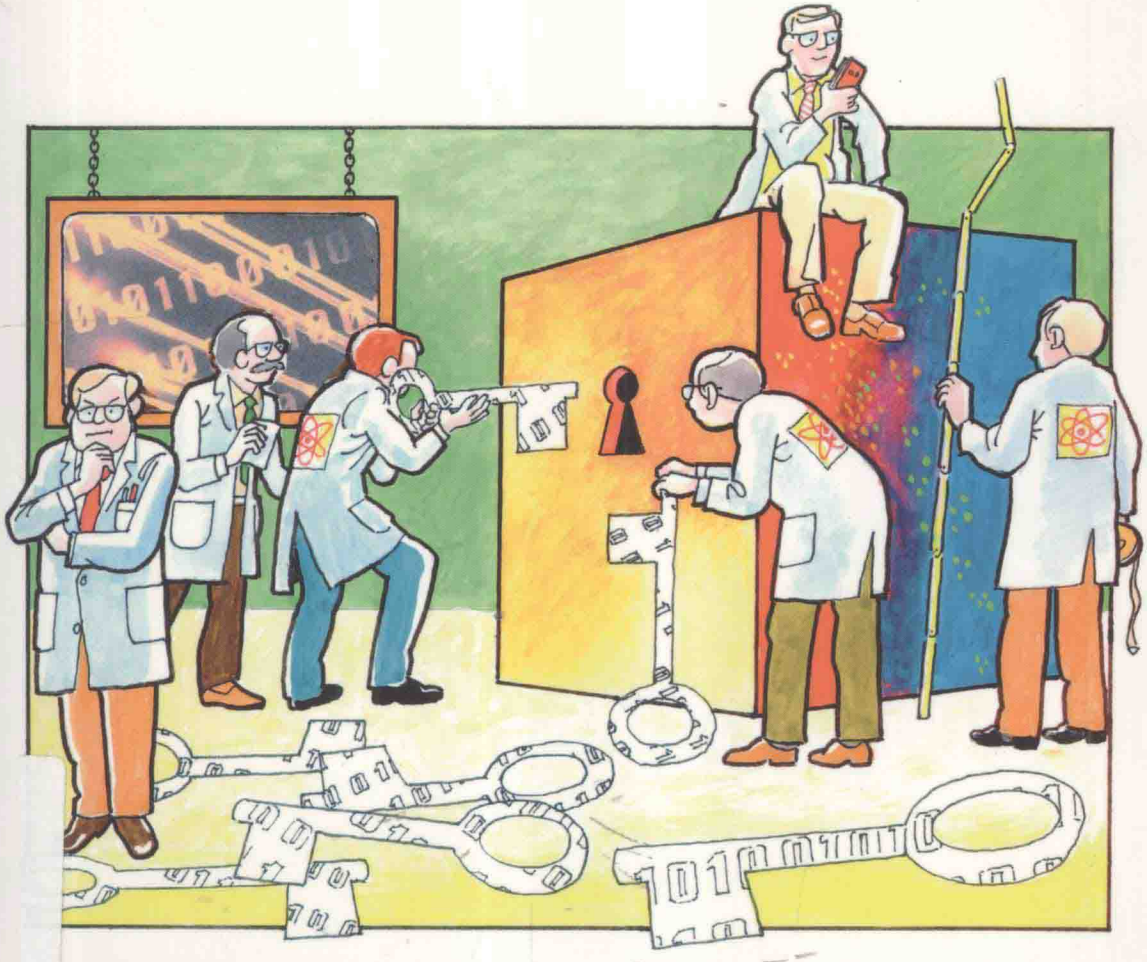
PHYSICS TEXTBOOK

Oliver Morsch

WILEY-VCH

Quantum Bits and Quantum Secrets

How Quantum Physics is Revolutionizing Codes and Computers



Oliver Morsch

Quantum Bits and Quantum Secrets

How Quantum Physics is Revolutionizing Codes and Computers

WILEY-VCH Verlag GmbH & Co. KGaA

The Author

Dr. Oliver Morsch
Dipartimento di Fisica
Universitá di Pisa
Pisa, Italy

Cover

© ***Wolfgang Beyer***

Library of Congress Card No.:
applied for

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

Bibliographic information published by the Deutsche Nationalbibliothek
Die Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at <http://dnb.d-nb.de>.

