Entanglement and Non-Local Measurements

Olaf Schubert*

July 3, 2008

Fachbereich Physik, University of Konstanz, Universitätsstraße 10, D-78457 Konstanz

Quantum physics plays an increasing role in our daily life: most modern computer chips are structured on length scales of several nanometers and even sunscreen often contains nanoparticles to increase its effectiveness. On these length scales quantum effects begin to play an important role. Though most people don't know about these applications of quantum physics, experiments on quantum teleportation and quantum cryptography have led to a high publicity of this interesting field of physics. Here I would like to review some quantum-mechanical concepts needed to understand the physics behind these topics and discuss how quantum teleportation and quantum cryptography work.

Overview This work is organized as follows: first the mathematical framework needed to describe measurements on entangled systems is introduced. In the second chapter it is shown, that local measurements destroy the entanglement of entangled states, and how this can be circumvented by performing non-local measurements. The central result of the second chapter, the Bell measurement, is then used to show how quantum teleportation and quantum cryptography work. In the last part it is shown how entanglement distillation can be used to increase the degree of entanglement of a quantum mechanical system. Basic knowledge of quantum mechanics and entangled systems is presumed. This work closely follows chapter 9 and 11 of ref. [1].

Mathematical framework An entangled system S^{AB} is made up of (at least) two subsystems S^A and S^B. Each system (qubit) is in a state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ (with the two linearly independent basis states $|0\rangle$ and $|1\rangle$ and constants $\alpha, \beta \in \mathbb{C}$). It is useful to define the "Bell basis":

$$\left|\Phi_\pm^{AB}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^A\right\rangle\left|0^B\right\rangle \pm \left|1^A\right\rangle\left|1^B\right\rangle\right) \tag{1}$$

$$\left|\Psi_\pm^{AB}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^A\right\rangle\left|1^B\right\rangle \pm \left|1^A\right\rangle\left|0^B\right\rangle\right) \tag{2}$$

As can be seen from eq. (1) and (2) each Bell state has a parity bit (either Φ or Ψ) and a phase bit (plus or minus). Thus, two bits can be stored in the Bell states (in the entanglement; non-locally). The non-locality of information storage makes reading out this information much harder, but also leads to interesting new phenomena, as will be shown below.

It is useful to discuss some properties of Bell states. Bell states are maximally entangled and are eigenvectors of the product operator $\sigma_k^A\sigma_k^B$ $(k = x, y, z)$ corresponding to eigenvalues of ± 1. I will show this for one example and leave the rest of the proof as an exercise to the interested reader:

$$\begin{aligned}\sigma_z^A\sigma_z^B\left|\Psi_+^{AB}\right\rangle &= \sigma_z^A\sigma_z^B\frac{1}{\sqrt{2}}\left(\left|0^A\right\rangle\left|1^B\right\rangle + \left|1^A\right\rangle\left|0^B\right\rangle\right)\\ &= \sigma_z^A\frac{1}{\sqrt{2}}\left(-\left|0^A\right\rangle\left|1^B\right\rangle + \left|1^A\right\rangle\left|0^B\right\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(-\left|0^A\right\rangle\left|1^B\right\rangle - \left|1^A\right\rangle\left|0^B\right\rangle\right)\\ &= -\left|\Psi_+^{AB}\right\rangle.\end{aligned}$$

Another useful property of Bell states is, that any Bell state can be transformed unitarily into any other Bell state by acting on only one subsystem with the Pauli operators σ_k :[1]

$$\begin{aligned}\sigma_x^A\left|\Psi_+^{AB}\right\rangle &= \sigma_x^A\frac{1}{\sqrt{2}}\left(\left|0^A\right\rangle\left|1^B\right\rangle + \left|1^A\right\rangle\left|0^B\right\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(\left|1^A\right\rangle\left|1^B\right\rangle + \left|0^A\right\rangle\left|0^B\right\rangle\right) = \left|\Phi_+^{AB}\right\rangle\end{aligned}$$

A similar property of the Bell states is, that the action of a Pauli-operator σ_k^A in one subsystem can be replaced by the action of a Pauli operator σ_k^B in the other subsystem

