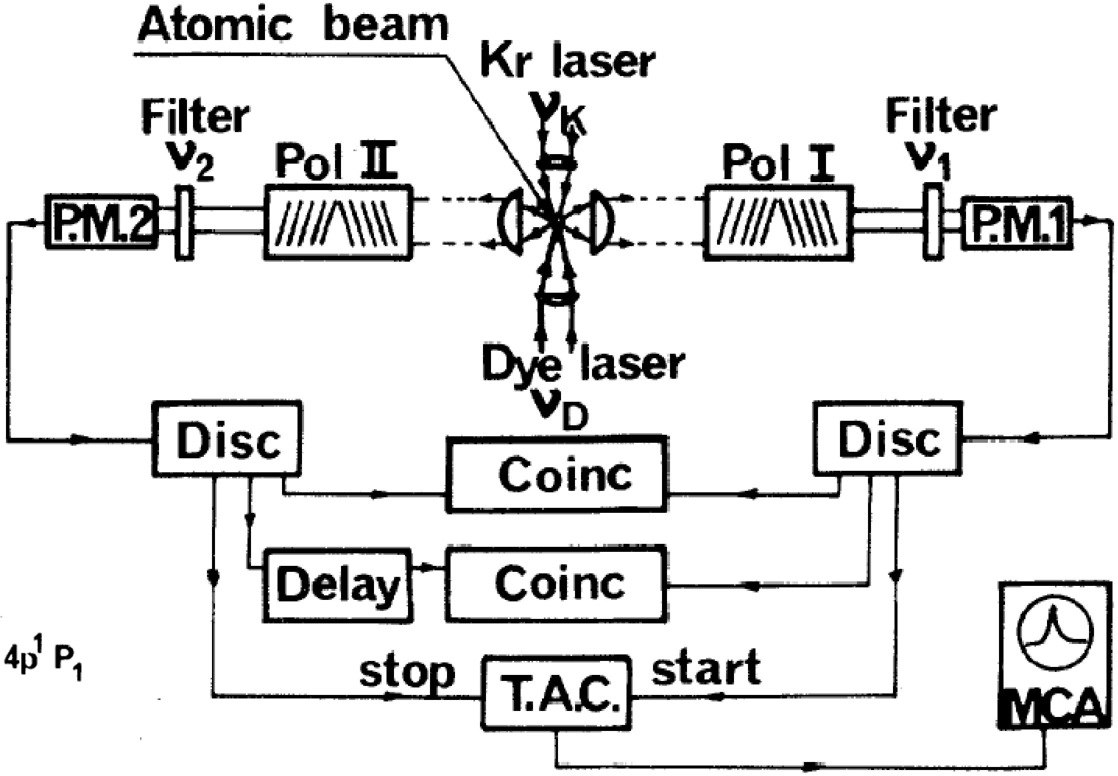
3.1.5 Quantum dense coding: Experimental setup



