面向21世纪物理学丛书

量子计算与通信加密

张镇九 张昭理 李爱民 编著

华中师范大学出版社

MIANXIANG ERSHIYI SHIJI WULIXUE CONGSHU

(鄂)新登字 11 号

图书在版编目(CIP)数据

量子计算与通信加密/张镇九　张昭理　李爱民编著.
-武汉:华中师范大学出版社,2002.9
(面向 21 世纪物理学丛书)
ISBN 7-5622-1316-X/O·135

Ⅰ.量…　Ⅱ.①张…　②张…　③李…
Ⅲ.量子无线电物理学　Ⅳ.0455

中国版本图书馆 CIP 数据核字(2002)第 053318 号

面向 21 世纪物理学丛书

量子计算与通信加密

华中师范大学出版社出版发行
(武昌桂子山　邮编:430079)
新华书店湖北发行所经销　　文字六〇三厂印刷

责任编辑:苏　睿　　封面设计:罗明波
责任校对:张　钟　　督　　印:方汉江

开本:850 mm×1168 mm　1/32　　印张:10　字数:237 千字
版次:2002 年 9 月第 1 版　　2002 年 9 月第 1 次印刷
印数:1—1 000　　定价:30.00 元(精)

本书如有印装质量问题,可向承印厂调换。

序　言

不论是在人生的道路上，还是在科学探索的过程中，有时候要回顾过去、审视现在并展望将来。物理学已有很长的发展历史，将来也必定还将有更大的发展。在这世纪相交之际，希望有这样的关于物理学的书：它能在整体上以较为一致的观点将迄今为止人们认为对物理学既是最重要、又是最基本的认识和问题作一个较为系统的概括；它是在科学上比较严格和比较可靠的科学专著；它在内容的选取上应力求简明，即不过于深邃和庞杂；它应是对物理学科内部的各分支学科、物理学的边沿学科以及与物理学相交叉的学科感兴趣的学者可作为学习和进一步开展研究的参考。本丛书正是为满足上述希望所作的尝试。

周光召

一九九七年九月七日

Preface

From time to time, we need to review the history, examine the present and the future perspectives. Physics has quite a long history, and is bound to have magnificent future. Standing at the turning point of the century, one will find such books on physics interesting and revealing: that the books should provide a systematic review of the mature understandings of the fundamental and important concerns in physics. The content of the book needs to be concise, without involving too much detailed derivatives and being encyclopedic. They should serve as useful reference books for the investigators engaged in branches of physics and relevant fields. The organizing of this series of books is an attempt with this goal in mind.

Zhou Guang Zhao

周光召

September 7, 1997

《面向21世纪物理学丛书》

内容简介

本书是国家“九五”重点出版规划图书——《面向21世纪物理学丛书》中的一卷，是论述量子计算与通信加密的理论和实验基础及其最新进展的一部专著。本书适合对量子物理学、量子信息论、量子通信及加密、量子计算机以及量子理论的基本问题等相关方面感兴趣的学者及教学、科研人员参考。

本书首先论述量子物理和量子信息的理论基础，然后分别论述量子通信、量子计算和量子加密的基础和实验实现，特别在量子交缠态的基础上对量子通信和加密、量子计算机的原理、量子算法、退相干和纠错码的研究进展做了论述，并对量子理论中的某些基本问题的实验检验现状进行了简介和讨论。

量子论创立100年以来，不仅其思想基础和基本问题在争论中得到了发展，而且在固体特性和光辐射方面的应用导致了半导体和激光器的产生。近年来，一些新的量子现象，如量子交缠、量子超距传态、量子非定域性均已得到实验证实，这是可以肯定的，而且是非常重要的。我们认为，由信息科学、量子力学和计算机科学结合而成的新的量子信息科学已经建立起来。量子技术在信息科学方面的应用正导致量子通信和加密系统以及量子计算机从实验室走向实用。就其对科学本身发展的重要性以及在应用方面的前景来看，发展量子技术将可能带来信息科学的革命性发展，因而是新世纪的巨大挑战之一。

尽管如此，撇开量子力学与(狭义和广义)相对论之间的一致性不谈，这些新量子现象后面的物理思想，如量子超距传态的量子因果性、量子态在整个空间的瞬时塌缩、量子测量等，我们还是感到没有弄明白。

Abstract

This book, entitled "Quantum information, computation and cryptography", is one of the volumes of Facing 21 – Century Advanced Series in Physics, the key series of the Publishing Plan of "the Ninth Five – year (1996 – 2000) Project" of China. It is intended for graduates, teachers and researchers in the branches of quantum physics, quantum information, quantum communication and cryptography, quantum computers and fundamental problems in quantum physics and related specialties.

