Springer Tracts in Modern Physics
173

G. Alber · T. Beth · M. Horodecki
P. Horodecki · R. Horodecki · M. Rötteler
H. Weinfurter · R. Werner · A. Zeilinger

Quantum Information

An Introduction to Basic Theoretical Concepts and Experiments

量子信息

Springer
世界图书出版公司

G. Alber T. Beth M. Horodecki P. Horodecki
R. Horodecki M. Rötteler
H. Weinfurter R. Werner A. Zeilinger

Quantum Information

An Introduction to Basic Theoretical Concepts and Experiments

With 60 Figures

Springer
世界图书出版公司

书　　名：Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments
作　　者：G.Alber, T.Beth et al
中 译 名：量子信息
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
发　　行：世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开　　本：24 开　　　印　张：10
出版年代：2004 年 4 月
书　　号：7-5062-6615-6/O·468
版权登记：图字：01-2004-1161
定　　价：49.00 元

The corresponding author:

Dr. Gernot Alber

Universität Ulm
Abteilung für Quantenphysik
Albert-Einstein-Allee 11
89069 Ulm, GERMANY
E-mail: gernot.alber@physik.uni-ulm.de

The complete list of authors see page XI

Library of Congress Cataloging-in-Publication Data.

Quantum information: an introduction to basic theoretical concepts and experiments/G. Alber ... [et al.]. p.cm. - (Springer tracts in modern physics; 173). Includes bibliographical references and index. ISBN 3-540-41666-8 (alk. paper) 1. Quantum computers. I. Alber, Gernot. II. Series. QA76.889.Q848 2001 004.1-dc21 2001020642

Physics and Astronomy Classification Scheme (PACS): 03.67.-a, 03.67.Hk, 03.67.Lx, 03.67.Dd

ISSN print edition: 0081-3869
ISSN electronic edition: 1615-0430
ISBN 3-540-41666-8 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in
the People's Republic of China only and not for export therefrom.
Reprinted in China by Beijing World Publishing Corporation, 2004

Preface

Though quantum theory is celebrating its 100th anniversary this year, quantum information processing is still a remarkably young research field. The questions driving this research field reflect a profound change in the general attitude towards the fundamental aspects of quantum theory. So far, research on the foundations of quantum theory has been concerned mainly with the theoretical exploration of those particular features which distinguish quantum theory from classical physics. The main intention of quantum information processing is to exploit these specific features for technological purposes. As early as 1935, Erwin Schrödinger had already noted that one of these characteristic features of quantum theory is the phenomenon of entanglement. Many years passed from this early insight until John Bell realized the quantitative consequences of the corresponding quantum correlations in his famous work from 1964. These theoretical predictions inspired numerous experiments, which all support the peculiar features predicted for quantum correlations. From these purely theoretical insights, it again required a long period of development to arrive at those potentially useful applications which are now of central interest for the processing of quantum information.

The following contributions provide an introductory overview of basic problems, methods and topical results in this research field. The idea of producing this volume was born at a symposium on this subject which was held at the 1999 annual spring meeting of the Deutsche Physikalische Gesellschaft in Heidelberg. This symposium was organized jointly by the Quantum Optics and Mathematical Physics sections. The widespread interest, the success of this symposium and the initiative of Prof. Frank Steiner, the head of the Mathematical Physics section, motivated us to edit a volume on basic problems, methods and recent results in this rapidly evolving field. This book should be useful for students and active researchers in physics, computer science and mathematics who want to learn about the most recent developments in this exciting research field.

Ulm, March 2001 *Gernot Alber*

List of Authors

Gernot Alber
Abteilung für Quantenphysik
Universität Ulm
Albert-Einstein-Allee 11
89069 Ulm, Germany
gernot.alber@physik.uni-ulm.de

Thomas Beth
Institut für Algorithmen
und Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5
76128 Karlsruhe, Germany
EISS_Office@ira.uka.de

Michał Horodecki
Institute of Theoretical Physics
and Astrophysics
University of Gdansk
ul. Wita Stwosza 51
80–952 Gdansk, Poland
michalh@iftia.univ.gda.pl

Paweł Horodecki
Dept. of Technical Physics
and Applied Mathematics
Technical University of Gdansk
ul. Narutowicza 11/12
81–952 Gdansk, Poland
pawel@mifgate.pg.gda.pl