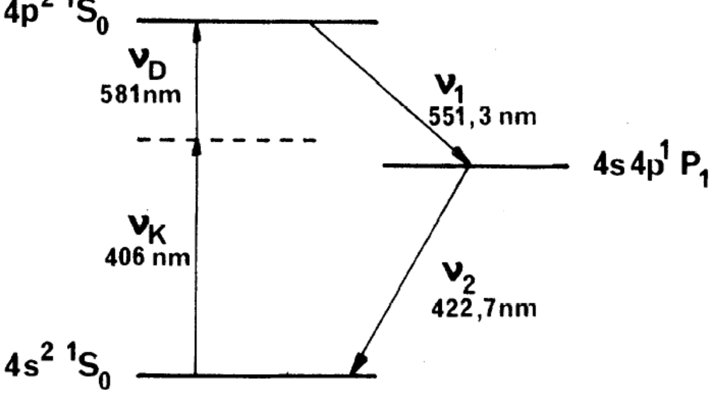
4. Testing EPR

4.1.2 The Aspect experiments: Setup

- Experimental setup



- Atomic cascade



4.2.2 GHZ: Source for three-photon GHZ states

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

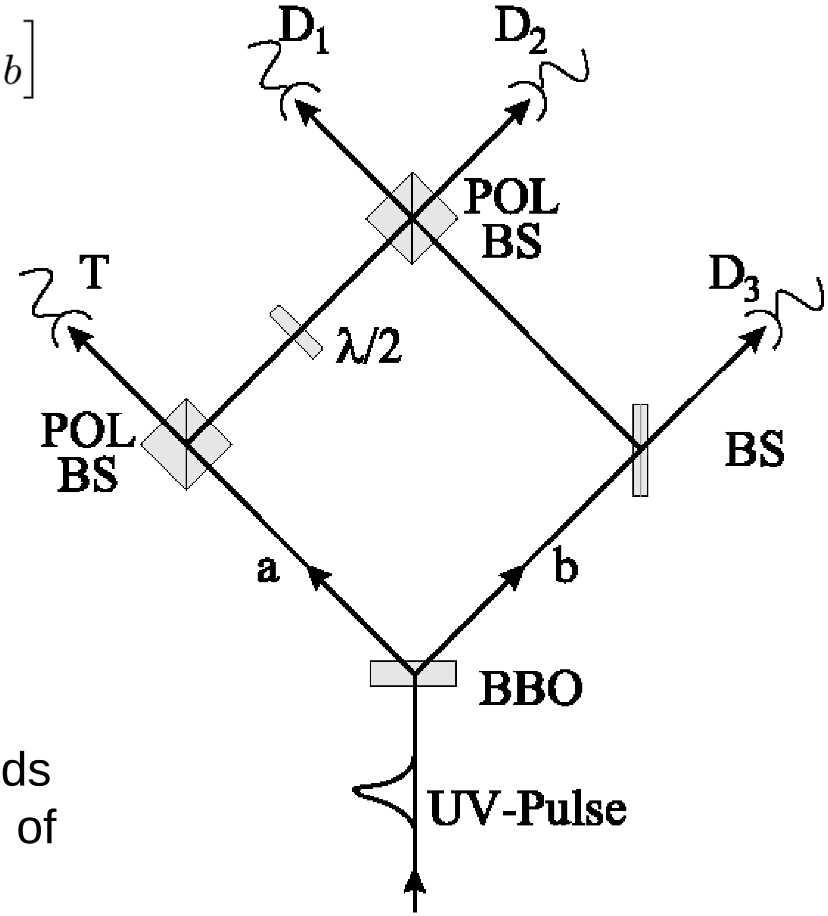
$$|\Psi\rangle \;=\; \frac{1}{\sqrt{2}}\left[|H\rangle_a|V\rangle_b + e^{i\phi}|V\rangle_a|H\rangle_b\right]$$

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

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

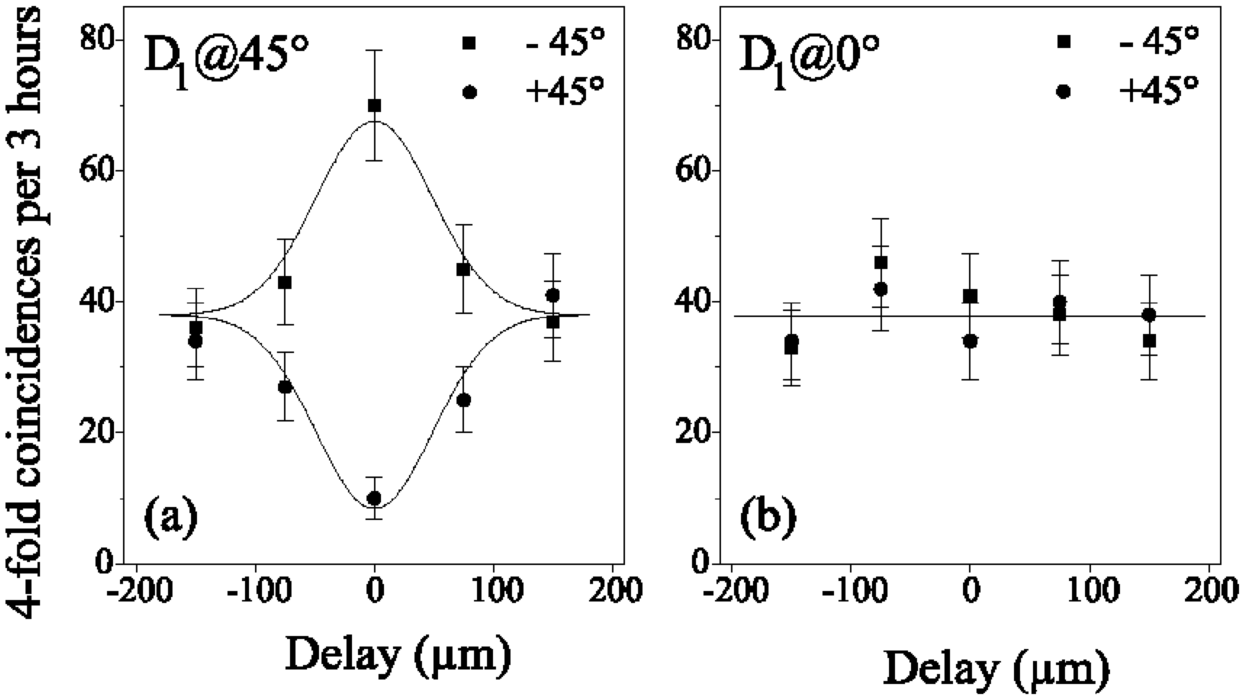
  at the detectors D1, D2, D3.

