Chapter 10
Stopover; Then on to Quantum Cryptography

We first compare formulations of the analytic and algebraic approaches to quantum mechanics. In the second section, we see that the properties of the measurement process in quantum mechanics permit an encryption method which is in principle absolutely secure.

10.1 Outline

This chapter is exceptional insofar as the formalism is not developed further. Rather, it serves to collect our previously acquired knowledge, to compare and to check where there are open questions of form or content. In the second part of the chapter, we take up quantum cryptography. We will see that even allegedly abstract or theoretical peculiarities of quantum mechanics, such as those of the measurement process, can have immediate practical applications.

10.2 Summary and Open Questions

First, we collect the essential concepts and structures of quantum mechanics which we have developed up to now in the preceding chapters. Comparison of the analytical and algebraic approaches (ana and ala) shows, on the one hand, that there are many significant parallels, but also that a few components are missing in each case. To keep the text readable, we dispense with detailed remarks about which chapter introduced or treated the particular subject matter.

J. Pade, *Quantum Mechanics for Pedestrians 1*, Undergraduate Lecture Notes in Physics, https://doi.org/10.1007/978-3-030-00464-4_10

10.2.1 Summary

10.2.1.1 States

We started with *states*, which we wrote in the analytical approach in terms of a position- and time-dependent wavefunction $\psi(\mathbf{r}, t)$, and in the algebraic approach as a ket $|\psi(t)\rangle$ or its representation as a column vector. It should be pointed out again that $|\psi(t)\rangle$ does *not* depend on position, but only on time. The states are in both cases elements of vector spaces.

10.2.1.2 Time-Dependent SEq, Hamiltonian

The time behavior of both approaches is described by the time-dependent SEq. It reads

$$\begin{aligned} i\hbar\frac{\partial}{\partial t}\psi(\mathbf{r}, t) &= H\psi(\mathbf{r}, t) \\ i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle &= H|\psi(t)\rangle . \end{aligned} \tag{10.1}$$

In the analytical approach, H is the Hamiltonian $-\frac{\hbar^2}{2m}\nabla^2 + V$, while in the algebraic approach it is an abstract operator, about which we know almost nothing so far—except that it can be represented as a matrix.[1] In any case, H is a Hermitian operator, where this property is defined in the ana by integrals, in the ala by scalar products:

$$\begin{aligned} \int \psi^* H\varphi \mathrm{d}V &= \int (H\psi)^* \varphi \mathrm{d}V \\ \langle\psi| H |\varphi\rangle &= \langle\psi| H^\dagger |\varphi\rangle . \end{aligned} \tag{10.2}$$

10.2.1.3 Mean Value and Expectation Value

If the system is in the state $\psi(\mathbf{r}, t)$, we can obtain the expectation value $\langle A\rangle$ of an operator A (that is, the expectation value of the corresponding physical quantity) as

$$\langle A\rangle = \int \psi^* H\psi \mathrm{d}V. \tag{10.3}$$

A corresponding formulation in the algebraic approach is still pending.

We note that the expectation value of a time-independent operator A in general depends on time because of $\psi = \psi(\mathbf{r}, t)$. It is a conserved quantity (i.e. is independent of time) if the operator A commutes with H, i.e. $[A, H] = 0$.

[1] A comment on the notation: although the Hamiltonians of the two approaches in (10.1) are completely different mathematical objects, it is customary to denote them with the same symbol H. The same holds for the eigenfunctions and vectors.

10.2.1.4 Time-Independent SEq, Eigenvalues and Eigenvectors

The time evolution of the states can be developed by means of the eigenvalues and eigenvectors of H. We assume discrete, nondegenerate spectra with eigenvalues E_n. We denote the analytical eigenvectors (eigenfunctions) by $\varphi_n(\mathbf{r})$, the algebraic ones by $|\varphi_n\rangle$. They are the solutions of the eigenvalue problems (stationary SEq):

$$\begin{aligned} H\varphi_n(\mathbf{r}) &= E_n\varphi_n(\mathbf{r}) \\ H|\varphi_n\rangle &= E_n|\varphi_n\rangle . \end{aligned} \tag{10.4}$$

We note that the range of values of n can be finite or infinite.

