Chapter 13

Quantum communication

In this chapter we will review several promising applications and protocols of quantum communications, such as quantum key distribution, quantum teleportation and quantum repeater by entanglement swapping.

13.1 Quantum key distribution

Cryptography, despite a colorful history that goes back to 400 B.C., only became part of mathematics and information theory this century, in the late 1940s, mainly due to the seminal paper of Shannon[1]. Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation[2, 3]. Deutsch has shown that quantum physics enriches our computational possibilities far beyond classical Turing machines[2, 3], and current work in quantum cryptography originated by Bennett and Brassard provides a good example of this fact[4, 5, 6].

Originally the security of a cryptotext depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a *key*, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key, which is very important, may consist of any randomly chosen, sufficiently long string of bits. Once the key is established, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive interception (e.g., public announcement in mass media). However, in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. Since the interception is a set of measurements performed by the eavesdropper on this channel, however difficult this might be from a technological point of view, in principle any classical channel can always be passively monitored, without the legitimate users being aware that any eavesdropping

has taken place. This is not so for quantum channels[4, 5, 6].

13.1.1 Single photon QKD system (BB84)[7]

13.1.1.A Basic principle

In traditional public-key cryptography, trapdoor functions are used to conceal the meaning of messages between two users from a passive eavesdropper, despite the lack of any initial shared secret information between the two users. In quantum public key distribution, the quantum channel is not used directly to send meaningful messages, but is rather used to transmit a supply of random bits between two users who share no secret information initially, in such a way that the users, by subsequent consultation over an ordinary non-quantum channel subject to passive eavesdropping, can tell with high probability whether the original quantum transmission has be disturbed in transit, as it would be by an eavesdropper (it is the quantum channel's peculiar virtue to compel eavesdropping to be active). If the transmission has not been disturbed, they agree to use these shared secret bits in the well-known way as a one-time pad to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications (e.g. authentication tags) requiring shared secret random information. If transmission has been disturbed, they discard it and try again, deferring any meaningful communications until they have succeeded in transmitting enough random bits through the quantum channel to serve as a one-time pad.

In more detail one user ('Alice') chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user (Bob) a train of photons, each representing one bit of the string in the basis chosen for that bit position, a horizontal or 45-degree photon standing for a binary zero and a vertical or 135-degree photon standing for a binary one. As Bob receives the photons he decides, randomly for each photon and independently of Alice, whether to measure the photon's rectilinear polarization or its diagonal polarization, and interprets the result of the measurement as a binary zero or one. A random answer is produced and all information lost when one attempts to measure the rectilinear polarization of a diagonal photon, or vice versa. Thus Bob obtains meaningful data from only half the photons he receives – those for which he guessed the correct polarization basis. Bob's information is further degraded by the fact that, realistically, some of the photons would be lost in transit or would fail to be counted by Bob's imperfectly-efficient detectors.

Subsequent steps of the protocol take place over an ordinary public communications channel, assumed to be susceptible to eavesdropping but not to the injection or alteration of messages. Bob and Alice first determine, by public exchange of message, which photons were successfully received and of these which were detected with the correct basis. If the quantum transmission has been undisturbed, Alice and Bob should agree on the bits encoded by these photons, even this data has never been discussed over the public channel. Each of these photons, in other words, presumably carries one bit of random information (e.g., whether a rectilinear photon was vertical or horizontal) known to Alice and Bob but to no one else.

Because of the random mix of rectilinear and diagonal photons in the quantum transmission, any eavesdropping carries the risk of altering the transmission in such a way as to produce disagreement between Bob and Alice on some of the bits on which they think they

should agree. Specifically, it can be shown that no measurement on a photon in transit, by an eavesdropper ('Eve') who is informed of the photon's original basis only after he has performed his measurement, can yield more than 1/2 expected bits of information about the key bit encoded by that photon; and that any such measurement yielding b bits of expected information $b \leq 1/2$ must induce a disagreement with probability at least $b/2$ if the measured photon, or an attempted forgery of it, is later re-measured in its original basis. (This optimum tradeoff occurs, for example, when Eve measures and retransmits all intercepted photons in the rectilinear basis, thereby leaning the correct polarizations of half the photons and inducing disagreements in 1/4 of those that are later re-measured in the original basis.)

Alice and Bob can therefore test for eavesdropping by publicly comparing some of the bits on which they think they should agree, though of course positions used in this comparison should be a random subset (say one third) of the correctly received bits, so that eavesdropping on more than a few photons is unlikely to escape detection. The probability of escaping detection scales as $\sim \left(\frac{3}{4}\right)^n$, which goes to zero when the number of test bits n increases. If all the comparisons agree, Alice and Bob can conclude that the quantum transmission has been free of significant eavesdropping, and those of the remaining bits that were sent and received with the same basis also agree, and can safely be used as a one time pad for subsequent secure communications over the public channel. When this on-time pad is used up, the protocol is repeated to send a new body of random information over the quantum channel.

The following example illustrates the above protocol.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending basis	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Random receiving basis	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC TRANSMISSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which basis were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirm them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman-Carter multiple-message authentication tags[8] for their messages over the public channel. In this separate-world attack, Eve pretends false Bob against Alice and also false Alice against Bob. In more detail the Wegman-Carter multiple-

message authentication scheme uses a small random key to produce a message-dependent 'tag' (rather like a check sum) for an arbitrary large message, in such a way that Eve, who is ignorant of the key, has only a small probability of being able to generate any other valid message-tag pairs. The tag thus provides evidence that the message is legitimate, and was not generated or altered by someone ignorant of the key. (Key bits are gradually used up in the Wegman-Carter scheme, and cannot be reused without compromising the system's provable security; however, in the present application, these key bits can be replaced by fresh random bits successfully transmitted through the quantum channel.) Eve can still prevent communication by suppressing messages in the public channel, as of course he can by suppressing or excessively perturbing the photons sent through the quantum channel. However in either case, Alice and Bob will conclude with high probability that their secret communications are being suppressed, and will not be fooled into thinking their communications are secure when in fact they're not.

13.1.1.B Error correction and privacy amplification

In a real communication system, errors are bound to occur. (We will shortly discuss actual device imperfections which cause a bit error.) One way to correct a bit error is the use of parity check[11]. The shifted keys are grouped into blocks, where the block size is chosen to have not more than two errors. The parity of each block is announced publicly between Alice and Bob. If their parities agree, they proceed to the next block. If their parities disagree, they recursively cut the block into sub-groups to find which sub-group has an error. They shuffle the positions of the bits and repeat the process. This scheme does not need to discard any bit from the shifted key but suffers from the leakage of bit information to Eve. According to Shannon's channel coding theorem, the bits of information r that must be exchanged publicly in order to correct the bit error for the shifted key with a length of n bits and an error rate of ε is

$$\lim_{n\to\infty} \frac{r}{n} \geq H(\varepsilon) = \Big[-\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log(1-\varepsilon) \Big] \quad . \tag{13.1}$$

Even though Alice and Bob now share an error free shifted key, Eve has substantial information about the shifted key, which was gained by her during raw quantum transmission and subsequent error correction. Alice and Bob jointly decrease the size of the key such that Eve has negligible information about the final key. This step is called privacy amplification[12]. Alice sends Bob a $n \times (n-\tau)$ random binary matrix K. They distil the final key with $(n-\tau)$ bits from the shifted key with n bits by an operation, $k_{\text{final}} = K \cdot k_{\text{shift}} \pmod 2$. The compression parameter τ is determined such that Eve's residual mutual information is negligibly small:

$$I_E(k_{\text{final}}; K \cdot V) = H(k_{\text{final}}) - H(k_{\text{final}}/K \cdot V) \to 0 \quad , \tag{13.2}$$

where V is the information available to Eve about the shifted key before privacy amplification, $H(k_{\text{final}})$ is the entropy of the final key and $H(k_{\text{final}}/K \cdot V)$ is the conditional entropy of Eve. If the final key's size satisfy

$$n - \tau = n[-\log_2 p_c] - \kappa - t - s \quad , \tag{13.3}$$

Eve's mutual information is bounded by

$$I_E \leq 2^{-t}(n-\tau) + \frac{2^{-s}}{\ln 2} \quad . \tag{13.4}$$

Here κ is the number of bits of information that Eve obtains from error correction, s and t are security parameters chosen by Alice and Bob, and p_c is the collision probability which satisfies

$$p_c \leq \frac{1}{2} + 2\varepsilon - 2\varepsilon^2 \quad . \tag{13.5}$$

If an error rate is $\varepsilon = 0$, $p_c = \frac{1}{2}$ (random guess) and Eve gets no information from the raw quantum transmission. There is no need to perform the error correction and thus no need to shorten the shifted key. If an error rate is $\varepsilon = \frac{1}{2}$, $p_c = 1$ (perfect guess) and Eve can learn the entire string by the intercept and resend attack. Alice and Bob cannot create any secure key. Thus, the protocol works when $0 < \varepsilon < \frac{1}{2}$ and Eve's mutual information can be decreased to an arbitrarily small value by choosing the two parameters t and s properly.

13.1.1.C Security of practical BB84 protocol (I) —Poissonian photon source—

We study the security of a practical BB84 QKD system with a standard semiconductor laser source in this section. The photon number distributions of input and output pulses of a quantum channel are both Poissonian:

$$p(n) = \frac{\bar{n}^n e^{-\bar{n}}}{n!} \quad , \tag{13.6}$$

$$p(m) = \frac{(\alpha\bar{n})^m e^{-\alpha\bar{n}}}{m!} \quad , \tag{13.7}$$

where $\bar{n}$ is the input average photon number per pulse and α is the loss rate of a quantum channel. We consider the following Eve's hybrid attack. Eve performs the QND measurement of photon number for each pulse sent by Alice, which is insensitive to the polarization state, so Eve can extract only information about photon number but no information about polarization. If the photon number is equal or greater than two, she extracts and keeps one photon in her quantum memory until Alice and Bob disclose their (matched) modulation/demodulation bases and sends remaining photons to Bob. By performing the polarization measurement with this basis, she can get full information without causing any bit error. If the photon number is one, Eve measures the polarization with a rectilinear basis and sends a new photon with a measured polarization state to Bob. This intercept and resend attack must create a bit error of 1/4.

If a transmission line is lossy, Bob's photon receiving rate is smaller than Alice's photon sending rate, i.e. $\bar{n} < \alpha\bar{n}$. Eve can replace a lossy transmission line with a lossless transmission line. If the $(n-1)$ transmitted photons out of multi-photon states ($n \geq 2$) make the average photon arrival rate $\alpha\bar{n}$, Eve can simply block all one photon states and extract complete information about the key out of the multiphoton states without being detected. The entire key is completely insecure. In order to avoid such a situation, Alice must decrease the average photon number $\bar{n}$ with the increase of a loss α. What is a maximum allowable loss α in order to create a secure key?