* *E-mail: olaf.schubert@uni-konstanz.de*

[1] again, only one example is shown

times a constant (i.e. $\sigma_k^A \rightarrow \beta \cdot \sigma_k^B$ with β=1, i or -i). For example we have:

$$\begin{aligned}\sigma_z^A \left|\Phi_+^{AB}\right\rangle &= \sigma_z^A \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle + \left|1^A\right\rangle \left|1^B\right\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle - \left|1^A\right\rangle \left|1^B\right\rangle\right) \\ &= \sigma_z^B \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle + \left|1^A\right\rangle \left|1^B\right\rangle\right) \\ &= \sigma_z^B \left|\Phi_+^{AB}\right\rangle .\end{aligned}$$

Measurements on entangled systems In the last part we have seen some properties of the Bell states, which are useful for possible applications. Of course one needs to extract information (phase bit and parity bit) from the Bell states in order to use them in applications like quantum cryptography.

A (projective) quantum mechanical measurement always involves a projection onto the eigenstates of a linear hermitian operator A (*observable*), which is associated with a physical quantity and can be written in its spectral decomposition as $A = \sum a_j |a_j\rangle \langle a_j|$. If we perform a selective measurement on our system, the initial state $|\varphi\rangle$ is transformed with a probability $p_j = \langle a_j| A |\varphi\rangle$ into the final state $|a_j\rangle$ (and eigenstate of A).

What happens if we try to measure the observable $\sigma_z^A \sigma_z^B$ of a Bell state $\left|\Phi_+^{AB}\right\rangle$ in a "local" way (i.e. by first measuring σ_z^B in S^B and then σ_z^A in S^A)?

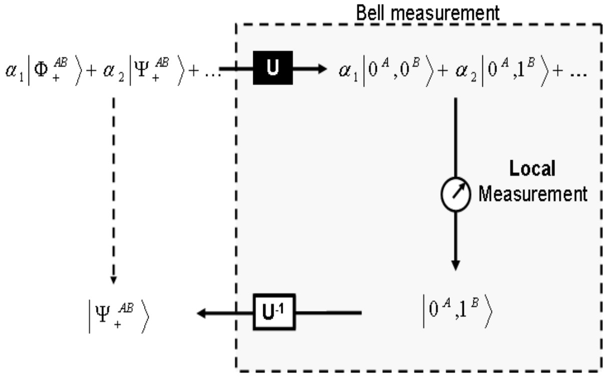
Bell measurement
$\alpha_1|\Phi_+^{AB}\rangle + \alpha_2|\Psi_+^{AB}\rangle + ...$
U
$\alpha_1|0^A,0^B\rangle + \alpha_2|0^A,1^B\rangle + ...$
Local Measurement
$|\Psi_+^{AB}\rangle$
U-1
$|0^A,1^B\rangle$

Figure 1: Scheme of the Bell measurement: a transformation U transforms an arbitrary state from the Bell basis into the computational basis. A local measurement projects onto the states of the computational basis, and the inverse transformation U^{-1} transforms the resulting state back into the Bell basis again.

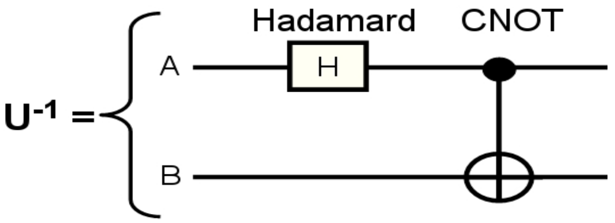

Figure 2: A quantum circuit for a Bell measurement. The circuit transforms states of the computational basis into states in the Bell basis. If the states are passed through the circuit in the reverse direction (i.e. first subjected to the CNOT operation and then to the Hadamard gate), Bell states are transformed into states in the computational basis

If a measurement of σ_z^B is performed on the subsystem S^B, the initial (entangled) Bell state

$$\left|\Phi_+^{AB}\right\rangle = \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle + \left|1^A\right\rangle \left|1^B\right\rangle\right)$$

is - depending on the measurement result - transformed into the state $\left|0^A\right\rangle \left|0^B\right\rangle$ or $\left|1^A\right\rangle \left|1^B\right\rangle$. A subsequent measurement of σ_z^A in S^A will not change this result. Obviously a local measurement breaks the entanglement and a "non-local" measurement would be needed to prevent this. Note, that the results of the two measurements are perfectly correlated.

