信息安全技术丛书

应用量子密码学

Applied Quantum Cryptography

〔奥〕Christian Kollmitzer Mario Pivk 编著
李 琼 赵 强 乐 丹 译
牛夏牧 审

科学出版社

信息安全技术丛书

应用量子密码学

Applied Quantum Cryptography

〔奥〕Christian Kollmitzer　Mario Pivk　编著

李 琼　赵 强　乐 丹　译

牛夏牧　审

科 学 出 版 社

北　京

图字：01-2013-6659

内 容 简 介

本书主要介绍应用量子密码学的发展现状，并讨论如何在标准的通信框架下实现量子密码。应用量子密码，即量子密钥分发（Quantum Key Distribution，QKD），是最接近于实用的量子信息技术。本书第1章为简介；第2章介绍基础理论知识；第3～5章分别介绍QKD的协议、系统组成和工作原理，误码纠正协议Cascade，以及攻击策略；第6章介绍七个不同的QKD系统；第7章对实际环境下的QKD网络进行统计分析；第8～10章讨论如何构建QKD网络。

本书可作为高年级本科生、研究生的参考书，也可供相关领域的科研人员和工程技术人员参考。

图书在版编目（CIP）数据

应用量子密码学 /（奥）科米策（Kollmitzer, C.），（奥）皮夫克（Pivk, M.）编著；李琼，赵强，乐丹译. —北京：科学出版社，2015.3
（信息安全技术丛书）书名原文：Applied quantum cryptography
ISBN 978-7-03-042305-0

Ⅰ. ①应… Ⅱ. ①科…②皮… ③李… ④赵… ⑤乐… Ⅲ. ①量子－密码－通信理论 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字（2014）第251745号

责任编辑：王 哲 闫 悦 / 责任校对：张怡君
责任印制：赵 博 / 封面设计：迷底书装

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

三河市骏杰印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2015年3月第 一 版 开本：720×1 000 1/16
2015年3月第一次印刷 印张：12 1/4
字数：228 000
定价：70.00元
（如有印装质量问题，我社负责调换）

译 者 序

应用量子密码学，或者说量子密钥分发（Quantum Key Distribution，QKD）是一项源于物理学领域、发展于信息领域的新兴技术。将信息安全建立在量子物理特性的基础之上，这在信息科学中是前所未有的，QKD 也因此具有无条件安全性，至少在理论上是这样的。

但是，任何理论向真正的实用技术转换都必须解决大量的具体问题，这些具体问题或者是对理论的进一步诠释，或者是向真实世界的过渡甚至妥协。在跨过这片具体问题的海洋之后，理论是否还能保持其原有的全部属性呢？答案也许会让理论家失望，但这不是实践家的错，而是真实世界太复杂。以理论为基础，着力解决其在真实世界中的实现问题，恐怕是很多当代科学家们工作的主旋律，这一点在 QKD 技术上体现得淋漓尽致。从 1984 年 BB84 协议的提出，到现在凤毛麟角的商业公司和实用化设备，大批来自物理学、信息学、电子学、计算机科学的科学家们努力推动着这一诱人技术的实现和实用化。30 年来，科学家们发现并解决了协议安全性、攻击与对抗、物理元器件、算法效率与速率优化、系统集成、网络化等方面的诸多问题，终于让我们看到了 QKD 技术实用化的曙光。

欧盟组织的大型研究项目 SECOQC 成功地解决了 QKD 技术的大量实际问题，成为 QKD 技术实用化进程中的一个里程碑。基于该项目的诸多研究成果，C. Kollmitzer 等专家学者共同编写了 *Applied Quantum Cryptography*，很好地梳理了这些年来 QKD 领域的关键问题和解决方案。译者在阅读这本书的过程中，将其介绍给国内读者的冲动越来越强烈，最终在科学出版社的鼓励和支持下，下定决心翻译了本书。虽然领域内的学者们大多不介意阅读英文书籍，但译者相信中文版的出版仍是很有意义的，一来可以扩大这本书的影响力；二来也能方便相关领域的工作者快速理解实用 QKD 技术的相关概念和问题，从而吸引更多的人参与 QKD 技术的研究、推动 QKD 技术的应用。如果能对 QKD 技术的发展和应用尽一份绵薄之力，译者将感到无比欣慰。