Typesetting Uwe Krieg, Berlin
Printing Strauss GmbH, Mörlenbach
Binding Litges & Dopf GmbH, Heppenheim

Printed in the Federal Republic of Germany
Printed on acid-free paper

ISBN: 978-3-527-40710-1

Oliver Morsch

Quantum Bits and Quantum Secrets

Related Titles

Audretsch, J.

Entangled Systems

Directions in Quantum Physics

2007. Softcover

ISBN: 978-3-527-40684-5

Audretsch, J. (ed.)

Entangled World

The Fascination of Quantum Information and Computation

2006. Hardcover

ISBN: 978-3-527-40470-4

Stolze, J., Suter, D.

Quantum Computing

A Short Course from Theory to Experiment

2004. Softcover

ISBN: 978-3-527-40438-4

Aczel, A.

Entanglement

The Greatest Mystery in Physics

2002. Hardcover

ISBN: 978-0-470-85046-6

Acknowledgments

This book would not have been completed without the enthusiasm and support of many people. First of all I want to thank Alexander Grossmann at Wiley-VCH for believing in this project from the start and continuing to support it over a period of three years. Many thanks also to Anja Tschörtner for helping me overcome the initial hurdles, and to Esther Dörring for being patient when progress was slower than hoped, especially as the deadline for submission approached.

Also, I thank my brother André for his hospitality in Amsterdam, where part of this book was written. My parents have, as always, been supporting and encouraging. Finally, and most importantly, Matilde Colatosti has been a constant source of encouragement and love. I cannot thank her enough for that.

Quantum Bits and Quantum Secrets: How Quantum Physics is Revolutionizing Codes and Computers.
Oliver Morsch

ISBN: 978-3-527-40710-1

Contents

1 Introduction *1*

2 The Colors of the Rainbow
A Prelude *5*
2.1 The Early Beginnings *6*
2.2 How Fast is Light? *7*
2.3 Particle or Wave? *8*
2.4 Ripples on a Lake *11*
2.5 A Spark Flies *13*
2.6 In Search of the Ether *15*
2.7 Enter Einstein *16*

3 Light, Waves and Oscillations
Some Useful Facts *19*
3.1 Wavelength, Phase and Interference *19*
3.2 Coherence *23*
3.3 Polarization *25*

4 Nature's Currency
The Story of the Quantum *29*
4.1 An act of Desperation *29*
4.2 Photons Galore *31*
4.3 Uncertainty *33*
4.4 Have You Ever Seen an Atom? *34*
4.5 A Question of Stability *35*

5 Surprising Discoveries
A Glimpse at Quantum Mechanics *41*
5.1 Young Again *41*
5.2 Which Way to the Screen? *42*
5.3 Distant Relations *47*

Quantum Bits and Quantum Secrets: How Quantum Physics is Revolutionizing Codes and Computers.
Oliver Morsch

ISBN: 978-3-527-40710-1

6 When Alice Met Bob
The Principles of Quantum Cryptography *53*
6.1 A History of Secrets *53*
6.2 Zeroes and Ones *55*
6.3 One-time Pads *58*
6.4 Secret Photons *60*
6.5 An Element of Randomness *62*
6.6 Sifting Keys *63*
6.7 The BB84 Protocol *65*
6.8 No Cloning, Please *66*
6.9 Noisy Business *71*
6.10 Growing Secrecy *71*
6.11 Ekert's Idea *73*
6.12 Real-world Quantum Cryptography *73*

7 The Logic of Superpositions
How Quantum Computing Works *77*
7.1 Logic Gates *78*
7.2 The Basic Idea *80*
7.3 Reversibility *81*
7.4 The CNOT Gate *82*
7.5 Something New *85*
7.6 A Magic Test *87*
7.7 Balanced and Unbalanced *89*
7.8 One Step Closer ... *91*