In a lab only local operations can be performed: obviously a "non-local" measurement has to be done using local measurements. One way to realize this is the so called "Bell measurement". Its basic idea is to rotate the Bell basis such that it coincides with the computational basis and then perform a local measurement in this basis. The resulting state is then rotated back into the Bell basis to ensure that the state after the measurement is a Bell state (cf. Fig. 1). Mathematically the rotation is done by a unitary transformation $U = H \cdot \text{CNOT}$ (cf. Fig. 2), where H denotes a Hadamard transformation and CNOT a "controlled not" operation (sometimes also called XOR).

The proof is very simple:

$$\begin{aligned}(H \cdot \text{CNOT}) \left|\phi_+^{AB}\right\rangle &= (H \cdot \text{CNOT}) \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle + \left|1^A\right\rangle \left|1^B\right\rangle\right) \\ &= H \, \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle \left|0^B\right\rangle + \left|1^A\right\rangle \left|0^B\right\rangle\right) \\ &= H \, \frac{1}{\sqrt{2}} \left(\left|0^A\right\rangle + \left|1^A\right\rangle\right) \left|0^B\right\rangle \\ &= \left|0^A, 0^B\right\rangle .\end{aligned}$$

The reverse direction and the proof for the remaining three Bell states is trivial[2] [3].

Using the transformation U, we can now transform the Bell states into states in the computational basis, perform

[2] The reverse direction is clear because of the unitarity of H and CNOT (the quantum circuit is simply traversed in reverse)

[3] For the state$\left|\Phi_-^{AB}\right\rangle$ the Hadamard transform leads to the state $\left|1^A, 0^B\right\rangle$ (due to the minus sign). For the states $\left|\Psi_\pm^{AB}\right\rangle$ the CNOT operation leads to the states $\left|..., 1^B\right\rangle$

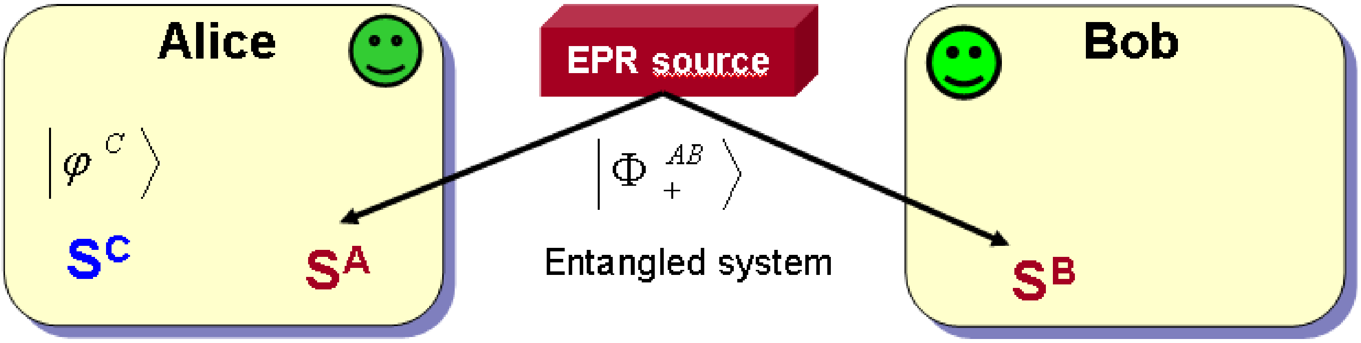
Alice
Bob
EPR source
$\left|\varphi^{C}\right\rangle$
$\left|\Phi^{AB}_{+}\right\rangle$
Entangled system
S^C
S^A
S^B

Figure 3: Setup for the teleportation of a quantum mechanical state (quantum teleportation). The state $\left|\varphi^{C}\right\rangle$ is teleported from Alice to Bob. To this end an entangled system is prepared and one subsystem (S^A) is sent to Alice, the other subsystem (S^B) to Bob. Apart from this initial preparation, no exchange of matter takes place.

a local measurement in the computational basis and transform the resulting state back into the Bell basis. These three steps are called a "Bell measurement". A Bell measurement yields the full information (parity and phase bit) about a Bell state and does not break the entanglement.