Ryszard Horodecki
Institute of Theoretical Physics
and Astrophysics
University of Gdansk
ul. Wita Stwosza 51
80–952 Gdansk, Poland
fizrh@univ.gda.pl

Martin Rötteler
Institut für Algorithmen
und Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5
762128 Karlsruhe, Germany
martin.roetteler
@informatik.uni-karlsruhe.de

Harald Weinfurter
Sektion Physik
Universität München
Schellingstr. 4
80797 München, Germany
harald.weinfurter
@physik.uni-muenchen.de

Reinhard Werner
Institut für Mathematische Physik
TU Braunschweig
Mendelsohnstr. 3
38106 Braunschweig, Germany
r.werner@tu-bs.de

Anton Zeilinger
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria
anton.zeilinger@univie.ac.at

Contents

1 From the Foundations of Quantum Theory to Quantum Technology – an Introduction

Gernot Alber

Nowadays, the new technological prospects of processing quantum information in quantum cryptography [1], quantum computation [2] and quantum communication [3] attract not only physicists but also researchers from other scientific communities, mainly computer scientists, discrete mathematicians and electrical engineers. Current developments demonstrate that characteristic quantum phenomena which appear to be surprising from the point of view of classical physics may enable one to perform tasks of practical interest better than by any other known method. In quantum cryptography, the no-cloning property of quantum states [4] or the phenomenon of entanglement [5] helps in the exchange of secret keys between various parties, thus ensuring the security of one-time-pad cryptosystems [6]. Quantum parallelism [7], which relies on quantum interference and which typically also involves entanglement [8], may be exploited for accelerating computations. Quantum algorithms are even capable of factorizing numbers more efficiently than any known classical method is [9], thus challenging the security of public-key cryptosystems such as the RSA system [6]. Classical information and quantum information based on entangled quantum systems can be used for quantum communication purposes such as teleporting quantum states [10, 11].

Owing to significant experimental advances, methods for processing quantum information have developed rapidly during the last few years.[1] Basic quantum communication schemes have been realized with photons [10, 11], and basic quantum logical operations have been demonstrated with trapped ions [13, 14] and with nuclear spins of organic molecules [15]. Also, cavity quantum electrodynamical setups [16], atom chips [17], ultracold atoms in optical lattices [18, 19], ions in an array of microtraps [20] and solid-state devices [21–23] are promising physical systems for future developments in this research area. All these technologically oriented, current developments rely on fundamental quantum phenomena, such as quantum interference, the measurement process and entanglement. These phenomena and their distinctive differences from basic concepts of classical physics have always been of central interest in research on the foundations of quantum theory. However, in emphasizing their technological potential, the advances in quantum infor-

[1] Numerous recent experimental and theoretical achievements are discussed in [12].

mation processing reflect a profound change in the general attitude towards these fundamental phenomena. Thus, after almost two decades of impressive scientific achievements, it is time to retrace some of those significant early developments in quantum physics which are at the heart of quantum technology and which have shaped its present-day appearance.

1.1 Early Developments

Many of the current methods and developments in the processing of quantum information have grown out of a long struggle of physicists with the foundations of modern quantum theory. The famous considerations by Einstein, Podolsky and Rosen (EPR) [24] on reality, locality and completeness of physical theories are an early example in this respect. The critical questions raised by these authors inspired many researchers to study quantitatively the essential difference between quantum physics and the classical concepts of reality and locality. The breakthrough was the discovery by J.S. Bell [25] that the statistical correlations of entangled quantum states are incompatible with the predictions of any theory which is based on the concepts of reality and locality of EPR. The constraints imposed on statistical correlations within the framework of a local, realistic theory (LRT) are expressed by Bell's inequality [25]. As the concept of entanglement and its peculiar correlation properties have been of fundamental significance for the development of quantum information processing, it is worth recalling some of its most elementary features in more detail.