为了使本书的翻译尽可能术语准确、风格一致，我们在翻译过程中字斟句酌，但由于水平有限，难免有不足之处，殷切希望读者批评指正。在本书的翻译和审校过程中得到了哈尔滨工业大学牛夏牧教授的诸多指点和帮助，在此表示衷心感谢。北京大学量子信息与测量教育部重点实验室的李政宇、乔宇澄也对本书的翻译给予了热情帮助，在此表示衷心感谢。

李 琼

于哈尔滨工业大学科学园

2015 年 1 月

前　言

在通信双方之间利用单光子的量子属性交换二进制密钥，进而对秘密数据进行加密，的确是一项新兴技术。仅仅在几年前，应用量子密码学(或者更确切地说，量子密钥分发(Quantum Key Distribution，QKD))还仅限于大学实验室的基础研究。但是近几年来，情况已经发生了改变，经过几个研究团队面向实际应用的研究工作，QKD 已经走出实验室，从令人惊讶的基础研究变为具有广泛用途的实用技术。

由欧盟资助的大型项目 SECOQC(Secure Communication based on Quantum Cryptography)是 QKD 技术发展史上的一个重要里程碑，该项目旨在联合欧洲物理学和相关领域(包括电子学、软件、网络等)最优秀的专家一同寻求未来密码学的解决方案。

SECOQC 由奥地利研究中心(Austrian Research Centers，ARC)牵头，其在标准光纤网络中实现了量子密钥分发，让世人得以一窥未来的安全通信。QKD 技术虽然已经有了一定的基础，但是距离真正实现未来的安全通信还有很长的路要走。QKD 并不是安全的万能药，不可能解决所有的问题，但 QKD 有潜力替换对称加密中最薄弱的环节，即密钥交换环节。可以证明：只要保证一些额外的条件，QKD 密钥交换过程不会被攻破，用量子特性产生和交换的密钥是安全的。

本书主要介绍量子密码学的发展现状，并描绘如何在标准的通信框架下实现量子密码。敏感数据日益增长的脆弱性呼唤着新的安全技术，QKD 有望成为目前众多安全问题的解决方案！

Christian Monyk

奥地利，维也纳

致　谢

非常感谢奥地利研究中心克拉根福和维也纳分部对本书的支持。本书得到了EC/IST集成项目SECOQC(合同编号：506813)的大力支持。

非常感谢T.Länger、T. Lorünser、C. Pacher、M. Peev和A. Poppe在第6章编写过程中给予的帮助。

借此机会感谢奥地利气象和地球动力学中央研究所(Central Institute for Meteorology and Geodynamics，ZAMG)的Roland Potzmann提供气候数据。

特别感谢维也纳大学多位研究者的支持。

Christian Kollmitzer非常感谢Gerald Dissauer对医学信息系统(medical information systems)进行讨论和解释。

非常感谢滑铁卢大学(加拿大安大略)的Michele Mosca、Norbert Lütkenhaus和Daniel Gottesman，感谢约安诺姆应用科学大学(奥地利卡芬堡)的Takashi Linzbichler及其学生，作者与他们对“信任环”模型进行了长时间的讨论。