This book consists of 6 chapters. The Chapter 1 is an introduction. The Chapter 2 is the basis of quantum physics, including basic experimental facts, bases of quantum mechanics, entaglement states, macroscopic quantum states and comments on some fundamental problems in quantum physics. In Chapters 3, we discuss quantum information and quantum communications. In chapter 4, we discuss principles of quantum computers. Chapter 5 deals with the quantum algorithms and their experimental realization. In the last chapter, we discuss quantum cryptography.

Since the discussion between Einstein and Bohr which culminated in 1935 with the incompleteness and inconsistency argument and its rebuttal by Bohr, a great deal has been written and recently a lot of experiments have been performed. The famous Bell inequality in 1964, the famous experiment by Aspect in 1981, by Jian – Wei Pan et al. in 2000, and by Rowe in 2001, push us to recognize the nonlocality as an important quantum phenomenon.

The entangled state becomes a very important subject for us. The preparation of entangled EPR－pairs and the quantum teleportation have been realized in laboratory by Bouwmeester D et al. in 1997.

A new area called quantum information combined of information theory, quantum mechanics and computer sciences has been established. The applications of quantum information such as quantum communications and quantum computation are also active areas.

Developing quantum technologies is identified as one of the grand challenges for physics based on their intrinsic scientific importance, their potential for broad impact and application, and their promise for major progress during the next decade.

We have confidence to think that the recently theoretical and experimental developments on entanglement and nonlocality are solid and important for our understanding quantum mechanics and that the developments on quantum information, computation and cryptography are very important, but further developments will not be easy, therefore will be wonderful and attractive.

Even so, when we put aside the consistency between quantum mechanics and relativity, both special and general, the physical ideas underlying new quantum phenomena, such as the quantum causality of the quantum teleportation, the instantaneous collapse of a quantum state in the whole space, and the quantum measurements are still not so clear to us.

前　言

从21世纪回头看，如果将1609年伽利略使用望远镜观看月球作为以观察和实验为基础的现代科学的起点，那么现代科学的历史竟然才近400年。近400年来，科学技术有了巨大的发展，从蒸汽机、载人宇宙飞船、国际互联网、克隆生物到量子计算机；从农业革命、工业革命到信息革命，人类社会生活发生了前人难以想象的巨大变化。

量子论创立100年以来，量子力学在固体特性和光辐射方面的应用已导致半导体和激光器的产生。现在，相对论、量子论和信息论的结合形成量子信息论，它的应用使光量子通信和加密系统以及量子计算机正从实验室走向实用，成为信息革命的新的重要内容。

促使作者写这本书的主要动因有三个：一是近20年来量子物理的理论和实验基础有重要新进展，希望在新的基础上加以认识；二是近年来在量子信息的传递、处理、加密以及纠错的理论和实验实现方面的重要新进展，量子计算机和安全的量子通信技术正从实验室走向实用，对此，希望有个阶段性的概括；三是希望将这些认识和概括结合起来。著者试图在这方面作一点尝试，故成此书。

本书假设读者具有大学物理和高等数学的基础，但不预先要求相对论、量子力学、量子电动力学以及计算机方面的专门知识。在要用到这些专门知识的地方会作相应的过渡。

本书撰写的分工如下：第4章及第5章由张昭理执笔；第2章部分(2.2,2.3,2.4)、第3章部分(3.1,3.2,3.5)及第6章由李爱民执笔；其余部分由张镇九执笔，全书由张镇九统稿。

作者之一(张镇九)感谢国家自然科学基金资助。感谢张端明教授、杨亲德教授、黄焕然教授提出宝贵的修改意见。

新的发展日新月异,著者的水平有限,书中的不足必定不少,诚希读者不吝指正。

作 者

2002 年 3 月于武昌桂子山

目　录