1.1.1 Entanglement and Local, Realistic Theories

In order to clarify the characteristic differences between quantum mechanical correlations originating from entangled states and classical correlations originating from local, realistic theories, let us consider the following basic experimental setup (Fig. 1.1). A quantum mechanical two-particle system, such as a photon pair, is produced by a source s. Polarization properties of

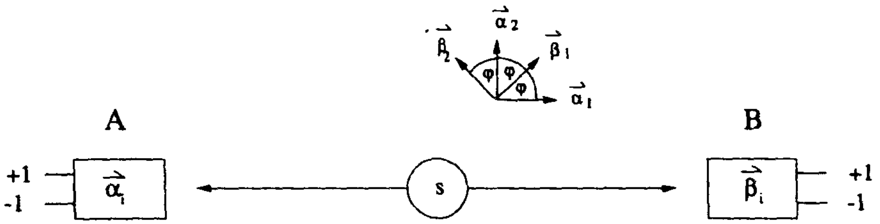

Fig. 1.1. Basic experimental setup for testing Bell's inequality; the choices of the directions of polarization on the Bloch sphere for optimal violation of the CHSH inequality (1.3) correspond to $\varphi = \pi/4$ for spin-1/2 systems

each of these particles are measured subsequently by two distant observers A and B. Observers A and B perform polarization measurements by randomly selecting one of the directions $\boldsymbol{\alpha}_1$ or $\boldsymbol{\alpha}_2$, and $\boldsymbol{\beta}_1$ or $\boldsymbol{\beta}_2$, respectively, in each experiment. Furthermore, let us assume that for each of these directions only two measurement results are possible, namely $+1$ or -1. In the case of photons these measurement results would correspond to horizontal or vertical polarization.

What are the restrictions imposed on correlations of the measurement results if the physical process can be described by an underlying LRT with unknown (hidden) parameters? For this purpose, let us first of all summarize the minimal set of conditions any LRT should fulfill.

1. The state of the two-particle system is determined uniquely by a parameter λ, which may denote an arbitrary set of discrete or continuous labels. Thus the most general observable of observer A or B for the experimental setup depicted in Fig. 1.1 is a function of the variables $(\boldsymbol{\alpha}_i, \boldsymbol{\beta}_j, \lambda)$. If the actual value of the parameter λ is unknown (hidden), the state of the two-particle system has to be described by a normalized probability distribution $P(\lambda)$, i.e. $\int_\Lambda \mathrm{d}\lambda\, P(\lambda) = 1$, where Λ characterizes the set of all possible states. The state variable λ determines all results of all possible measurements, irrespective of whether these measurements are performed or not. It represents the element of physical reality inherent in the arguments of EPR: "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity" [24].
2. The measurement results of each of the distant (space-like separated) observers are independent of the choice of polarizations of the other observer. This assumption reflects the locality concept inherent in the arguments of EPR: "The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former" [24]. Thus, taking into account also this locality requirement, the most general observable of observer A for the experimental setup depicted in Fig. 1.1 can depend on the variables $\boldsymbol{\alpha}_i$ and λ (for B, $\boldsymbol{\beta}_j$ and λ) only.

These two assumptions, which reflect fundamental notions of classical physics as used in the arguments of EPR, restrict significantly the possible correlations of measurements performed by both distant observers. According to these assumptions, the following measurement results are possible: $a(\boldsymbol{\alpha}_i, \lambda) \equiv a_i = \pm 1$ $(i = 1, 2)$ for observer A, and $b(\boldsymbol{\beta}_i, \lambda) \equiv b_i = \pm 1$ $(i = 1, 2)$ for observer B. For a given value of the state variable λ, all these possible measurement results of the dichotomic (two-valued) variables a_i and b_i $(i = 1, 2)$ can be combined in the single relation

$$|(a_1 + a_2)b_1 + (a_2 - a_1)b_2| = 2\,. \qquad (1.1)$$

It should be mentioned that this relation is counterfactual [26] in the sense that it involves both results of actually performed measurements and possible results of unperformed measurements. All these measurement results are determined uniquely by the state variable λ. If this state variable is unknown (hidden), (1.1) has to be averaged over the corresponding probability distribution $P(\lambda)$. This yields an inequality for the statistical mean values,

$$\langle a_i b_j \rangle_{\mathrm{LRT}} = \int_{\Lambda} \mathrm{d}\,\lambda \; P(\lambda) a(\boldsymbol{\alpha}_i, \lambda) b(\boldsymbol{\beta}_j, \lambda) \quad (i, j = 1, 2), \tag{1.2}$$

which is a variant of Bell's inequality and which is due to Clauser, Horne, Shimony and Holt (CHSH) [27], namely

$$\mid \langle a_1 b_1 \rangle_{\mathrm{LRT}} + \langle a_2 b_1 \rangle_{\mathrm{LRT}} + \langle a_2 b_2 \rangle_{\mathrm{LRT}} - \langle a_1 b_2 \rangle_{\mathrm{LRT}} \mid \leq 2 \; . \tag{1.3}$$

This inequality characterizes the restrictions imposed on the correlations between dichotomic variables of two distant observers within the framework of any LRT. There are other, equivalent forms of Bell's inequality, one of which was proposed by Wigner [28] and will be discussed in Chap. 3.

