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!