“十三五”科学技术专著丛书

量子保密通信协议新进展

秦素娟 温巧燕 高飞 李丹丹 著

Liangzi Baomi Tongxin Xieyi Xinjinzhan

北京邮电大学出版社
www.buptpress.com

“十三五”科学技术专著丛书

量子保密通信协议新进展

秦素娟　温巧燕　高　飞　李丹丹　著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书以作者及其课题组多年的研究成果为主体，结合国内外学者在量子保密通信领域的代表性成果，对这一领域的几个主要研究内容作了系统论述，并提出一些与目前研究紧密相关的新研究课题。全书共分 8 章，第 1 章介绍量子保密通信研究所需要的量子力学基础知识；第 2 章研究量子密钥分发；第 3 章研究量子秘密共享；第 4 章研究量子安全多方计算；第 5 章研究量子保密查询；第 6 章研究量子签名；第 7 章研究量子匿名通信；第 8 章研究可验证的量子随机数扩展。

本书自成体系，内容由浅入深，参考文献丰富，方便读者自学。它既可作为对量子保密通信感兴趣的读者的入门教材，帮助他们尽快熟悉量子密码领域并了解国际前沿进展，也可作为量子保密通信领域研究工作者的参考用书，适用于物理学、密码学、数学等学科的科研人员、教师、研究生和高年级本科生。

图书在版编目（CIP）数据

量子保密通信协议新进展 / 秦素娟等著. -- 北京：北京邮电大学出版社，2017.8
ISBN 978-7-5635-5107-1

Ⅰ. ①量… Ⅱ. ①秦… Ⅲ. ①量子力学—保密通信 Ⅳ. ①O413. 1②TN918

中国版本图书馆 CIP 数据核字（2017）第 114593 号

书　　名：量子保密通信协议新进展
著作责任者：秦素娟　温巧燕　高　飞　李丹丹　著
责 任 编 辑：满志文　姚　顺
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京九州迅驰传媒文化有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：20.5
字　　数：511 千字
版　　次：2017 年 8 月第 1 版　2017 年 8 月第 1 次印刷

ISBN 978-7-5635-5107-1　　定　价：58.00 元

· 如有印装质量问题，请与北京邮电大学出版社发行部联系 ·

前　言

随着信息与网络技术的快速发展和普及，人类处理和交换信息的能力及方式都发生了巨大的变化。信息网络使得身处世界各地的人们联系得更加紧密，并且在社会、文化、经济和军事等领域中发挥着越来越重要的作用。然而，任何事物都具有两面性，信息时代在给人类社会带来巨大进步的同时，也带来了许多严峻的挑战。在信息社会中，每时每刻都有大量的数据和信息在网络中进行传输。随着云计算、大数据、物联网等新技术的发展和应用，未来人们生活中的绝大部分信息都将通过网络进行传输和存储。这些信息小到个人隐私，大到国家决策，大都是和国计民生息息相关的，足见保护信息安全已经成为信息时代的一个必须解决的关键问题。

密码技术是保障信息安全的核心手段，它的发展由来已久。从最初的移位密码、置换密码到如今的公钥密码体制，密码学已经由一种技术逐步发展成了一门科学。我们目前使用的大部分经典密码学协议是基于数学难解问题的，例如大整数分解问题、离散对数问题等。在现有计算能力下，上述难题都难以在短时间内获得结果，所以基于这些难题的经典密码协议也无法在有效时间内被破解。换句话说，在现有的运算速度下，大部分经典密码协议都是计算安全的。然而，随着计算机运算能力的飞速提高（特别是量子计算机的研制）以及各种先进算法（尤其是量子算法）的提出，基于计算复杂性假设的经典密码系统的安全性受到了严峻挑战。为了应对量子计算机及量子算法带给经典密码体制的威胁，人们开始研究能够对抗量子攻击的新型密码算法，量子密码就是在这种背景下应运而生的。

量子密码是经典密码理论和量子力学基本原理相结合而产生的新型密码体制。不同于经典数字信号的正交编码方式，量子信息往往是非正交的且多样化的。这种特殊的编码方式以量子态作为信息载体，依据物理规律而设计，其安全性由 Heisenberg 测不准原理，非正交量子态不可可靠区分定理以及量子不可克隆定理等量子力学特性所保证，与攻击者计算能力的大小无关。根据量子力学性质，窃听者（或非法参与者）对量子密码系统的任何有效窃听行为都将不可避免地给相应的量子信息载体（量子态）带来扰动，从而会在窃听检测中被合

法参与者察觉，这正是量子密码独特的特点。目前量子保密通信理论已成为国内外研究热点，相关的理论和实验研究都获得了快速发展，本书着重从理论角度系统介绍量子保密通信在各个方面的研究进展。

本书是在课题组于2009年出版的《量子保密通信协议的设计与分析》基础上写作而成，是作者及课题组成员对量子保密通信理论近几年理论研究工作最新成果的详细归纳和整理，其内容包括了在量子密钥分发、量子保密查询、量子签名、量子随机数等相关方向取得的一系列成果。希望这些有助于本领域的研究者尽快对量子保密通信研究有一个全面的了解，进而走在国际前沿。

全书共分8章，第1章介绍量子保密通信研究所需要的量子力学基础知识；第2章研究量子密钥分发；第3章研究量子秘密共享；第4章研究量子安全多方计算；第5章研究量子保密查询；第6章研究量子签名；第7章研究量子匿名通信；第8章研究可验证的量子随机数扩展。

本书的完成离不开课题组全体成员的帮助和支持。课题组的林崧博士、王天银博士、孙莹博士、贾恒越博士、宋婷婷博士、黄伟博士、刘斌博士、张可佳博士、王庆乐博士、王玉坤博士、周玉倩博士等的研究工作为本书提供了丰富的资料，在此表示深深的感谢。全书的编写工作还得到了实验室的曹雅博士、李新慧博士、潘世杰博士、万林春博士、宋燕琪硕士、李润泽硕士等的协助，在此一并对他们表示衷心的感谢。

本书的出版得到了国家自然科学基金项目（编号：61671082）和网络与交换技术国家重点实验室课题的资助，也得到了很多学者的鼓励和帮助，在此深表谢意。

希望本书能为广大读者带来帮助。鉴于编者水平有限，对书中的疏漏与不足之处，敬请读者批评指正。

秦素娟

试读结束，需要全本PDF请购买 www.ertongbook.com

目　录

试读结束，需要全本PDF请购买 www.ertongbook.com

第 1 章　量子力学基础知识

这一章把本书所用到的量子力学基础知识简单加以论述，使一些对量子力学不太熟悉的读者易于掌握后面的内容。有关量子力学的参考资料有很多，本章的写作主要参考了文献[1-8]。

1.1　基 本 概 念

量子保密通信以量子力学为基础，其安全性由量子力学基本原理来保证。在介绍协议的设计与分析之前先介绍所使用的一些量子力学基本概念。掌握初等线性代数是理解好量子力学的基础。所以为方便读者阅读，下面先给出本书中出现的量子力学术语（或其记号）所对应的线性代数解释，如表 1.1 所示。

表 1.1　常见记号及其含义

记 号	含 义
$z*$	复数 z 的复共轭，例如：$(1+\mathrm{i})^*=1-\mathrm{i}$
$\|\psi\rangle$	系统的状态向量（Hilbert 空间中的一个列向量）
$\langle\psi\|$	$\|\psi\rangle$ 的对偶向量（$\|\psi\rangle$ 的转置加复共轭）
$\langle\phi\|\psi\rangle$	向量 $\|\phi\rangle$ 和 $\|\psi\rangle$ 的内积
$\|\phi\rangle\otimes\|\psi\rangle$	$\|\phi\rangle$ 和 $\|\psi\rangle$ 的张量积
$\|\phi\rangle\|\psi\rangle$	$\|\phi\rangle$ 和 $\|\psi\rangle$ 的张量积的缩写
$\boldsymbol{A}^*$	矩阵 $\boldsymbol{A}$ 的复共轭
$\boldsymbol{A}^{\mathrm{T}}$	矩阵 $\boldsymbol{A}$ 的转置
$\boldsymbol{A}^\dagger$	矩阵 $\boldsymbol{A}$ 的厄米共轭，$\boldsymbol{A}^\dagger=(\boldsymbol{A}^{\mathrm{T}})^*$
$\langle\phi\|\boldsymbol{A}\|\psi\rangle$	向量 $\|\phi\rangle$ 和 $A\|\psi\rangle$ 的内积，或者 $\boldsymbol{A}^\dagger\|\phi\rangle$ 和 $\|\psi\rangle$ 的内积

1.1.1　状态空间和量子态

任一孤立物理系统都有一个系统状态空间，该状态空间用线性代数的语言描述就是定义了内积的复向量空间——Hilbert 空间。

具体地说，一个复向量空间 $\boldsymbol{L}$ 就是一个集合 $\boldsymbol{L}=\{\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3,\cdots,\boldsymbol{a}_n\}$，满足：(1) 任取 $\boldsymbol{a}_i$，$\boldsymbol{a}_j\in\boldsymbol{L}$，都有 $\boldsymbol{a}_i+\boldsymbol{a}_j\in\boldsymbol{L}$。(2) 任取复数 $c\in\mathbb{C}$，$\boldsymbol{a}_i\in\boldsymbol{L}$，都有 $c\cdot\boldsymbol{a}_i\in\boldsymbol{L}$，则称 $\boldsymbol{L}$ 为复向量空间，$\boldsymbol{L}$ 中元素称为向量。复向量空间 $\boldsymbol{L}$ 上的内积定义为一种映射：对于任意的一对向量 $\boldsymbol{a}_i,\boldsymbol{a}_j\in$

$\boldsymbol{L}$，都有一个复数 $c=(\boldsymbol{a}_i,\boldsymbol{a}_j)$ 与之对应，称为 $\boldsymbol{a}_i$ 和 $\boldsymbol{a}_j$ 的内积，它具有如下性质：

$$\left.\begin{aligned}&(\boldsymbol{a}_i,\boldsymbol{a}_i)\geqslant 0\\&(\boldsymbol{a}_i,\boldsymbol{a}_j)=(\boldsymbol{a}_j,\boldsymbol{a}_i)^*\\&(\boldsymbol{a}_l,c_1\boldsymbol{a}_i+c_2\boldsymbol{a}_j)=c_1(\boldsymbol{a}_l,\boldsymbol{a}_i)+c_2(\boldsymbol{a}_l,\boldsymbol{a}_j)\end{aligned}\right\}\tag{1-1}$$

上述定义了内积的复向量空间 $\boldsymbol{L}$ 称为 Hilbert 空间，对应量子系统的状态空间。量子力学系统所处的状态称为量子态，由 Hilbert 空间中的单位列向量描述，该向量通常称为态向量（或态矢），常用 $|\cdot\rangle$ 表示，也称为右矢。例如 $|\phi\rangle$，$|0\rangle$ 等都表示量子态，其中 ϕ 和 0 是量子态的标号。一个量子态可以用任意标号，习惯上常用 ϕ，φ 和 ψ 等。$\langle\phi|$ 表示 $|\phi\rangle$ 的对偶向量，由 Hilbert 空间中的单位行向量描述。

量子态满足态叠加原理：若量子力学系统可能处在 $|\phi\rangle$ 和 $|\psi\rangle$ 描述的态中，则系统也可能处于态 $|\Phi\rangle=c_1|\phi\rangle+c_2|\psi\rangle$，其中 c_1，c_2 是两复数，且满足 $|c_1|^2+|c_2|^2=1$。当系统处于态 $|\Phi\rangle=c_1|\phi\rangle+c_2|\psi\rangle$ 时，处于 $|\phi\rangle$ 的概率为 $|c_1|^2$，处于 $|\psi\rangle$ 的概率为 $|c_2|^2$。态叠加原理使得量子力学系统具有呈指数增长的存储能力，使得量子计算具有并行计算能力，是量子力学系统与经典系统之间最重要的区别之一。

若量子系统由系统 1 和系统 2 复合而成，且系统 1 处于态 $|\phi_1\rangle$，系统 2 处于态 $|\phi_2\rangle$，则复合系统的状态为两子系统状态的张量积 $|\phi_1\rangle\otimes|\phi_2\rangle$，常记为 $|\phi_1\rangle|\phi_2\rangle$ 或 $|\phi_1\phi_2\rangle$。

设 $\boldsymbol{V}$ 和 $\boldsymbol{W}$ 是维数分别为 m 和 n 的希尔伯特空间，于是 $\boldsymbol{V}\otimes\boldsymbol{W}$ 是一个 mn 维向量空间，具体的来说，设

$$|\phi_1\rangle=\begin{bmatrix}a_1\\a_2\\\vdots\\a_m\end{bmatrix},\quad |\phi_2\rangle=\begin{bmatrix}b_1\\b_2\\\vdots\\b_n\end{bmatrix}\tag{1-2}$$

