VII. TRANSMISSION AND CRYPTOGRAPHY USING QUANTUM RESOURCES

In this chapter we will discuss some tasks which cannot be performed classically but which can be performed quantum mechanically and vice versa.

A. Mission: impossible — The no-cloning theorem

In the classical world of our everyday work we take the possibility of copying something for granted: we distribute copies of our research papers to our colleagues and we (hopefully) make backup copies of our important data files on a regular basis. In Chap. II we discussed possibilities to copy classical bits, using either the classical irreversible NAND/NOT gate, or the reversible classical CNOT gate with the target bit initialized to zero:

$$(x, y) \longrightarrow (x,\ \text{XOR}\ y) \Longrightarrow (x, 0) \longrightarrow (x, x).$$

Obviously the quantum CNOT gate performs exactly the same operation on the input states $|0\rangle$ and $|1\rangle$:

$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle \quad ; \quad |1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$$

So, where is the problem?
As soon as you initialize qubit 1 to a state

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

you see that CNOT maps

$$|\psi\rangle|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle \longrightarrow \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq |\psi\rangle|\psi\rangle,$$

because $|\psi\rangle|\psi\rangle$ contains "mixed terms" $|0\rangle|1\rangle$ and $|1\rangle|0\rangle$.
This example shows that it may be possible to copy every member of a finite set of mutually orthogonal quantum states, but *not* every superposition of these states. The ability of copying classical states may thus be interpreted as the ability to copy special quantum states.
In general it is not possible to make a copy (or clone) of an *unknown* (pure) quantum state by means of *unitary* operations. This is the famous "no-cloning theorem" of Wootters and Zurek [35] and also Dieks [36]. The proof is amazingly simple. Let $|\psi\rangle$ be a pure state from some Hilbert space $\mathcal{H}_{\text{source}}$, and $|s\rangle$ some "standard" (initial) state from a Hilbert space $\mathcal{H}_{\text{target}}$ which has the same structure as $\mathcal{H}_{\text{source}}$. A "quantum state cloner" would then be a unitary operator $\mathbf{U}$ (defined on the direct product $\mathcal{H}_{\text{source}} \otimes \mathcal{H}_{\text{target}}$) with the property

$$\mathbf{U}|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle \quad \forall|\psi\rangle \in \mathcal{H}_{\text{source}}.$$

Now consider the cloning of a second state $|\phi\rangle$:

$$\mathbf{U}|\phi\rangle|s\rangle = |\phi\rangle|\phi\rangle.$$

For simplicity assume that $|\psi\rangle$, $|\phi\rangle$, and $|s\rangle$ are normalized. Take the scalar product of the two equations above and keep in mind that $\mathbf{U}$ is unitary, that is, it preserves scalar products:

$$\left(\langle s|\langle\psi|\mathbf{U}^\dagger\right)\left(\mathbf{U}|\phi\rangle|s\rangle\right) = \langle s|s\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle$$

$$= \left(\langle\psi|\langle\psi|\right)\left(|\phi\rangle|\phi\rangle\right) = \left(\langle\psi|\phi\rangle\right)^2$$

and this is possible only if $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$, that is, if the two states to be copied by the same operation are either identical or orthogonal. This proves the theorem.
Several questions arise regarding the assumptions of the theorem:

- Can we allow non-unitary cloning operations? A possible idea might be to enlarge the Hilbert space by taking into account the environment's Hilbert space. It is easy to see (exercise for the reader) that this idea leads to the same problems as above.
- Can mixed states be cloned?
- Are less than perfect copies possible and useful?

All these questions have been addressed in the research literature, pointers to which can be found, for example, on p. 604 of Ref. 3.
The no-cloning theorem may be considered an obstacle in quantum computation, where it would be desirable to "store a copy in a safe place". It should be noted, however, that the theorem is at the very heart of the concept of secure quantum communication to be discussed later.