The probability of receiving signal photons per pulse is

$$p_s = \sum_{n=1}^{\infty} \frac{(\alpha\eta\bar{n})^n e^{-\alpha\eta\bar{n}}}{n!} \quad , \tag{13.8}$$

where η is a detector quantum efficiency. A practical detector has a finite dark count rate d_B per measurement slot and two detectors must be used to distinguish logical zero or one. Therefore, the total count rate is

$$p_{\rm exp} = p_s + 2d_B \quad . \tag{13.9}$$

The probability of Eve's finding more than two photons per pulse is

$$p_{\rm multi} = \sum_{n=2}^{\infty} \frac{(\bar{n})^n e^{-\bar{n}}}{n!} \quad . \tag{13.10}$$

The secure communication becomes impossible if an innocent error caused by a detector dark count becomes greater than the error introduced by Eve's intercept and resend attack,

$$\frac{1}{2} \times 2d_B \geq \frac{1}{4}(p_{\rm exp} - p_{\rm multi}) \quad , \tag{13.11}$$

where it is assumed that exactly one half of the detector dark count makes an error and Eve must perform an intercept and resend attack only on part of the one photon pulse with a probability $p_{\rm exp} - p_{\rm multi}$. If $p_{\rm multi} \geq p_{\rm exp}$, she does not need to perform an intercept and resend attack, as mentioned above. From the above relation, we have a bound on the transmission loss:

$$\alpha \leq \frac{2d_B}{\eta\bar{n}} + \frac{\bar{n}}{2\eta} \leq \frac{2\sqrt{d_B}}{\eta} \quad . \tag{13.12}$$

The equality holds at the optimum average photon number $\overline{n_{\rm opt}} = 2\sqrt{d_B}$. If $\bar{n} > \overline{n_{\rm opt}}$, Eve's photon splitting attack becomes more effective and α becomes smaller. If $\bar{n} < \overline{n_{\rm opt}}$, Eve's intercept and resend attack becomes more effective and α becomes smaller.

13.1.1.D Security of practical BB84 system —Single photon source—

We study the security of a practical BB84 QKD system with a sub-Poissonian and single photon source. A sub-Poissonian and single photon source can be experimentally evaluated by the second-order coherence function:

$$g^{(2)}(0) = \frac{\int_0^\Delta \int_0^\Delta \langle \hat{a}^+(t)\hat{a}^+(t')\hat{a}(t')\hat{a}(t)\rangle dt dt'}{\left(\int_0^\Delta \langle \hat{a}^+(t)\hat{a}(t)\rangle dt\right)^2} \quad , \tag{13.13}$$

where Δ is a pulse duration. If we use $[\hat{a}(t), \hat{a}(t')^+] = \delta(t-t')$ in the above definition, we have

$$\begin{aligned} g^{(2)}(0) &= \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\langle \hat{n}\rangle^2} \\ &= \frac{\sum_{i=2}^{\infty} i(i-1)p(i)}{\langle \hat{n}\rangle^2} \\ &\geq \frac{\sum_{i=2}^{\infty} 2p(i)}{\langle \hat{n}\rangle^2} = \frac{2p_m}{\langle \hat{n}\rangle^2} \quad . \end{aligned} \tag{13.14}$$

Here $p(i)$ is the probability for i photons in a source, p_m is the probability sum for multi-photon states ($n \geq 2$). Thus, p_m is upper bounded by

$$p_m \leq \frac{\langle \hat{n}\rangle^2 g^{(2)}(0)}{2} \quad . \tag{13.15}$$

Let us calculate the final key generation rate R for a practical BB84 system. The probability for total detection event per pulse is

$$p_{\rm click} = p_{\rm signal} + p_{\rm dark} - p_{\rm signal} \cdot p_{\rm dark} \simeq p_{\rm signal} + p_{\rm dark} \quad , \tag{13.16}$$

where the signal count probability is determined by the average photon number per pulse $\langle \hat{n} \rangle$, fiber loss rate α and detector efficiency η,

$$p_{\rm signal} = \sum_{n=0}^{\infty} p(n) \left[1 - (1 - \alpha\eta)^n \right] \simeq \alpha\eta \langle \hat{n} \rangle \quad . \tag{13.17}$$

We assume $\alpha\eta \ll 1$ (high loss limit). The probability of finding true single count per pulse is

$$\beta = \frac{p_{\rm click} - p_m}{p_{\rm click}} \quad . \tag{13.18}$$

The bit error rate is determined by a parameter μ which accounts for imperfect optics and the detector dark count rate,

$$\varepsilon = \frac{\mu p_{\rm signal} + \frac{1}{2} p_{\rm dark}}{p_{\rm click}} \quad . \tag{13.19}$$

The total number of shifted key after raw quantum transmission is $n = p_{\rm click} N$ against the total number of pulse slots. The final key generation rate R after error correction and privacy amplification is now given by

$$\begin{aligned} R &= \lim_{N \to \infty} \frac{n - r}{N} \\ &= \lim_{n \to \infty} p_{\rm click} \left[-\beta \log_2 p_c \left(\frac{\varepsilon}{\beta} \right) - \frac{\kappa}{n} - \frac{s + t}{n} \right] \quad , \end{aligned} \tag{13.20}$$

where the new collision probability, $p_c \left(\frac{\varepsilon}{\beta} \right) \leq \frac{1}{2} + 2 \left(\frac{\varepsilon}{\beta} \right) - 2 \left(\frac{\varepsilon}{\beta} \right)^2$, accounts for the finite fiber loss/detector efficiency and multi-photon state. The side information that Eve can obtain from error correction is

$$\lim_{n \to \infty} \frac{\kappa}{n} = f(\varepsilon) \cdot h(\varepsilon) = f(\varepsilon) \Big[-\varepsilon \log \varepsilon - (1 - \varepsilon) \log (1 - \varepsilon) \Big] \quad . \tag{13.21}$$

Here $f(\varepsilon) \geq 1$ represents the degradation from Shannon limit for the error correction.

As one can see from the above, if $\langle \hat{n} \rangle$ is too high, R will drop due to an increase in p_m and a decrease in β. On the contrary, if $\langle \hat{n} \rangle$ is too low, R will drop due to a decrease in $p_{\rm click}$. There is an optimum $\langle \hat{n} \rangle$ to maximize R for given $\alpha\eta$. Figure 13.1 shows the final key rate R vs. system loss $\alpha\eta$ for various $g^{(2)}(0)$ values and for the following parameters: $d = 4 \times 10^{-8}$, $\mu = 0.01$ and $\eta_{\rm device} = 1$. Here $\eta_{\rm device}$ is the quantum efficiency of a source. Figure 13.2 shows the final key rate R vs. system loss $\alpha\eta$ for $g^{(2)}(0) = 0.01$ (fixed) and various source efficiencies $\eta_{\rm device}$. Even if the source efficiency $\eta_{\rm device}$ is very low, say $0.1 - 1\%$, such a system can achieve the same cutoff loss as an ideal source $\eta_{\rm device} = 1$. This is a rather remarkable result.

13.1.1.E Cutoff loss rate

A cutoff loss rate, at which an entire message is insecure, is determined by the condition

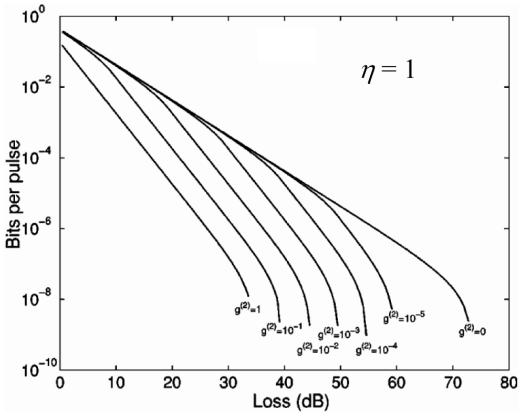

Figure 13.1:

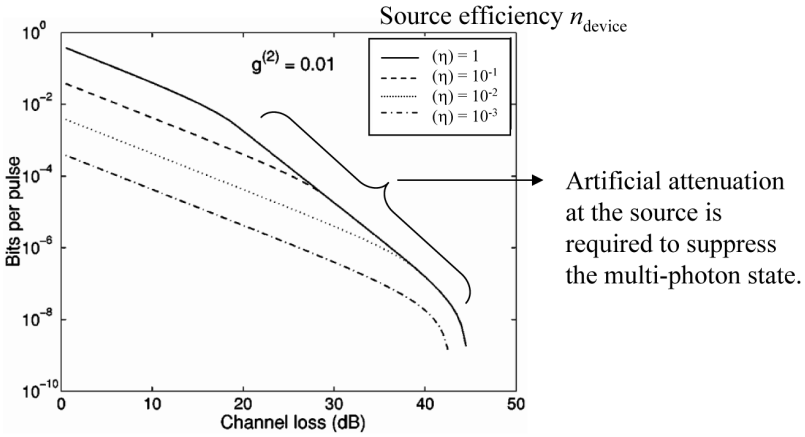

Figure 13.2:

that Eve can intercept and resend all single photon states within an allowable bit error rate while she performs photon-split-attack all multi-photon states. This condition is given by

$$\varepsilon = \frac{1}{4}\beta \quad , \tag{13.22}$$

where ε is an innocent error of the system and β is a fraction of single photons states in the shifted keys,

$$\varepsilon = \frac{\mu p_{\text{signal}} + \frac{1}{2} p_{\text{dark}}}{p_{\text{click}}} \quad , \tag{13.23}$$

$$\beta = \frac{p_{\text{click}} - p_{\text{mult}}}{p_{\text{click}}} \quad . \tag{13.24}$$

We can optimize $\langle \hat{n} \rangle \in [0, 1]$ in order to maximize a cutoff loss rate,

$$\alpha = \frac{1}{1 - 4\mu} \left(\frac{d}{\langle \hat{n} \rangle} + \frac{\langle \hat{n} \rangle g^{(2)}(0)}{2} \right) \quad . \tag{13.25}$$

For an ideal single photon with $\eta_{\text{device}} = 1$ and $g^{(2)}(0) = 0$, the optimum average photon number is $\langle \hat{n} \rangle = 1$ and we obtain

$$\alpha = \frac{d}{1 - 4\mu} \quad . \tag{13.26}$$

For a non-ideal photon source with $\eta_{\text{device}} = 1$ but $g^{(2)}(0) > 0$, the optimum photon average photon number is

$$\langle \hat{n} \rangle = \sqrt{\frac{2d}{g^{(2)}(0)}} \leq 1 \quad , \tag{13.27}$$

and the cutoff loss rate becomes

$$\alpha = \frac{\sqrt{2dg^{(2)}(0)}}{1 - 4\mu} \quad . \tag{13.28}$$

Figure 13.3 shows the two curves for α and $\langle \hat{n} \rangle$ vs. $g^{(2)}(0)$, calculated by the above closed form solutions and the exact numerical analysis. As far as η_{device} exceeds $\langle \hat{n} \rangle$, which is smaller than one, one can always achieve the above cutoff rate.