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



4.2.2 GHZ: Experimental proof of GHZ entanglement

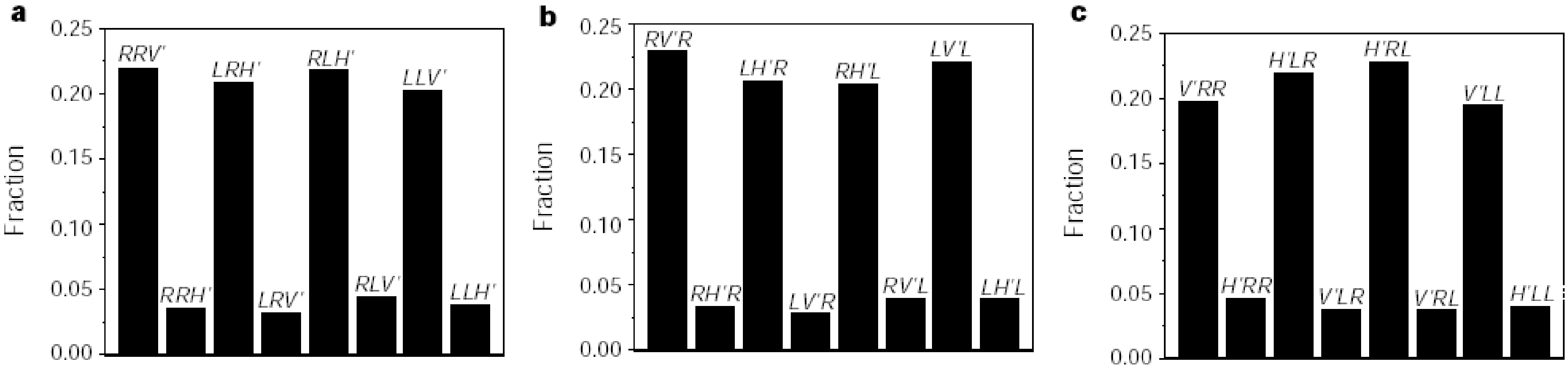
- As a first step |GHZ⟩ entanglement has to be confirmed experimentally. Four fold coincidences are detected for variable delays in path a



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°

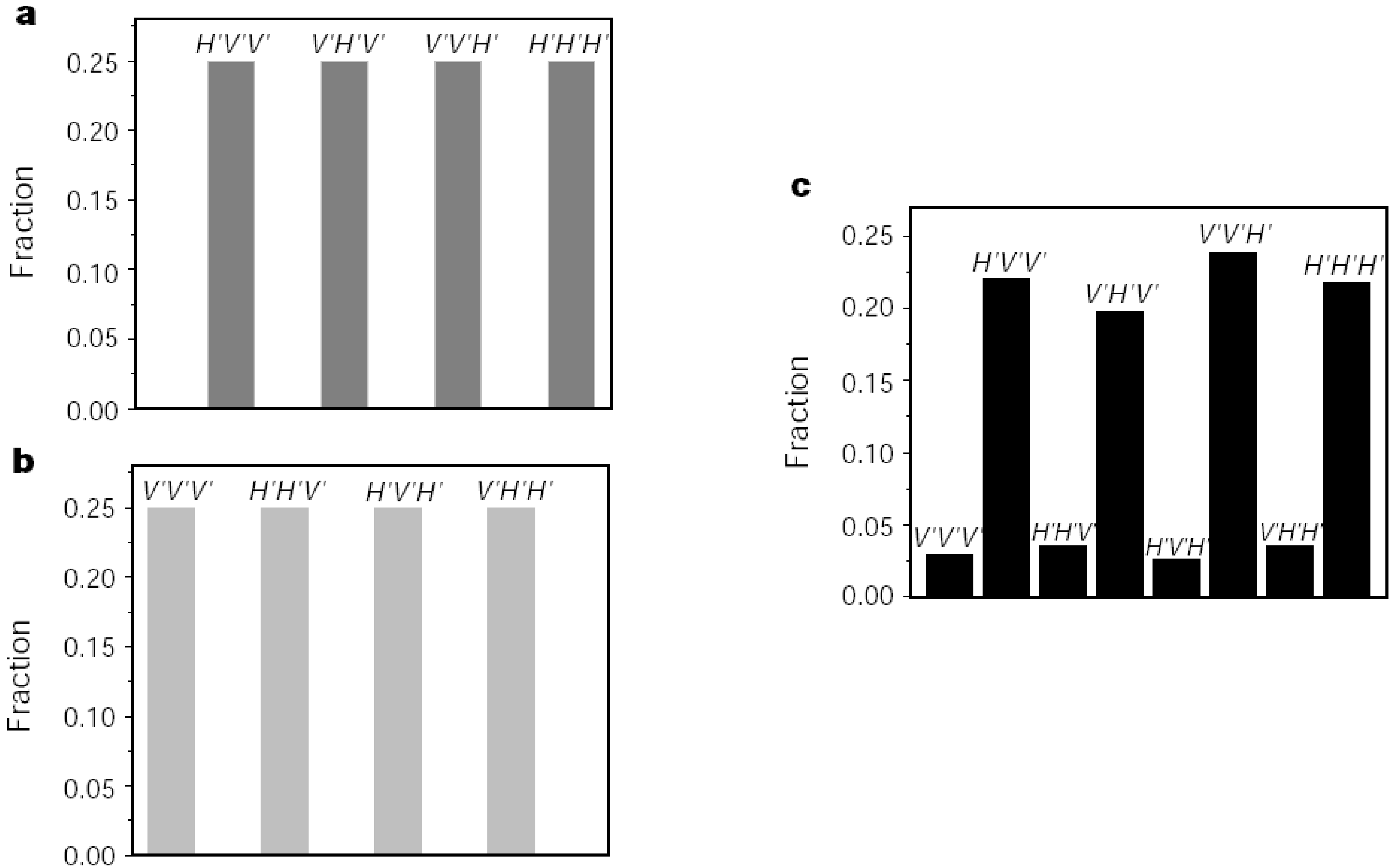
4.2.2 GHZ: Measurements in different bases