Quantum mechanical correlations can violate this inequality. For this purpose let us consider, for example, the spin-entangled singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|+1\rangle_{\mathrm{A}} |-1\rangle_{\mathrm{B}} - |-1\rangle_{\mathrm{A}} |+1\rangle_{\mathrm{B}}) \; , \tag{1.4}$$

where $|\pm 1\rangle_{\mathrm{A}}$ and $|\pm 1\rangle_{\mathrm{B}}$ denote the eigenstates of the Pauli spin operators σ_z^{A} and σ_z^{B}, with eigenvalues ± 1. Quantum mechanically, the measurement of the dichotomic polarization variables a_i and b_i is represented by the spin operators $\hat{a}_i = \boldsymbol{\alpha}_i \cdot \boldsymbol{\sigma}^{\mathrm{A}}$ and $\hat{b}_i = \boldsymbol{\beta}_i \cdot \boldsymbol{\sigma}^{\mathrm{B}}$. ($\boldsymbol{\sigma}^{\mathrm{A}}$, for example, denotes the vector of Pauli spin operators referring to observer A, i.e. $\boldsymbol{\sigma}^{\mathrm{A}} = \sum_{i=x,y,z} \sigma_i^{\mathrm{A}} \mathbf{e}_i$, where $\mathbf{e}_i$ are the unit vectors.) The corresponding quantum mechanical correlations entering the CHSH inequality (1.3) are given by

$$\langle \hat{a}_i \hat{b}_j \rangle_{\mathrm{QM}} = \langle \psi | \hat{a}_i \hat{b}_j | \psi \rangle = -\boldsymbol{\alpha}_i \cdot \boldsymbol{\beta}_j \; . \tag{1.5}$$

Choosing the directions of the polarizations $(\boldsymbol{\alpha}_1, \boldsymbol{\beta}_1)$, $(\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2)$, $(\boldsymbol{\alpha}_2, \boldsymbol{\beta}_2)$ on the Bloch sphere so that they involve an angle of $\pi/4$ (see Fig. 1.1), one finds a maximal violation of inequality (1.3), namely

$$\mid \langle \hat{a}_1 \hat{b}_1 \rangle_{\mathrm{QM}} + \langle \hat{a}_2 \hat{b}_1 \rangle_{\mathrm{QM}} + \langle \hat{a}_2 \hat{b}_2 \rangle_{\mathrm{QM}} - \langle \hat{a}_1 \hat{b}_2 \rangle_{\mathrm{QM}} \mid = 2\sqrt{2} > 2 \; . \tag{1.6}$$

Thus, for this entangled state, the quantum mechanical correlations between the measurement results of the distant observers A and B are stronger than any possible correlation within the framework of an LRT. Obviously, these correlations are incompatible with the classical notions of reality and locality of any LRT. It is these peculiar quantum correlations originating from entanglement which have been of central interest in research on the foundations of quantum theory and which are also of central interest for quantum information processing.

So far, numerous experiments testing and supporting violations of Bell's inequality [29–31] have been performed.[2] However, from a strictly logical point of view, the results of all these experiments could still be explained by an LRT, owing to two loopholes, namely the locality and the detection loopholes. The locality loophole concerns violations of the crucial locality assumption underlying the derivation of Bell's inequality. According to this assumption one has to ensure that any signaling between two distant observers A and B is impossible. The recently performed experiment of G. Weihs et al. [31] succeeded in fulfilling this locality requirement by choosing the separation between these observers to be sufficiently large. However, so far all experiments have involved low detection efficiencies, so that in principle the observed correlations which violate Bell's inequality can still be explained by an LRT [32,33]. This latter detection loophole constitutes a major experimental challenge, and it is one of the current experimental aims to close both the detection loophole and the locality loophole simultaneously [34–36].