13.1.2 EPR photon-pair QKD system (Ekert 91)[11]

In this section a method is presented in which the security of the key distribution process in cryptography depends on the completeness of quantum mechanics. Here completeness means that quantum description provides maximum possible information about any system under consideration. The proposed scheme is based on the Bohm's well known version of the Einstein Podolsky Rosen *gedanken experiment*[12, 13]; the generalized Bell's theorem (Clauser Horne Shimony Holt inequalities)[14, 15] is used to test for eavesdropping. From a theoretical point of view the scheme provides an interesting and new extension of Bennett and Brassard's original idea, and from an experimental perspective offers a practical realization by a small modification of experiments that were set up to test Bell's theorem.

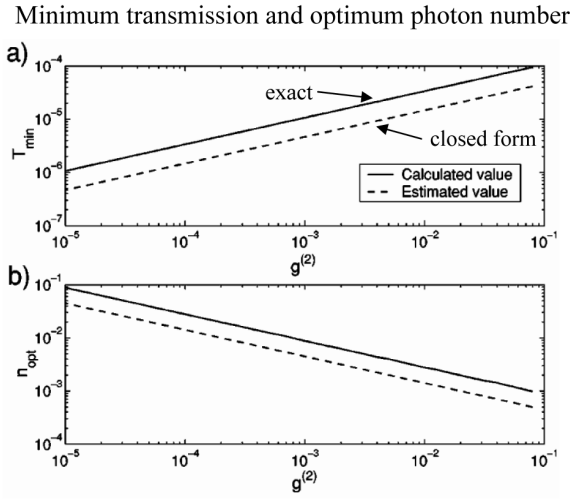

Figure 13.3:

The channel consists of a source that emits pairs of photons considered as spin $\frac{1}{2}$ particles, in a singlet state. The particles fly apart along the z axis, towards the two legitimate users of the channel, say, Alice and Bob, who, after the particles have separated, perform measurements on spin components along one of three directions given by unit vectors $\mathbf{a}_i$ and $\mathbf{b}_j$ $(i, j = 1, 2, 3)$, respectively, for Alice and Bob. For simplicity, both $\mathbf{a}_i$ and $\mathbf{b}_j$ vectors lie in the x-y plane, perpendicular to the trajectory of the particles, and are characterized by azimuthal angles: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$, $\phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{1}{2}\pi$, $\phi_3^b = \frac{3}{4}\pi$. Superscripts "$a$" and "$b$" refer to Alice and Bob's analyzers, respectively, and the angle is measured from the vertical x axis. The users choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement, in $\frac{1}{2}\hbar$ units, can yield two results, $+1$ (spin up) and -1 (spin down), and can potentially reveal one bit of information.

The quantity

$$E(\mathbf{a}_i, \mathbf{b}_j) = P_{++}(\mathbf{a}_i, \mathbf{b}_j) + P_{--}(\mathbf{a}_i, \mathbf{b}_j) \tag{13.29}$$

$$- \; P_{+-}(\mathbf{a}_i, \mathbf{b}_j) - P_{-+}(\mathbf{a}_i, \mathbf{b}_j) \tag{13.30}$$

is the correlation coefficient of the measurements performed by Alice along $\mathbf{a}_i$ and by Bob along $\mathbf{b}_j$. Here $P_{\pm\pm}(\mathbf{a}_i, \mathbf{b}_j)$ denotes the probability that result ± 1 has been obtained along $\mathbf{a}_i$ and ± 1 along $\mathbf{b}_j$. According to the quantum rules (see Chapter 1 for details)

$$E(\mathbf{a}_i, \mathbf{b}_j) = -\mathbf{a}_i \cdot \mathbf{b}_j \quad . \tag{13.31}$$

For the two pairs of analyzers of the same orientation ($\mathbf{a}_2$, $\mathbf{b}_1$ and $\mathbf{a}_3$, $\mathbf{b}_2$) quantum mechanics predicts total anticorrelation of the results obtained by Alice and Bob: $E(\mathbf{a}_2, \mathbf{b}_1) = E(\mathbf{a}_3, \mathbf{b}_2) = -1$.

Let us also, following Clauser, Horne, Shimony, and Holt[14, 15], define a quantity composed of the correlation coefficients for which Alice and Bob used analyzers of different orientation,

$$S = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3) \quad . \tag{13.32}$$

Again, quantum mechanics requires

$$S = -2\sqrt{2} \quad . \tag{13.33}$$

After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they used different orientation of analyzers, and a second group for which they used the same orientation of their analyzers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently, Alice and Bob can reveal publicly the results they obtained but within the first group of measurements only. This allows them to establish the value of S, which, if the particles were not directly or indirectly "disturbed," should reproduce the result of Eq. (13.33). This assures the legitimate users that the results they obtained within the second group of measurements are anticorrelated and can be converted into a secret string of bits – key. This secret key may be then used in a conventional cryptographic communication between Alice and Bob.

The eavesdropper cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. The eavesdropper may try to substitute his own prepared data for Alice and Bob to misguide them, but as he does not know which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape from being detected. In this case his intervention will be equivalent to introducing elements of physical reality to the measurements of the spin components. This can be easily seen if we put appropriately modified (by the eavesdropper perfect measurement) correlation coefficients into Eq. (13.32). We obtain

$$\begin{aligned} S \;\; = \;\; & \int \rho(\mathbf{n}_a, \mathbf{n}_b) \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b [(\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) - (\mathbf{a}_1 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b) \\ & + (\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_1 \cdot \mathbf{n}_b) + (\mathbf{a}_3 \cdot \mathbf{n}_a)(\mathbf{b}_3 \cdot \mathbf{n}_b)] \quad , \end{aligned} \tag{13.34}$$

where $\mathbf{n}_a$ and $\mathbf{n}_b$ are two unit vectors (for particles a and b, respectively), oriented along the directions of the quantization axes for which the eavesdropper acquired information about the spin component of a given particle. This information could be acquired either through a direct, "brute" measurement of the spin components or through a more subtle attack on the source, e.g., substituting a source that produces a state of two spin $\frac{1}{2}$ particles correlated with another quantum system on which the actual measurement will be performed by the eavesdropper. The normalized probability measure $\rho(\mathbf{n}_a, \mathbf{n}_b)$ describes the eavesdropper strategy (probability of intercepting a spin component along a given direction for a particular measurement). If only one particle (say, a) is exposed to the measurement performed by the eavesdropper along the direction $\mathbf{n}_a$, one may put $\mathbf{n}_b = -\mathbf{n}_a$ as a particular case in Eq. (13.34).

Simple calculation for a given orientation of $\mathbf{a}_1$, $\mathbf{a}_3$ or $\mathbf{b}_1$, $\mathbf{b}_3$ gives

$$S = \int \rho(\mathbf{n}_a, \mathbf{n}_b) \mathrm{d}\mathbf{n}_a \mathrm{d}\mathbf{n}_b [\sqrt{2}\mathbf{n}_a \cdot \mathbf{n}_b] \quad , \tag{13.35}$$

which implies

$$-\sqrt{2} \leq S \leq \sqrt{2} \quad , \tag{13.36}$$

and contradicts Eq. (13.33) for any strategy described by the measure $\rho(\mathbf{n}_a, \mathbf{n}_b)$. This way it has been shown that the generalized Bell's theorem can have a practical application in cryptography, namely, it can test the safety of the key distribution. It is not a mathematical difficulty of a particular computation, but a fundamental physical law that protects the system, and as long as quantum theory is not refuted as a complete theory the system is secure.

Regarding more refined attacks associated with the faked source of three (or more) correlated particles, one may think, for example, about delayed measurement on the third particle which is correlated with the two spin $\frac{1}{2}$ particles. By "delayed" it means "after the orientation of the analyzers has been publicly revealed by Alice and Bob." However, as we want the two particles to be in pure, singlet state, and Alice and Bob test for it through Bell's theorem, then we cannot correlate the third particle with the other two without disturbing the purity of the singlet state. Therefore it is likely that there is no universal (good for all orientations $\mathbf{a}_i$, $\mathbf{b}_j$ state of the faked source which will pass the statistical test of the legitimate users on the subsystem of the two correlated particles a and b. As Alice and Bob can also delay their public communication, the eavesdropper faces the problem of storing the third particle undisturbed for an appropriately long period of time.

The proposed channel can be realized as a modification of experiments that tested Bell's theorem. In particular, the celebrated experiment of Aspect and co workers[16], in which polarized photons were used instead of spin $\frac{1}{2}$ particles, would be the most obvious choice. In the experiment, every 10 ns pairs of photons were emitted in a radiative atomic cascade of calcium. Acousto-optical switches were used to change the orientation of the analyzers in a time short compared with the photon transit time, and the detection efficiency was over 95%. Apart from changing the main objective of the experiment, and some details in the setup, one will also need software to simulate Alice, Bob, and optionally the eavesdropper.

13.1.3 EPR photon-pair QKD system (BBM92)

13.1.3.A Basic principle

A slightly different way of producing a secret key using an EPR-Bell photon-pair is illustrated in Fig. 13.4. A photon-pair source is placed again at the midpoint of the transmission line and each photon of a pair is sent to Alice and Bob through a quantum channel. Let us consider a measurement performed by Alice, first. She can randomly choose the demodulation basis between the $H-V$ basis and the $R-L$ basis for each photon. Suppose Alice and Bob's photon are prepared in a singlet state,

$$\begin{aligned} |\psi_{ab}\rangle &= \frac{1}{\sqrt{2}}(|H\rangle_a |V\rangle_b - |V\rangle_a |H\rangle_b) \\ &= \frac{1}{\sqrt{2}}(|R\rangle_a |L\rangle_b - |L\rangle_a |R\rangle_b) \quad . \end{aligned} \tag{13.37}$$

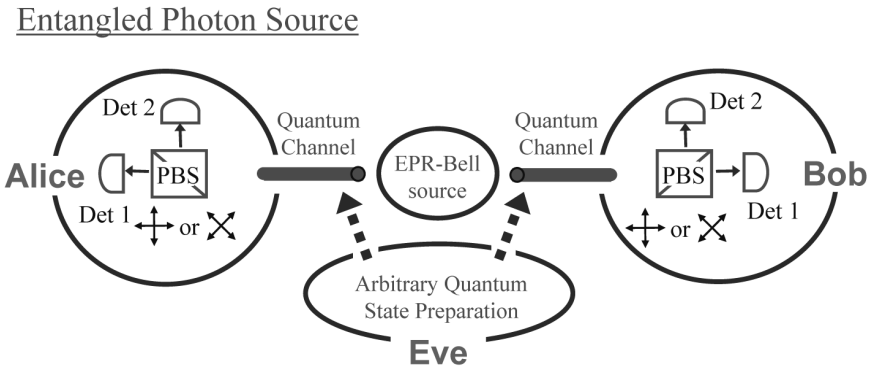

Figure 13.4:

Because of the entanglement, Bob's photon is always collapsed to the opposite and orthogonal polarization to the measured polarization of Alice's photon. In a sense Alice can prepare Bob's photon in one of the four polarization states which are not orthogonal with each other. This is the situation of BB84 protocol we studied already. Bob randomly chooses the demodulation basis between $H-V$ basis and $R-V$ basis. Alice and Bob publicly announce their bases and if they match, they know their results are completely anti-correlated (opposite) and keep the results as shifted keys. An actual timing of Alice and Bob's detection of a photon does not change the result.

