

# 量子逻辑门与 量子退相干

张登玉 著



科学出版社

湖南省重点学科建设项目资助

# 量子逻辑门与量子退相干

张登玉 著

科学出版社

北京

## 内 容 简 介

量子信息是量子力学、信息科学和计算机科学结合成的新学科。本书研究量子信息中量子逻辑门与量子退相干及其相关问题。每一章节均以专题进行探讨。主要内容包括：量子信息中的基本问题（量子计算的量子力学原理、激光与分子相互作用制备量子态、量子信息中的纯态和混合态以及量子态的矩阵表示等）；在量子逻辑门这一章中，重点研究用基本的两位量子逻辑门实现  $n$  位量子逻辑门的功能、Fredkin 量子门的实现方法和辐射场与二能级原子相互作用的量子逻辑功能等问题，提出和分析利用激光选态激发实现量子 XOR 门和量子 Fredkin 门的功能；针对多种相互作用模型，研究辐射场中单个二能级原子退相干特性，分析二能级原子与环境（多模光场）相互作用时自发发射导致的退相干问题以及热辐射场中两个二能级原子退相干及其消除；运用 Kraus 算子分析二能级原子及多能级（三能级和四能级）量子态的退相干特性和激光器中离子密度矩阵元的演化规律；用半经典理论和量子理论研究二能级原子的量子态保真度，对热辐射中存在偶极相互作用以及二能级原子与热辐射场 Raman 相互作用时原子量子态保真度进行探讨。

本书可供物理学和光学相关专业本科生、量子光学和量子信息方向硕士研究生及相关研究人员作为学术参考。

### 图书在版编目 (CIP) 数据

量子逻辑门与量子退相干 / 张登玉著。—北京：科学出版社，2013

ISBN 978-7-03-035993-3

I. ①量… II. ①张… III. ①量子力学—研究 IV. ①O413.1

中国版本图书馆 CIP 数据核字(2012) 第 26667 号

责任编辑：刘凤娟 尹彦芳 / 责任校对：朱光兰

责任印制：钱玉芬 / 封面设计：新者设计

科 学 出 版 社 出 版

北京东黄城根北街 16 号

邮政编码：100717

<http://www.sciencep.com>

骏 主 印 刷 厂 印 刷

科学出版社发行 各地新华书店经销

\*

2013 年 1 月第 一 版 开本：B5(720 × 1000)

2013 年 1 月第一次印刷 印张：16 1/2

字数：315 000

定 价：59.00 元

(如有印装质量问题，我社负责调换)

## 前　　言

量子信息技术以量子力学原理为基础, 充分利用量子相干性来探索以全新的方式进行计算、编码和信息传输的可能性, 为突破芯片极限提供新概念、新思路和新途径, 实现有信息技术无法做到的新的信息功能. 由于量子信息处理在提高运算速度、确保信息传输安全、增大信息容量和提高检测精度等各方面具有潜在的巨大应用价值, 量子信息不仅引起了各国政府和科技界的广泛关注, 而且受到信息产业界和军事部门的高度重视. 毋庸置疑, 量子信息科学的迅速发展, 必将引起划时代的信息技术革命, 人类将进入量子信息技术时代. 因此, 量子信息学的研究被确定为我国中长期科学和技术发展规划纲要(2006~2020年)重大科学研究计划“量子调控研究”的主要内容之一. 量子信息学的研究内容主要包括量子计算、量子通信、量子密码、量子测量和量子模拟等.

实现量子计算, 一方面要求量子比特要能很好地保持其相干性, 能够实现与外界良好的隔离; 另一方面又要求能精确而有效地控制系统的演化, 即需要量子系统之间有很好的耦合. 因此, 选择什么样的物理体系来实施量子计算要兼顾这两个方面的要求. 量子计算要通过许多量子处理器(量子比特)来实现, 因此适用于研制量子计算的物理体系要能实现由一定数量的量子处理器构成的“量子芯片”, 而且还要能对任意一个和两个量子处理器实施精确的操控. 当前实现量子计算的瓶颈在于如何研制含有大数目量子处理器的物理体系, 它既可有效地克服退相干的影响, 又具有物理可扩展性. 近年来, 科学家正在努力寻找能实现量子计算的物理系统, 目前的研究主流集中在下列两个方向: ①固态量子计算, 包括超导、量子点等; ②基于量子光学的量子计算, 包括离子阱、腔量子电动力学(QED)、线性光学、光子晶体、光格子等. 这些不同的物理系统各有优缺点: 固态量子计算系统的物理可扩展性较好, 但退相干严重; 而基于量子光学的量子计算系统, 量子相干性较好, 但物理可扩展性较差.