B. Beam it up, Scotty — Quantum teleportation

We may be unable to give a *copy* of a quantum state to a friend, but under certain circumstances we are able to transmit some classical information to our friend which allows him or her to prepare precisely the state that we originally had. Our state will then be destroyed, of course, because otherwise we would have been able to violate the no-cloning theorem. A necessary resource for this teleportation of an unknown state is entanglement, that is, both partners must share among them two qubits (in the simplest case) in an entangled state. Quantum teleportation was discovered 1993 by Bennett et al. [37] and is, again, surprisingly simple.
Let Alice be in possession of a qubit in the state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

(Of course she does not *know* α and β, otherwise the problem would be trivial.) Furthermore Alice and Bob share an EPR pair

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

where Alice can manipulate only the first qubit and Bob only the second one. The initial state of the combined three-qubit system thus is

$$|\psi\rangle|\phi\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right].$$

Alice now applies $\mathbf{H}_1$ CNOT $_{12}$ where the indices refer to the qubits numbered from left to right, to obtain the state (Hadamard gate: $\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$)

$$\mathbf{H}_1 \text{ CNOT }_{12}|\psi\rangle|\phi\rangle = \mathbf{H}_1\frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

$$= \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right] = \ldots$$

We rewrite this state in order to bring out clearly what has happened on Bob's end

$$\ldots = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

$$= \frac{1}{\sqrt{2}}\left[|00\rangle|\psi\rangle + |01\rangle\mathbf{X}_3|\psi\rangle + |10\rangle\mathbf{Z}_3|\psi\rangle + |11\rangle\underbrace{(-i\mathbf{Y}_3)}_{\mathbf{X}_3\mathbf{Z}_3}|\psi\rangle\right].$$

Recall

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i\mathbf{Z}\mathbf{X} = i\mathbf{X}\mathbf{Z}.$$

Evidently Bob now possesses a superposition of four distorted variants of Alice's original state. Alice now performs a measurement on the two qubits 1,2 to which she has access. She obtains one of the four combinations $|M_1M_2\rangle(M_1, M_2 = 0, 1)$ with equal probabilities. After the measurement the state of the complete system has been projected to

$$|M_1M_2\rangle\mathbf{X}_3^{M_2}\mathbf{Z}_3^{M_1}|\psi\rangle$$

so that Bob *possesses a definite modification of the desired state* $|\psi\rangle$, *but he does not yet know which one*! To let him know, Alice transmits the two classical bits (M_1, M_2) through a classical channel. The transmission through the classical channel is limited by the special theory of relativity and prevents superluminal communication, or, as Einstein put it, "spukhafte Fernwirkungen" (spooky actions at a distance). Bob then applies to his qubit the operator

$$\mathbf{Z}_3^{M_1}\mathbf{X}_3^{M_2} = (\mathbf{X}_3^{M_2}\mathbf{Z}_3^{M_1})^{-1}$$

and can enjoy the state $|\psi\rangle$ which is now in his possession, while Alice's original qubit is in the state $|M_1\rangle$. It is important to note that in this process neither matter nor energy were transported "explicitly", only two classical bits. Surprisingly enough these two classical bits were sufficient to reconstruct on Bob's side the state $|\psi\rangle$ which contains two real numbers' worth of information (one amplitude, one phase, assuming normalization), that is, "infinitely more" than was transmitted. This points out very clearly how powerful a resource a shared EPR pair is. On the other hand, the necessity to have a shared EPR pair for every qubit (or electron, nucleon) to be teleported makes it very clear that we are still quite far away from any kind of "beam me up, Scotty" scenario. Nevertheless, single qubits have been successfully teleported in more than one laboratory, using optical and NMR techniques. References to those experiments (and to critical comments on them) can be found in [7] and in [3], p. 59.

C. (Super-) Dense coding

This was discovered by Bennett and Wiesner in 1992 [38]. In a sense, it is the inverse process of teleportation: Alice and Bob share an EPR pair and can transmit two classical bits by a single qubit. It is difficult to implement and it is not important as a means of practical fast communication. However, it demonstrates the possibility of secure communication, as we shall see.
Again Alice and Bob are supposed to share the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

(By the way, there is no need for any prior direct communication between Alice and Bob: they could have obtained their respective qubits from an "EPR pair

distribution agency".) Now, if Alice wants to send the two classical bits (M_1, M_2) to Bob, she applies $\mathbf{X}_1^{M_1}\mathbf{Z}_1^{M_2}$ (to the only qubit accessible to her, that is, qubit 1). This yields

$$\begin{aligned}
|\phi_{00}\rangle &:= \mathbf{X}_1^0\mathbf{Z}_1^0|\phi\rangle = |\phi\rangle \\
|\phi_{10}\rangle &:= \mathbf{X}_1^1\mathbf{Z}_1^0|\phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\
|\phi_{01}\rangle &:= \mathbf{X}_1^0\mathbf{Z}_1^1|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\phi_{11}\rangle &:= \mathbf{X}_1^1\mathbf{Z}_1^1|\phi\rangle = -i\mathbf{Y}_1|\phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle).
\end{aligned}$$