Only difference and improvement of this new protocol compared to BB84 is that there is no definite polarization, namely a key does not exist in the transmission line. Rather it is created by the measurements. Therefore, Eve's photon splitting attack is irrelevant. A pure singlet state cannot be correlated to the third particle without losing its purity, so if Eve tries to extract a partial information about a photon-pair, it necessarily introduces a bit error between Alice and Bob.

13.1.3.B Security of a practical system

However, in a practical system, a bit error is caused by imperfection of the system components. This innocent bit error cannot be distinguished from the bit error caused by the Eve's dropping.

Let us consider an ideal EPR photon-pair source which emits one and only one photon-pair per pulse. The coincidence count probability is the sum of the true coincidence caused by a photon-pair and the false coincidence caused by detector dark count,

$$p_{\rm coin} = p_{\rm true} + p_{\rm false} \quad , \tag{13.38}$$

$$p_{\rm true} = T_x T_{L-x} = T \quad , \tag{13.39}$$

$$p_{\rm false} = 4T_x d + 4T_{L-x} d + (4d)^2 \quad , \tag{13.40}$$

where we assume dual fire events, $p_{\rm true} \cdot p_{\rm false}$, are negligible, and a source is located at a distance x from Alice and $L-x$ from Bob. The transmission coefficient is $T_x = 10^{-(\alpha x/10)}$ if the transmission loss is expressed in unit of dB/Km. The true coincidence count rate is

independent of the source location but the false coincidence count rate takes a minimum value, $8T_{\frac{L}{2}}d$, if the source is located at the mid-point. The bit error rate is

$$\varepsilon = \frac{\mu p_{\rm true} + \frac{1}{2}p_{\rm false}}{p_{\rm coin}} \quad , \tag{13.41}$$

where μ stands for imperfection of optical components. Eve can intercept one photon of the pair and resend a fake photon by taking advantage of this innocent bit errors. An amount of information leaked to Eve is represented by the collision probability,

$$p_c \leq \frac{1}{2} + 2\varepsilon - 2\varepsilon^2 \quad . \tag{13.42}$$

We can use privacy amplification after error correction to reduce Eve's information to a negligible level. This process decreases the key size according to

$$n - \tau = n\left[-\log_2 p_c - \frac{\kappa}{n}\right] - t - s \quad , \tag{13.43}$$

where $n = \frac{1}{2}Np_{\rm coin}$ is the length of an error corrected key, N is the total number of received pulses, κ represents an additional information leaked to Eve during error correction. Since the security parameter t and s can be chosen at least a logarithmic function of N, the final key generation rate is

$$R = \lim_{N\to\infty}\frac{n-\tau}{N} = \frac{p_{\rm coin}}{2}\left\{ -\log_2 p_c + f(\varepsilon)\Big[\varepsilon\log_2\varepsilon + (1-\varepsilon)\log_2(1-\varepsilon)\Big]\right\} \quad . \tag{13.44}$$

Figure 13.5 shows the numerical results for a BBM92 system with $d = 5\times10^{-8}$ and $\mu = 0.01$. Initially the performance is similar to a BB84 system with a single photon source but the cutoff loss due to the impact of a detector dark count is much more relaxed. This is because the error is caused only by the false coincidence for a BBM92 system, while it is caused by a single dark count for a BB84 system.

Let us consider next a more realistic Poissonian EPR photon-pair source, such as a parametric downconverter. The output of such a photon-pair source is not an EPR-Bell state Eq. (13.37) but is expressed as

$$|\psi_{ab}\rangle = \frac{1}{\cosh^2(\chi)}\sum_{n=0}^{\infty}\tanh^n(\chi)(|n\rangle_{aH}|0\rangle_{aV}|0\rangle_{bH}|n\rangle_{aV} - |0\rangle_{aH}|n\rangle_{aV}|n\rangle_{bH}|0\rangle_{bV}) \quad . \tag{13.45}$$

Here a parameter χ represents a downconversion efficiency determined by the second order nonlinearly of a crystal, pump power, interaction length and etc. This pure state is converted to the mixed state by a transmission loss:

$$\begin{aligned}\hat{\rho}_{ab} \;=\; & A\hat{\rho}_{\psi_{ab}} + B\hat{\rho}_0^a\otimes\hat{\rho}_0^b + C(\hat{\rho}_u^a\otimes\hat{\rho}_0^b + \hat{\rho}_0^a\otimes\hat{\rho}_u^b) + D\hat{\rho}_u^a\otimes\hat{\rho}_u^b \\ & +(1-A-B-2C-D)\hat{\rho}_D \quad ,\end{aligned} \tag{13.46}$$

where $\hat{\rho}_0 = |0\rangle\langle 0|$ is a vacuum state, $\hat{\rho}_u = \frac{1}{2}\hat{I}$ is an unpolarized state and $\hat{\rho}_D$ is the state where more than one photon in either a or b mode. The coefficients $A-D$ represent the

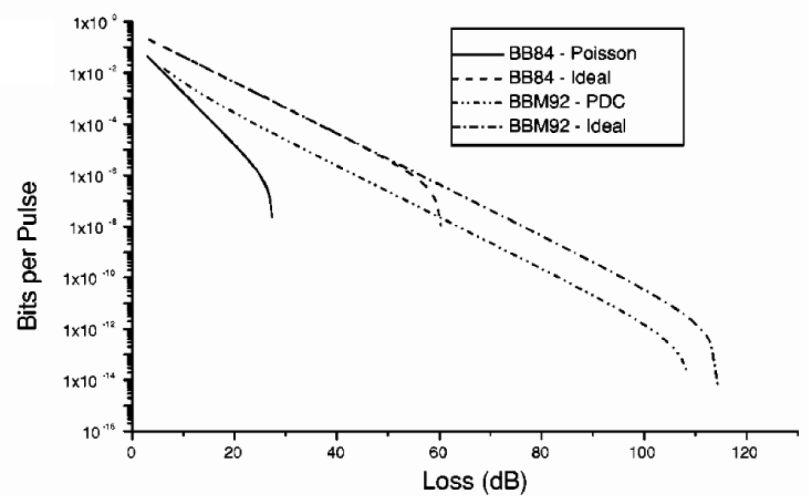

Figure 13.5:

true coincidence event, no detection event, one detection event and false coincidence event due to uncorrelated photons:

$$A = \frac{1}{\cosh^4\chi}\frac{2T_{L/2}^2\tanh^2\chi}{\left(1-\tanh^2\chi\left(1-T_{L/2}\right)^2\right)^4} \quad , \tag{13.47}$$

$$B = \frac{1}{\cosh^4\chi}\frac{1}{\left(1-\tanh^2\chi\left(1-T_{L/2}\right)^2\right)^2} \quad , \tag{13.48}$$

$$C = \frac{1}{\cosh^4\chi}\frac{2T_{L/2}\left(1-T_{L/2}\right)\tanh^2\chi}{\left(1-\tanh^2\chi\left(1-T_{L/2}\right)^2\right)^3} \quad , \tag{13.49}$$

$$D = \frac{1}{\cosh^4\chi}\frac{4T_{L/2}^2\left(1-T_{L/2}\right)^2\tanh^4\chi}{\left(1-\tanh^2\chi\left(1-T_{L/2}\right)^2\right)^4} \quad . \tag{13.50}$$

The true coincidence rate and false coincidence rate are respectively

$$p_{\text{true}} = A \quad , \tag{13.51}$$

$$p_{\text{false}} = (4d)^2B + 2(4d)C + D \quad . \tag{13.52}$$

Using these results in the previous equations, we can calculate the final key generation rate for this case by optimizing the downconversion efficiency χ for each channel loss. The result is shown in Fig. 13.5. Compared to the BB84 system with a Poissonian photon source, the final key generation rate is higher due to the absence of Eve's photon splitting attack[17].

13.2 Quantum teleportation[18]

The existence of long range correlations between Einstein-Podolsky-Rosen (EPR)[12, 13] pairs of particles raises the question of their use for information transfer. Einstein himself used the word "telepathically" in this context[19]. It is known that *instantaneous* information transfer is definitely impossible[20]. Here, we show that EPR correlations can nevertheless assist in the "teleportation" of an intact quantum state from one place to another, by a sender who knows neither the state to be teleported nor the location of the intended receiver.

Suppose one observer, whom we shall call "Alice", has been given a quantum system such as a photon or spin-$\frac{1}{2}$ particle, prepared in a state $|\phi\rangle$ unknown to her, and she wishes to communicate to another observer, "Bob", sufficient information about the quantum system for him to make an accurate copy of it. Knowing the state vector $|\phi\rangle$ itself would be sufficient information, but in general there is no way to learn it. Only if Alice knows beforehand that $|\phi\rangle$ belongs to a given orthonormal set can she make a measurement whose result will allow her to make an accurate copy of $|\phi\rangle$. Conversely, if the possibilities for $|\phi\rangle$ include two or more nonorthogonal states, then no measurement will yield sufficient information to prepare a perfectly accurate copy.

A trivial way for Alice to provide Bob with all the information in $|\phi\rangle$ would be to send the particle itself. If she wants to avoid transferring the original particle, she can make it interact unitarily with another system, or "ancilla", initially in a known state $|a_0\rangle$, in such a way that after the interaction the original particle is left in a standard state $|\phi_0\rangle$ and the ancilla is in an unknown state $|a\rangle$ containing complete information about $|\phi\rangle$. If Alice now sends Bob the ancilla (perhaps technically easier than sending the original particle), Bob can reverse her actions to prepare a replica of her original state $|\phi\rangle$. This "spin-exchange measurement"[21] illustrates an essential feature of quantum information: it can be swapped from one system to another, but it cannot be duplicated or "cloned"[22]. In this regard it is quite unlike classical information, which can be duplicated at will. The most tangible manifestation of the nonclassicality of quantum information is the violation of Bell's inequalities[14, 15] observed[23] in experiments on EPR states. Other manifestations include the possibility of quantum cryptography[6, 7, 11, 24, 25, 26, 27, 28], quantum parallel computation[2, 29, 30], and the superiority of interactive measurements for extracting information from a pair of identically prepared particles[31].