量子通信与量子计算中最容易导致信息传输中状态失真或计算结果错误的原因是由退相干引起的. 如果量子态的演化过程不是幺正变换, 则量子态之间的相干性消失, 即发生退相干现象. 或者说, 当量子系统从相干叠加态演化为完全混合态时, 量子干涉性消失, 即发生退相干. 由于量子系统不是完全隔离于它的环境, 量子通信与量子计算的运作与周围器件(环境)的量子动力学规律有关, 使得量子态的演化不是幺正变换, 从而导致量子状态失真或计算结果错误. 减少或消除退相干, 是量子通信与量子计算技术变成现实的关键.

围绕减少或消除退相干, 国外学者和国内(如中国科技大学、清华大学、中国科学院理论物理研究所、中国科学院武汉物理与数学研究所、国防科技大学和湖南师范大学等)一些专家教授做了一些富有成效的研究工作. 另外, 提出了各种不同的量子编码方案, 其中两类最重要的量子编码是量子纠错码和量子防错码, 以便减少退相干. 近几年, 一些学者对量子系统的退相干做了较深入的研究, 例如, 利用低  $Q$  腔在无退相干子空间实现量子信息操控; 研究环形腔中两个原子空间退相干的量子动力学特性, 结果表明两原子空间退相干强烈依赖于两原子的相对位置. 考虑空间自由度时, 研究了两原子内态纠缠动力学, 得出解纠缠时间依赖于原子空间分布波包的宽度, 在有限时间内, 纠缠衰减接近零. D. Amrit 探讨了量子位与量子位之间的相互作用能否使纠缠持续时间延长, 存在随机电报噪声(telegraph) 和  $1/f$  噪声时, 当一对量子位通过交换相互作用进行耦合, 对于最大纠缠态(Bell 态), 交换相互作用能抑制退相干和解纠缠; 研究了开放量子系统通过与非马尔可夫库的强耦合的退相干抑制问题. Chaudhry 利用连续波驱动场研究了两量子位和两位逻辑门的退相干控制问题. 最近, 一些研究人员考虑相互独立的自旋链环境与量子比特耦合的退相干(退纠缠)问题.

量子逻辑门与量子退相干是量子信息中非常重要的课题, 是近几年极活跃的前沿研究领域. 本书在构造量子逻辑门的方法、量子逻辑门的物理实现、量子逻辑门系统的退相干、环境对量子位作用导致退相干、量子选态激发、量子计算机存储单元的退相干以及消除量子系统的退相干等方面提出了一些新的理论研究方法和实验可行性方案, 在国内外已引起一定反响. 本书大部分内容已在专业核心刊物上发表. 相关科研成果“量子计算中的逻辑门与退相干”2001 年获衡阳市政府科技进步一等奖; “量子信息中多量子比特的操纵和控制”2011 年获湖南省人民政府自然科学奖三等奖. 本书作者多次获湖南省自然科学优秀论文奖. 本书所涉内容可为多量子比特系统的相干操控研究提供重要的知识积累, 为可拓展的量子信息处理实验研究提供一些基本的理论依据.

本人主要科研方向为量子光学与量子信息. 1988 年 9 月至 1991 年 6 月, 在核工业理化工程研究院激光应用专业读硕士研究生, 主要从事激光与原子相互作用方面的研究工作. 1998 年 6 月获中国科学院安徽光学精密机械研究所光学专业博士学位. 1991 年 7 月至今, 一直在高校从事教学和科研工作, 多年来担任量子力学和电动力学教学工作, 并对这两门基础学科进行了较深入的研究, 为科研奠定了比较坚实的基础. 1993 年 9 月至 1994 年 7 月, 在国防科技大学计算机系全脱产进修计算机一年, 较全面地掌握了(经典)计算机原理, 对目前从事量子计算及量子信息技术方面的研究工作有很大帮助. 1995 年 9 月至 1995 年 12 月, 在中国科学院安徽光学精密机械研究所激光光谱学开放实验室从事科研工作. 1996 年 1 月至 1998 年 6 月, 在中国科学院武汉物理与数学研究所波谱与原子分子物理国家重点实验室从事量子计

算的研究,是中国科学院“百人计划”工程的子课题“量子计算与量子计算机”主要参与者。近几年,主持完成湖南省中青年科技基金项目、湖南省自然科学基金项目和湖南省教育厅重点项目等8项省级课题,是3项国家自然科学基金资助课题的主要研究人员。在量子态制备、激光选态激发、量子逻辑门在光学等物理系统中的实现以及量子计算与量子通信物理实现中的退相干问题等方面取得了比较突出的成果。已在 *Physical Review A*、*Journal of Physics B*、*Optics Communications*、*Chinese Physics Letters*、*Chinese Physics* 和《物理学报》等国内外专业学术期刊上发表有关量子信息、激光与物质(原子和分子等)相互作用等方面论文30余篇,其中被SCI、EI摘(收)录20余篇(次)。

本书出版之际,我衷心感谢博士生导师詹明生教授、读博士期间的师兄弟(刘堂昆、王继锁、冯健、王谨、柳晓军、赵宏太、周本汉等)、衡阳师范学院领导以及物理与电子信息科学系的高峰、汪新文、唐世清和谢利军等老师。由于本人学识水平有限,书中肯定还存在许多不足甚至错误之处,敬请专家、读者指正!

张登玉

2012年4月

# 目 录

## 前言

<b>第 1 章 量子信息基础</b> .....	<b>1</b>
1.1 量子计算基础 .....	1
1.1.1 量子计算的量子力学原理 .....	2
1.1.2 量子位 .....	3
1.1.3 量子态的叠加 .....	4
1.1.4 量子逻辑门 .....	6
1.1.5 量子计算中的退相干 .....	10
1.1.6 量子纠错及防错 .....	13
1.2 态的相干与非相干 .....	14
1.2.1 经典理论中态的相干性 .....	14
1.2.2 量子理论中态的相干性 .....	15
1.2.3 相干性的密度矩阵描述 .....	15
1.2.4 量子测量中的相干性问题 .....	16
1.3 激光与分子相互作用制备量子态 .....	16
1.4 激光的偏振与量子信息中的量子态 .....	22
1.4.1 激光的各种偏振态及矩阵表示法 .....	22
1.4.2 光子的偏振态可作为量子信息中的量子态 .....	23
1.4.3 偏振器的量子逻辑功能 .....	24
1.5 量子信息中的纯态和混合态 .....	25
1.5.1 量子纯态和混合态 .....	25
1.5.2 纯态和混合态密度算符的区别 .....	26
1.5.3 量子纠缠态与量子纯态和混合态 .....	27
1.5.4 纯态演化为混合态导致退相干 .....	28
1.6 量子态的矩阵表示 .....	29
1.6.1 波函数的物理解释 .....	29
1.6.2 量子纯态和量子混合态的矩阵表示 .....	30
1.6.3 量子纠缠态的矩阵表示 .....	33
1.6.4 相干叠加态的矩阵表示及其退化 .....	34

---

1.7 量子相干与量子退相干 .....	38
1.7.1 经典相干 .....	38
1.7.2 量子相干 .....	39
1.7.3 经典相干和量子相干的比较 .....	40
1.7.4 量子退相干 .....	41
1.8 量子纯态与混合态中力学量的测量 .....	44
1.8.1 量子纯态中力学量的测量 .....	46
1.8.2 量子混合态中力学量的测量 .....	47
主要参考文献 .....	49
<b>第 2 章 量子逻辑门 .....</b>	<b>51</b>
2.1 用基本的两位量子逻辑门实现 $n$ 位量子逻辑门的功能 .....	51
2.1.1 用基本的量子逻辑门实现多位量子逻辑门的功能 .....	51
2.1.2 两位量子门实现多位量子门方案与 Barenco 方案的比较 .....	53
2.2 构造 Fredkin 量子门的一种简易方法 .....	54
2.2.1 六个基本的两位量子门完成 Fredkin 门的功能 .....	55
2.2.2 “条件翻转方案”的特点 .....	56
2.3 激光对分子振动态的控制与量子 Fredkin 逻辑门 .....	56
2.3.1 分子的局域模振动态 .....	56
2.3.2 激光对分子振动态的控制实现量子 Fredkin 逻辑门功能 .....	58
2.4 光学偏振器的量子逻辑功能 .....	59
2.4.1 泡利矩阵变换对应偏振器的操作 .....	60
2.4.2 利用偏振器实现量子非门和量子异或门的操作 .....	60
2.4.3 偏振器在构造量子 Toffoli 门和量子 Fredkin 门中的作用 .....	62
2.5 量子逻辑门的算符及矩阵表示 .....	63
2.5.1 量子逻辑门的哈密顿算符及对应的幺正变换矩阵 .....	64
2.5.2 量子逻辑门的输入输出态与量子力学系统波函数 .....	70
2.6 量子逻辑门中的编码量子位研究 .....	72
2.6.1 量子字节被控编码方法 .....	73
2.6.2 字节被控编码方法特点 .....	76
2.7 激光选态激发的量子逻辑功能 .....	76
2.7.1 激光选态激发理论模型 .....	77
2.7.2 激光选态激发实现量子 XOR 门和 Fredkin 门的功能 .....	79
2.7.3 利用激光选态构造四位量子防错码 .....	81
2.8 辐射场与二能级原子相互作用的量子逻辑功能 .....	82
2.8.1 辐射场与二能级原子相互作用的半经典理论分析 .....	83