Quantum cryptography Quantum cryptography is a very promising candidate for commercial applications of entangled systems. The term "quantum cryptography" might be a little bit misleading: quantum cryptography is usually only used to exchange a key or increase the length of an already established key.[4] If a long, random key is established, that is used only once, simple, unbreakable protocols can be used to encode text.

One such protocol is the Vernam coding: Imagine that Alice has a message, consisting of a sequence of zeros and ones (length N, e.g.'00110100110'), which she would like to send to Bob. Both Alice and Bob have the same key of length $L \geq N$ (e.g. '01011101011'). Alice adds (bit by bit, modulo two[5]) the message and the key:

$$\begin{aligned} &00110100110\\ +&01011101011\\ =&01101001101 \end{aligned}$$

and sends the result (01101001101 in the example) to Bob. Bob sums the encoded text and the key and retrieves the original message:

$$\begin{aligned} &01101001101\\ +&01011101011\\ =&00110100110 \end{aligned}$$

An eavesdropper (Eve) would not be able to read the text, because she does not have the key.

The remaining question to ensure totally secure communication is: How can the key be exchanged in a secure way? Here quantum mechanics can be used advantageously, because any measurement by Eve would change the state and could be noticed.

A conceptually simple protocol for the key-exchange is the BBM92 protocol [2]. Here an entangled system is prepared in the Bell state $\left|\Phi^{AB}_{+}\right\rangle$ and one subsystem (S^A) is sent to Alice and one (S^B) is sent to Bob. Both have two bases to perform a measurement: $\{\left|H\right\rangle, \left|V\right\rangle\}$ and $\{\left|H'\right\rangle, \left|V'\right\rangle\}$, where H' and V' are rotated by 45° relative to H and V. These states can be thought of as photons with linear polarizations H/V and H'/V' (i.e. polarized in the horizontal/vertical direction and at -45°/45°, respectively). For each photon pair, Alice and Bob choose from the two possible bases in a completely random manner and independently of each other. Afterwards Alice and Bob exchange information about the chosen polarization directions and throw away all the results for which they did not use the same basis. If there was no eavesdropper, the other results are perfectly correlated and can be used as a key. The key is perfectly random, because it was obtained with a quantum mechanical meausurement.

To check, whether someone was trying to listen, Alice and Bob have to exchange a part of the key publicly. Because the polarization of the photon cannot be determined in one measurement and quantum states cannot be copied (no-cloning theorem), Eve cannot get the key. She is, however, of course able to prevent Alice and Bob from exchanging the key, by simply measuring or absorbing all the photons. A man-in-the-middle attack is also possible, if Eve controls all communication between Alice and Bob (i.e. both the quantum channel and the classical channel).

Quantum teleportation Teleportation has long been used as a convenient method to save the hero in science-fiction movies in the most improbable of ways. "Teleportation" usually refers to the process of one human or object appearing at a different location while disappearing at the original location. Here another type of teleportation is discussed: quantum teleportation, where a *state* is teleported to a different location. It is important to emphasize, that

[4] To prevent a man-in-the-middle-attack a previously established key has to be used to authenticate the communication-partners.

[5] i.e. 0+0=1+1=0 and 1+0=0+1=1

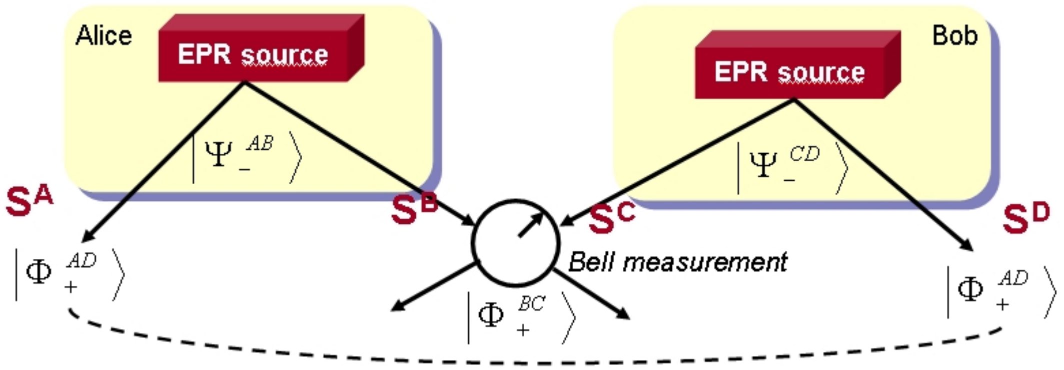
Alice
EPR source
$\left|\Psi_-^{AB}\right\rangle$
Bob
EPR source
$\left|\Psi_-^{CD}\right\rangle$
S^A
S^B
S^C
S^D
Bell measurement
$\left|\Phi_+^{AD}\right\rangle$
$\left|\Phi_+^{BC}\right\rangle$
$\left|\Phi_+^{AD}\right\rangle$