8 Shor's Revolution
An Introduction to Quantum Algorithms *93*
8.1 Grover's Database Search *94*
8.2 How Fast? *99*
8.3 Shor's Factorization Algorithm *100*
8.3.1 Slow Calculations *101*
8.3.2 A Nice Trick *104*
8.3.3 Finding the Period *109*
8.3.4 The RSA Code *112*

9 Promising Prototypes
How Quantum Computers Might be Built *115*
9.1 Moore's End *116*
9.2 The DiVincenzo Criteria *116*
9.3 Qubits in Different Physical Systems *119*
9.3.1 Ions in Electric Traps *120*
9.3.2 Optical Lattices *127*

9.3.3 Superconducting Qubits *134*
9.3.4 Electrons in Quantum Dots *137*
9.3.5 Nuclear Magnetic Resonance *137*
9.3.6 Photonic Quantum Computers *140*

10 Sensitive States
Why Quantum Error Correction is Important *141*
10.1 Classical Error Correction *141*
10.2 A Simple Case *142*

11 Trying the Impossible
More Quantum Tricks *147*
11.1 Teleportation *147*
11.2 Dense Coding *152*

12 Dream or Reality?
The Past, Present and Future of Quantum Information *157*
12.1 The Past *157*
12.1.1 Feynman's Input *158*
12.2 The Present *160*
12.3 The ARDA Roadmap *162*
12.4 Quantum Simulators *162*
12.5 Commercial Systems *163*
12.6 The Future *164*

Internet Resources *167*

Further Reading *169*

Glossary *171*

Bibliography *175*

Index *177*

1
Introduction

Can you keep a secret? And, if necessary, can you also safely convey that secret to someone else? I don't mean the kind of secret that you transmit by whispering it in someone's ear, but rather more mundane, and nevertheless extremely important, everyday secrets: PIN numbers for cash machines, internet shopping with your credit card, even sending an email, in fact. You may not have given this question much thought up to now, except if you are one of the unfortunate people who have had their credit cards cloned or their computers hacked into. Also, you may ask yourself: what does quantum physics have to do with all this? After all, you probably bought this book because its title suggested some connection between quantum physics, computers and secrets, whatever these secrets might be. When you have finished reading this book, you will know what these connections are, and possibly never think about computers, communication and information in quite the same way again.

If someone asked you what quantum physics has ever done for you, what would you tell them? Maybe you wouldn't be able to answer at all, but most likely you would think of electronics (the transistor, for example, owes its existence to the fact that its inventors knew a thing or two about quantum mechanics) and all that was spawned by it, not least computers and all other kinds of entertaining and useful things. You might also know that the laser is based on quantum mechanical principles (even if you are not quite aware of what they actually are), and without the laser we wouldn't have compact discs or laser surgery, to name just two. The list of technologies that in some way or another are closely linked to quantum physics is virtually endless (I could go on about things like atomic clocks and the GPS navigation system, for instance). Every day we use devices based on quantum physics that make our lives easier, safer or simply more entertaining. And yet, the biggest revolution involving the quantum is still to come. Actually, it's happening as we speak.

All over the world, thousands of scientists – not just physicists, but also mathematicians, engineers and computer experts – are involved in what may one day be called the "quantum information revolution", or something very much like it. "Quantum information", we will see, is a double-edged sword: it

Quantum Bits and Quantum Secrets: How Quantum Physics is Revolutionizing Codes and Computers.
Oliver Morsch

ISBN: 978-3-527-40710-1

can make sending and keeping secrets both *easier* and *harder* at the same time. If you have ever had any encounter at all with quantum physics, this kind of schizophrenia may be familiar to you. In the quantum world, particles can be here, there and somewhere else at the same time; they can behave like little solid spheres or like waves on a lake; and two particles that are light years apart can instantly "feel" what happens to the other particle without having to exchange any messages. That in such a strange world it should be possible to use the same physical phenomena to convey messages with absolute security and to build computers that can crack any secret code ever devised by man, may come as no surprise, after all. What may surprise you is that that's exactly the world we live in.