感谢Claus Ascheron为本书的出版付出的努力。

最后非常感谢审稿人十分有价值的评论和意见。

目　录

第1章 简 介

C.Kollmitzer

量子密码(或者更确切地说，量子密钥分发(Quantum Key Distribution，QKD))是一项受到全球高度关注的新技术。QKD 使得以可证明安全的形式交换信息成为可能，这在通信技术发展史上是一个重要的里程碑。目前 QKD 最大的问题是通信距离受限，不过几个实验表明通信距离还有很大提升空间。在这些实验中，有的利用光纤技术，有的利用自由空间技术。除此之外，目前已经有可能构建基于 QKD 的通信网络，不仅能实现端到端的 QKD 连接，还可能构建现代通信结构。

2008 年 10 月，在奥地利维也纳成功开发了第一个基于 QKD 的全功能网络。该网络作为视频会议网络的基础层，将一个城市的几个节点连接起来，并部署了五个采用不同技术的 QKD 系统。每一次通信使用其中的一项或几项技术，但对于用户来说是透明的。

本书主要包含如下内容。

讨论基础技术，详细介绍 QKD 系统中通信的几个步骤：筛选、协商、纠错和保密增强。

对于纠错步骤，详细介绍原始 Cascade 协议及其改进协议，改进协议研究如何确定优化的初始分块大小，可增强原始 Cascade 协议的效率。

为了确保通信系统的安全，必须考察不同的攻击策略。除了关注对 QKD 系统的经典攻击策略外，还会介绍一些新的攻击策略。

详细介绍目前的 QKD 系统，也就是欧盟 SECOQC 网络项目中使用的 QKD 系统，这也是 2008 年在奥地利维也纳开发的第一个基于 QKD 的网络中的一部分。

虽然 QKD 系统已经在不同的实验配置下使用了几年，但是许多实验仅限于实验室环境。而 SECOQC 网络的部署使其可以收集到系统在城市环境下长时间运行的数据。首次详细讨论了环境、温湿度等的影响，包括收集的数据以及统计分析。

QKD 系统是现有通信网络的增强，如何将其集成到现有的通信系统中是至关重要的。因此必须开发特殊的网络协议，本书以量子点到点协议(Quantum Point to Point Protocol，Q3P)为例对特殊网络协议进行了详细介绍。

为了推进实际化应用，通信网络十分关键。本书介绍了该方面的相关基础内容。另外还介绍了如何对待终端用户以及终端用户使用 QKD 网络的好处，特别介绍了如何利用通用通信设备(如 iPhone)使用 QKD 生成的密钥。

因为 QKD 系统的距离受限，如何开发全球网络是最受关注的研究领域之一。本书介绍了一个基于可信通信中心的网络模型。该模型的主要优点是按需产生密钥、用户不必在相对不确定的环境下存储密钥。

希望本书可以激起大家对 QKD 和相关新技术的兴趣。这些新技术今后将成为全球范围的研究热点，并对未来的通信架构产生广泛深远的影响。

第2章 预 备 知 识

M.Pivk

本章介绍后续章节所需的基础知识。所有涉及内容均仅作简略介绍，因为如果深入探讨这些内容将需要很大篇幅，而这些内容已超出本章范围。

2.1 量子信息论

本节简要介绍量子信息论。更多详细内容，请参考 Nielsen 和 Chuang 的 *Quantum Computation and Quantum Information*[4]。

2.1.1 量子比特

自从香农提出信息论以来，比特(bit)已成为经典信息论的基本术语。一个比特的值为 0 或者 1。与此相对应，量子信息使用量子比特(quantum bit，qubit)的概念。与经典比特类似，量子比特也有两种可能的状态：$|0\rangle$ 和 $|1\rangle$。特殊符号“$|\ \rangle$”称为 Dirac 符号，或 ket 符号，这是量子力学中表示“态”的标准符号。与经典比特的主要区别是：经典比特只有 0 和 1 两种可能的态，而量子比特(qubit)的状态可能是 $|0\rangle$ 和 $|1\rangle$ 之间的所有状态，这称为叠加(superposition)。我们将量子比特的态表示为

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{2-1}$$

其中，$\alpha,\beta\in\mathbb{C}$。因为系数是一些复数，量子比特的状态可以用二维复向量空间 $\mathbb{C}^2$（也称为希尔伯特空间(Hilbert space)）里的向量来表示。$|0\rangle$ 和 $|1\rangle$ 构成计算基(参阅定义 2-4)，且二者相互正交，即 $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$，$|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$。既然一个量子比特态是单位向量，其长度应归一化为 1，以下的公式都应使标量 α、β 满足

$$|\alpha|^2+|\beta|^2=1 \tag{2-2}$$

这样，可以将量子比特态重写为

$$|\psi\rangle=\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle \tag{2-3}$$

其中，θ、φ 为实数，定义了 Bloch 球(Bloch sphere)上的一个点，如图 2.1 所示。

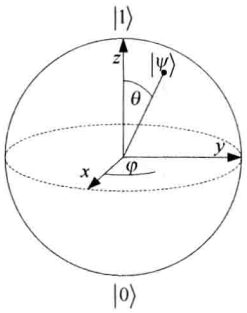

图 2.1　qubit 在 Bloch 球上的表示

量子比特的测量非常重要。在 α 或 β 等于 0 的特殊情况下，量子比特分别映射为经典比特 1 或 0。但是，如果 α 和 β 都不等于 0 的话，情况会如何呢？根据标量的不同取值，量子比特以某个概率测量为 1，或以互补概率测量为 0。因为标量满足式(2-2)，量子比特测量为 0 的概率为 $|\alpha|^2$，测量为 1 的概率为 $|\beta|^2$，更详细的内容参阅 2.1.3 节。

在量子力学中，标量 α、β 也分别称为态 $|0\rangle$ 和 $|1\rangle$ 的幅度(amplitude)。另一个描述量子比特的术语是相位(phase)。考虑态 $e^{i\varphi}|\psi\rangle$，其中，$|\psi\rangle$ 为一个态矢量，φ 为实数。我们认为态 $e^{i\varphi}|\psi\rangle$ 与 $|\psi\rangle$ 是相等的，因为系数 $e^{i\varphi}$ 是全局相位因子(global phase factor)。从统计的角度看，这两种态的测量结果也是相同的，参阅 2.1.2 节。

另一种相位称为相对相位(relative phase)。考虑如下的两个态：

$$|+\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),\quad |-\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) \tag{2-4}$$

在态 $|+\rangle$ 中，$|1\rangle$ 的幅度为 $\frac{1}{\sqrt{2}}$，在态 $|-\rangle$ 中，$|1\rangle$ 的幅度为 $-\frac{1}{\sqrt{2}}$，也就是说它们的幅度值相同、符号相反。对一些相对相位不同的态，可以定义两个幅度 α_1、α_2，找到一个实数 φ，使得 $\alpha_1=e^{i\varphi}\alpha_2$。与全局相位对比，相对相位只有一个幅度相差系数 $e^{i\varphi}$，而全局相位的两个幅度都相差系数 $e^{i\varphi}$。

2.1.2　线性算子

改变一个量子比特的态，需要利用线性算子完成。令函数 A 将向量 $\mathcal{V}$ 变换为 $\mathcal{W}$（$\mathcal{V}$,$\mathcal{W}$ 是 $\mathbb{C}^*$ 的向量空间），比较方便的方式是将函数 A 表示为矩阵形式(matrix representation)。若矩阵 $\boldsymbol{A}$ 为 m 行、n 列，该矩阵与矢量 $|\boldsymbol{v}\rangle\in\mathbb{C}^*$ 相乘，得到新的矢量 $|\boldsymbol{w}\rangle\in\mathbb{C}^m$。这样的矩阵应满足线性公式[4]，即

$$\boldsymbol{A}\left(\sum_i a_i|\boldsymbol{v}_i\rangle\right)=\sum_i a_i\boldsymbol{A}|\boldsymbol{v}_i\rangle \tag{2-5}$$

令 $\boldsymbol{A}:\mathcal{V}\to\mathcal{W}$ 是一个线性算子，$|\boldsymbol{v}_1\rangle,\cdots,|\boldsymbol{v}_n\rangle$ 是 $\mathcal{V}$ 的基，$|\boldsymbol{w}_1\rangle,\cdots,|\boldsymbol{w}_n\rangle$ 是 $\mathcal{W}$ 的基。存在复数 $A_{1j},\cdots,A_{mj}$ 使得

$$\boldsymbol{A}|\boldsymbol{v}_j\rangle=\sum_i A_{ij}|\boldsymbol{w}_i\rangle,\quad 1\leqslant i\leqslant m,1\leqslant j\leqslant n \tag{2-6}$$

这就构成了操作 A 的矩阵表示。

相对的，$n\times m$ 矩阵可以理解为一个反线性算子符，将矢量空间 $\mathcal{W}$ 中的矢量转换为 $\mathcal{V}$ 中的矢量。

我们使用的符号与线性几何中的常用符号有所不同。表 2.1 列出了量子力学中常用的符号。我们知道，一个矢量可以表示为计算基的和。为了简化，令计算基 $\boldsymbol{v}_1=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$，$\boldsymbol{v}_2=\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix},\cdots,\boldsymbol{v}_n=\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$，因此矢量 $|\boldsymbol{v}\rangle=\sum_i a_i|v_i\rangle$ 也可以写为 $|\boldsymbol{v}\rangle=\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix}$。如果采用另一组计算基，则表达形式有所不同。

表 2.1　常用量子力学符号

符　号	描　述
z^*	复数的复共轭，如 $(1+\mathrm{i})^*=1-\mathrm{i}$
$\|v\rangle$	一个矢量，即一个 ket，$\|\boldsymbol{v}\rangle=\sum_i a_i\|v_i\rangle$
$\langle v\|$	$\|v\rangle$ 的对偶矢量，即一个 bra，$\langle\boldsymbol{v}\|=\sum_i a_i^*\|v_i\rangle^{\mathrm{T}}$
$\lambda\|v\rangle$	与标量 λ 相乘，$\lambda\|\boldsymbol{v}\rangle=\sum_i \lambda a_i\|v_i\rangle$
$\langle v\|w\rangle$	矢量 $\|v\rangle$ 和 $\|w\rangle$ 的内积
$\|v\rangle\otimes\|w\rangle$	矢量 $\|v\rangle$ 和 $\|w\rangle$ 的张量积
$\boldsymbol{A}^*$	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，$\boldsymbol{A}^\dagger=(\boldsymbol{A}^{\mathrm{T}})^*$
$\langle\varphi\|\boldsymbol{A}\|\psi\rangle$	$\|\varphi\rangle$ 与 $\boldsymbol{A}\|\psi\rangle$ 的内积

2.1.2.1　Pauli 阵

Pauli 阵(Pauli matrix)是四个非常有用的 2×2 矩阵，这些矩阵可以表示对量子比特进行的一些处理，它们分别为

$$\boldsymbol{X}=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \boldsymbol{Y}=\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix},\quad \boldsymbol{Z}=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\tag{2-7}$$

其中，$\boldsymbol{X}$ 和 $\boldsymbol{Z}$ 分别称为比特翻转(bit flip)和相位翻转(phase flip)操作符。如果对一个量子比特进行 $\boldsymbol{X}$ 操作，$|0\rangle$ 会转换为 $|1\rangle$，$|1\rangle$ 会转换为 $|0\rangle$，即

$$\boldsymbol{X}|0\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix},\quad \boldsymbol{X}|1\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$