Figure 4: Setup for entanglement swapping. Two entangled systems, S^{AB} and S^{DC} are prepared at Alice's and Bob's location, respectively. The subsystems S^B and S^C are sent to a common location and a Bell measurement is performed on the system S^{BC}. This measurement entangles the system S^{AD} - even though the subsystems S^A and S^D can be at completely different locations.

only a state, not matter, is teleported.

To see how this works we use the same system as in the last paragraph, i.e. an entangled system, which was prepared in the Bell state Φ_+^{AB} and in part sent to Alice (subsystem S^A) and Bob (subsystem S^B). At Alice's location there is a third system S^C which is in a state $\left|\varphi^C\right\rangle$. (cf. Fig. 3) The goal is to teleport the state of $\left|\varphi^C\right\rangle$ to Bob.

In order to do this, the total state of the tripartite system is rewritten in a different form:

$$\begin{aligned}\left|\varphi^C\right\rangle\left|\Phi_+^C\right\rangle &= \frac{1}{\sqrt{2}}\left(a\left|0^C\right\rangle + b\left|1^C\right\rangle\right)\left(\left|0^A\right\rangle\left|0^B\right\rangle + \left|1^A\right\rangle\left|1^B\right\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(a\left|0^C\right\rangle\left|0^A\right\rangle\left|0^B\right\rangle + \ldots\right)\\ &= \frac{1}{2}\left(a(\left|\Phi_+^{AC}\right\rangle + \left|\Phi_-^{AC}\right\rangle)\left|0^B\right\rangle + \ldots\right)\\ &= \frac{1}{2}(\left|\Phi_+^{AC}\right\rangle\left|\varphi^B\right\rangle + \left|\Psi_+^{AC}\right\rangle\sigma_x^B\left|\varphi^B\right\rangle\\ &\quad + \left|\Psi_-^{AC}\right\rangle(-i\sigma_y^B)\left|\varphi^B\right\rangle + \left|\Phi_-^{AC}\right\rangle\sigma_z^B\left|\varphi^B\right\rangle).\end{aligned} \tag{3}$$

In the second equality, the brackets were factored out and the terms of the form $\left|X^C\right\rangle\left|Y^A\right\rangle$ (X and Y are either 0 or 1) rewritten in terms of a new Bell basis of the subsystem S^{AC}. In the fourth equality a new state $\left|\varphi^B\right\rangle := a\left|0^B\right\rangle + b\left|1^B\right\rangle$ was defined. It is important to note, that until now nothing has changed physically.

To carry out the teleportation, Alice performs a selective Bell measurement on the system S^{AC}. This projects onto a Bell state and all terms, but one drop out of the sum in the last line of eq. (3). Now Bob's system S^B is in a state $\beta \cdot \sigma_k^B\left|\varphi^B\right\rangle$. If Alice tells Bob the result of her measurement he can perform the corresponding unitary operation and his system ends up in the state $\left|\varphi^B\right\rangle$ - the state $\left|\varphi^C\right\rangle$ has been teleported to Bob.

Even though it might look as if teleportation violates fundamental physical laws, this is not the case: Because Alice has to call Bob, before the system is teleported, no information can be teleported faster than light using quantum teleportation and the special theory of relativity is not violated. The no-cloning-theorem is not violated either, because the state $\left|\varphi^C\right\rangle$ is no longer present at Alice's location.