The spin-exchange method of sending full information to Bob still lumps classical and nonclassical information together in a single transmission. Below, we show how Alice can divide the full information encoded in $|\phi\rangle$ into two parts, one purely classical and the other purely nonclassical, and send them to Bob through two different channels. Having received these two transmissions, Bob can construct an accurate replica of $|\phi\rangle$. Of course Alice's original $|\phi\rangle$ is destroyed in the process, as it must be to obey the no-cloning theorem. We call the process we are about to describe teleportation, a term from science fiction meaning to make a person or object disappear while an exact replica appears somewhere else. It must be emphasized that our teleportation, unlike some science fiction versions, defies no physical laws. In particular, it cannot take place instantaneously or over a spacelike interval, because it requires, among other things, sending a classical message from Alice to Bob. The net result of teleportation is completely prosaic: the removal of $|\phi\rangle$ from Alice's hands and its appearance in Bob's hands a suitable time later. The only remarkable feature

is that, in the interim, the information in $|\phi\rangle$ has been cleanly separated into classical and nonclassical parts. First we shall show how to teleport the quantum state $|\phi\rangle$ of a spin-$\frac{1}{2}$ particle. Later we discuss teleportation of more complicated states.

The nonclassical part is transmitted first. To do so, two spin-$\frac{1}{2}$ particles are prepared in an EPR singlet state

$$\left|\Psi_{23}^{-}\right\rangle = \sqrt{\frac{1}{2}}(|\uparrow_2\rangle\,|\downarrow_3\rangle - |\downarrow_2\rangle\,|\uparrow_3\rangle) \quad . \tag{13.53}$$

The subscripts 2 and 3 label the particles in this EPR pair. Alice's original particle, whose unknown state $|\phi\rangle$ she seeks to teleport to Bob, will be designated by a subscript 1 when necessary. These three particles may be of different kinds, e.g., one or more may be photons, the polarization degree of freedom having the same algebra as a spin.

One EPR particle (particle 2) is given to Alice, while the other (particle 3) is given to Bob. Although this establishes the possibility of nonclassical correlations between Alice and Bob, the EPR pair at this stage contains no information about $|\phi\rangle$. Indeed the entire system, comprising Alice's unknown particle 1 and the EPR pair, is in a pure product state, $|\phi_1\rangle\left|\Psi_{23}^{(-)}\right\rangle$, involving neither classical correlation nor quantum entanglement between the unknown particle and the EPR pair. Therefore no measurement on either member of the EPR pair, or both together, can yield any information about $|\phi\rangle$. An entanglement between these two subsystems is brought about in the next step.

To couple the first particle with the EPR pair, Alice performs a complete measurement of the von Neumann type on the joint system consisting of particle 1 and particle 2 (her EPR particle). This measurement is performed in the Bell operator basis[32] consisting of $\left|\Psi_{12}^{(-)}\right\rangle$ and

$$\begin{aligned} \left|\Psi_{12}^{(+)}\right\rangle &= \sqrt{\tfrac{1}{2}}(|\uparrow_1\rangle\,|\downarrow_2\rangle + |\downarrow_1\rangle\,|\uparrow_2\rangle) \quad , \\ \left|\Phi_{12}^{(\pm)}\right\rangle &= \sqrt{\tfrac{1}{2}}(|\uparrow_1\rangle\,|\uparrow_2\rangle \pm |\downarrow_1\rangle\,|\downarrow_2\rangle) \quad . \end{aligned} \tag{13.54}$$

Note that these four states are a complete orthonormal basis for particles 1 and 2.

It is convenient to write the unknown state of the first particle as

$$|\phi_1\rangle = a\,|\uparrow_1\rangle + b\,|\downarrow_1\rangle \quad , \tag{13.55}$$

with $|a|^2 + |b|^2 = 1$. The complete state of the three particles before Alice's measurement is thus

$$\begin{aligned} |\Psi_{123}\rangle \;=\; & \frac{a}{\sqrt{2}}(|\uparrow_1\rangle\,|\uparrow_2\rangle\,|\downarrow_3\rangle - |\uparrow_1\rangle\,|\downarrow_2\rangle\,|\uparrow_3\rangle) \\ & + \frac{b}{\sqrt{2}}(|\downarrow_1\rangle\,|\uparrow_2\rangle\,|\downarrow_3\rangle - |\downarrow_1\rangle\,|\downarrow_2\rangle\,|\uparrow_3\rangle) \quad . \end{aligned} \tag{13.56}$$

In this equation, each direct product $|_1\rangle\,|_2\rangle$ can be expressed in terms of the Bell operator basis vectors $\left|\Phi_{12}^{(\pm)}\right\rangle$ and $\left|\Psi_{12}^{(\pm)}\right\rangle$, and we obtain

$$\begin{aligned} |\Psi_{123}\rangle \;=\; & \frac{1}{2}\left[\left|\Psi_{12}^{(-)}\right\rangle(-a\,|\uparrow_3\rangle - b\,|\downarrow_3\rangle) + \left|\Psi_{12}^{(+)}\right\rangle(-a\,|\uparrow_3\rangle + b\,|\downarrow_3\rangle)\right. \\ & \left. + \left|\Phi_{12}^{(-)}\right\rangle(a\,|\downarrow_3\rangle + b\,|\uparrow_3\rangle) + \left|\Phi_{12}^{(+)}\right\rangle(a\,|\downarrow_3\rangle - b\,|\uparrow_3\rangle)\right] \quad . \end{aligned} \tag{13.57}$$

It follows that, regardless of the unknown state $|\phi_1\rangle$, the four measurement outcomes are equally likely, each occurring with probability 1/4. Furthermore, after Alice's measurement, Bob's particle 3 will have been projected into one of the four pure states superposed in Eq. (13.57), according to the measurement outcome. These are, respectively,

$$\begin{aligned} -|\phi_3\rangle \equiv -\begin{pmatrix} a \\ b \end{pmatrix} \quad , \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} |\phi_3\rangle \quad , \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\phi_3\rangle \quad , \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} |\phi_3\rangle \quad . \end{aligned} \tag{13.58}$$

Each of these possible resultant states for Bob's EPR particle is related in a simple way to the original state $|\phi\rangle$ which Alice sought to teleport. In the case of the first (singlet) outcome, Bob's state is the same except for an irrelevant phase factor, so Bob need do nothing further to produce a replica of Alice's spin. In the three other cases, Bob must apply one of the unitary operators in Eq. (13.58), corresponding, respectively, 180° rotations around the z, x, and y axes, in order to convert his EPR particle into a replica of Alice's original state $|\phi\rangle$. (If $|\phi\rangle$ represents a photon polarization state, a suitable combination of half-wave plates will perform these unitary operations.) Thus an accurate teleportation can be achieved in all cases by having Alice tell Bob the classical outcome of her measurement, after which Bob applies the required rotation to transform the state of his particle into a replica of $|\phi\rangle$. Alice, on the other hand, is left with particles 1 and 2 in one of the states $\left|\Psi_{12}^{(\pm)}\right\rangle$ or $\left|\Phi_{12}^{(\pm)}\right\rangle$, without any trace of the original state $|\phi\rangle$.

Unlike the quantum correlation of Bob's EPR particle 3 to Alice's particle 2, the result of Alice's measurement is purely classical information, which can be transmitted, copied, and stored at will in any suitable physical medium. In particular, this information need not be destroyed or canceled to bring the teleportation process to a successful conclusion: The teleportation of $|\phi\rangle$ from Alice to Bob has the side effect of producing two bits of random classical information, uncorrelated to $|\phi\rangle$, which are left behind at the end of the process.

Since teleportation is a *linear* operation applied to the quantum state $|\phi\rangle$, it will work not only with pure states, but also with mixed or entangled states. For example, let Alice's original particle 1 be itself part of an EPR singlet with another particle, labeled 0, which may be far away from both Alice and Bob. Then, after teleportation, particles 0 and 3 would be left in a singlet state, even though they had originally belonged to separate EPR pairs.

All of what we have said above can be generalized to systems having $N > 2$ orthogonal states. In place of an EPR spin pair in the single state, Alice would use a pair of N-state particles in a completely entangled state. For definiteness let us write this entangle state as $\sum_j |j\rangle \otimes |j\rangle / \sqrt{N}$, where $j = 0, 1, \cdots, N-1$ labels the N elements of an orthonormal basis for each of the N-state systems. As before, Alice performs a joint measurement on particles 1 and 2. One such measurement that has the desired effect is the one whose eigenstates are $|\psi_{nm}\rangle$, defined by

$$|\psi_{nm}\rangle = \sum_j e^{2\pi i j n/N} |j\rangle \otimes |(j+m) \pmod N\rangle / \sqrt{N} \quad . \tag{13.59}$$

Once Bob learns from Alice that she has obtained the result nm, he performs on his previously entangled particle (particle 3) the unitary transformation

$$U_{nm} = \sum_k e^{2\pi ikn/N} \left|k\right\rangle \left\langle (k+m) \pmod N \right| \quad . \tag{13.60}$$

This transformation brings Bob's particle to the original state of Alice's particle 1, and the teleportation is complete.

The classical message plays an essential role in teleportation. To see why, suppose that Bob is impatient, and tries to complete the teleportation by guessing Alice's classical message before it arrives. Then Alice's expected $|\phi\rangle$ will be reconstructed (in the spin-$\frac{1}{2}$ case) as a random mixture of the four state of Eq. (13.58). For any $|\phi\rangle$, this is a maximally mixed state, giving no information about the input state $|\phi\rangle$. It could not be otherwise, because any correlation between the input and the guessed output could not be used to send a superluminal signal.

One may still inquire whether accurate teleportation of a two-state particle requires a full two bits of classical information. Could it be done, for example, using only two or three distinct classical messages instead of four, or four messages of unequal probability? Later we show that a full two bits of classical channel capacity are necessary. Accurate teleportation using a classical channel of any lesser capacity would allow Bob to send superluminal messages through the teleported particle, by guessing the classical message before it arrived.

Conversely one may inquire whether other states besides an EPR singlet can be used as the nonclassical channel of the teleportation process. Clearly any direct product state of particles 2 and 3 is useless, because for such states manipulation of particle 2 has no effect on what can be predicted about particle 3. Consider now a nonfactorable state $|\Upsilon_{23}\rangle$. It can be readily be seen that after Alice's measurement, Bob's particle 3 will be related to $|\phi_1\rangle$ by four fixed unitary operations if and only if $|\Upsilon_{23}\rangle$ has the form

$$\sqrt{\frac{1}{2}}(\left|u_2\right\rangle \left|p_3\right\rangle + \left|v_2\right\rangle \left|q_3\right\rangle) \tag{13.61}$$

where $\{\left|u\right\rangle, \left|v\right\rangle\}$ and $\{\left|p\right\rangle, \left|q\right\rangle\}$ are any two pairs of orthonormal states. These are maximally entangled states[32], having maximally random marginal statistics for measurements on either particle separately. States which are less entangled reduced the fidelity of teleportation, and/or the range of states $|\phi\rangle$ that can be accurately teleported. The states in Eq. (13.61) are also precisely those obtainable from the EPR singlet by a local one-particle unitary operation[33]. Their use for the nonclassical channel is entirely equivalent to that of the singlet Eq. (13.53). Maximal entanglement is necessary and sufficient for faithful teleportation.