This book is about quantum physics and how the weird properties of the quantum world are being exploited by scientists to construct new kinds of computers, coding machines and information networks. The quantum information revolution is a work in progress, and so the story I will tell in this book doesn't have an ending. It begins with how quantum physics was discovered, then goes on to tell the exciting and very recent story of quantum cryptography and how secrets can be shared using quantum effects, and finally deals with a new kind of computer that scientists are working on, the so-called quantum computer. At least in theory, quantum computers are unimaginably more powerful than even the most sophisticated supercomputers currently in existence. As we will see, so far only a few prototypes exist, and these can't yet do anything very useful. But what they will be able to do – and how – once a "real" one is built, is incredibly exciting. So exciting, in fact, that even if you never thought that you might get interested in quantum physics (or physics in general, for that matter) learning how and why quantum computers work will probably make you think differently about the subject.

I wrote this book with a mixed readership in mind consisting of high-school students, beginning university students and the famous "interested layman". This may not sound like a very homogeneous group of people, and it isn't. Also, there are already a few books out there that would appeal either to someone who knows absolutely nothing about physics, and even more books that are suitable for people who know (or are willing to learn) a lot about that subject, but there is little for those who belong to neither group. So, if you think that you are one of those people, not exactly a science geek, but quite curious to learn about all those fascinating things mentioned above, then this book is for you.

Another common trait I imagined would unite the potential readers of this work is the fear, if not hate, of anything that vaguely resembles a mathematical formula. That's why books written for non-experts usually contain no formulas at all, while books for experts (or those wanting to become experts) are full of them. So, how does a book that aims to appeal to those in between

the extremes deal with the issue of equations, numbers and symbols? I'll confess: yes, this book does contain a few mathematical equations. But don't be disheartened. Believe me, equations and formulas are your friends.

In reality, mathematical equations are nothing other than short-hand notations for things that would take many lines of text to write down, but which can be easily expressed with a couple of symbols. Let me give you an example. If I tell you that "the energy contained in a body of a certain mass is equal to that mass multiplied by the square of the velocity of light", then all I have stated is Einstein's famous formula

$$E = mc^2$$

You will agree that using this short-hand notation saves a lot of space and shows you at a glance what would have taken me several lines to write down in plain English.

Formulas have another advantage. Imagine I want you to tell me what the square-root of 35105374 is. Not easy, unless you have a pocket calculator handy. However, you could do the following. You define that you will represent 35105374 by the symbol a, and its square root by the symbol b. Then you can solve the problem by simply writing

$$b = \sqrt{a}$$

This may seem like cheating, but actually you have only done what mathematicians and physicists do all the time: you have stated a problem in a symbolic way, indicating how the different symbols are mathematically related to each other. If you now want the numerical value of the square-root of 35105374, you'll have to work it out by hand or use a calculator. But in many cases it might be enough just to know how, in our example, a and b are mathematically related. In the course of this book, we shall encounter many examples of mathematical relations that we can use to describe physical phenomena, and in most cases we'll be satisfied with that, without having to actually write down any numbers (in fact, even physicists quite often can only write down the formulas, without being able to work out the numbers). So, I hope you'll agree that using some maths in this book wasn't such a bad idea. But enough apologies. You bought this book because you wanted to find out about quantum bits and quantum secrets. So let the journey begin!

2
The Colors of the Rainbow
A Prelude

The new century was only a few weeks old when the celebrated physicist Lord Kelvin, addressing the British Association for the Advancement of Science in 1900, declared that the discipline he himself had done so much to further was essentially dead. The exact words of his obituary were: "There is nothing new to be discovered in physics now. All that remains is more and more precise measurement." One hundred years later, Kelvin's verdict on the fate of physics ranks among the top ten worst predictions of all times, probably on a par with "I think there is a world market for maybe five computers" (IBM chief Thomas Watson in 1943) and "Heavier-than-air flying machines are impossible", pronounced in 1895 by ... yes, Kelvin again.