Entanglement swapping It was just shown, how a selective Bell measurement can be used to teleport a state. A similar application of entangled systems is called "entanglement swapping". Two Bell states $\left|\psi_-^{AB}\right\rangle$ and $\left|\psi_-^{CD}\right\rangle$ are prepared at Alice's and Bob's location (cf. Fig. 4) and the total state of the system S^{ABCD} can be written as[6]:

$$\begin{aligned}\left|\psi_-^{AB}\right\rangle\left|\psi_-^{CD}\right\rangle = \frac{1}{2}\left|\psi_+^{AD}\right\rangle\left|\psi_+^{BC}\right\rangle - \frac{1}{2}\left|\psi_-^{AD}\right\rangle\left|\psi_+^{BC}\right\rangle\\ -\frac{1}{2}\left|\phi_+^{AD}\right\rangle\left|\phi_+^{BC}\right\rangle + \frac{1}{2}\left|\phi_-^{AD}\right\rangle\left|\phi_-^{BC}\right\rangle\end{aligned}$$

If a selective Bell measurement is performed on the subsystem S^{BC}, again all terms in the sum but one drop out. The subsystem S^{BC} will be left in a Bell state (e.g. $\left|\Phi_+^{BC}\right\rangle$), corresponding to the measurement result - the system S^{BC} is now entangled. The interesting thing is, that the subsystem S^{AD} will be left in a Bell state (e.g. $\left|\Phi_+^{AD}\right\rangle$), too. This means, that the Bell measurement on S^{BC} has entangled the subsystems S^A and S^D, even though S^A and S^D might be thousands of miles apart!

Entanglement distillation Until now it was always assumed, that maximally entangled pure states are readily available and that quantum channels are noise-free. In an experimental situation this is, however, usually not the case. Therefore, it is important to show how the (average) degree of entanglement of mixtures can be increased using a "distillation protocol".

The idea of this protocol is to use two pairs of entangled states, perform a selection based on local operations and classical communication and sacrifice some pairs. The remaining pairs then have a higher degree of entanglement.

[6] The maths is basically the same as in eq.(3). The only difference is, that now two new Bell basis (AD and BC) are defined and used to express the state.

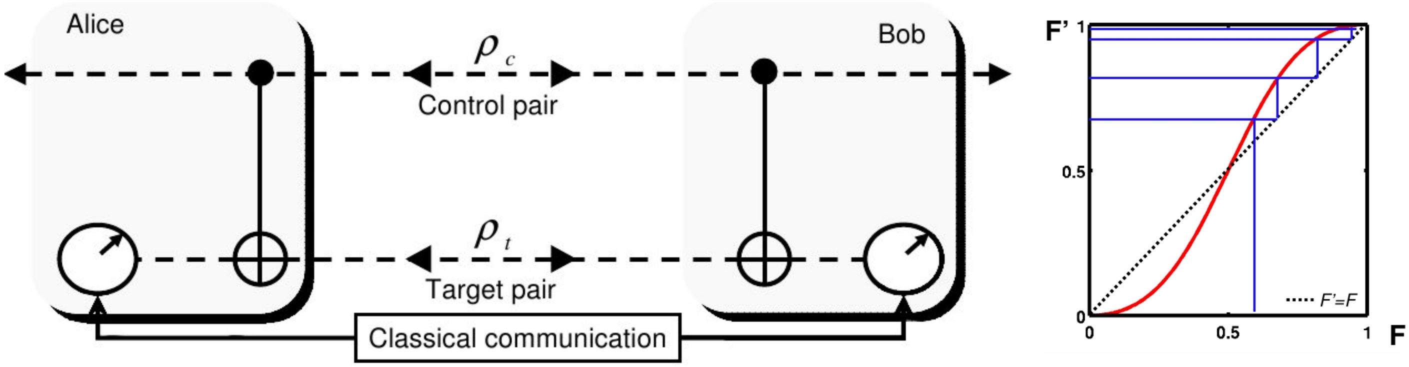

Figure 5: The quantum circuit for entanglement distillation (*left*) consists of two CNOT-gates and two measurement devices at Alice's and Bob's locations, respectively. The target pair is always sacrificed (the entanglement is destroyed by the local measurement), the control pair is only destroyed, if the measurement results disagree. From the plot of the function $F'(F)$ it is obvious, that the degree of entanglement for the remaining pairs is increased, if the original degree of entanglement was $F > 0.5$ (*right*). Blue lines correspond to one example for the protocol, starting from a fidelity of $F \approx 0.6$