Although it is currently unfeasible to store separated EPR particles for more than a brief time, if it becomes feasible to do so, quantum teleportation could be quite useful. Alice and Bob would only need a stockpile of EPR pairs (whose reliability can be tested by violations of Bell's inequality[23]) and a channel capable of carrying robust classical messages. Alice could then teleport quantum states to Bob over arbitrarily great distances, without worrying about the effects of attenuation and noise on, say, a single photon sent through a long optical fiber. As an application of teleportation, consider the problem investigated by Peres and Wootters[31], in which Bob already has another copy of $|\phi\rangle$. If

he acquires Alice's copy, he can measure both together, thereby determining the state $|\phi\rangle$ more accurately than can be done by making a separate measurement on each one. Finally, teleportation has the advantage of still being possible in situations where Alice and Bob, after sharing their EPR pairs, have wandered about independently and no longer know each others' locations. Alice cannot reliably send Bob the original quantum particle, or a spin-exchanged version of it, if she does not know where he is; but she can still teleport the quantum state to him, by broadcasting the classical information to all places where he might be.

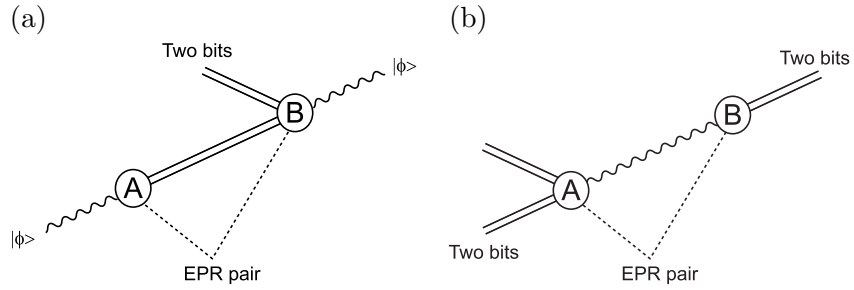

Figure 13.6: Spacetime diagrams for (a) quantum teleportation, and (b) 4-way coding[33]. As usual, time increases from bottom to top. The solid lines represent a classical pair of bits, the dashed lines an EPR pair of particles (which may be of different types), and the wavy line a quantum particle in an unknown state $|\phi\rangle$. Alice (A) performs a quantum measurement, and Bob (B) a unitary operation.

Teleportation resembles another recent scheme for using EPR correlations to help transmit useful information. In "4-way coding"[33] modulation of one member of an EPR pair serves to reliably encode a 2-bit message in the joint state of the complete pair. Teleportation and 4-way coding can be seen as variations on the same underlying process, illustrated by the spacetime diagrams in Fig. 13.6. Note that *closed loops* are involved for both processes. Trying to draw similar "Feynman diagrams" with tree structure, rather than loops, would lead to physically impossible processes.

On the other hand, more complicated closed-loop diagrams are possible, such as Fig. 13.7, obtained by substituting Fig. 13.6(a) into the wavy line of Fig. 13.6(b). This represents a 4-way coding scheme in which the modulated EPR particle is teleported instead of being transmitted directly. Two incoming classical bits on the lower left are reproduced reliably on the upper right, with the assistance of two shared EPR pairs and two other classical bits, uncorrelated with the external bits, in an internal channel from A' to B'. This diagram is of interest because it can be used to show that a full two bits of classical channel capacity are necessary for accurate teleportation of a two-state particle.

13.3 Quantum repeater[52]

In quantum communication via noisy channels, the error probability scales exponentially with the length of the channel. We present a scheme of a quantum repeater that overcomes

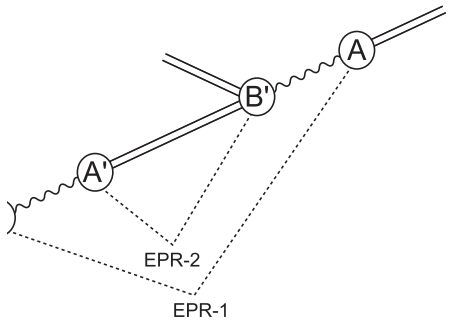

Figure 13.7: Spacetime diagram of a more complex 4-way coding scheme in which the modulated EPR particle (wavy line) is teleported rather than being transmitted directly. This diagram can be used to prove that a classical channel of two bits of capacity is necessary for teleportation. To do so, assume on the contrary that the teleportation from A' to B' uses an internal classical channel of capacity $C < 2$ bits, but is still able to transmit the wavy particle's state accurately from A' to B', and therefore still transmit the external two bit message accurately from B to A. The assumed lower capacity $C < 2$ of the internal channel means that if B' were to guess the internal classical message superluminally instead of waiting for it to arrive, his probability 2^{-C} of guessing correctly would exceed 1/4, resulting in a probability greater than 1/4 for successful superluminal transmission of the external two bit message from B to A. This in turn entails the existence of two distinct external two bit messages, r and s, such that $P(r|s)$, the probability of superluminally receiving r if s was sent, is less than 1/4, while $P(r|r)$, the probability of superluminally receiving r if r was sent, is greater than 1/4. By redundant coding, even this statistical difference between r and s could be used to send reliable superluminal messages; therefore reliable teleportation of a two state particle cannot be achieved with a classical channel of less than two bits of capacity. By the same argument, reliable teleportation of an N-state particle requires a classical channel of $2\log_2(N)$ bits capacity.

this limitation. The central idea is to connect a string of (imperfect) entangled pairs of particles by using a novel nested purification protocol, thereby creating a single distant pair of high fidelity. The scheme tolerates general errors on the percent level.

Quantum communication deals with the transmission and exchange of quantum information between distant nodes of a network. Remarkable experimental progress has been reported recently, for example, on secret key distribution for quantum cryptography[53, 54], teleportation of the polarization state of a single photon[55, 56], and the creation of entanglement between different atoms[57]. On the other hand, first steps towards the implementation of quantum logical operations, which are the building blocks of quantum computing, have been demonstrated[58, 59]. In view of this progress, it is not far-fetched to expect the creation of small quantum networks in the near future. Such networks will involve nodes, where qubits are stored and locally manipulated, and which are connected by quantum channels over which communication takes place by sending qubits. This will open the possibility for more complex activities such as multi-party communication and distributed quantum computing[60].

The bottleneck for communication between distant nodes is the scaling of the error probability with the length of the channel connecting the nodes. For channels such as

an optical fiber, the probability for both absorption and depolarization of a photon (i.e. the qubit) grows exponentially with the length l of the fiber. This has two effects: (i) to transmit a photon without absorption, the number of trials scales exponentially with l; (ii) even when a photon arrives, the fidelity of the transmitted state decreases exponentially with l. One may think that this last problem can be circumvented by standard purification schemes[40, 61, 62]. However, purification schemes require a certain minimum fidelity $F_{\min}$ to operate, which cannot be achieved as l increases. The distance between the nodes is thus essentially limited by the absorption length of the fiber[63].

In the context of fault-tolerant quantum computing[64], using concatenated quantum codes[65, 66, 67], Knill and Laflamme have discussed an important scheme that allows, in principle, to transmit a qubit over arbitrarily long distances with a polynomial overhead in the resources. The method requires to encode a single qubit into an entangled state of a large number of qubits, and to operate on this code repeatedly during the transmission process. The tolerable error probabilities for transmission are less than 10^{-2}, whereas for local operations they are less than 5×10^{-5}. This seems to be outside the range of any practical implementation in the near future.

We present a model of a *quantum repeater* that allows to create an entangled (EPR) pair over arbitrarily large distances with a polynomial overhead in the resources and with a tolerability of errors in the percent region. Once an EPR pair is created, it can be employed to teleport any quantum information[18, 38]. Our solution of this problem comprises three novel elements: (i) a method for creation of entanglement between particles at distant nodes, which uses auxiliary particles at intermediate "connection points" and a *nested purification protocol*; (ii) entanglement purification with imperfect means, including results for the maximum attainable fidelity $F_{\max}$ and the minimum required fidelity $F_{\min}$; (iii) a protocol for which the time needed for entanglement creation scales polynomially whereas the required material resources per connection point grow only logarithmically with the distance.

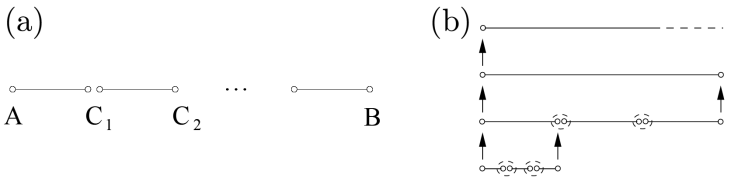

Figure 13.8: (a) Connection of a sequence of N EPR pairs. (b) Nested purification with repeated creation of auxiliary pairs.

In classical communication, the problem of exponential attenuation can be overcome by using repeaters at certain points in the channel, which amplify the signal and restore it to its original shape. Guided by these ideas, for quantum communication, we divide the channel into N segments with connection points (i.e. auxiliary nodes) in between. We then create N elementary EPR pairs of fidelity F_1 between the nodes A & C_1, C_1 & C_2, $\ldots C_{N-1}$ & B, as in Fig. 13.8(a). The number N is chosen such that $F_{\min} <$

$F_1 \underset{\sim}{<} F_{\max}$. Subsequently, we connect these pairs by making Bell measurements at the nodes C_i and classically communicating the results between the nodes as in the schemes for teleportation[18] and entanglement swapping[18, 68]. Unfortunately, with every connection the fidelity F' of the resulting pair will decrease: on the one hand, the connection process involves imperfect operations which introduce noise; on the other hand, even for perfect connections, the fidelity decreases. Both effects lead to an exponential decrease of the fidelity F_N with N of the final pair shared between A & B. Eventually, the value of F_N drops below $F_{\min}$ and therefore it will not be possible to increase the fidelity by purification (e.g. with the aid of many similar pairs that are constructed in parallel). The only way to circumvent this limitation is to connect a smaller number $L \ll N$ of pairs so that $F_L > F_{\min}$ and purification is possible. The idea is then to purify, connect the resulting pairs, purify again, and continue in the same vein. The way in which these alternating sequences of connections and purifications is done has to be properly designed so that the number of resources needed does not grow exponentially with N and thus with the length l of the channel ($N \propto l$).