- Performing the measurements in the YYX (a), YXY (b), and XYY (c) basis confirms the entanglement properties of the |GHZ⟩ 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.



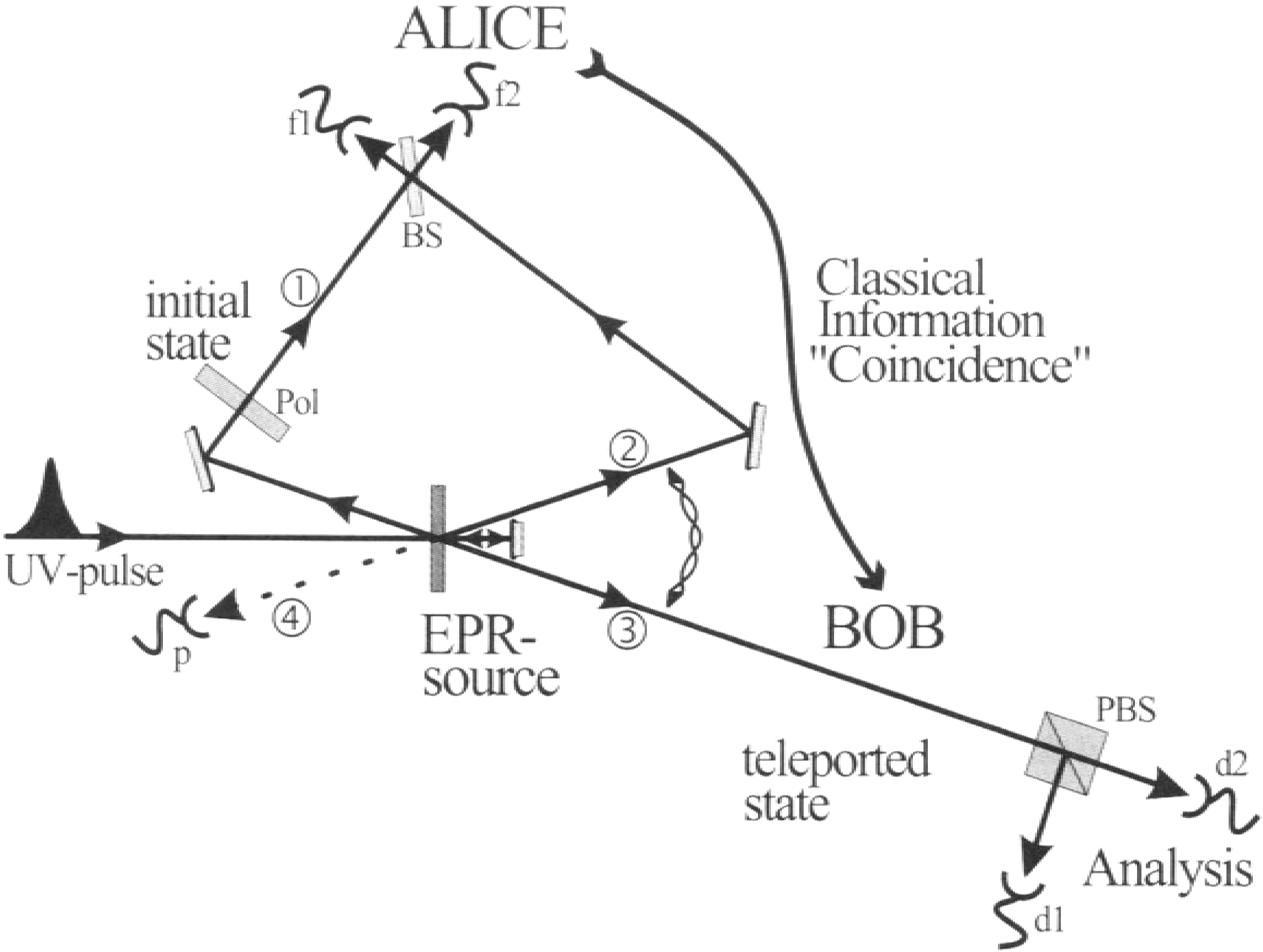
4.2.2 GHZ: Local realism vs. quantum mechanics