则 $|\phi_1\rangle$ 和 $|\phi_2\rangle$ 的张量积定义为

$$|\phi_1\rangle\otimes|\phi_2\rangle=(a_1b_1,a_1b_2,\cdots,a_1b_n,a_2b_1,a_2b_2,\cdots,a_2b_n,\cdots,a_mb_1,a_mb_2,\cdots,a_mb_n)^{\mathrm{T}}$$

或者等价的表示为

$$|\phi_1\rangle\otimes|\phi_2\rangle=\begin{bmatrix}a_1|\phi_2\rangle\\a_2|\phi_2\rangle\\\vdots\\a_m|\phi_2\rangle\end{bmatrix}\tag{1-3}$$

1.1.2 完备正交基

一个 n 维 Hilbert 空间 $\boldsymbol{L}$ 的一组基是其上的一组线性无关的向量 $\{|v_1\rangle,|v_2\rangle,\cdots,|v_n\rangle\}$，使得对于任意的 $|u\rangle\in\boldsymbol{L}$，满足 $|u\rangle=\sum_{i=1}^{n}a_i|v_i\rangle$，其中 $a_i\neq 0$ 且是复数。进一步，若其中的向量两两相互正交（内积为 0），且任一向量的模（即 $\sqrt{\langle v_i|v_i\rangle}$）均为 1，则这样的一组基称为完备正交基（或标准正交基）。采用 Gram-Schmidt 正交归一化过程可以把空间的任意一组基构造一组完备正交基。

例如，$\mathbb{C}^2$ 的一组基是

$$|v_1\rangle=\begin{pmatrix}1\\0\end{pmatrix},\quad |v_2\rangle=\begin{pmatrix}0\\1\end{pmatrix} \tag{1-4}$$

因为$\mathbb{C}^2$中任意向量$|v\rangle=(a_1,a_2)^{\mathrm{T}}=a_1|v_1\rangle+a_2|v_2\rangle$。又因为$|v_1\rangle$和$|v_2\rangle$相互正交，且每一个向量的模都为1，所以$\{|v_1\rangle,|v_2\rangle\}$是$\mathbb{C}^2$的一组完备正交基。通常记$|v_1\rangle$为$|0\rangle$，$|v_2\rangle$为$|1\rangle$。此外$\mathbb{C}^2$的另一组常见完备正交基是：

$$|v_3\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},\quad |v_4\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{1-5}$$

因为$\mathbb{C}^2$中任意向量$|v\rangle=\frac{a_1+a_2}{2}|v_3\rangle+\frac{a_1-a_2}{2}|v_4\rangle$，且$|v_3\rangle$和$|v_4\rangle$相互正交，模为1。通常记$|v_3\rangle$为$|+\rangle$，$|v_4\rangle$为$|-\rangle$。容易验证这两组基满足如下关系：

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\quad |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{1-6}$$

可以看出一个Hilbert空间可以由其一组完备正交基完全确定，基中的向量称为基态，基中所含向量的个数称为空间的维数。

进一步地，由于$|0\rangle$和$|1\rangle$恰好是Pauli算子$\boldsymbol{\sigma}_z$的本征向量，$|+\rangle$和$|-\rangle$恰好是σ_x的本征向量，所以也常常把基$\{|0\rangle,|1\rangle\}$记作$\{|z+\rangle,|z-\rangle\}$，把$\{|+\rangle,|-\rangle\}$记作$\{|x+\rangle,|x-\rangle\}$。此外，有的文献里面还会记作$\{|+z\rangle,|-z\rangle\}$和$\{|+x\rangle,|-x\rangle\}$。总之，量子态记号可能会随着不同作者的写作习惯而不同，大家只需要理解其本质表示的是哪个态向量即可。既然$\boldsymbol{\sigma}_z$和$\boldsymbol{\sigma}_x$的本征向量都构成$\mathbb{C}^2$的一组完备正交基，$\boldsymbol{\sigma}_y$的本征向量是否也构成$\mathbb{C}^2$的一组完备正交基呢？答案是肯定的。习惯上把由$\boldsymbol{\sigma}_y$的本征向量构成的基记作$\{|+y\rangle,|-y\rangle\}$或$\{|y+\rangle,|y-\rangle\}$。有关Pauli算子及其本征向量的介绍读者可以参看本书1.1.4节。在不影响阅读的情况下，本书在不同章节也没有对这些记号做最终统一。

1.1.3 量子比特

量子比特(qubit)，或称为量子位，是量子信息中最关心的量子系统。它是经典比特(bit)的量子对应，但不同于经典比特。一个量子比特是一个二维Hilbert空间，或者说是一个双态量子系统。对量子比特的讨论总是相对于某个已固定的完备正交基进行的。如果记该空间的一组基为$\{|0\rangle,|1\rangle\}$，这个量子比特可以处在$|0\rangle$和$|1\rangle$这两个状态。则根据态叠加原理，它也可以处于叠加态$|\varphi\rangle=c_1|0\rangle+c_2|1\rangle$，其中$c_1,c_2$是复数，且满足$|c_1|^2+|c_2|^2=1$。于是原则上[①]通过确定$c_1$和$c_2$，可以在一个量子比特中编码无穷多的信息。

如表1.1所示，两个或多个量子比特系统是单个量子比特系统的张量积，若一个量子系统由两个量子比特组成，则这个量子系统的状态是两量子比特状态的张量积。例如：两量子比特可处于态$|0\rangle\otimes|1\rangle\equiv|0\rangle|1\rangle\equiv|01\rangle$，具体为

$$|0\rangle\otimes|1\rangle\equiv|01\rangle=\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix} \tag{1-7}$$

① 因为这样的态并不相互正交，没有可靠的量子方法可以将编码的信息提取出来，所以编码无穷多的信息只是理论上成立。

显然，两个量子比特系统是一个四维 Hilbert 空间，两量子比特所处的状态是四维 Hilbert 空间的一个向量。$\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$构成该空间的一组完备正交基。一个两量子比特态可以处在任意一个基态中，因而也可以处在它们的均匀(每个态前面复系数的模平方相同或者说是处在每个态上的概率相同)叠加态中。依此类推，n 个量子比特系统是一个 2^n 维 Hilbert 空间，系统所处状态是该空间中的一个向量，系统的状态可以是 2^n 个相互正交的态的均匀叠加态。量子系统的存储能力正是以这种方式呈指数增长。需要指出，两量子比特系统的完备正交基可以由单量子比特系统的完备正交基通过张量积运算得到，$\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$就是由$\{|0\rangle,|1\rangle\}$得来。类似可以求得任意 n 个量子比特系统的一组完备正交基。

此外，两量子比特系统还有另外一组完备正交基，即$\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$，其中：

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{1-8}$$

这一组基常称为 Bell 基。四个基态通常被称为 Bell 态，有时候也称为 EPR 态(或 EPR 对)，这是根据首次发现这些状态的奇特性质的学者 Bell 和 Einstein、Podolsky 与 Rosen 命名的。这里仍然需要强调的是$|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle$和$|\psi^-\rangle$只是 Bell 态的一种习惯记号，有的文献里面也经常采用其他记号，包括$|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle$和$|\Psi^-\rangle$来表示。在不影响阅读的情况下，本书也没有作最终统一。

1.1.4 算子

算子(operator)是作用到态矢上的一种运算或操作。通常，如果运算 $\hat{F}$ 作用到态矢$|\psi\rangle$上，结果仍然是一个态矢$|\phi\rangle$，即有$|\phi\rangle=\hat{F}|\psi\rangle$成立，则 $\hat{F}$ 为一个算子。若 $\hat{F}$ 的作用满足式(1-9)所示关系，则称 $\hat{F}$ 为线性算子，其中 c_1,c_2 是复数。

$$\hat{F}(c_1|\psi_1\rangle+c_2|\psi_2\rangle)=c_1\hat{F}|\psi_1\rangle+c_2\hat{F}|\psi_2\rangle \tag{1-9}$$

在量子力学中用到的算子都是线性的，所以本书后面不再特别指出线性二字，而直接称算子。在 Hilbert 空间中，一个算子对应一个矩阵[①]。算子 $\hat{F}$ 作用到态矢$|\psi\rangle$上定义为用其对应矩阵 F 去乘该态矢，即 $\hat{F}|\psi\rangle=F|\psi\rangle$。算子 $\hat{F}_1$ 和 $\hat{F}_2$ 的复合定义为：

$$\hat{F}_1\hat{F}_2|\psi\rangle=\hat{F}_1(\hat{F}_2|\psi\rangle)=\hat{F}_1|\phi\rangle \tag{1-10}$$

其中$|\phi\rangle=\hat{F}_2|\psi\rangle$，算子复合相当于对应矩阵的乘积运算。若 $\hat{F}_1\hat{F}_2=\hat{I}$，则称 $\hat{F}_1$ 和 $\hat{F}_2$ 互为逆算子，记为 $\hat{F}_1=\hat{F}_2^{-1}$。此外，与矩阵完全对应，可以定义单位算子，转置算子和共轭算子等。$\hat{F}$ 的厄米共轭算子 $\hat{F}^\dagger$ 定义为 $\hat{F}$ 的转置算子 $\hat{F}^{\mathrm{T}}$ 再取复共轭，即 $\hat{F}^\dagger=(\hat{F}^{\mathrm{T}})^*$。

若 $\hat{F}^\dagger=\hat{F}$，则称 $\hat{F}$ 为厄米算子。

若 $\hat{F}^\dagger=\hat{F}^{-1}$，则称 $\hat{F}$ 为酉算子。

① 这里算子对应的矩阵和前面态矢对应的向量(或矩阵)实际都是根据某种表象得来，同线性代数中线性变换和向量的表示对应于所选的基类似。表象的概念将在 1.1.6 节介绍。

厄米算子和酉算子是量子力学乃至量子保密通信中所用到的最重要的两类算子。

厄米算子对应的厄米矩阵有很多重要的性质，最重要的一条就是可以对角化。将厄米矩阵对角化可以借助其本征值和本征向量。与线性代数中完全类似，若算子 $\hat{F}$ 作用到某个态矢 $|u\rangle$ 上的结果等于一个常数 u 与这个态矢的乘积：

$$\hat{F}|u\rangle = u|u\rangle \tag{1-11}$$

则上述方程称为算子 $\hat{F}$ 的本征方程，其中 u 称为本征值，$|u\rangle$ 称为算子 $\hat{F}$ 属于本征值 u 的本征向量。其本征值和本征向量还具有特性：本征值都是实数；属于不同本征值的本征向量正交；属于同一本征值的本征向量可以通过 Schmidt 正交化方法使其相互正交；所有本征向量张起一个向量空间，经过 Schmidt 正交化过程后得到的相互正交的本征向量经过归一化构成该向量空间的一组完备正交基 $\{|u_1\rangle, |u_2\rangle, \cdots, |u_n\rangle\}$；算子 $\hat{F}$ 具有谱分解

$$F = \sum_{i=1}^{n} u_i \mid u_i\rangle \tag{1-12}$$

厄米算子的这些性质决定了它可以表示物理系统的可观测力学量。

酉算子也是非常重要的一类，酉算子是可逆的，酉变换不改变两个态矢的内积，不改变算子的本征值，不改变算子所对应的矩阵的迹，不改变算子的线性性质和厄米性质，也不改变算子间的代数关系。这些性质决定了酉算子可以描述孤立量子系统态矢随时间的变化和量子计算中的一切逻辑操作。

量子信息处理就是对编码的量子态进行一系列酉演化，对量子比特最基本的操作称为逻辑门，逻辑门按照其作用的量子比特个数可分为一位门、二位门、三位门等。逻辑门的操作按照它对 Hilbert 空间基矢的作用来定义。常见的一位门有相位门和 Pauli 门，其中相位门定义为

$$\boldsymbol{p}(\theta) = |0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\theta}|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta} \end{pmatrix} \tag{1-13}$$

其作用为 $\boldsymbol{p}(\theta)|0\rangle = |0\rangle$，$\boldsymbol{p}(\theta)|1\rangle = \mathrm{e}^{\mathrm{i}\theta}|1\rangle$，可以改变两个基矢的相对相位。四个 Pauli 门定义为

$$\begin{aligned} \boldsymbol{I} &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \boldsymbol{X}(\boldsymbol{\sigma}_x) = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \boldsymbol{Z}(\boldsymbol{\sigma}_z) &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \boldsymbol{Y}(\boldsymbol{\sigma}_y) = -\mathrm{i}|0\rangle\langle 1| + \mathrm{i}|1\rangle\langle 0| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \end{aligned} \tag{1-14}$$

通常也称为 Pauli 算子(矩阵)，有时 Pauli 算子只指后面三个算子。另外一个重要的一位门是 Hadamard 门

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)|0\rangle + (|0\rangle - |1\rangle)|1\rangle] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1-15}$$