The proposal, the *nested purification protocol*, consists of connecting and purifying the pairs simultaneously in the following sense. For simplicity, assume that $N = L^n$ for some integer n. On the first level, we simultaneously connect the pairs (initial fidelity F_1) at all the checkpoints except at $C_L, C_{2L}, \ldots, C_{N-L}$. As a result, we have N/L pairs of length L and fidelity F_L between A & C_L, C_L & C_{2L} and so on. To purify these pairs, we need a certain number M of copies that we construct in parallel fashion. We then use these copies on the segments A & C_L, C_L & C_{2L} etc., to purify and obtain one pair of fidelity $\geq F_1$ on each segment. This last condition determines the (average) number of copies M that we need, which will depend on the initial fidelity, the degradation of the fidelity under connections, and the efficiency of the purification protocol. The total number of elementary pairs involved in constructing one of the more distant pairs of length L is LM. On the second level, we connect L of these more distant pairs at every checkpoint C_{kL} ($k = 1, 2 \ldots$) except at $C_{L^2}, C_{2L^2}, \ldots, C_{N-L^2}$. As a result, we have N/L^2 pairs of length L^2 between A & C_{L^2}, C_{L^2} & C_{2L^2}, and so on of fidelity $\geq F_L$. Again, we need M parallel copies of these long pairs to repurify up to the fidelity $\geq F_1$. The total number of elementary pairs involved in constructing one pair of length L^2 is thus $(LM)^2$. We iterate the procedure to higher and higher levels, until we reach the n–th level. As a result, we have obtained a final pair between A & B of length N and fidelity $\geq F_1$. In this way, the total number R of elementary pairs will be $(LM)^n$. We can re-express this result in the form

$$R = N^{\log_L M + 1} \tag{13.62}$$

which shows that the resources grow polynomially with the distance N. A similar formula was obtained in [65, 66, 67] for the overhead required in propagating the concatenated quantum code. Note that R depends only on L and M. In order to evaluate M, we need to know the specific form of the error mechanisms involved in the purification and connections, which in turn depend on the specific physical implementation of the quantum network. In general, we have only limited knowledge of these details. In order to estimate M, we will choose a generic error model for imperfect operations and measurements.

We define *imperfect operations* on states of one or more qubits by the following maps

$$\rho \longrightarrow O_1\rho = p_1\rho_{\rm ideal} + \frac{1-p_1}{2}{\rm Tr}_1\{\rho\}\otimes I_1 \tag{13.63}$$

$$\rho \longrightarrow O_{12}\rho = p_2\rho_{\rm ideal} + \frac{1-p_2}{4}{\rm Tr}_{12}\{\rho\}\otimes I_{12} \quad , \tag{13.64}$$

the first of which describes an imperfect one-qubit operation on particle 1, and the second an imperfect two-qubit operation on particles 1 and 2. In these expressions, $\rho_{\rm ideal}$ is the state that results from an *ideal* operation, and I_1 and I_{12} denote unit operators on the subspace where the ideal operation acts. The quantities p_1 and p_2 measure the *reliability* of the operations. The expressions (13.63) and (13.64) describe a situation where we have no knowledge about the result of an error occuring during some operation ("white noise"), except that it happens with a certain probability $(1-p_j)$. An *imperfect measurement* on a single qubit in the computational basis is described by a POVM corresponding to

$$\begin{aligned} P_0^\eta &= \eta|0\rangle\langle 0| + (1-\eta)|1\rangle\langle 1| \quad , \\ P_1^\eta &= \eta|1\rangle\langle 1| + (1-\eta)|0\rangle\langle 0| \quad . \end{aligned} \tag{13.65}$$

The parameter η is a measure for the quality of the projection onto the basis states. For example, for the state $\rho = |0\rangle\langle 0|$ the measuring apparatus will give the wrong result ("1") with probability $1-\eta \geq 0$. A detailed discussion of this and more general models for imperfect operations will be given elsewhere[69]. With these error models we have a toolbox to analyze all the processes involved in the connection and purification procedures. For example, the Bell measurement required in the connection can be decomposed into a controlled-NOT (CNOT) operation, effecting e.g. $|0\rangle|0\rangle \pm |1\rangle|1\rangle \rightarrow (|0\rangle \pm |1\rangle)|0\rangle$, followed by two single-qubit measurements.

The basic elements of the nested purification protocol are: (i) pair connections; (ii) purification. In the following we analyze these elements using the error models introduced above. Assume now that all of the pairs in Fig. 13.8(a) are in Werner states (which can be achieved using depolarization[40]). Connecting L neighboring pairs as explained earlier, one obtains a new "L-pair" with fidelity

$$F_L = \frac{1}{4} + \frac{3}{4}\left(\frac{p_1p_2(4\eta^2-1)}{3}\right)^{L-1}\left(\frac{4F-1}{3}\right)^L \quad . \tag{13.66}$$

This formula describes an exponential decrease of the resulting fidelity, unless both the elementary pairs and all the operations involved in the connection process are perfect. There are several possibilities to do the purification, and we first generalize the scheme introduced by Bennett *et al.*[40] to the case of imperfect gate and measurement operations. In short, the scheme takes two adjacent L-pairs of fidelity F, performs local (1 & 2-bit) operations on the particles at the same ends of the pairs, and obtains with a certain probability $p_{\rm succ}$ a new pair of fidelity

$$F' = \frac{[F^2+(\frac{1-F}{3})^2][\eta^2+(1-\eta)^2] + [F(\frac{1-F}{3})+(\frac{1-F}{3})^2)][2\eta(1-\eta)] + (\frac{1-p_2^2}{8p_2^2})}{[F^2+\frac{2}{3}F(1-F)+\frac{5}{9}(1-F)^2][\eta^2+(1-\eta)^2] + [F(\frac{1-F}{3})+(\frac{1-F}{3})^2)][8\eta(1-\eta)] + 4(\frac{1-p_2^2}{8p_2^2})} .$$

(13.67)

The value of $p_{\rm succ}$ is given by the denominator of this expression. For perfect operations, $\eta = 1$ and $p_2 = 1$, (13.67) reduces to the formula given in Ref. [40].

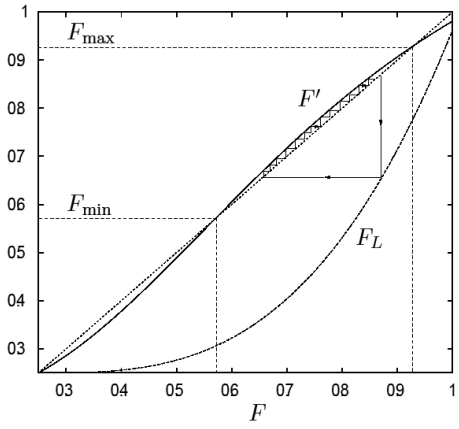

Figure 13.9: 'Purification loop' for connecting and purifying EPR pairs. Parameters are $L = 3$, $\eta = p_1 = 1$, and $p_2 = 0.97$.

Figure 13.9 shows the curves for connection (13.66) and purification (13.67) for a certain set of parameters. The purification curve has two intersection points with the diagonal, which are the fix points of the map (13.67). The upper point, $F_{\rm max} < 1$ is an attractor and gives the maximum value of the fidelity beyond which no pair can be purified. Note also the existence of the minimum value $F_{\rm min} > 1/2$. Together, they define the interval within which purification is possible. The connection curve, which looks like a simple power in Fig. 13.9, stays below the diagonal for all values of F between $1/4$ and 1. The offset of this curve at $F = 1$ from the ideal value $F' = 1$ quantifies the amount of noise that is introduced through imperfect operations in the connection process.

With the above results, we can now analyze the nested purification protocol. Let us consider a given level k in this protocol, where we have N/L^{k-1} pairs of fidelity F each. The two-step process connection–purification can now be visualized as follows (see Fig. 13.9). Starting from F, the fidelity F_L after connecting L pairs can be read off from the curve below the diagonal. Reflecting this value back to the diagonal line, as indicated by the arrows in Fig. 13.9, sets the starting value for the purification curve. If F_L lies within the purification interval, then iterated application of (13.67) leads back to the initial value F (staircase). Once the initial value F is reobtained, we have N/L^k pairs and we can start with the level $k + 1$. In summary, each level in the protocol corresponds to one cycle in Fig. 13.9. Note that if, in the loop, $F_L \leq F_{\rm min}$ then purification is not possible. Being polynomial in L, the lower curve gets steeper and steeper near $F = 1$ for higher values of L. From this, one sees that for a given starting fidelity F, there is a maximum number of pairs one can connect before purification becomes impossible.

For the resources we obtain $M = \prod_m^{m_{\rm max}} 2/p_{\rm succ}^{(m)}$ where $p_{\rm succ}^{(m)}$ is the probability for

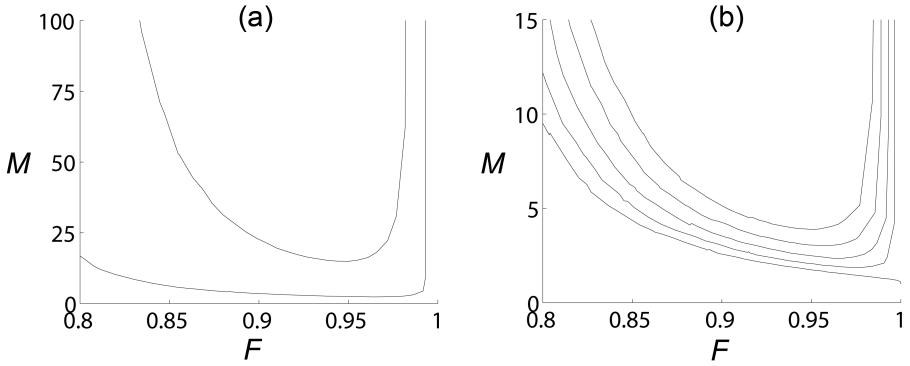

Figure 13.10: M (see text) versus working fidelity F. (a) Realization of the repeater with the aid of the purification schemes of Refs. [40] (upper curve) and [61] (lower curve). The error probabilities of all operations are 0.5% (error parameters 0.995), and $L = 2$. (b) Lower curve in (a) for different error probabilities. From bottom to top: 0%, 0.25%, 0.5%, 0.75%, 1%.

increasing the fidelity in the m-th purification step. The total number of steps, $m_{\max}$, is the same as in the staircase of Fig. 13.9.

In Fig. 13.10(a), M is plotted against the working fidelity F. Due to the discrete nature of the purification process, the fidelity of the repurified pairs need not be exactly the same on each nesting level. The working fidelity is thus defined as the fidelity maintained *on average* when going through different nesting levels. The error parameters for this plot are $\eta = p_1 = p_2 = 0.995$. One can see that there exists an optimum working fidelity of about 0.94 which requires a minimum number of about 15 resources.

A purification protocol that converges faster and therefore involves less parallel channels was proposed by Deutsch *et al.*[61]. We have employed this protocol, using imperfect operations (13.63)–(13.65). As is demonstrated in Fig. 13.10(a), M can be reduced by a factor of the order of 10. Since this number has to be taken to the n-th power, this reduces the number of total resources by many orders of magnitude, as is discussed in Table 13.1. In Fig. 13.10(b), M is plotted versus the working fidelity for different error parameters. One can see that for errors in the one-per-cent region, a working fidelity can be maintained with on average 5 L-pairs on each nesting level. We note that the procedure also works for error probabilities up to about 3%, but the number of purification resources gets larger.