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



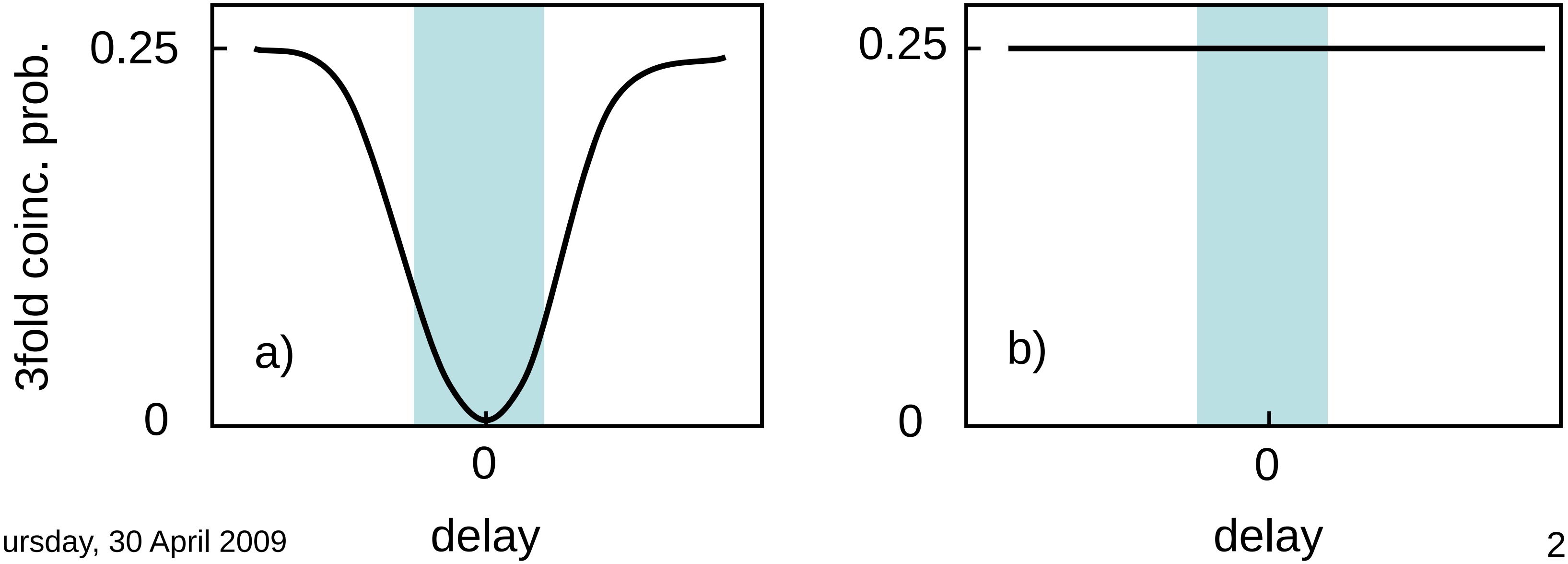
5. Quantum communication

5.1 Quantum teleportation: Setup



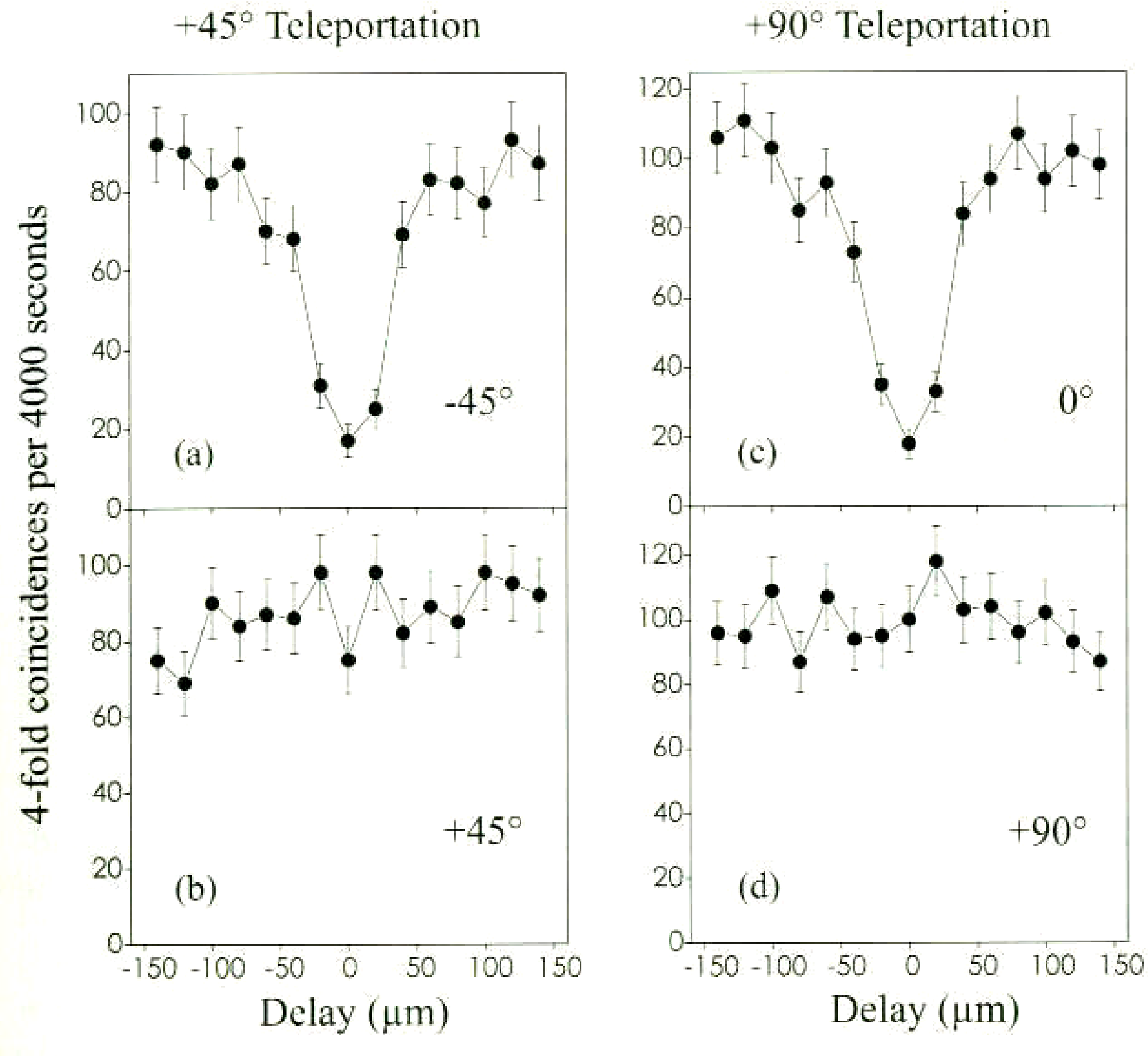
5.1 Quantum teleportation: Analysis

- A UV pulse creates the ancillary pair of photons 2 and 3. After retroflection it can create a second pair of photons 1 and 4 where 1 is prepared in the initial state to be teleported. Photon 4 serves as a trigger at detector p.
- Alice looks for coincidences after the BS where the photon to be teleported and photon 2 are superposed. She identifies only the state $|\Psi^{-}\rangle_{12}$ by finding coincidence counts at f_1 and f_2.
- Bob then knows that his photon 3 is in the initial state of photon 1.
- Bob checks this state using polarization analysis using the PBS (a) d1f1f2 coincidence for -45° and (b) d2f1f2 coincidence for 45° for a 45° photon 1.



5.1 Quantum teleportation: Experimental results

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



6. Quantum cryptography

6.4 Free space cryptography: Polarization encoding

- Polarization is conserved in free space.
- Strongly attenuated laser pulses are created by sending laser pulses through two pinholes with a diameter of 100µm separated by 9mm.
- Strong attenuation → only very few pulses result in detection events.
- A record of these detected has to be kept and communicated from Bob to Alice.
- Distance of 23.4km achieved between Karwendelspitze (2244m) and Zugspitze (2960m).
  - Reduced air turbulence effects due to elevated beam path, but high demands on temperature and weather condition stability of devices.
  - Possible range: Up to 1000km (connections to satellites possible!)
- High voltage Pockels cells for rotating the polarization replaced by four lasers creating different polarizations (indistinguishability of lasers?)
- Non-polarizing beam splitter for choosing the measurement at Bob’s.
- Galilean telescope to produce a near diffraction-limited 40mm beam.
- Bob collects the light in a 25cm aperture Schmidt-Cassegrainian telescope.
- A final net key rate of approx 500Bits/sec was achieved