Since H is a Hermitian operator in both of these approaches, its eigenfunctions $\{\varphi_n(\mathbf{r})\}$ or $\{|\varphi_n\rangle\}$ form an orthonormal system (ONS):

$$\begin{aligned} \int \varphi_m^*(\mathbf{r})\,\varphi_n(\mathbf{r})\,\mathrm{d}V &= \delta_{nm} \\ \langle\varphi_m|\varphi_n\rangle &= \delta_{nm}. \end{aligned} \tag{10.5}$$

In the ala, we described the completeness of an ONS by $\sum_n |\varphi_n\rangle\langle\varphi_n| = 1$. An analogous formulation in the ana is still pending.

10.2.1.5 Time-Dependent Solution

Using eigenvalues and eigenvectors, the time-dependent solution of the SEq can be written as

$$\begin{aligned} \psi(\mathbf{r},t) &= \sum_n c_n\varphi_n(\mathbf{r})\,e^{-iE_nt/\hbar} \\ |\psi(t)\rangle &= \sum_n c_n|\varphi_n\rangle\,e^{-iE_nt/\hbar}. \end{aligned} \tag{10.6}$$

Being solutions of the deterministic SEq (10.1), these states are defined uniquely and for all times by specifying an initial condition $\psi(\mathbf{r},0)$ or $|\psi(0)\rangle$. We can see this by using (10.5) to obtain

$$\begin{aligned} \int \varphi_m^*(\mathbf{r})\,\psi(\mathbf{r},0)\,\mathrm{d}V &= \sum_n c_n \int \varphi_m^*(\mathbf{r})\,\varphi_n(\mathbf{r})\,\mathrm{d}V = \sum_n \delta_{nm}c_n = c_m \\ \langle\varphi_m|\psi(0)\rangle &= \sum_n c_n\langle\varphi_m|\varphi_n\rangle = \sum_n \delta_{nm}c_n = c_m. \end{aligned} \tag{10.7}$$

or, more compactly,

$$\begin{aligned} c_n &= \int \varphi_n^*(\mathbf{r})\,\psi(\mathbf{r},0)\,\mathrm{d}V \\ c_n &= \langle\varphi_n|\psi(0)\rangle . \end{aligned} \tag{10.8}$$

Up to this point, the formalisms developed in the ana and ala are very similar, in spite of some differences (definition of a Hermitian operator, state, SEq as a differential equation or as a matrix equation). We conclude that there obviously *must* be a close connection. For example, the (10.8) suggest that the integral $\int \varphi_n^* (\mathbf{r})\, \psi (\mathbf{r}, 0)\, \mathrm{d}V$ of the ana corresponds to a scalar product in the ala. We take up this issue again in the next chapter.

10.2.1.6 Measurement, Probability

The formalism of quantum mechanics just outlined is strictly deterministic. A random element occurs only if we want to obtain information about the system by means of a measurement. We have seen in previous chapters that the coefficients of the form $|c_n|^2$ which appear in (10.6) give the probabilities of finding the system in the state $\varphi_n (\mathbf{r})$ or $|\varphi_n\rangle$. With quantized values (such as the energy or the state of a neutrino, i.e. muon neutrino or electron neutrino, etc.), one can always measure only *one* of the values of the spectrum. Other results are not possible.

In the ala, we formulated the measurement process by using projection operators. If we want to measure e.g. the state $|\chi\rangle$, we model this by applying the projection operator $P_\chi = |\chi\rangle \langle\chi|$ to the state $|\psi\rangle$:

$$|\chi\rangle \langle\chi |\psi\rangle = c\, |\chi\rangle\,. \tag{10.9}$$

Here, the term $|c|^2 = |\langle\chi |\psi\rangle|^2$ denotes the probability of in fact obtaining the state $|\chi\rangle$ by a measurement on $|\psi\rangle$. In the ana, we have not yet introduced projection operators. The parallelism of the descriptions in the ana and ala suggests, however, that there must be an equivalent in the ana.