Then Alice transmits her qubit to Bob. Note that the four states on the right hand side are an orthonormal set (the Bell basis which we encountered already in chapter IV) and thus can be distinguished by an appropriate measurement. Here is what Bob might do: First apply $\mathrm{CNOT}_{(12)}$ and then measure the target bit 2. This yields

$$\begin{aligned}
\mathrm{CNOT}\ |\phi_{00}\rangle &\sim |10\rangle + |00\rangle \longrightarrow 0 \\
\mathrm{CNOT}\ |\phi_{10}\rangle &\sim |11\rangle + |01\rangle \longrightarrow 1 \\
\mathrm{CNOT}\ |\phi_{01}\rangle &\sim |00\rangle - |10\rangle \longrightarrow 0 \\
\mathrm{CNOT}\ |\phi_{11}\rangle &\sim |11\rangle - |01\rangle \longrightarrow 1.
\end{aligned}$$

Obviously this yields the first classical bit M_1 transmitted by Alice. The second qubit now has been used up in the measurement. The remaining classical bit is obviously equivalent to the sign in the four superpositions above; this can be decoded by applying the Hadamard gate $\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z})$ to the remaining qubit and then measuring it :

$$\mathbf{H}(|1\rangle + |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle - |1\rangle + |0\rangle) \sim |0\rangle$$

(for $|\phi_{00}\rangle$ and $|\phi_{10}\rangle$),

$$\pm\mathbf{H}(|0\rangle - |1\rangle) = \pm\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle + |0\rangle + |1\rangle) \sim |1\rangle.$$

Experimentally this has been implemented by both optical and NMR techniques, see [7] for the references. Now, what about Eve the eavesdropper, that is, is this procedure secure? Note that, regardless of the classical bit sequence to be encoded, the state of qubit 1 (which Eve may intercept and measure) is $|0\rangle$ or $|1\rangle$ with equal probability so that Eve gets no informations whatsoever. Formally inclined readers may convince themselves that the reduced density matrix (see chapters I and IV) of the state intercepted by Eve does not depend on the classical bits to be transmitted. This leads us straight to the last topic of this chapter.

D. Look who's talking — Secure communication

Secure communication is a field where quantum mechanics may contribute in several ways to create or destroy security. Here our discussion will be restricted to the case where quantum mechanics helps to make secure communication possible, that is, *quantum key distribution*. We will later learn how quantum mechanics may help to break classical codes by Shor's algorithm.

A *key* is a (random) sequence of (classical) bits $\{k_i\}(i = 1, \ldots, N)$ which Alice uses to encode the N-bit *message* $\{m_i\}$ and transform it to the *code* $\{c_i\}$ by

$$c_i = k_i \oplus m_i = k_i \text{ XOR } m_i = (k_i + m_i) \bmod 2.$$

Bob can decipher the code if he possesses the key:

$$m_i = c_i \oplus k_i$$

as can be easily verified for all four possible combinations (k_i, m_i).

This method of encoding is only safe if the key is used only once. If two messages m and m' are encoded with the same key the codes c and c' can be intercept ed and as

$$c_i \oplus c_i' = m_i \oplus m_i'$$

the deliberate irregularities introduced by encoding can be eliminated. Subsequently standard correlation analyses can be applied in an attempt to separate m from m'. Given this situation there is obviously a need to distribute fresh keys among Alice and Bob. Quantum key distribution serves that purpose. There exist several schemes or "protocols" to do this quantum mechanically, see [7]. Here we will discuss only two schemes which are closely related to each other.