In the remainder of this section we study a protocol for which the resources grow only logarithmically with the distance, whereas the total *time* needed for building the pair scales polynomially. Imagine that we purify a pair not with the help of M copies, but instead with one auxiliary pair of constant fidelity π_0 that is repeatedly created at each purification step. The purification with the help of such a pair leads to a maximum achievable fidelity $F_{\max}(\pi_0)$ that depends on the value of π_0 and, more generally, on the state of the auxiliary pair. This purification method is a variant of the standard schemes[40, 61], with the important difference that the purification limit $F_{\max}$ for this method is usually smaller than for the destillation method. In the context of the repeater protocol, it is

	Continental scale		Intercontinental scale	
	resources	time $[s]$	resources	time $[s]$
A	$1.58 * 10^9$	$3.88 * 10^{-2}$	$9.01 * 10^{12}$	0.298
B	329	$1.34 * 10^{-2}$	4118	0.103
C	7	0.241	10	3.275

Table 13.1: Parallel resources M^n and time T needed for creating a distant EPR pair via optical fibers (see text). Continental scale means $2^7 = 128$ segments, intercontinental scale means $2^{10} = 1024$ segments. Error parameters are $\eta = p_1 = p_2 = 0.995$. For (C), the resources grow only logarithmically, i.e. $M^n = n + 1$.

therefore not a priori clear whether the fidelity that is lost by the connection process can be regained with this variant of the purification method.

When connecting L pairs of fidelity F as in Fig. 13.8(b), we obtain a resulting L-pair of fidelity $\pi_0 \equiv F_L$. In the first step, this pair is swapped to two auxiliary particles at the ends of the L-pair, as indicated by the arrows in Fig. 13.8(b). In the next step, an L-pair of fidelity π_0 is again created by using the same string of particles as before, which is now used to purify the pair stored between the auxiliary particles. This procedure can be iterated and thus the stored pair be purified back to the fidelity F *given that* the purification condition $F_{\max}(F_L) > F$ is satisfied. If this is the case, then the same procedure can be applied at higher levels, thereby purifying correlations between more and more distant particles as indicated in Fig. 13.8(b). We find that the scheme of Ref. [40] does not satisfy this condition, whereas the scheme of Ref. [61] generally does.

In Table 13.1, the total time T and the resources M^n needed to maintain (or distribute) a fidelity of 96% over a typical "continental" (1280km) and "intercontinental" (10240km) distance are listed. We compare three situations, when the purification part of the repeater protocol is realized by (A) the scheme of Bennett *et al.*[40], (B) the scheme of Deutsch *et al.*[61], and (C) using an auxiliary pair of constant fidelity as described above. In calculating T, two time scales enter: The time τ_{op} needed for a local operation and measurement, and the time τ_{comm} needed to communicate measurement results between the nodes. The time for creating an elementary pair depends both on τ_{op} and τ_{comm}, and on the specific physical implementation[70]. To estimate orders of magnitude, we assume that $\tau_{\text{op}} = 10^{-5}s$ and that the repeaters are placed at distances of 10km, corresponding to the absorption length of standard optical fibers. For the time needed to create an elementary pair we have used the model of the photonic channel[71, 72] which gives a typical value of 3×10^{-4}s. These results demonstrate that the new scheme for a quantum repeater allows quantum communication over distances much longer than the absorption length.

Bibliography

[1] C. E. Shannon, *Bell Syst. Tech. J.* **28**, 656 (1949).

[2] D. Deutsch, *Proc. R. Soc. London A* **400**, 97 (1985).

[3] D. Deutsch, *Proc. Roy. Soc. London A* **425** , 73 (1989).

[4] C. H. Bennett, G. Brassard, *SIGACT News* **20**, 78 (1989).

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *J. Cryptology* **5**, 3 (1992).

[6] S. Wiesner, *SIGACT News* **15**, 78 (1983).

[7] C. H. Bennett, G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.

[8] M. N. Wegman, J. L. Carter, *J. Comput. Syst. Sci.* **22**, 256 (1981).

[9] G. Brassard and L. Salvail, Eurocrypt '93, vol. 765, ed. by T. Hellseth (Springer, Berlin, 1994), p. 410.

[10] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, *IEEE Trans. Inform. Theory* **41**, 1915 (1995).

[11] A. K. Ekert, *Phys. Rev. Lett.* **68**, 661 (1991).

[12] A. Einstein, B. Podolsky, *N. Rosen, Phys. Rev.* **47**, 777 (1935).

[13] D. Bohm, *Quantum Theory* (Prentice Hall, Englewood Cliffs, NJ, 1951).

[14] J. S. Bell, *Physics* (Long Island City, N.Y.) **1**,195 (1965).

[15] J. Clauser, M. Horne, A. Shimony, R. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).

[16] A. Aspect, P. Grangier, G. Roger, *Phys. Rev. Lett.* **49**, 91 (1982); A. Aspect, J. Dalibard, G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982).

[17] E. Waks, A. Zeevi and Y. Yamamoto, *Phys. Rev. A* **65**, 052310 (2002).

[18] C. H. Bennett, C. H. Brassard, C. Crepeau, R. Josza, A. Peres, W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).

[19] A. Einstein, in Albert Einstein, *Philosopher Scientist*, edited by P. A. Schilpp (Library of Living Philosophers, Evanston, 1949) p. 85.

[20] A. Shimony, in , *Proceedings of the International Symposium on Foundations of Quantum Theory* (Physical Society of Japan, Tokyo, 1984).

[21] J. L. Park, *Found. Phys.* **1**, 23 (1970).

[22] W. K. Wootters, W. H. Zurek, *Nature* **299**, 802 (1982).

[23] A. Aspect, J. Dalibard, G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982); Y. H. Shih, C. C. O. Alley, *Phys. Rev. Lett.* **61**, 2921 (1988).

[24] C. H. Bennett, G. Brassard, N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).

[25] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).

[26] A. K. Ekert, J. G. Rarity, P. R. Tapster, G. M. Palma, *Phys. Rev. Lett.* **69**, 1293 (1992).

[27] C. H. Bennett, G. Brassard, C. Crepeau, M.-H. Skubiszewska, *Advances in Cryptology Crypto '91 Proceedings*, August 1991 (Springer, New York, 1992), p. 351.

[28] G. Brassard, C. Crepeau, *Advances in Cryptology Crypto '90 Proceedings*, August 1990 (Springer, New York, 1991), p. 49.

[29] D. Deutsch, R. Jozsa, *Proc. R. Soc. London A* **439**, 553 (1992).

[30] A. Berthiaume, G. Brassard, in *Proceedings of the Seventh Annual IEEE Conference on Structure in Complexity Theory*, Boston, June 1992, (IEEE, New York, 1989), p. 132.

[31] A. Peres, W. K. Wootters, *Phys. Rev. Lett.* **66**, 1119 (1991).

[32] S. L. Braunstein, A. Mann, M. Revzen, *Phys. Rev. Lett.* **68**, 3259 (1992).

[33] C. H. Bennett, S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).

[34] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, *Phys. Rev. A* **78**, 3217 (1997).

[35] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory, Lecture Notes in Physics*, vol. 190 (Springer, Berlin, 1983).

[36] B. Schumacher, *Phys. Rev. A* **54**, 2614 (1996); B. Schumacher, M. D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).

[37] R. Jozsa, B. Schumacher, *J. Mod. Opt.* **41**, 2343, (1994); R. Jozsa, *J. Mod. Opt.* **41**, 2315 (1994).

[38] C. H. Bennett, D. V. DiVincenzo, J. A. Smolin, W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).

[39] M. Grassl, T. Beth, T. Pellizzari, *Phys. Rev. A* **56**, 33 (1997).

[40] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

[41] A. Ekert, C. Macchiavello, *Phys. Rev. Lett.* **77**, 2585 (1996).

[42] E. Knill, R. Laflamme, *Phys. Rev. A* **55**, 900 (1997).

[43] P. W. Shor, J. A. Smolin, *quant-ph/9604006.*

[44] cf. [38] section V.B where it is shown that capacity cannot be superadditive for convex combinations of a noisy with a noiseless channel.

[45] cf. [38] section III.B.3. These are identical to random linear stabilizer codes; see [50] and references therein.

[46] A. S. Kholevo, *Probl. Inf. Transm.* (USSR) **9**,177 (1973).

[47] C. H. Bennett, C. A. Fuchs, J. A. Smolin, *quant-ph/9611006.*

[48] A. S. Holevo, *IEEE Trans. on Info. Theory* **44**, 269 (1998).

[49] B. Schumacher, M. A. Nielsen, *Phys. Rev. A* **54**, 2629 (1996).

[50] E. Rains, *IEEE Trans. on Information Theory* **45**, 2361 (1999).

[51] R. J. McEliece, E. R. Rodernich, H. C. Rumsey, L. R. Welch, *IEEE Trans. on Info. Theory* **23**,157 (1977).

[52] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **28**, 5932 (1998).

[53] W. Tittel, J. Brendel, H. Zbinden, N. Gisin, *Phys. Rev. Lett.* **81**, 3563 (1998).

[54] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, C. M. Simmons, *Phys. Rev. Lett.* **81**, 3283 (1998).

[55] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, *Nature* **390**, 575 (1997).

[56] D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, *Phys. Rev. Lett.* **80**, 1121 (1998).

[57] E. Hagley, X. Maitre, C. Nogues, C. Wunderlich, M. Brune, J. M. Raimond, S. Haroche, *Phys. Rev. Lett.* **79**, 1 (1997).

[58] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, D. J. Wineland, *Phys. Rev. Lett.* **75**, 4714 (1995).

[59] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, H. J. Kimble, *Phys. Rev. Lett.* **75**, 4710 (1995).

[60] L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).

[61] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

[62] N. Gisin, *Phys. Lett. A* **210**, 151 (1996).

[63] For standard optical fibers, this length is typically 10km (see [53]).

[64] P. Shor, *quant-ph/9605011*; A. M. Steane, *Phys. Rev. Lett.* **78**, 2252 (1997).

[65] E. Knill, R. Laflamme, E. Knill, R. Laflamme, W. Zurek, *Science* **279**, 342 (1998).

[66] D. Aharonov, M. Ben-Or, *quant-ph/9611025.*

[67] A. Yu. Kitaev, *Russ. Math. Surv.* **52**, 1191 (1997).

[68] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287(1993).

[69] G. Giedke, H. Briegel, J. I. Cirac, P. Zoller, *Phys. Rev. A* **59**, 2641 (1999).

[70] W. Dür, H. -J. Briegel, J. I. Cirac, P. Zoller, *Phys. Rev. A* **59**, 169 (1999).

[71] S. J. van Enk, J. I. Cirac, P. Zoller, *Science* **279**, 205 (1998).

[72] S. J. van Enk, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **78**, 4293 (1997).