6.4 Free space cryptograph: Alice – the sender

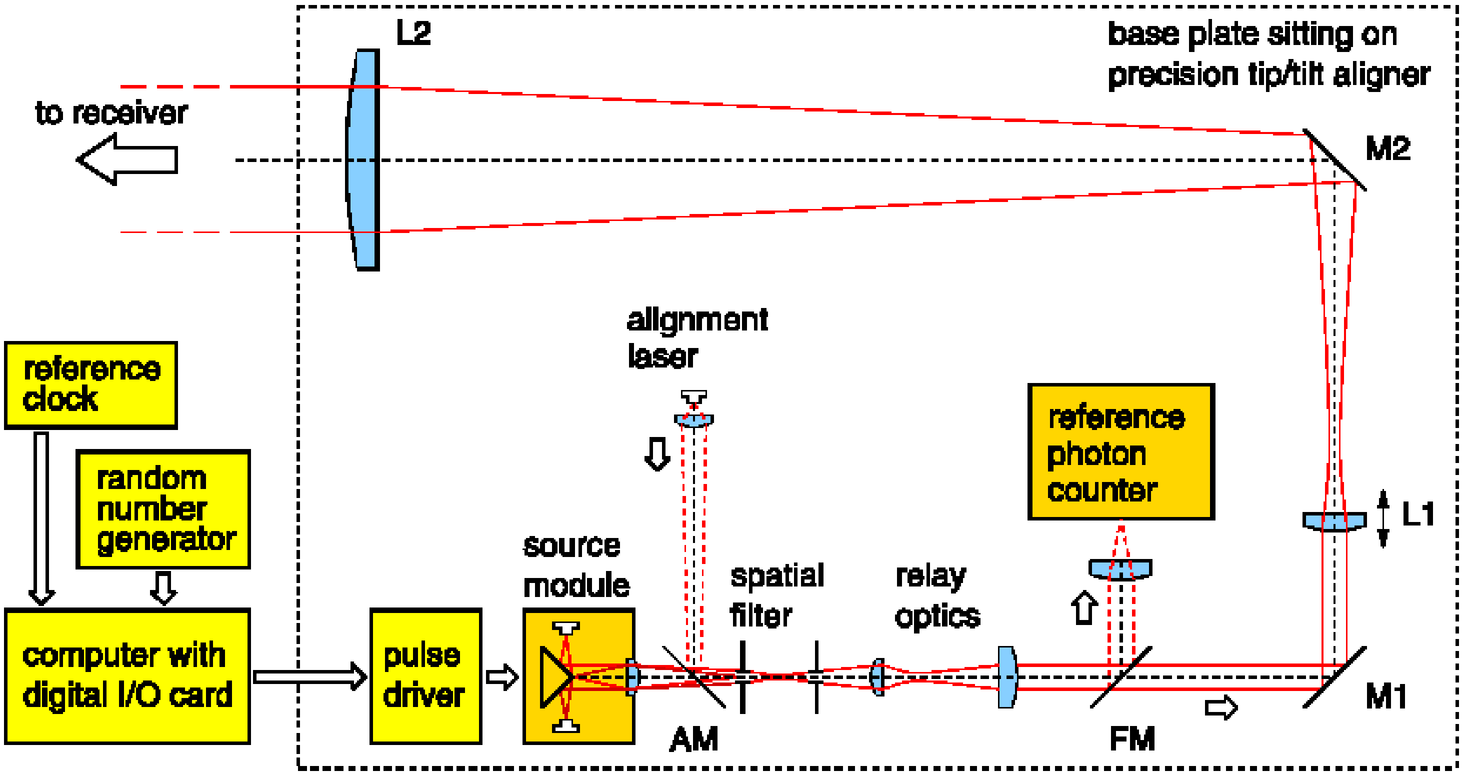


Figure 1: The Alice compact breadboard transmitter. The digital I/O card delivers a random 2-bit signal at 10 MHz synchronised to the reference clock. This signal is used in the pulse driver for randomly firing one of four lasers in the miniature source module. The four lasers are combined in a spatial 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.