---

2.8.2 辐射场与二能级原子相互作用的量子理论分析 .....	85
2.8.3 利用辐射场与二能级原子相互作用实现量子逻辑功能 .....	86
主要参考文献 .....	87
<b>第 3 章 量子退相干及其消除 .....</b>	<b>90</b>
3.1 辐射场中二能级原子的退相干特性 .....	90
3.1.1 大失谐相互作用时二能级原子退相干的消除 .....	90
3.1.2 二能级原子与热库以任意强度耦合时原子的退相干特性 .....	93
3.1.3 压缩真空场中二能级原子的退相干 .....	96
3.1.4 运动的二能级原子相干性的保持 .....	99
3.1.5 超 J-C 模型中的原子置于热辐射场时相干性的保持 .....	102
3.1.6 噪声场中二能级原子相干性的保持 .....	106
3.1.7 囚禁粒子在热库型驻波场中的量子相干特性 .....	110
3.1.8 消除热库中二能级原子的退相干 .....	114
3.1.9 简并双光子过程中二能级原子退相干的消除 .....	130
3.1.10 简并多光子过程中二能级原子退相干的消除 .....	133
3.2 非旋波近似中二能级原子相干性的保持 .....	137
3.2.1 单光子相互作用过程原子相干性的保持 .....	138
3.2.2 简并双光子作用过程原子相干性的保持 .....	141
3.3 类 Kerr 介质中二能级原子与驱动场作用时的相干性 .....	146
3.4 自发发射与量子计算机存储单元的退相干 .....	150
3.4.1 理论模型 .....	150
3.4.2 自发发射导致存储单元退相干 .....	152
3.4.3 两个二能级原子的自发发射导致退相干 .....	153
3.5 量子计算机存储器中的退相干 .....	155
3.5.1 量子计算机中的测量及纠缠 .....	156
3.5.2 编码方法 .....	156
3.5.3 量子位的幺正变换 .....	158
3.6 V 型三能级原子与热辐射场 Raman 相互作用时原子的相干特性 .....	159
3.7 热辐射场中两个二能级原子退相干的消除 .....	161
3.8 存在偶极间相互作用的两个二能级原子的相干特性 .....	165
3.9 两个二能级原子与热辐射场 Raman 相互作用时原子的退相干 动力学 .....	169
主要参考文献 .....	171
<b>第 4 章 运用 Kraus 算子分析量子态的退相干特性 .....</b>	<b>176</b>
4.1 二能级原子同时存在衰变和跃迁时的退相干特性 .....	176

---

4.1.1 Kraus 算子 .....	176
4.1.2 二能级原子同时存在跃迁和自发衰变引起的退相干 .....	178
4.2 三能级原子自发辐射的相干特性 .....	181
4.2.1 三能级原子自发辐射的密度矩阵元 .....	181
4.2.2 自发辐射引起的退相干 .....	185
4.3 热辐射环境中三能级原子的相干特性 .....	187
4.3.1 三能级原子同时存在辐射和吸收时密度矩阵元 .....	187
4.3.2 三能级原子量子态的相干特性 .....	190
4.4 三能级原子中相对位相阻尼引起的退相干 .....	192
4.4.1 三能级原子和环境相互作用时复合系统的幺正演化 .....	192
4.4.2 相对位相阻尼引起的退相干 .....	193
4.5 四能级原子自发辐射的量子相干特性 .....	194
4.5.1 四能级原子自发辐射的密度矩阵元 .....	194
4.5.2 四能级原子自发辐射导致退相干 .....	199
4.6 辐射和单步吸收同时存在时四能级原子相干特性 .....	200
4.6.1 四能级原子的密度矩阵元 .....	200
4.6.2 四能级原子的相干特性 .....	206
4.7 红宝石激光器中离子密度矩阵元的演化 .....	207
4.7.1 红宝石激光器三能级体系的密度矩阵元 .....	207
4.7.2 三能级激光系统粒子数变化规律 .....	210
4.8 固体激光器的四能级系统密度矩阵元的演化 .....	211
4.8.1 固体激光器四能级粒子系统密度矩阵元 .....	212
4.8.2 四能级激光系统粒子数变化规律 .....	215
主要参考文献 .....	217
<b>第 5 章 量子态保真度 .....</b>	<b>219</b>
5.1 半经典理论中二能级原子的量子态保真度 .....	219
5.1.1 辐射场与二能级系统相互作用的半经典理论分析 .....	219
5.1.2 二能级原子的量子态保真度 .....	222
5.2 辐射场中二能级原子的量子态保真度 .....	224
5.2.1 二能级原子与磁场相互作用的半经典理论及原子量子态保真度 .....	224
5.2.2 辐射场与二能级原子相互作用的量子理论及原子量子态保真度 .....	228
5.3 强热辐射环境中二能级原子的量子态保真度 .....	232
5.3.1 强热辐射环境中二能级原子的约化密度矩阵 .....	233
5.3.2 强热辐射环境中二能级原子量子态保真度 .....	237
5.4 热辐射中存在偶极相互作用时原子量子态保真度 .....	238

---

5.4.1 存在偶极相互作用时二能级原子的约化密度矩阵 ······	239
5.4.2 存在偶极相互作用时二能级原子量子态保真度 ······	242
5.5 二能级原子与热辐射场 Raman 相互作用时原子的量子态保真度 ······	243
5.5.1 存在 Raman 相互作用时二能级原子的约化密度矩阵 ······	244
5.5.2 存在 Raman 相互作用时二能级原子的量子态保真度 ······	246
主要参考文献 ······	248