Mixed states are assumed to be of the form (with a parameter $0 < F < 1$, known as the fidelity):

$$\rho = F \left|\Phi_+^{AB}\right\rangle \left\langle\Phi_+^{AB}\right| + (1-F) \left|\Psi_+^{AB}\right\rangle \left\langle\Psi_+^{AB}\right| \qquad (4)$$

The quantum circuit for this protocol of entanglement distillation is shown in Fig. 5. If the states of both target and control pair can be written like eq. (4), the mixed state of all 4 qubits before the CNOT-transformations has terms proportional to F^2, $(1-F)^2$ and $F(1-F)$. After the CNOT transformations these terms become[7]:

$$\begin{aligned}
\sim F^2 \left|\Phi_c\right\rangle \left|\Phi_t\right\rangle &= \left|\Phi_c\right\rangle \frac{1}{\sqrt{2}} \left(\left|0_t^A\right\rangle \left|0_t^B\right\rangle + \left|1_t^A\right\rangle \left|1_t^B\right\rangle\right) \\
\sim (1-F)^2 \left|\Psi_c\right\rangle \left|\Phi_t\right\rangle &= \left|\Psi_c\right\rangle \frac{1}{\sqrt{2}} \left(\left|0_t^A\right\rangle \left|0_t^B\right\rangle + \left|1_t^A\right\rangle \left|1_t^B\right\rangle\right) \\
\sim F(1-F) \left|\Phi_c\right\rangle \left|\Psi_t\right\rangle &= \left|\Phi_c\right\rangle \frac{1}{\sqrt{2}} \left(\left|0_t^A\right\rangle \left|1_t^B\right\rangle + \left|1_t^A\right\rangle \left|0_t^B\right\rangle\right) \\
\sim F(1-F) \left|\Psi_c\right\rangle \left|\Psi_t\right\rangle &= \left|\Psi_c\right\rangle \frac{1}{\sqrt{2}} \left(\left|0_t^A\right\rangle \left|1_t^B\right\rangle + \left|1_t^A\right\rangle \left|0_t^B\right\rangle\right)
\end{aligned}$$

Now two local selective measurements in the computational basis are performed on the target pair. If the results agree, the control pair is kept, if not, it is destroyed. This means, that the terms proportional to $F(1-F)$ drop out. The density operator of the resulting state can be written as in eq. (4), but with a new fidelity F':

$$F' = \frac{F^2}{F^2 + (1-F)^2}$$

From this function it is clear, that the degree of entanglement is increased, if the initial fidelity F was greater than 0.5. In principle the degree of entanglement can be increased to arbitrary high values (by sacrificing an arbitrary large number of states!). In practice a balance between the number of pairs sacrificed and the degree of entanglement achieved has to be found. In practice noise also limits the maximal degree of entanglement achievable.

Summary In this work, some applications of entangled systems were presented. To understand the physics behind these applications, the Bell basis was introduced and some of its properties were discussed. It was shown, that a local measurement on an entangled system breaks the entanglement and how this can be circumvented, by rotating the basis (Bell measurement). This tool was then used to show, how quantum cryptography makes a secure key-exchange possible and how quantum teleportation works. In the last part we have discussed entanglement distillation and it was shown, that an arbitrary high degree of entanglement can - in principle - be reached by sacrificing some of the qubit pairs.

Acknowledgements: I would like to thank Fabian Mohn for helpful discussions.

References

[1] Jürgen Audretsch. *Entangled Systems - New Directions in Quantum Physics*. Wiley-VCH, Weinheim, 2007.

[2] C.H.Bennett, G.Brassard, N.D.Mermin. Quantum cryptography without bell's theorem. *Phys.Rev.Lett.*, 68:557–559, 1992.

[7] Here the subscript "c" denotes the control qubit, the subscript "t" denotes states of the target qubit. The index "+" is dropped to simplify the notation.