First we discuss the 4-state protocol known as BB84 [39]. This protocol uses four pairwise orthogonal states

$$|0\rangle, |1\rangle, |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

which can be easily prepared as linearly polarized photons with $\vec{E}$ along $\hat{x}$, $\hat{y}$, and $\hat{x} \pm \hat{y}$. Measurements are performed with linear polarizers along these directions, and detectors. A photon polarized along $\hat{x}$ passes through a polarizer along $\hat{x}$ and is detected, one along $\hat{y}$ is not. To get an unambiguous result the observer must know *that* a photon should be coming along his way and that it is polarized *either* along $\hat{x}$ *or* along $\hat{y}$. A photon polarized along one of the diagonal directions $\hat{x} \pm \hat{y}$ will not yield any information when analyzed with a polarizer along $\hat{x}$, because both possibilities will give a signal in half of all cases.

Alice prepares $2n$ qubits randomly in one of the four states. Each qubit i contains two classical bits, namely

- $b_{p,i}$ telling which basis, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, was used to prepare the state, and
- $s_{p,i}$ telling which state (1st or 2nd) of the given basis was prepared.

Bob (ideally) receives all these qubits and measures them, randomly switching the basis used for measuring. He also obtains two bits for each qubit, namely

- $b_{m,i}$, telling which basis was used to measure the qubit, and
- $s_{m,i}$, telling which state of the given basis was measured.

Alice now (*after* the transmission) tells Bob (over a public channel) the sequence $\{b_{p,i}\}$ which Bob compares to his sequence $\{b_{m,i}\}$. He keeps only qubits with $b_{p,i} = b_{m,i}$ and throws away all the others (roughly n). For the remaining qubits the classical bits $s_{p,i} = s_{m,i}$ are known to both Alice and Bob. They constitute the key.

The security aspects of this procedure become visible if Eve intercepts and measures the qubits. During transmission Eve does not know which basis Bob uses for measuring (only later, but that is too late!). Thus she will use the wrong basis about 50 % of the time for measuring. Half of these states measured by Eve in the wrong basis and then passed on to Bob will be projected back into the right state by Bob's measurement, so the overall error rate caused by Eve will be 25 %. Alice and Bob can agree to publicly compare a certain share of the key (thereby sacrificing that share, of course), and if they detect no differences they can be pretty certain that no eavesdropping has occurred. (If m bits are compared the probability that they are all correct by chance in the presence of eavesdropping is $\left(\frac{3}{4}\right)^m = 3 \cdot 10^{-13}$ for $m = 100$.) Of course Eve might be clever enough not to intercept *every* qubit, and also there might be errors in a less than perfect transmission line. All these problems have been analyzed and may be overcome, see [5, 7].

The scheme has been demonstrated using 23 km of public telecom glass fiber beneath Lake Geneva by Zbinden et al. 1997 [40]. In that experiment polarized light pulses with $\lesssim 0.1$ photons per pulse were used: there must be (practically) no pulses with two or more photons because an eavesdropper might intercept just one photon and go unnoticed. (By the way, this problem is one of the reasons for the interest in "single photon on demand" sources.) The bit error rate was $\sim 1\%$ and the data transfer rate was of the order of MHz instead of the usual (in non-secure communication) GHz.

Other protocols for secure communication involve entangled states, for example EPR pairs, and it was shown that the Bell inequalities (mentioned in chapter IV) distinguishing genuine quantum correlations from classical ones can be used to detect eavesdroppers. An extremely simple scheme involving EPR pairs but no Bell inequalities was suggested by Bennett, Brassard, and Mermin in 1992 [41]. This scheme is essentially equivalent to the BB84 protocol just discussed.

Alice and Bob share $2n$ EPR pairs

$$|\phi_i\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

in the usual way. Both measure the qubit accessible to them, and thus project it on one of the eigenstates of $\mathbf{X}$ or $\mathbf{Z}$ (at random). They inform each other publicly about the $(\mathbf{X}, \mathbf{Z})$ sequence used, but not about the results of the measurements. They discard all measurements where one has measured $\mathbf{X}$ and the other $\mathbf{Z}$. The remaining measurement results are perfectly anticorrelated and can be used to produce two equal bit strings of length $\sim n$. A part of the key may again be sacrificed to detect eavesdropping. The scheme has an additional advantage: the EPR pairs can be left untouched until just before the key is needed so that the period when the key is kept in classical storage and can be copied by a thief is minimal. Of course this requires the ability to preserve EPR pairs over long times, but that is a different story.