# 第1章 量子信息基础

## 1.1 量子计算基础

量子计算是量子力学与计算机科学结合成的新领域。几十年以前，IBM 公司 T.J.Watson 研究中心的 R.Landauer 和 C.H.Bennett 便开始研究信息处理电路的物理性质，提出了可能发展到何种地步的若干问题：电路能够做成多小？计算过程中必须使用多少能量？由于计算机是物理器件，因此它们的基本工作过程可用物理学描述。一个严峻的物理事实是，当计算机元件的尺寸变得非常之小，以致达到原子的线度，必须用量子力学原理对它们进行描述。20 世纪 80 年代初，P.Benioff 根据 R.Landauer 和 C.H.Bennett 的早期成果，证明了一台计算机原则上可以以纯粹量子力学的方式运行。此后不久，牛津大学数学研究所的 D.Deutsch 和美国以及以色列的其他科学家对量子计算机进行模拟，以弄清它们与经典计算机有什么区别。到 80 年代中期，这一研究领域由于若干原因而衰落了。首先，所有这些研究人员都是从抽象的角度来考虑量子计算机，而不是研究实际的物理系统。其次，量子计算机可能容易出错误，而且不容易纠正错误。

近些年，量子计算引起了人们的极大兴趣。这是因为量子计算比经典计算效率高得多，并且能够求解大数的质因子。大数质因子的分解在密码术方面非常有用，而当今的经典计算没法解决。另外，量子计算能够精确模拟一些物理系统，如新的或未观察过的物质形式，并且能对系统的叠加态进行并行计算。量子计算的原理是计算机科学家将量子力学的叠加原理应用于计算机算法时提出来的。两态系统能够作为量子位(或量子比特，即 quantum bit)。两态系统之间的相互作用能构造量子逻辑门，它遵守非经典的逻辑运算。原则上讲，许多量子逻辑门形成的网络能够以叠加态的形式操纵大量量子位，并以比经典机器更小的计算步程进行并行计算。为了实现量子计算，物理学家和计算机专家提出了一些设计方案，如原子力显微镜 (atomic force microscope)、齿轮箱量子计算机 (gearbox Q.C) 以及用冷却的囚禁粒子和核磁共振 (NMR) 进行计算。但是，设计者面对的最大挑战是量子信息传输过程中，如何在实现量子信息载体间强的可控制的相互作用(如原子力显微镜使两个原子核自旋相互靠近、两个原子通过高精细度光腔进行耦合)的同时，保持量子信息足够好地隔离于宏观的环境，以避免快速的退相干 (decoherence) 过程。

### 1.1.1 量子计算的量子力学原理

量子计算的数字计算结果由一个量子物理过程决定。这就是说，量子计算对应于波函数的演化。虽然经典计算机里所谓“模拟机”，它也是由某种物理过程作运算，但它并不是作数字计算。量子计算以量子力学建立逻辑体系。它的最显著特征是相干叠加性及运算过程中的幺正变换性。这里简单介绍与量子计算紧密相关的量子力学原理，即量子态的主要性质。

(1) 叠加性及干涉性。量子力学中的薛定谔方程  $i\hbar \frac{\partial \Psi}{\partial t} = H\Psi$  是一个线性方程。

如果  $\Psi_1, \Psi_2, \dots, \Psi_n$  分别是方程的解，则它们的线性组合  $\Psi = c_1\Psi_1 + c_2\Psi_2 + \dots + c_n\Psi_n = \sum^n c_n\Psi_n$  也是方程的解 ( $c_1, c_2, \dots, c_n$  是任意常数)。它的物理意义是：如果  $\Psi_1, \Psi_2, \dots, \Psi_n$  所描写的都是体系可能的量子态，那么它们的线性叠加  $\Psi$  所描写的也是体系的一个可能的量子态。对应于量子计算，这表示量子计算机可以同时代表经典计算机中许多态，使得大规模量子并行存储和计算成为可能。对于量子态之间的干涉性，我们以双狭缝衍射实验为例进行简要分析：设  $\Psi_1$  和  $\Psi_2$  分别表示微观粒子穿过上、下狭缝到达屏幕的量子态，则  $\Psi = c_1\Psi_1 + c_2\Psi_2$  表示粒子穿过两个狭缝到达屏幕的量子态。按照态叠加原理，在屏幕上某一点  $P$  出现的几率密度是

$$|\Psi|^2 = |c_1\Psi_1 + c_2\Psi_2|^2 = |c_1\Psi_1|^2 + |c_2\Psi_2|^2 + c_1^*c_2\Psi_1^*\Psi_2 + c_1c_2^*\Psi_1\Psi_2^* \quad (1.1)$$