The concepts of physical reality and locality which lead to inequality (1.3) can also lead to logical contradictions with quantum theory which are not of statistical origin. This becomes particularly apparent when one considers an entangled three-particle state of the form

$$|\psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}(|+1\rangle_{\mathrm{A}}|+1\rangle_{\mathrm{B}}|+1\rangle_{\mathrm{C}} - |-1\rangle_{\mathrm{A}}|-1\rangle_{\mathrm{B}}|-1\rangle_{\mathrm{C}}) , \tag{1.7}$$

a so-called Greenberger–Horne–Zeilinger (GHZ) state [37]. Again $|\pm 1\rangle_{\mathrm{A}}$, $|\pm 1\rangle_{\mathrm{B}}$, and $|\pm 1\rangle_{\mathrm{C}}$ denote the eigenstates of the Pauli spin operators σ_z^{A}, σ_z^{B}, and σ_z^{C}, with eigenvalues ±1. Similarly to Fig. 1.1, let us assume that the polarization properties of this entangled quantum state are investigated by three distant (space-like separated) observers A, B and C. Each of these observers chooses his or her direction of polarization randomly along either the x or the y axis.

What are the consequences an LRT would predict? As the three observers are space-like separated, the locality assumption implies that a polarization measurement by one of these observers cannot influence the results of the other observers. Following the notation of Fig. 1.1, the possible results of the polarization measurements of observers A, B and C along directions $\boldsymbol{\alpha}_i$, $\boldsymbol{\beta}_j$ and $\boldsymbol{\gamma}_k$ are $a_i = \pm 1$, $b_j = \pm 1$ and $c_k = \pm 1$. Let us now consider four possible coincidence measurements of these three distant observers, with results (a_x, b_x, c_x), (a_x, b_y, c_y), (a_y, b_x, c_y) and (a_y, b_y, c_x). As we are dealing with dichotomic variables, within an LRT the product of all these measurement results is always given by

$$R_{\mathrm{LRT}} = (a_x b_x c_x)(a_x b_y c_y)(a_y b_x c_y)(a_y b_y c_x) = a_x^2 b_x^2 c_x^2 a_y^2 b_y^2 c_y^2 = 1 \ . \tag{1.8}$$

What are the corresponding predictions of quantum theory? In quantum theory the variables a_i, b_j and c_k are replaced by the Pauli spin operators

[2] For a comprehensive discussion of experiments performed before 1989, see [29].

$\hat{a}_i = \boldsymbol{\alpha}_i \cdot \boldsymbol{\sigma}^{\mathrm{A}}$, $\hat{b}_j = \boldsymbol{\beta}_j \cdot \boldsymbol{\sigma}^{\mathrm{B}}$ and $\hat{c}_k = \boldsymbol{\gamma}_k \cdot \boldsymbol{\sigma}^{\mathrm{C}}$. The GHZ state of (1.7) fulfills the relations

$$\begin{aligned} &\hat{a}_x\hat{b}_x\hat{c}_x|\psi\rangle_{\mathrm{GHZ}} = -|\psi\rangle_{\mathrm{GHZ}} \,, \\ &\hat{a}_x\hat{b}_y\hat{c}_y|\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y\hat{b}_x\hat{c}_y|\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y\hat{b}_y\hat{c}_x|\psi\rangle_{\mathrm{GHZ}} = |\psi\rangle_{\mathrm{GHZ}} \,. \end{aligned} \tag{1.9}$$

Therefore the quantum mechanical result for the product of (1.8) is given by

$$R_{\mathrm{QM}}|\psi\rangle_{\mathrm{GHZ}} = (\hat{a}_x\hat{b}_x\hat{c}_x)(\hat{a}_x\hat{b}_y\hat{c}_y)(\hat{a}_y\hat{b}_x\hat{c}_y)(\hat{a}_y\hat{b}_y\hat{c}_x)|\psi\rangle_{\mathrm{GHZ}} = (-1)|\psi\rangle_{\mathrm{GHZ}} \tag{1.10}$$

and contradicts the corresponding result of an LRT. These peculiar quantum mechanical predictions have recently been observed experimentally [38]. The entanglement inherent in these states offers interesting perspectives on the possibility of distributing quantum information between three parties [39].