10.2.1.7 Measurement, Collapse

Through the measurement, the system is transferred from the state $|\psi\rangle$ into $|\chi\rangle$ (provided $c = \langle\chi |\psi\rangle \neq 0$). In the formulation of the ala, this can be written as

$$|\psi\rangle \underset{\text{with probability } |c|^2}{\rightarrow} \frac{P_\chi |\psi\rangle}{\left|P_\chi |\psi\rangle\right|} = \frac{\langle\chi |\psi\rangle}{|\langle\chi |\psi\rangle|} |\chi\rangle. \tag{10.10}$$

On measurement, a superposition of states generally breaks down[2] and the result is *one* single state. We have described this behavior in terms of state reduction or collapse of the state. After the measurement, we again have a normalized state, where a possibly remaining global phase is irrelevant,[3] since states are physically the same if they differ only by a phase (we will discuss this point later, in Chap. 14). The state

[2] In other words, if the initial and final states are not the same.

[3] Quantum mechanics is very well-behaved in this sense.

after the measurement can be interpreted as a new initial state[4] (at time T, we start our clock again), which evolves in a unitary manner until the next measurement.

We remark again that the actual measurement process itself is not modelled, but rather only the situation before and after the measurement.

10.2.2 Open Questions

The descriptions in the ana and ala outlined above leave open some questions which we now summarize briefly. These questions are in part of a more formal nature, and in part concern content (although this division is not necessarily clearcut). The answers to the open questions will be provided in the following chapters.

10.2.2.1 Formal Questions

As mentioned above, the great similarity of the expressions (10.1) and (10.8) suggests that there is a direct connection between the two approaches and the corresponding formulations. So it must be clarified, for example, which relationship exists between the description of states as kets and as wavefunctions. As a result, we will find among other things a representation of the projection operator in the ana, thus far defined only in the ala. In addition, this connection must explain the different formulations, as in (10.8); this is also true for the definitions of the Hamiltonians in the two approaches (as $-\frac{\hbar^2}{2m}\nabla^2 + V$ and as a matrix) which at first glance seem quite distinct.

Another topic still to be treated is that of degenerate as well as continuous spectra. This will be done in Chap. 12.

10.2.2.2 Questions of Content

A measurement, as described in (10.10), is generally (i.e. for $|c|^2 \neq 1$) not reversible, so it is not a unitary process. Assuming the validity of the projection principle for determining the measurement probabilities, we must explain how this state reduction comes about, i.e. the transition from a superposition such as $|\nu(t)\rangle$ to a single state such as $|\nu_e\rangle$. Meanwhile, it is accepted that this collapse of the state is a non-local, i.e. superluminal effect.[5] Some of following considerations answer part of the open questions, but another part is still poorly understood and still under discussion. We will come back to these topics in several chapters in volume 2.

[4] In this case one speaks of 'state preparation'.

[5] This makes it perhaps understandable that Einstein dismissed it as 'spooky action at a distance'. It can be shown that the effect is not suitable for the superluminal transmission of information—the validity of the theory of relativity thus remains unquestioned.

To avoid misunderstandings: Here, we have a problem at the level of the *interpretation* of quantum mechanics; that is, of its *comprehension*. On a formal level—technically, so to speak—quantum mechanics works extremely well; it is simply *fapp* (after a proverbial expression due to John S. Bell: 'Ordinary quantum mechanics is just *f*ine for *a*ll *p*ractical *p*urposes').[6]

We will resume the discussion of the issues of content in Chap. 14. In the rest of this chapter, we will examine a practical application of quantum mechanics—to some extent a case of *fapp*.