上式告诉我们：微观粒子穿过狭缝到达  $P$  点的几率密度  $|\Psi|^2$  一般不等于粒子穿过上狭缝到达  $P$  点的几率密度  $|c_1\Psi_1|^2$  与粒子穿过下狭缝到达  $P$  点的几率密度  $|c_2\Psi_2|^2$  之和，而是等于  $|c_1\Psi_1|^2 + |c_2\Psi_2|^2 +$  干涉项。衍射图案的产生证实了干涉项的存在。由于量子态叠加时各态之间存在相对位相差，在并行计算过程中出现干涉相长或相消，这是经典计算机的布尔态不具备的特征。

(2) 态演化。量子态按照幺正变换法则由体系的哈密顿量决定演化过程。体系各个态按照幺正变换同时演化，所以一次量子计算可作用在多个数据上。

(3) 纠缠性 (entanglement)。即一个完整的量子系统的一些确定的态与子系统的确定态并不对应，这说明各子系统之间有关联。它与量子密码和量子通信紧密相关。

(4) 不可自我复制性及不确定性 (nonclonability and uncertainty)。即一个未知的量子态在未受干扰的情况下，既不能被精确地复制也不能被精确地观察。它使得量子通信免于窃听或被窃听的信息无法解读。密码钥 (cryptographic keys) 能够用量子的方法来实现，它是一个近乎完美的反窃取 (eavesdropping) 的保密方法。量子信息的传输特点与经典情况有本质区别，量子态能够被“量子远距传态”(quantum teleportation)，即将一个粒子的真实量子态包含在经典数据与 Einstein-Podolsky-

Rosen(EPR) 关联之中, 然后利用这些成分转生 (reincarnate) 在不处于第一个粒子附近的另一个粒子的态上.

### 1.1.2 量子位

一个光子的偏振或一个自旋为  $1/2$  的粒子的自旋分量或两态系统的上下能态, 对应于布尔态 0 和 1, 可用一对正交的量子位表示, 即  $|0\rangle = |\leftarrow\rangle$ ,  $|1\rangle = |\beta\rangle$  (或  $|0\rangle = |\downarrow\rangle$ ,  $|1\rangle = |\uparrow\rangle$ ), 并且量子位存在叠加, 如  $|\varphi^+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  或  $|\varphi^-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ . 设想一个二能级原子, 初始时处于低能态, 其能量为  $E_0$ , 要向这个原子写入信息 0, 实际上就是不采取任何行动. 要向这个原子写入 1, 就把它激发到高能态 (能量为  $E_1$ ). 为此, 可以用一束激光照射原子, 激光的光子能量等于  $(E_1 - E_0)$ , 如果激光的强度合适, 且照射一段适当的时间, 则该原子在吸收了一个光子后将从低能态跃迁到高能态. 如果这个原子已经处于高能态, 则同一束激光脉冲可使此原子发射一个光子, 并回到低能态. 用信息传输的术语来说, 就是脉冲使原子的信息位 (量子位) 翻转. 如果光的频率合适, 但照射的时间只是使原子从 0 翻转到 1 所需时间的一半, 则原子所处的状态将等于与  $|0\rangle$  对应的波函数和与  $|1\rangle$  对应的波函数的叠加, 每个波函数具有相同的振幅, 这样一种量子位只翻转了一半. 在经典计算机中, 半充电的电容器将造成计算结果错误 (设充电的电容器表示信息 1, 放电的电容器表示信息 0), 但在量子计算机中半翻转的量子位 (对应量子力学中的叠加态) 则开辟了新型计算的途径. 对于两个量子位, 可存在纠缠态, 如  $\Psi^- = (|01\rangle - |10\rangle)/\sqrt{2}$ , 对于  $n$  个量子位, 能叠加成这样的态

$$\Psi = \sum_{x=00\cdots 0}^{11\cdots 1} C_x |x\rangle \quad (1.2)$$

式中,  $C_x$  是复数,  $x$  可取  $2^n$  个值. 对于经典计算机, 在某一时刻有确定的状态, 比如说 011100101…, 然而, 在量子计算机中, 量子位的状态将用一个波函数来描述, 它或许具有下列形式

$$\psi = a |011100101\cdots\rangle + b |111010001\cdots\rangle + \dots \quad (1.3)$$

式中, 系数  $a, b, \dots$  是复数. 量子计算机处于态  $|011100101\cdots\rangle$  的几率是  $|a|^2$ , 处于态  $|111010001\cdots\rangle$  的几率是  $|b|^2$ , 等等. 我们用波函数描述量子计算机的状态, 用几率描述状态的不确定性, 并且复系数  $a, b, \dots$  的位相有真实而重要的意义, 它决定量子态的干涉相长和干涉相消, 能够描述量子计算机中不同态之间的相干性, 在计算过程中非常重要.

量子计算机的状态可存在于所有的量子波函数之中, 当我们进行测量时, 某一特定的状态 (对应于某一波函数) 只能以一定的几率被观察到. 目前还没有一台经

典计算机用上述提到的波函数来描述, 我们现在使用的机器是准确地遵守经典物理规律的。假如将来某一天, 经典计算机位的载体缩小到原子的线度, 那时位的状态以及经典计算机的动力学规律的量子描述将是必需的。Feynman 对这种可能性持乐观态度, 他在 1985 年说: “现今的物理规律并不妨碍减少计算机的体积, 以致将位的载体减小到原子线度的大小, 到那时, 量子行为将起绝对性的支配作用”。

经典计算机中, 一个布尔态只能代表一个数(二进制), 每次运算只能改变一个数值, 但一个量子态理论上可以代表无限个数。量子位运算对应幺正变换

$$|\psi'\rangle = U|\psi\rangle = U \sum_x C_x |x\rangle = \sum_x C'_x |x\rangle \quad (1.4)$$

从计算上讲, 这代表并行运算, 一组数  $C_1, C_2, \dots, C_N$  只经一次运算(幺正变换)即变到另一组数  $C'_1, C'_2, \dots, C'_N$ 。由于  $N$  并无原则上的限制, 故量子计算机可实现经典并行计算所不能达到的超巨大规模的并行计算。这一计算效率的提高所引起的效果远不在速度增强本身, 更重要的是会带来许多质的变化。由于幺正变换决定了计算规则, 量子计算是可逆计算, 因此可以实现逆运算, 即可以从计算结果反推出初值。

存储大量量子位的体系称为量子存储器, 也称量子寄存器。量子存储器的状态可描写成 Hilbert 空间中的一个波函数或状态。量子存储器的状态是可以改变的, 有时我们并不严格区分量子存储器与它所处的状态。

### 1.1.3 量子态的叠加

量子态的叠加原理是量子力学中最基本的、最重要的规律之一。我们可以以光子的偏振来简要地说明态的叠加原理: 假定一束光通过一个方解石晶体, 如果这个晶体只让垂直于光轴的平面偏振光通过, 当光束垂直于光轴偏振, 则它全部通过此晶体; 当光束平行于光轴偏振, 则它完全不能通过此晶体; 当光束的偏振面与光轴成一个角度  $\alpha$ , 则只有全部光的  $\sin^2 \alpha$  通过晶体。如果一束光中只有一个光子, 当光束的偏振面与光轴也是成一个角度  $\alpha$ , 我们观察到的实验事实是: 有时候人们能在晶体的背后发现一个光子, 而另一些时候, 人们找不到任何光子, 我们无论任何时候, 都没有发现一个光子的一部分。如果我们重复这个实验许多次, 则发现在晶体的背后找到光子的几率正比于  $\sin^2 \alpha$ 。设垂直于光轴的平面偏振光子的状态(假设为水平偏振)表示为  $|0\rangle$ , 平行于光轴的平面偏振光子的状态(假设为竖直偏振)表示为  $|1\rangle$ , 则晶体的背后单个光子的状态可表示为

$$|\psi\rangle = \sin \alpha |0\rangle + \cos \alpha |1\rangle \quad (1.5)$$

(1.5) 式的物理意义: 一个光子处于  $|\psi\rangle$  时, 即处于  $|0\rangle$  和  $|1\rangle$  的叠加态, 表示这个光

子处于  $|0\rangle$  的几率为  $\sin^2 \alpha$ , 处于  $|1\rangle$  的几率为  $\cos^2 \alpha$ . 如果  $N$  个光子处于  $|\psi\rangle$  时, 表示处于  $|0\rangle$  的光子数为  $N \sin^2 \alpha$ , 处于  $|1\rangle$  的光子数为  $N \cos^2 \alpha$ .

量子计算中的逻辑门对量子态的作用, 等效于对量子态作幺正变换. 多个量子位的初态为单个量子态, 经过幺正变换后的终态可能变成几个量子态的叠加. 态的叠加结果表现为干涉相长和干涉相消, 即位相相同的量子态得到加强(合并), 位相相反的量子态得到削弱(抵消). 下面在给出量子位叠加态的基础上, 通过具体的实例, 探讨量子计算中态叠加引起的干涉相长和干涉相消现象, 我们举例加以说明. 对于孤立的两态系统, 当哈密顿算符为

$$H = \frac{1}{2}g\mu[H_0\sigma_z + H_1\sigma_yP(t)\sin(\omega t)] \quad (1.6)$$

时, 两态系统(这里指的是光子的水平偏振和竖直偏振)状态的演化矩阵为

$$U(\Omega T) = \begin{pmatrix} e^{i\omega T/2} & 0 \\ 0 & e^{-i\omega T/2} \end{pmatrix} \begin{pmatrix} \cos \Omega T/2 & -\sin \Omega T/2 \\ \sin \Omega T/2 & \cos \Omega T/2 \end{pmatrix} \quad (1.7)$$

(1.6) 式和 (1.7) 式中,  $\Omega = g\mu H_1/4\hbar$  是 Rabi 频率,  $H_1$  是沿  $Y$  轴方向交变磁场的振幅;  $\hbar\omega = g\mu H_0$ ,  $g\mu$  是磁偶极矩,  $H_0$  是沿  $Z$  轴方向的静磁场;  $\sigma_z$  是泡利自旋矩阵;  $P(t)$  是脉冲包络函数. 如果系统中有三个量子位  $a, b, c$ , 假设初始是  $|b\rangle = |0\rangle$ , 其量子逻辑线路示意为图 1.1.