1.1.2 Characteristic Quantum Effects for Practical Purposes

According to a suggestion of Feynman [40], quantum systems are not only of interest for their own sake but might also serve specific practical purposes. Simple quantum systems may be used, for example, for simulating other, more complicated quantum systems. This early suggestion of Feynman emphasizes possible practical applications and thus indicates already a change in the attitude towards characteristic quantum phenomena.

In the same spirit, but independently, Wiesner suggested in the 1960s the use of nonorthogonal quantum states for the practical purpose of encoding secret classical information [41].[3] The security of such an encoding procedure is based on a characteristic quantum phenomenon which does not involve entanglement, namely the impossibility of copying (or cloning) nonorthogonal quantum states [4]. This impossibility becomes apparent from the following elementary consideration. Let us imagine a quantum process which is capable of copying two nonorthogonal quantum states, say $|0\rangle$ and $|1\rangle$, with $0 < |\langle 0|1\rangle| < 1$. This process is assumed to perform the transformation

$$\begin{aligned} &|0\rangle|\varphi\rangle|a\rangle \to |0\rangle|0\rangle|a_0\rangle \,, \\ &|1\rangle|\varphi\rangle|a\rangle \to |1\rangle|1\rangle|a_1\rangle \,, \end{aligned} \tag{1.11}$$

where $|\varphi\rangle$ represents the initial quantum state of the (empty) copy and $|a\rangle$, $|a_0\rangle$, $|a_1\rangle$ denote normalized quantum states of an ancilla system. This ancilla system describes the internal states of the copying device. As this copying process has to be unitary, it has to conserve the scalar product between the two input and the two output states. This implies the relation $\langle 0|1\rangle(1 - \langle 0|1\rangle\langle a_0|a_1\rangle) = 0$. This equality can be fulfilled only if either states

[3] Though this article was written in the 1960s, it was not published until 1983.

$|0\rangle$ and $|1\rangle$ are orthogonal, i.e. $\langle 0|1\rangle = 0$, or if $\langle 0|1\rangle = 1 = \langle a_0|a_1\rangle$. Both possibilities contradict the original assumption of nonorthogonal, nonidentical initial states. Therefore a quantum process capable of copying nonorthogonal quantum states is impossible. This is an early example of an impossible quantum process.

Soon afterwards, Bennett and Brassard [42] proposed the first quantum protocol (BB84) for secure transmission of a random, secret key using nonorthogonal states of polarized photons for the encoding (see Table 1.1). In the Vernam cipher, such a secret key is used for encoding and decoding messages safely [6,43]. In this latter encoding procedure the message and the secret key are added bit by bit, and in the decoding procedure they are subtracted again. If the random key is secret, the safety of this protocol is guaranteed provided the key is used only once, has the same length as the message and is truly random [44]. Nonorthogonal quantum states can help in transmitting such a random, secret key safely. For this purpose A(lice) sends photons to B(ob) which are polarized randomly either horizontally (+1) or vertically (−1) along two directions of polarization. It is convenient to choose the magnitude of the angle between these two directions of polarization to be $\pi/8$. B(ob) also chooses his polarizers randomly to be polarized along these directions. After A(lice) has sent all photons to B(ob), both communicate to each other their choices of directions of polarization over a public channel. However, the sent or measured polarizations of the photons are kept secret. Whenever they chose the same direction (yes), their measured polarizations are correlated perfectly and they keep the corresponding measured results for their secret key. The other measurement results (no) cannot be used for the key. Provided the transmission channel is ideal, A(lice) and B(ob) can use part of the key for detecting a possible eavesdropper because in this case some of the measurements are not correlated perfectly. In practice, however, the transmission channel is not perfect and A(lice) and B(ob) have to process their raw key further to extract from it a secret key [45]. It took some more years to realize that an exchange of secret keys can be achieved with the help of entangled quantum states [46]. Thereby, the characteristic quantum correlations of entangled states and the very fact that they are incompat-

Table 1.1. Part of a possible idealized protocol for transmitting a secret key, according to [42]

A(lice)'s direction i	1	2	1	1	2	1	2	2	1	2	···
A(lice)'s polarization	+1	−1	−1	+1	+ 1	+1	−1	−1	−1	+1	···
B(ob)'s direction i	2	1	1	2	2	1	2	1	1	2	···
B(ob)'s measured polarization	+1	−1	−1	−1	+1	+1	−1	+1	−1	+1	···
Public test of common direction	No	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	···
Secret key			−1		+1	+1	−1		−1	+1	···