10.3 Quantum Cryptography

There are some popular misconceptions about quantum mechanics. The 'quantum jump' is symptomatic—what in quantum mechanics means the 'smallest possible change' has become in everyday language a metaphor for a giant leap, a radical change.[7]

Two other misconceptions are that quantum mechanics always requires an enormous mathematical apparatus,[8] and that the abstract peculiarities of quantum mechanics such as the measurement problem are at most of theoretical interest. That both assertions are wrong is shown by *quantum cryptography*.[9] In fact, it is based on a peculiarity of the quantum-mechanical measurement process and can, in its simplest formulation, be described *without any formula* at all,[10] as we will see shortly. Of course, one can describe the whole situation more formally, but here we have one of the admittedly very few examples where this is not necessarily required.

The procedure is based on the quantum-mechanical principles that (i) there are superpositions of several states, and that (ii) before a measurement of such a superposition, we can specify only the probability of obtaining one of these states as a result. These principles are what make quantum cryptography possible, not only in theory, but also as a practical method.

[6] In an extension of Bell's one-liner, those theories which, on the one hand, one cannot really (or does not want to) justify, but which, on the other hand, agree well with experimental results and are very useful for all practical purposes, are called *fapp* theories. Quantum mechanics may be such a theory, if one regards it only as a tool (or judges it primarily by its usefulness) and is not willing (or able) to reflect upon its meaning.

[7] However, the movie title 'Quantum of Solace' promises not a 'quantum jump', but rather a minimum in terms of comfort for James Bond—quantum solace, so to speak.

[8] We have already seen that this is not always true, e.g. in the algebraic approach, where the basic ideas can be formulated using simple vector algebra.

[9] This term is short and to the point, but also a bit misleading. As we shall see shortly, quantum mechanics does not help to encrypt a message, but rather ensures that the key cannot be discovered by a spy.

[10] For this reason, the topic is also very well suited for discussion at the school level.

10.3.1 Introduction

Cipher texts and encryptions were already common in pre-Christian cultures. One of the most famous old encryption methods is attributed to Caesar, and is still called the *Caesar cipher*. Here, the text is encoded by replacing each letter with for example the third letter which follows it in the alphabet. Thus, 'cold' becomes 'frog' and 'bade' becomes 'edgh'.

Of course, nowadays it is a no-brainer to crack this ciphering method—it suffices that one knows very precisely for each language the frequency of occurrence of each letter. Modern cryptography has developed much more elaborate processes. It enjoyed an enormous boom in both world wars, where it also provided a strong impetus to the development of electronic computers. One of the first, called *Colossus*, was built at the end of the Second World War and was used for decoding purposes.

A word on nomenclature: One encodes, encrypts or ciphers an unencrypted or plain text by means of a cipher or key. The result is a encrypted text or cipher text. If it is decoded, decrypted or deciphered, one again recovers the plain text.

10.3.2 One-Time Pad

This encryption method was developed in 1917. Gilbert Vernam is usually named as its author. In 1949, Claude Shannon proved the *absolute security* of the method. In this process, it is known how to encrypt and decrypt. Its security is based exclusively on the fact that the *key is secret* (and only if this is guaranteed is the process absolutely secure).

The method works as follows: First, the alphabet (and some major punctuation marks, etc.) is converted into numbers. As an example, we might have:

A	B	C	D	E	...	X	Y	Z		,	.	?
00	01	02	03	04	...	23	24	25	26	27	28	29

as our pool of 30 characters. If the message consists of N characters, then the key must also consist of N characters. They are pulled out of the pool *at random*. Compared to 'normal' text, this has the advantage that each character occurs on average with equal frequency. Thus, even if pieces of the key are known, it cannot be reconstructed.

As a concrete example, we choose the key 06/29/01/27/ …. Encrypting the message 'BADE' leads to:

B	A	D	E	Message, plain text T
01	00	03	04	Plain text T, numbers
06	29	01	27	Key S
07	29	04	01	V = (T + S) (mod 30), numbers
H	?	E	B	Cipher text V

and decrypting leads to

H	?	E	B	Cipher text V
07	29	04	01	Ciphertext V, numbers
06	29	01	27	Key S
01	00	03	04	T = (V − S) (mod 30), numbers
B	A	D	E	Message, plain text T

Some remarks on practical procedures:

- The cipher text V is transmitted *publicly*. The security depends entirely on the fact that the key is known only to the sender and the recipient.
- The procedure is absolutely safe if each key is used only *once*. Hence the name ‘pad’—one can imagine the sender and receiver each having an identical (writing) pad, and there is just one key on each sheet. After encrypting and decrypting the key is obsolete; the top sheet of the pad is stripped off and thrown away. The next page on the pad contains the next key.
- In binary notation, the method is basically the same, but more adapted to computers. This could be as follows (1 + 1 = 0):

Text T	0	1	1	0	1	0	0	1	0	1	1	1
Key S	1	0	1	0	0	1	0	0	0	1	1	0
T + S	1	1	0	0	1	1	0	1	0	0	0	1
S	1	0	1	0	0	1	0	0	0	1	1	0
⇒ T = T + S ± S	0	1	1	0	1	0	0	1	0	1	1	1

- Especially in the English literature, certain names have become firmly entrenched. The sender is called ‘Alice’, the recipient ‘Bob’. We will consider in addition a third person, namely a spy. For the name of the spy, one could think that it should now begin with ‘C’, e.g. ‘Charlotte’ (and in French texts, one does indeed find this name); but the English word ‘eavesdropping’ suggests immediately the name ‘Eve’, and that is how the spy is usually named—not alphabetically, but gender-specifically correct.
- The one-time pad method is thus based on a *public* exchange of the encrypted message, while the key is transmitted *secretly*. The problem of safe and secret transfer of keys between Alice and Bob is called *key distribution*. The great difficulty here is: How can we be sure that Eve has not read the key in secrecy, without leaving traces on the paper or on the CD, or has photographed it? There is a kind of

mnemonic in cryptography which describes this classical dilemma ironically: 'You can communicate completely secretly, provided you can communicate completely secretly.'

Here, quantum mechanics enters the scene, and brings with it several methods. All have in common that they associate the key distribution to quantum-mechanical characteristics and thus secure it. This is called *quantum key distribution*. A particularly simple method is the so-called BB84 protocol (Bennett and Brassard, 1984).[11] It is essentially based on the idea of a Ph.D. student in the sixties. Stephen Wiesner at that time devised a method of making counterfeit-proof banknotes using polarized photons (so to speak 'quantum money'). Although the practical implementation of this idea is not readily possible even today, in retrospect it is not really understandable why Wiesner's attempts to publish this idea around 1970 were rejected rigorously by the journal reviewers. Wiesner had to wait more than ten years before he could describe his proposal in the literature.[12] In any case—at least Charles Bennett, a friend of Wiesner's, recognized the cryptographic potential of his idea and developed, together with Brassard, the *BB84 protocol*.

10.3.3 BB84 Protocol Without Eve

In the following, the information is transmitted by polarized photons, where we will consider only linear polarization. As usual, we denote the horizontally- and vertically-polarized states by $|h\rangle$ and $|v\rangle$.

As we said above, the secure and confidential transmission of the key is all-important. Alice could now send a key by forwarding to Bob a random sequence of $|h\rangle$ and $|v\rangle$. However, she must tell Bob the orientation of the polarizer (e.g. by phone), and when Eve overhears this communication, she could listen safely without Alice or Bob being aware of her. To increase security, we must use quantum mechanics; more precisely, projection and the superposition principle.

And this is how it works: Alice chooses randomly one of two polarization directions: horizontal/vertical or diagonally left/right, symbolized by ⊞ and ⊠, where the crosses in the squares mark the polarization planes.[13] We can represent the states as $|h\rangle$ and $|v\rangle$ plus $|\backslash\rangle$ and $|/\rangle$ for the 'diagonal' measurements. The superposition principle is expressed by the fact that the 'diagonal' states are linear combinations of the 'linear' ones, $[|h\rangle \pm |v\rangle]/\sqrt{2}$. So if one measures with a 'linear' polarizer a 'diagonal' state, one obtains $|h\rangle$ and $|v\rangle$, each with probability $\left(1/\sqrt{2}\right)^2 = 1/2$.

To keep the notation transparent, we assign values to the states:

[11] Another method, called the E91 protocol (the 'E' designates Artur Ekert), works with *entangled* photons (for this concept see Chap. 20, Vol. 2).

[12] Unfortunately, one must not be too far ahead of one's time. Depicting blue horses in the 15th century probably caused (at most) some head-shaking. That applies also in science.

[13] The ⊠ plane is of course the ⊞ plane, rotated by 45°. Moreover, the ⊞ states are the eigenvectors of σ_z, and the ⊠ states, up to a sign, are the eigenvectors of σ_x; cf. Chap. 4.

$1 \mathrel{\hat{=}} \vert h\rangle$	$1 \mathrel{\hat{=}} \vert \backslash\rangle$
$0 \mathrel{\hat{=}} \vert v\rangle$	$0 \mathrel{\hat{=}} \vert /\rangle$

The exact choice of this mapping plays no role,[14] but it must be agreed upon between Alice and Bob. Similarly, the orientation of the polarizers (= basis) is *publicly* known.

The BB84 protocol operates as follows:

1. Alice and Bob fix the start and the end of the key transmission and the timing with which the photons are sent, for example one photon every tenth of a second.
2. Alice dices (i.e. generates at random) a basis and a value, i.e. ⊞ or ⊠ and 1 or 0. The bit thus described[15] is sent to Bob as a polarized photon.
3. Of course, Bob does not know the basis and the value which Alice has sent. He dices a basis and measures the photon in this basis. He may or may not choose (by chance, with probability $1/2$) the same basis as Alice. In the first case, he always measures *the same value* as Alice—this is crucial for the functioning of the method. If the bases do not match, there is only a probability of $1/2$ that Bob measures the correct value. Up to this point the whole thing looks, for example, like this:

A basis	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
A value	1	0	0	1	1	0	0	1	0	1
B basis	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
B possible measurements	1 0	0	1 0	1	1	0	0	1 0	0	1 0
B actual measurement	1	0	1	1	1	0	0	0	0	1

For the first photon, Bob did not choose the basis used by Alice. His measurement can then be 1 or 0; we have inserted 1 as a concrete example.[16] By the way, the results obtained with different bases used by A and B do not matter for the key transmission, as we shall see in a moment.

4. In this way, the necessary number of photons is transmitted, while Alice and Bob record their bases and values. The transfer process is then completed. The next step is a *public* exchange: Bob tells Alice which basis he used for each photon, and Alice tells Bob whether it was the right one. It is important that the value (i.e. 0 or 1) is *not made public*. After that, Alice and Bob remove all values for which the polarization orientations do not match. This also applies to all

[14] For example, the mapping $0 \mathrel{\hat{=}} |h\rangle$ and $1 \mathrel{\hat{=}} |v\rangle$ would be just as good.

[15] By a *bit*, one denotes a quantity that can take on only two values, here 0 and 1.

[16] We remark that Bob, in his measurements with a 'wrong' basis, may of course also obtain other values, and these with equal probability. The last row in the table above is a concrete example of a total of 16. Other possibilities for Bob's actual measurements are e.g. $\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{0}$ or $\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{0}$.

measurements or times at which Alice did not send a photon or Bob did not detect one although one was underway (dark counts). Since Alice and Bob always get the same values for the same basis, the remaining values make up the key. In this eavesdropper-free scenario, it is known to no-one other than Alice and Bob. In our example, the key is

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}\hline \text{Key} & - & 0 & - & 1 & 1 & 0 & 0 & - & 0 & - \\ \hline\end{array} \rightarrow 011000.$$

However, the world is not so simple, and eavesdroppers and spies are everywhere. How do we deal with this problem?

10.3.4 BB84 Protocol with Eve

The situation is as follows: Alice sends one photon per time interval, and Eve intercepts each photon or a certain portion of them (of course without Alice and Bob being able to perceive this by ordinary means of observation), using e.g. a PBS, and transmits them on to Bob. This may seem simple, but actually it is not so easy for Eve to carry out this interception. One of the possible applications is, for example, to send keys from the earth (summit stations) to satellites. If one is really dealing with single-photon processes, it is impossible for Eve to intercept individual photons in transit and remain unnoticed, without in this case the whole world being able to look at her. For other types of transmission (via fiber-optic cable, etc.), espionage techniques are possible, but certainly not easy to implement.

But we assume in the following (for the purpose of a conservative estimate) that Eve can overcome this problem. However, quantum mechanics ensures that she still cannot listen without being recognized.

The argument runs like this: Since Eve never knows which basis Alice has set, she must choose her basis, just like Bob, randomly with a hit rate of 50%. When using the wrong basis, Eve will not measure the value chosen by Alice in 50% of the cases. Bob in turn measures, if he has chosen at random the same basis as Eve, the same value as she does; or otherwise, with probability 1/2, the value 0 or the value 1. This could for example look like this:

A basis	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
A value	1	0	0	1	1	0	0	1	0	1
E basis	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞
E possible measurements	1 0	1 0	1 0	1	1	1 0	1 0	1	0	1 0
E actual measurement	1	0	1	1	1	0	1	1	0	0
B basis	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
B possible measurements	1	1 0	1	1	1	1 0	1 0	1 0	0	0
B actual measurement	1	0	1	1	1	1	1	0	0	0

Alice and Bob again compare their bases for each photon and keep only the values for which the bases coincide. For example:

Alice	–	0	–	1	1	0	0	–	0	–
Bob	–	0	–	1	1	1	1	–	0	–

And here we see the great advantage of quantum cryptography. The difference in the keys of Alice and Bob makes it *in principle detectable* that Eve was spying! Quantum-mechanical methods of key distribution make it virtually impossible for Eve to remain unnoticed. In order to detect the spy, Alice and Bob have to compare publicly parts of their keys, and cannot use the whole key directly. But since one can transmit very large amounts of information very simply with photons, it is not a particular disadvantage for Alice and Bob to discard parts of their keys upon consultation. The essential details of the procedure can be found in Appendix P, Vol. 1.

We want to pursue the question of which level of certainty can be achieved for Eve's unmasking. To quantify the issue, we assume that Alice and Bob have chosen the same basis (the other photons are eliminated anyway). Eve can then chose randomly (and with probability 1/2) the same basis, in which case Alice's value is passed on, or the other basis, in which case there are four different possibilities. In detail, they are as follows:

Alice's basis	⊞	⊞	⊞	⊞	⊞
Alice's value	1	1	1	1	1
Eve's basis	⊞	⊠	⊠	⊠	⊠
Eve's value	1	1	1	0	0
Bob's basis	⊞	⊞	⊞	⊞	⊞
Bob's value	1	1	0	1	0
probability	1/2	1/8	1/8	1/8	1/8

After the elimination of the results of different bases used by Alice and Bob, we have the following situation: (a) Eve has 75 agreement with the values of Alice, and (b) in a quarter of the cases, a different value results at the corresponding position of the keys of Alice and Bob. Thus, there is a chance of $1 - 1/4$ per photon that Eve remains undetected. If Eve has spied on a total of N photons of the key, the chance of discovering her is given by $p_{\text{discover}} = \left(1 - [1 - 1/4]^N\right)$. For a very short key or very few measurements, Eve may be lucky and stay undetected (e.g. for the first five photons in the above example), but uncovering her is practically certain with even a moderately long key. Here are some numerical values:

N	10	10^2	10^3	10^4
$1 - p_{\text{discover}}$	$10^{-1.25} = 0.056$	$10^{-12.5}$	10^{-125}	10^{-1249}

Compared to this, the chance to win the lottery (6 out of 49) is relatively high; as is well known, it is $1/\binom{49}{6} = 1/13983816 \approx 10^{-7.1}$. Even for only a moderately large N of the order of 100 or 1000, it is virtually impossible that Eve can listen in without being recognized.

If Eve spies on each photon, this manifests itself in an average error rate of 25% when the keys of Alice and Bob are compared. If she spies on every second photon, it is 12.5%, etc. So, when Alice and Bob compare their keys, they see not only *whether* Eve has been spying, but also can estimate *how many* photons she has eavesdropped on. However, errors can also arise due to noise and other processes which, for example, unintentionally change the polarization. By comparing, Alice and Bob can determine which part of the key Eve knows *at most*. If the error rate is too high, say well over 10%, the key is discarded and a new key is transmitted.

Now one could imagine that Eve calmly replicates the photons sent by Alice, transmits the original to Bob and performs appropriate measurements on the copies. But this does not work, as is guaranteed by another peculiarity of quantum mechanics: Namely, the *no-cloning theorem* of quantum mechanics states that one cannot copy an arbitrary state, but only a state that is *already known*, as well as the states orthogonal to it. We will discuss this point in Chap. 26, Vol. 2 (quantum information). In the context of our current considerations, the theorem applies, since the two non-mutually-orthogonal basis systems $\boxplus$ and $\boxtimes$ are used.

Up to this point we have considered the contributions of quantum mechanics. What follows are classical, not quantum-mechanical methods; they are outlined in Appendix P, Vol. 1.

A final remark: We have assumed idealized conditions—all detection devices work with one hundred percent efficiency, there is no noise (behind which Eve could try to hide), and so on. So the question is whether the method is also suitable for actual, practical use. One can investigate this issue theoretically, and finds a positive answer. But here it is perhaps more interesting to note that the method indeed works well in practice. In fact, a number of quantum cryptographic experiments have been performed to date. Among others, the world's first quantum-encrypted money transfer was carried out on April 21st, 2004 in Vienna. The photons were guided through a 1500 m long fiber-optic cable that connected the city hall with a bank. Furthermore, there was an experiment in 2002 using a telescopic connection, i.e. without expensive fiber-optic cables. Here, the photon travelled through the clear mountain air from the summit station of the Karwendelbahn a distance of 23.4 km to the Max Planck hut on the Zugspitze.[17] But even in the polluted air of an urban area (Munich), the procedure has been successfully tested[18]; the photons travelled a free distance of 500 m. The transfer rate was around 60 kbit/s; the system was operated continuously and stably

[17] C. Kurtsiefer et al., 'A step towards global key distribution', *Nature* 419 (2002), p. 450.

[18] See the webpage 'Experimental Quantum Physics', http://xqp.physik.uni-muenchen.de/.

for 13 h. A much longer transmission distance was attained in 2007, when a quantum key was transferred over 144 km, namely between the Canary Islands of La Palma and Tenerife.[19] In principle, it therefore appears possible to use satellites for such secure and encrypted signaling, e.g. for transatlantic connections.[20]

[19] R. Ursin et al., 'Entanglement-based quantum communication over 144 km', *Nature Physics* 3 (2007), p. 481.

[20] See e.g. S. Liao et al., Satellite-to-ground quantum key distribution, *Nature* 549, 43–47, https://doi.org/10.1038/nature23655 (Sep 2017), where a quantum key distribution over a distance of up to 1,200 km is reported. Quantum keys may also be distributed in optical fibers over remarkable distances of up to 100 km; see e.g. K.A. Patel et al., Coexistence of high-bit-rate quantum key distribution and data on optical fiber, *Phys. Rev.* X 2, 041010 (2012)), or Paul Jouguet et al., Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* (2013), https://doi.org/10.1038/nphoton.2013.63. In addition, the feasibility of BB84 quantum key distribution between an aircraft moving at 290 km/h at a distance of 20 km was recently proven for the first time; see: Sebastian Nauert et al., Air-to-ground quantum communication, *Nature Photonics* (2013), https://doi.org/10.1038/nphoton.2013.46.