But it is easy for us to laugh at Lord Kelvin's shortsightedness now. After all, he was simply expressing a prevailing sentiment. Some of the greatest scientists of his time were convinced that physics had, indeed, managed to explain everything there was to be explained: the pull of gravity, the properties of light, the working mechanism of steam engines. There was nothing, it was widely believed, that couldn't in principle be calculated and understood. The only possible progress was in devising new and better ways of measuring the quantities involved.

Just a few years later, however, physics would undergo a fundamental revolution, and some of the consequences of that revolution scientists are only now beginning to understand and exploit. Although the main main part of this revolution that we will be dealing with in this book – quantum mechanics – was already fully developed by the 1930s, many of its fundamental implications were only appreciated decades later.

Obviously, when Kelvin gave his speech in 1900, physics had existed as a science for more than two thousand years. Much had happened in that time, and many of the discoveries that were made at a brisk pace in the early 20th century relied on what had come before. In this chapter I will relate a small part of the history of physics leading up to the discovery of quantum mechanics. It will be highly condensed, and it will deal almost entirely with one natural phenomenon that, on the one hand, was of the utmost importance in the development of physics and, on the other hand, will accompany us throughout this book. That phenomenon is light.

Quantum Bits and Quantum Secrets: How Quantum Physics is Revolutionizing Codes and Computers.
Oliver Morsch

ISBN: 978-3-527-40710-1

2.1 The Early Beginnings

Light has always fascinated mankind[1]. The early Greek philosophers writing in the centuries before the birth of Christ were particularly interested in vision. Empedocles, for instance, had romantic ideas about how man had received the power to see. His theory was that Aphrodite, goddess of love and beauty, had crafted the eyes of man from the elements earth, water, air and fire, using love as a kind of glue. The fire of the eye, finally, was lit using the "primal hearth fire" of the universe. The inner fire of the eye was an important element of the early theories of vision. Plato would later assume that the eye had a light of its own, a kind of radar beam that exits from the eye and mixes with daylight. This mixture of inner and outer light, Plato thought, allows us to perceive the outside world. Around 300 B.C. Euclid, the founder of geometry, even wrote a treatise entitled *Optics* in which he used arguments from geometry to explain the path taken by the eye's ray of vision.

Another school of Greek philosophers, the atomists, had a different (and in their view much more intuitive) explanation for vision. They believed that thin films called *eidola* or *simulacra* peeled off material objects and thus could arrive at the eye. To be sure, this theory had one big problem: how could the *eidolon* of a large object, say a mountain, be made small enough so as to pass through the opening in the eye? The atomists didn't have a satisfying answer to that.

The ancient philosophers weren't able either to explain atmospheric phenomena such as the rainbow, although they did describe them often and sometimes in great detail. Aristotle, for example, speaks of a sickle made of the colors red, green and purple, while the Roman poet Virgil even saw a thousand different hues. After Aristotle and Virgil the rainbow occupied the minds of people for several hundred years before revealing its secret.

In the centuries between the birth of Christ and the end of the Middle Ages there was a long pause in the interpretation of light, at least in the Western world. In the orient, meanwhile, the Arabic academic Ibn al-Haytham (also known as Alhazen), who was born in Basra (Iraq) in 965, occupied himself with the process of seeing. His theory was based on the observation that one's eye hurts if one looks at the sun for too long. This fact (which doubtless was also known to Empedokles and Plato) was difficult to reconcile with the theory of a "ray of vision" emanating from the eye. Whatever it was that hurt the eye, it had to come from the outside and, in all probability, had to be the same thing that was responsible for vision. According to Alhazen the eye did not contain a fire. Rather, it was dark and had to be illuminated from the outside. It was a *camera obscura*.

1) For a comprehensive history of light, see A. Zajonc (1995). A beautiful collection of light phenomena in nature is M. G. J. Minnaert (1994).