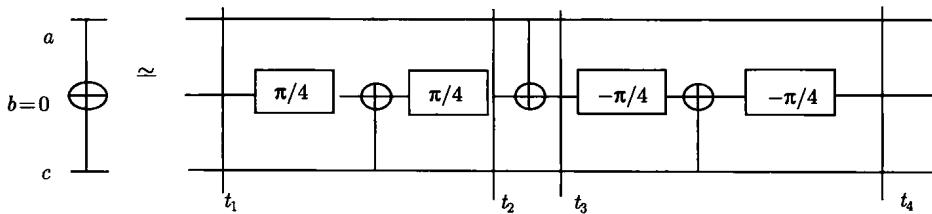


图 1.1 量子逻辑线路示意图

在图 1.1 中, 方框中的  $\pi/4$  表示  $\Omega T = \pi/4$ , 我们可以选取  $\omega T = 4\pi$ , 此时

$$U(\pi/4) = \begin{pmatrix} \cos \pi/8 & -\sin \pi/8 \\ \sin \pi/8 & \cos \pi/8 \end{pmatrix} \quad (1.8)$$

设  $t_1$  时刻三个量子位的状态为  $|abc\rangle_1 = |000\rangle$ , 对于单个量子位, 由于在运算过程中逻辑门的作用相当于幺正矩阵作用于量子位, 因此必须把量子位的状态表示为矩阵的形式, 即

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (1.9)$$

因  $|ac\rangle = |00\rangle$ , 图 1.1 中的异或门不起作用, 所以  $a, c$  的状态在任意时刻都是一样的, 即  $|a\rangle = |c\rangle = |0\rangle$ .  $t_2$  时刻  $|b\rangle$  的状态为

$$|b\rangle_2 = U(\pi/4) \cdot U(\pi/4) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \quad (1.10)$$

即处于  $|0\rangle$  和  $|1\rangle$  的叠加态, 它表示处于量子态  $|0\rangle$  和  $|1\rangle$  的几率均为  $1/2$ .  $t_2$  时刻  $|abc\rangle$  的状态为

$$|abc\rangle_2 = \frac{\sqrt{2}}{2}(|000\rangle + |010\rangle) \quad (1.11)$$

这是三个量子位的叠加态, 它表示处于量子态  $|000\rangle$  和  $|010\rangle$  的几率均是  $1/2$ . 因  $t_2$  时刻与  $t_3$  时刻之间的异或门的控制位为  $|0\rangle$ , 所以  $t_3$  时刻  $|b\rangle$  的状态为

$$|b\rangle_3 = |b\rangle_2 = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \quad (1.12)$$

$t_3$  时刻  $|abc\rangle$  的状态为

$$|abc\rangle_3 = |abc\rangle_2 = \frac{\sqrt{2}}{2}(|000\rangle + |010\rangle) \quad (1.13)$$

$t_4$  时刻  $|b\rangle$  的状态为

$$\begin{aligned} |b\rangle_4 &= U(-\pi/4) \cdot U(-\pi/4) \cdot \left[ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \\ &= \frac{1}{2}(|0\rangle - |1\rangle + |0\rangle + |1\rangle) = |0\rangle \end{aligned} \quad (1.14)$$

(1.14) 式中的量子态  $|0\rangle$  产生干涉相长, 量子态  $|1\rangle$  产生干涉相消, 从而在最后的结果只出现量子态  $|0\rangle$ .  $t_4$  时刻  $|abc\rangle$  的状态为

$$|abc\rangle_4 = |abc\rangle_1 = |000\rangle \quad (1.15)$$

如果  $t_1$  时刻三个量子位的状态为  $|abc\rangle_1 = |101\rangle$ , 我们用类似的方法可得到  $t_4$  时刻  $|abc\rangle$  的状态为  $|abc\rangle_4 = |111\rangle$ , 只是在分析量子位状态演化过程中要注意到量子异或门的作用.

#### 1.1.4 量子逻辑门

经典计算机是用电子电路作计算. 电子电路是由线性元件(如导线、电阻和电容器)和非线性元件(如二极管和三极管)构造而成. 线性元件独立地改变输入信号, 而非线性元件则使经过它的输入信号发生相互作用. 电路通过以极高的速度反复完成若干简单的线性和非线性任务来进行计算. 使信息位发生翻转, 是“非”(NOT)的