6.4 Free space cryptograph: Bob – the receiver

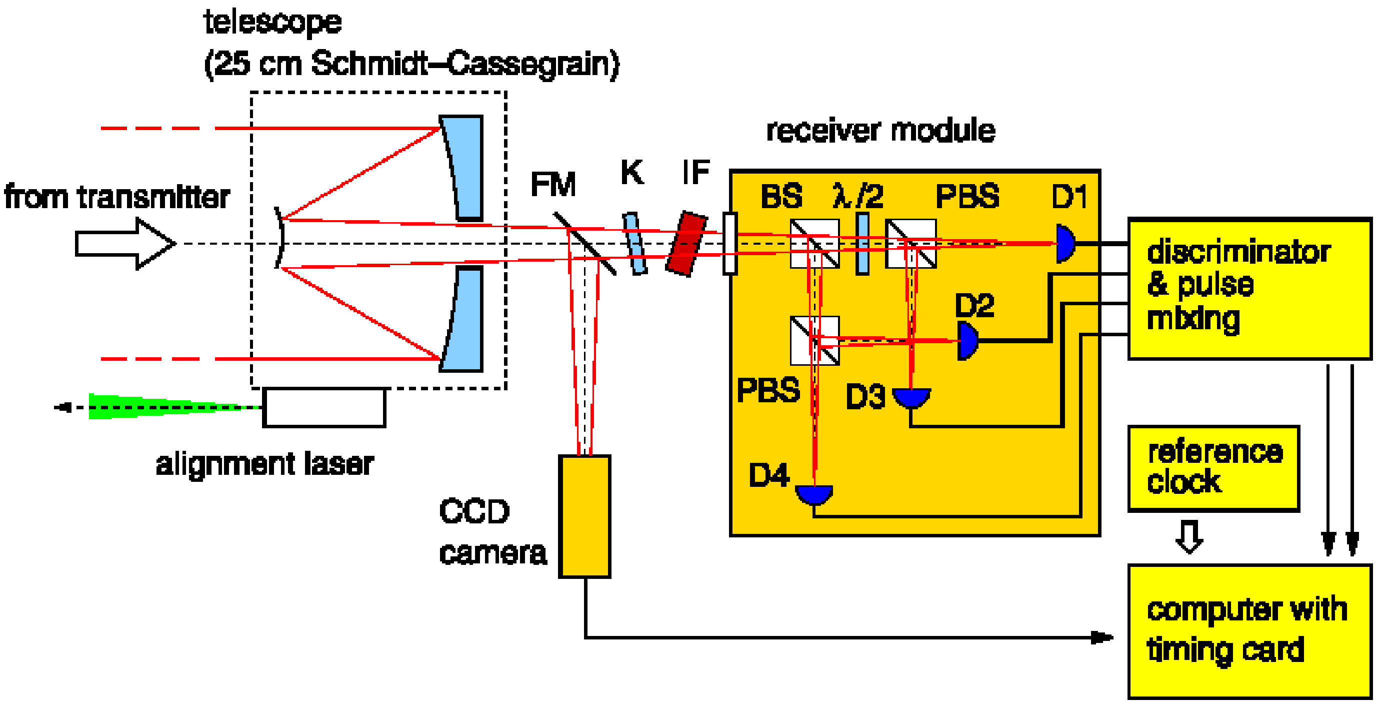
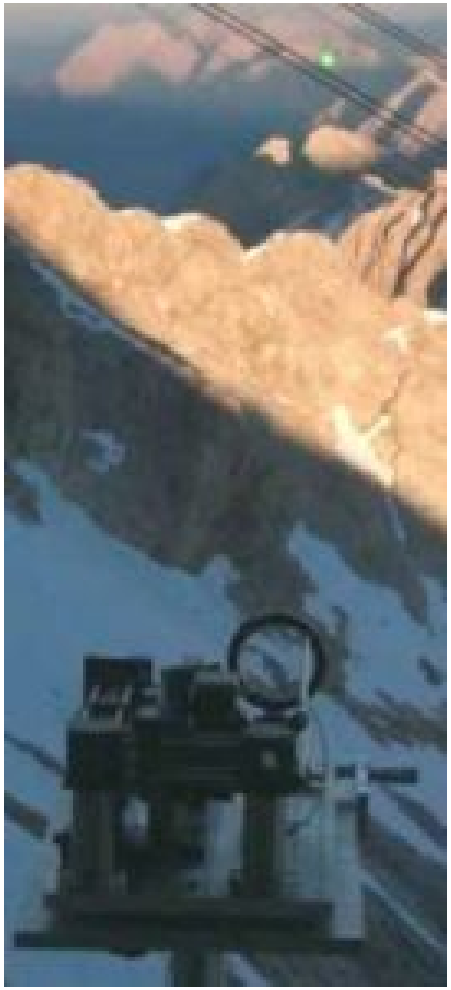
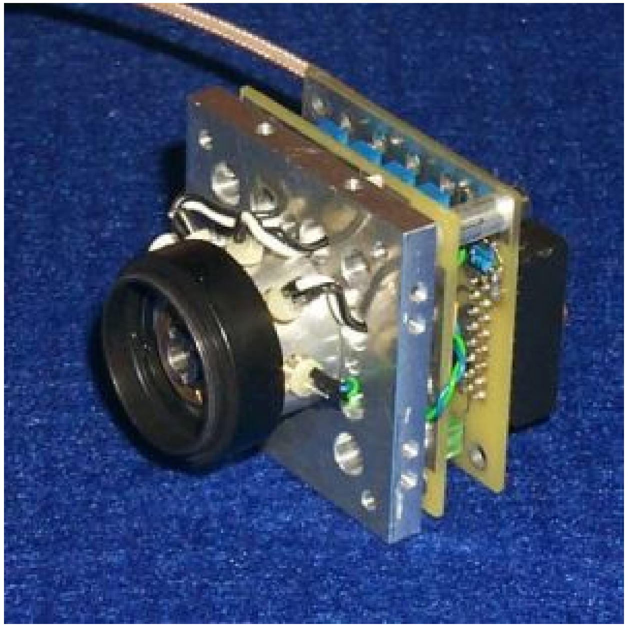


Figure 2 The receiver (Bob) consists of a 25 cm aperture Schmidt-Cassegrainian telescope. The miniature detector module is attached to the rear mounting of the telescope. It consists of a non-polarising beamsplitter (BS) followed by two polarising beamsplitters (PBS). Single photon detectors (D1-4) receive 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.

6.4 Free space cryptography – real experiment



Alice:



Bob: