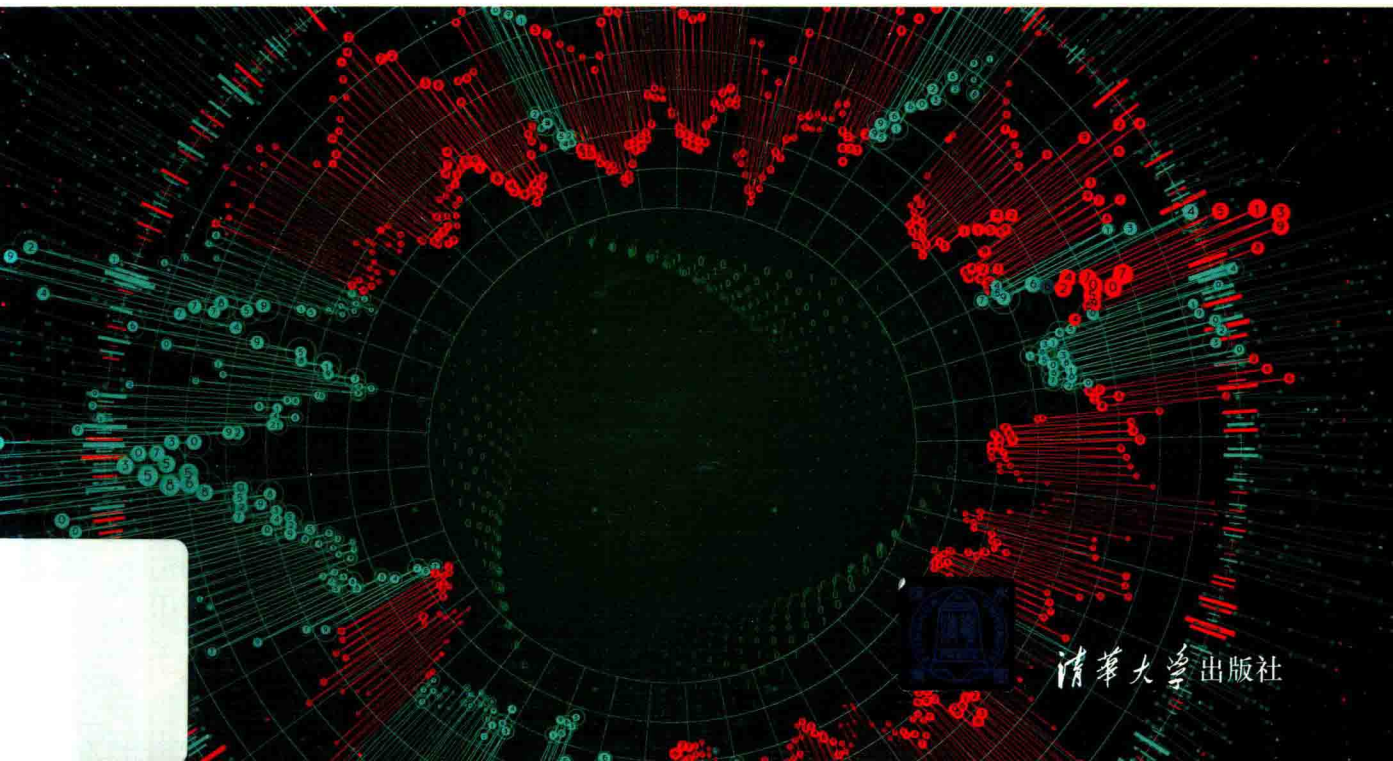
量子计算机

穿越未来世界

李联宁◎编著

了解量子力学和未来计算机，从这本书开始

- 量子技术是近年来发展的前沿技术领域，**大数据搜寻、破译密码、机器学习、人工智能、身份识别**都是量子计算擅长的方向。
- **量子计算**和**量子通信可以解决经典计算机无法解决的问题**，5年内将会出现相应的商业化运用，10年内会有普遍性的运用。
- 本书**适用于所有对量子计算机**领域感兴趣、具有强烈求知欲和希望走进未来世界的读者。



清華大學出版社

量子计算机

穿越未来世界

李联宁◎编著

清華大學出版社
北京

内 容 简 介

量子技术是近年来发展的前沿技术领域，大数据搜寻、破译密码、机器学习、人工智能、身份识别都是量子计算擅长的方向。无论是量子计算还是量子通信，目的都在于解决经典计算机无法解决的问题。预计，5 年内将会出现相应的商业化运用，10 年内会有普遍性的运用，国内外都很关注这一技术的发展。

本书以浅显易懂的方式讲解复杂的技术前沿问题，避免使用高深的量子力学、高等数学、计算机原理专业知识，深入浅出地详细介绍量子计算机的基础理论、最新技术。

本书按量子计算机发展阶段和不断扩展的应用范围依次介绍了涉及量子计算与通信的相关理论基础、量子计算、量子通信与网络、量子安全与密码系统、行业案例研究、量子技术发展前景。

近年来，量子技术有长足的发展，量子计算机与量子通信已经出现在未来世界的门口，目前国内图书市场上开始出现一些量子科学技术书籍，但主要是国外原版专著或其译本，大多数对应于研究生教学层次。为适应广大对现代技术有浓厚兴趣的读者的需求，作者编著了这本量子计算机入门科普书籍，必要时也可作为各级院校的专业教材。

图书在版编目(CIP)数据

量子计算机：穿越未来世界/李联宁编著. —北京：清华大学出版社，2019
ISBN 978-7-302-52305-5

Ⅰ. ①量…　Ⅱ. ①李…　Ⅲ. ①量子计算机—普及读物　Ⅳ. ①TP385-49

中国版本图书馆 CIP 数据核字(2019)第 029201 号

责任编辑：白立军
封面设计：杨玉兰
责任校对：梁　毅
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：20.5　　**字　　数**：349 千字
版　　次：2019 年 9 月第 1 版　　**印　　次**：2019 年 9 月第 1 次印刷
定　　价：49.00 元

产品编号：079354-01

前言

先问大家如下三个问题。

第一个问题，在世界IT行业最著名的与比尔·盖茨齐名、自学中文成才的华人女婿是谁？凡是IT行业的人纷纷举手，是Facebook（脸书）创始人兼首席执行官马克·扎克伯格。对！

第二个问题，马克·扎克伯格的孩子是男孩还是女孩？一半的人举手，女孩。有人还补充说，马克·扎克伯格准备在孩子长大以后把自己的99%的资产裸捐出去。对！

第三个问题，谁看过马克·扎克伯格抱着女儿读一本书的照片？只有25%的人有印象。如果我再加深一点，读的书的书名是什么？绝对没有人注意过！

我告诉你，书名是*Quantum Physics for Babies*，翻译成中文，书名就是《给宝宝的量子物理学》。有人问，这是她应该学的东西吗？马克·扎克伯格的回答是“不管她未来想做什么，做老师也好，像她妈妈那样，做医生也好，或者她想从事自己的事业，我希望她都能有这样的求知欲。求知欲就是我想知道为什么，以及我为什么不能做得更好。”

受马克·扎克伯格的启发，作者编写了下面这么一本书，全书分三部分。

第一部分　基础理论及概念，包括第1章～第4章。

第二部分　量子计算与通信部分，包括第5章和第6章。

第三部分　量子技术安全与应用技术部分，包括第7章和第8章。

在这本书里，你可以发现以下内容。

- 苹果有没有真正落在牛顿头上？
- 计算机怎么和力学搞到一起了？

- 原来我们反复学过的物理只是解释了宏观世界的规律，一到微观世界就不灵了。
- 挑战量子力学的带头大哥就是爱因斯坦！
- 爱因斯坦的“鬼魅学说”——量子纠缠。
- 千里之外的心灵感应——隐形传输。
- 量子隐形传态是“嗖”的一声把人传过去的瞬间传输吗？
- 量子密码的鼻祖——海森伯测不准原理。
- 所有计算机（包括量子计算机）的同一祖宗——图灵机。
- 我们说的“量子比特”不是“比特币”。
- 为什么当今所有的密码系统都失效了。
- 信息化战争：量子计算的意义不亚于核武器。
- 传统计算机渐渐接近它们的极限，近 20 年芯片的发展速度几乎没有提升！
- 量子计算机真的来了，全球第一台商用型量子计算机售价 1500 万美元。
- 在量子计算机给予一种新的计算能力水平的同时，IT 工程师会失业吗？

书名考虑选为《量子计算机——穿越未来世界》，其含义有两个层次：

第一，作为量子计算及通信的入门科普书籍；

第二，作为未来 10～20 年 IT 行业技术进步的入门基础知识储备教科书。

本书献给所有具有强烈求知欲和希望走进未来世界的朋友们，谢谢您看完以上这段文字。

编　者

2019 年 3 月

目 录

第1章

漫话：量子计算机来了

1.1 量子技术的前世今生

1.1.1 先说说什么是量子

量子究竟是什么？

我们知道，构成物质的最小单元是基本粒子，而量子就是质量、体积、能量等各种物理量的最小单元，而且它也要以某种粒子状态存在。简单地讲，量子不是粒子，它是计量能量的最小单位。

最早，量子是被一个叫普朗克的德国物理学家（如图 1-1 所示）在 1900 年提出来的，后来陆陆续续经过许多科学家的努力，其中也包括大名鼎鼎的爱因斯坦，使得量子科学体系不断完善。

图 1-1　德国物理学家普朗克

如果用通俗的话描述量子，就可以这么理解：世界上，有些东西是连续的，例如打

开水龙头，有水流出来，根据水龙头打开的大小，水流可以连续地发生变化。但有些东西就不能这样了，例如机枪，射出的子弹就不能连续变化，要么一个，要么两个，总之是 n 个，n 只能是整数，你用机枪发射 1/2 个子弹试试？

平常，人们看到的物质是由原子组成的，可是原子世界的运动规律与宏观世界完全不同。例如，原子的能量不是连续变化的，而是一份一份的，物理学家就把其中最小的一点点分量叫作量子。后面讲到的，当今最火的量子通信就是利用这种规律做出来的通信技术。

科学家发现，光线也是不连续的，而是由一个一个光子组成的，人们称之为光量子。研究量子的科学，叫量子力学。随着研究的深入，科学家发现，微观世界的各种基本粒子，无一例外，都服从量子力学的规律，这些规律和人们日常所见的宏观世界的规律大相径庭，这让人们瞠目结舌，困惑不解。

1.1.2 宏观世界和微观世界是那么的不同

宏观世界与微观世界是那么的不同，例如，在宏观世界，波和粒子是不同的概念，但在微观世界，两者可以统一起来。例如光线，既可以看成是波——光波，又可以看成是粒子——光子，具有“波粒二重性”。

当爱因斯坦第一次提出光的“波粒二重性”的时候，遭到大多数人的嘲笑和攻击：什么意思？每周 1、3、5 是波，2、4、6 是粒子，轮流坐庄？这不是胡说八道吗？

然而，实验证明，爱因斯坦是对的：任何时候，光都有波粒二重性。人们理解不了，也没有办法，只能慢慢理解吧。

还有，在宏观世界，一个物体的速度和位置，是可以同时准确测定的，例如飞机来了，雷达可以把飞机的速度、位置都准确测定。但对于微观粒子，就不行了，科学家发现，如果把一个基本粒子的位置测准了，它的速度就测不准了。还有，时间和能量，也只能测准其中之一。这就是著名的“测不准原理”。

顺便说一句，在微观世界，测量可不是一件简单的事，测量会破坏或改变微观粒子的状态。

还有一种难以理解的现象，就是量子纠缠。

如果把两个基本粒子“纠缠”起来（如何纠缠后面再讲），然后把这两个粒子分开，一个放在北京，一个放在上海，当你改变北京那个粒子的状态时，上海那一个粒子的状态也会同时改变，尽管它们之间没有发生任何联系。

这种“超距作用”的传播距离，还可以更远，理论上，即使两个粒子相隔若干光年，例如一个放在地球上，另一个放到织女星上，也是可以相互影响的。

这种现象，在历史上被爱因斯坦称为“鬼魅学说”，他认为违反了因果律和定域性原则，是不可信的，为此，他和量子力学的代表人物——丹麦物理学家玻尔，争论了很多年。

但是，近年来越来越多的实验证明，爱因斯坦可能错了。

2015 年 10 月 25 日，荷兰代尔夫特理工大学的科学家们把两颗钻石分别放在代尔夫特理工大学校园内的两侧，距离 1.3km。每块钻石含有一个可以俘获单个电子的微小空间，每个空间放置一个被纠缠过的电子，它们之间，没有任何方式的联系。实验证明，确实存在这种奇异的“超距作用”，改变其中一个的状态，另一个的状态也发生了改变。

1.2 世界上最小的“东西”是量子

1.2.1 分子、原子和量子，哪个最大？哪个最小

分子是由原子组成的。分子最大，量子最小。这三者之间有没有什么关系呢？

大家在上中学的物理和化学课时就知道：

质子 + 中子 = 原子核；

原子核 + 电子 = 原子；

原子 + 原子 = 分子；

原子失去或得到部分电子，就是离子。

至于等离子，这么说吧，带正电和负电的粒子，如原子核和电子，在一块，但又不组成原子，分散存在，这种状态叫作等离子状态，这种物体叫作等离子体。

总结一下，物质是由分子构成，分子是由原子构成，原子是由更小的粒子——质子、中

子和电子构成。后来又有中微子、夸克。如今人类科技发现最小的粒子还有重子、强子、介子及超子等。基本粒子的结构关系与尺寸关系如图 1-2 所示。

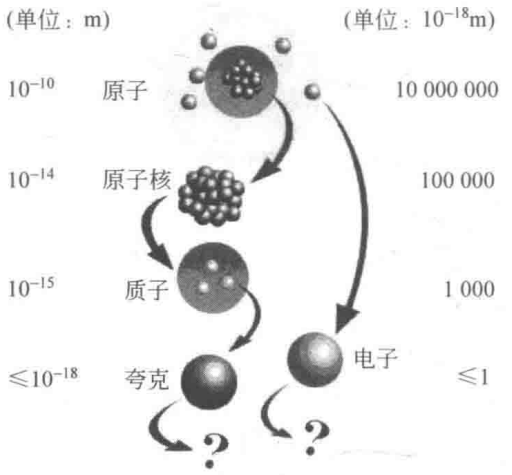


图 1-2　基本粒子的结构关系与尺寸关系

如果你说搞不清楚，一定是上课睡觉梦见周公去了，可以考虑重新再上一回物理课。

1. 原子

原子(atom)指化学反应不可再分的基本微粒，原子在化学反应中不可分割，但在物理状态中可以分割。原子由原子核和绕核运动的电子组成。原子是构成一般物质的最小单位，同类原子统称为元素。已知的元素有 118 种。

2. 质子

质子(proton)是一种带 1.6×10^{-19}C(库仑)正电荷的亚原子粒子，大约是电子质量的 1836.5 倍。原子核中质子数目决定其化学性质和它属于何种化学元素。

世界上原子不是最小的量子(量子是能量的单位)，质子是带正电的小微粒，就是小粒子，中子是不带电的小粒子，两者都非常小。电子是带负电的小粒子，比质子和中子还小。光是由粒子构成的，每个粒子就叫作光子。

3. 夸克

夸克(quark)是一种参与强相互作用的基本粒子，也是构成物质的基本单元。夸克互