2.2
How Fast is Light?

More than 600 years later it was René Descartes who confirmed Alhazen's hypothesis by checking directly with the help of a dissected eye. Not that of a human being, however, but of an ox. Still, Descartes found what he had been looking for: on the retina of the ox's eye he saw a scaled-down image of the outside world. The astronomers Johannes Kepler and Galileo Galilei also believed that the eye was nothing other than a physical instrument in which light arriving from the outside caused a visual sensation. There remained only one question: what was this light? What was it made of? And how did it enter the eye? At least to the last question Descartes seemed to know the answer. As light was a "divine halo" it reached the eye without delay, i.e., with infinite velocity.

This was also a consequence of his theory of the *plenum* according to which the entire universe is filled with a kind of liquid. Through this liquid all points in space are mechanically connected to one another so that, for instance, a luminous object can instantly cause a sensation in the eye. Just as a blind man can scan his surroundings using a stick and immediately feel a resistance when touching an obstacle, according to Descartes seeing was like scanning the surroundings for luminous objects.

But not all thinkers of his time shared Descartes's view, and a fierce debate about the speed of light had already started. Galileo Galilei wanted to settle the issue with the help of an experiment. His idea was to let two people climb two hills separated by a few miles between which there was good visibility. Before doing so, they were to synchronize their clocks, and one of them had to take a lantern equipped with a shutter with him. Once on top of the hill, the lantern was to be opened at a previously decided time. The second experimenter could then measure the time difference between the opening of the shutter and the arrival of the light on the second hill.

Needless to say that such an experiment was doomed to failure. The clocks of the time were not nearly accurate enough, and even with a distance between the hills of several miles the time difference to be measured would have only been a few thousandths of a second. The important point is, though, that Galilei didn't try to find an answer to the question "how fast is light?" by mere reflection. Treating physical problems by performing experiments was only coming into fashion then, and without a doubt Galilei was a trendsetter in that regard. Still, in order to carry out his experiment successfully, he would have needed much larger distances.

Such distances offer themselves naturally in cosmic dimensions. So, instead of sending a colleague up a far away hill one only had to look for an event happening in the vast expanses of the universe, of which one knew the exact timing. Such an event was the disappearance of the moons of Jupiter, first

observed by Galilei himself, behind their mother planet. In his observations of Jupiter in 1675, the Danish astronomer Ole Rømer found that the exact time of the lunar eclipse depended on the distance of the planet from the Earth at that moment. From this he concluded that the light coming from Jupiter's moons took a finite time to arrive on Earth. Shortly after Galilei had thought for the first time of how the speed of light could be measured, Rømer performed just such a measurement with the help of the stars.

The mathematical analysis of Rømer's data followed suit: a mere two years later the Dutch physicist Christian Huygens calculated the speed of light to be 230 000 kilometers per second. An unbelievably large velocity, to be sure, but *not* infinite. What is even more unbelievable is that Huygens's result was only 20 percent below the actual, exact value known today. The fact that this velocity was 600 000 times larger than the speed of sound didn't bother Huygens, by the way. Like Galilei, he wanted his opinions to be guided only by observations. If light propagated almost a million times faster than sound, then that was the way it was, and one had to accept it as a fact. The experimental results showing that light propagated with large but finite velocity led Huygens to another interesting conclusion: namely, that light was not a body, but a wave.

Galilei had been convinced that light was a material substance, but Huygens had freed himself from the common opinions of his time at an early age. He was irritated by that fact that many of the so-called "insights" of science were not sufficiently corroborated by observations. In his *Treatise* he writes:

> *On the other hand I am surprised that [those scientists] very often declare conclusions that are not at all intuitive to be highly certain and of great value as proofs; but to my knowledge no-one has ever even begun to explain the first and most important manifestations of light in a satisfactory manner.*

Huygens was particularly interested to know why light only propagated in a straight line and why rays of light that cross do not disturb one another.

2.3 Particle or Wave?

All of these properties, Huygens thought, could be effortlessly explained if one regarded light to be a wave. According to Huygens, this wave travelled in a medium just as acoustic waves did, and each point of the surface of a wave became the center of a new wave. As a consequence, light propagated across the outer shell of all these little waves (see Fig. 2.1). Based purely on these simple assumptions, Huygens was able to explain the reflection as well