这个门将基矢 $|0\rangle$ 和 $|1\rangle$ 分别变成 $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ 和 $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$，即 $|0\rangle$ 和 $|1\rangle$ 的均匀叠加态，系统等概率地(以 1/2 的概率)处于 $|0\rangle$ 和 $|1\rangle$ 态。量子保密通信中经常用 $\boldsymbol{H}$ 变换来产生这种最大“不确定态”来保证安全性。

两位门中最常用的是控制-U门，定义为：

$$U_C=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U \tag{1-16}$$

式中I是对一个量子比特的恒等操作，U是另外一个一位门，第一个量子比特称为控制量子比特，第二个称为目标量子比特。U_C对目标量子比特作用I或U，取决于控制量子比特处于$|0\rangle$还是$|1\rangle$。例如控制-非门(C-NOT)的作用定义为：

$$|00\rangle\rightarrow|00\rangle,|01\rangle\rightarrow|01\rangle,|10\rangle\rightarrow|11\rangle,|11\rangle\rightarrow|10\rangle \tag{1-17}$$

1.1.5 测量

测量算子是量子信息中提取信息的重要手段。与经典环境中测量物体的位置、速度等类似，对量子系统的观测实际也是对其某个力学量(可能是位置、动量、电子自旋等)的测量。本书常用的两类特殊测量有投影测量和POVM测量。

投影测量由被观测系统状态空间上的一个力学量算子描述。每一个力学量F都用一个厄米算子$\hat{F}$表示。对力学量$\boldsymbol{F}$测量的所有可能值是算子$\hat{F}$的本征值谱。

一般地，若对系统测量力学量$\boldsymbol{F}$，且$\boldsymbol{F}$具有式(1-12)给出的谱分解，将式中属于同一本征值m的部分项合并为与本征值m对应的本征空间上的投影算子$\boldsymbol{P}_m$，谱分解进一步化简为

$$\boldsymbol{F}=\sum_m m\boldsymbol{P}_m \tag{1-18}$$

则对应的一组测量算子可描述为$\{\boldsymbol{P}_m\}$，测量的可能结果对应于其本征值m。测量量子态$|\varphi\rangle$时，得到结果m的概率为

$$p(m)=\langle\varphi|\boldsymbol{P}_m|\varphi\rangle \tag{1-19}$$

给定测量结果m，测量后量子系统的状态塌缩为

$$\frac{\boldsymbol{P}_m|\varphi\rangle}{\sqrt{p(m)}} \tag{1-20}$$

测量平均值为

$$E(m)=\sum_m mp(m)=\langle\varphi|\boldsymbol{F}|\varphi\rangle \tag{1-21}$$

投影测量算子$\boldsymbol{P}_m$满足完备性关系和正交投影算子的条件：

$$\sum_m \boldsymbol{P}_m^{\dagger}\boldsymbol{P}_m=\boldsymbol{I},\boldsymbol{P}_m^{\dagger}=\boldsymbol{P}_m,\text{且 }\boldsymbol{P}_m\boldsymbol{P}_{m'}=\boldsymbol{\delta}_{m,m'}\boldsymbol{P}_m \tag{1-22}$$

特别地，若F对应于不同本征向量的本征值都不同，则测量算子可描述为$\{|u_i\rangle\langle u_i|\}$。当量子系统处在$\hat{F}$的本征态$|u_i\rangle$时，测量力学量$F$得到唯一可能的测量结果，即本征态$|u_i\rangle$对应的本征值。当系统处于态

$$|\Phi\rangle=c_1|u_1\rangle+c_2|u_2\rangle+\cdots+c_n|u_n\rangle \tag{1-23}$$

时，测量得到值u_i的概率是$|c_i|^2$，测量后的态塌缩为对应于测量结果u_i的本征向量$|u_i\rangle$。

所以经常把测量一个系统的某力学量$\boldsymbol{F}$，称为用$\boldsymbol{F}$的本征向量组成的基$\{|u_1\rangle,|u_2\rangle,\cdots,|u_n\rangle\}$测量该系统，也就是使用投影测量$\{|u_i\rangle\langle u_i|\}$，本书中多采用这一说法。

以常见的力学量——电子的自旋($\hat{\boldsymbol{\sigma}}_z$)为例，其本征值(可能的测量结果)为1和$-1$，对应的本征向量分别为$|0\rangle$和$|1\rangle$，$\{|0\rangle,|1\rangle\}$构成二维Hilbert空间的一组完备正交基，对应

试读结束，需要全本PDF请购买 www.ertongbook.com