如果对一个量子比特进行 $\boldsymbol{Z}$ 操作，$|1\rangle$ 的相位会改变符号，即

$$\boldsymbol{Z}|+\rangle=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\sqrt{2}\\ \sqrt{2}\end{pmatrix}=\begin{pmatrix}\sqrt{2}\\ -\sqrt{2}\end{pmatrix},\quad \boldsymbol{Z}|-\rangle=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\sqrt{2}\\ -\sqrt{2}\end{pmatrix}=\begin{pmatrix}\sqrt{2}\\ \sqrt{2}\end{pmatrix}$$

对 $\boldsymbol{Y}$ 的解释是，用虚部单位 i 与该矩阵相乘后得到的矩阵只包含自然数，即

$$\mathrm{i}\boldsymbol{Y}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

$\mathrm{i}\boldsymbol{Y}$ 操作符也同时产生比特翻转和相位翻转的效果，即

$$\mathrm{i}\boldsymbol{Y}=\boldsymbol{Z}\boldsymbol{X}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}=\mathrm{i}\begin{pmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{pmatrix}$$

因此，对态 $|0\rangle$ 和 $|1\rangle$ 分别进行 $\mathrm{i}\boldsymbol{Y}$ 操作，结果为

$$\mathrm{i}\boldsymbol{Y}|0\rangle=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}0\\ -1\end{pmatrix},\quad \mathrm{i}\boldsymbol{Y}|1\rangle=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}$$

2.1.2.2　内积

内积(inner product)也称为标量积(scalar product)，表示为 $\langle\boldsymbol{v}|\boldsymbol{w}\rangle$（一般线性代数中表示为 $(|\boldsymbol{v}\rangle,|\boldsymbol{w}\rangle)$），这是一个函数，两个输入分别为向量 $|\boldsymbol{v}\rangle$ 和 $|\boldsymbol{w}\rangle$，输出为一个复数。例如，两个 n 维向量在复数域上的内积定义为

$$\langle\boldsymbol{v}|\boldsymbol{w}\rangle=\sum_i a_i^* b_i=(a_1^*\cdots a_n^*)\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}\tag{2-8}$$

内积具有如下属性：

(1) 对于第二个参数是线性的，即 $(|\boldsymbol{v}\rangle,\sum_i\lambda_i|\boldsymbol{w}_i\rangle)=\sum_i\lambda_i(|\boldsymbol{v}\rangle,|\boldsymbol{w}_i\rangle)$；

(2) $\langle\boldsymbol{v}|\boldsymbol{w}\rangle=\langle\boldsymbol{w}|\boldsymbol{v}\rangle^*$；

(3) $\langle\boldsymbol{v}|\boldsymbol{v}\rangle\geqslant 0$，当且仅当 $|\boldsymbol{v}\rangle=0$ 时取等号。

下面给出一些与内积相关的定义。

定义 2-1　假设 $\mathcal{V}$ 是 $\mathbb{C}^n$ 上的一组向量，向量 $|\boldsymbol{v}\rangle,|\boldsymbol{w}\rangle\in\mathcal{V}$，如果 $\langle\boldsymbol{v}|\boldsymbol{w}\rangle=0$，称 $|\boldsymbol{v}\rangle$ 和 $|\boldsymbol{w}\rangle$ 是正交的(orthogonal)。

定义 2-2　假设 $\mathcal{V}$ 是 $\mathbb{C}^n$ 上的一组向量，向量 $|\boldsymbol{v}\rangle\in\mathcal{V}$ 的范数(norm)定义为 $\||\boldsymbol{v}\rangle\|=\sqrt{\langle\boldsymbol{v}|\boldsymbol{v}\rangle}$。以一种开放的思维方式，可以将一个向量的范数认为是这个向量的长度或尺寸。

定义 2-3　假设 $\mathcal{V}$ 是 $\mathbb{C}^n$ 上的一组向量，如果向量 $|\boldsymbol{v}\rangle\in\mathcal{V}$ 的范数等于 1，即 $\||\boldsymbol{v}\rangle\|=1$，称该向量为单位向量。对一个向量进行归一化，就是将其除以它的范数，即 $\left\|\frac{|\boldsymbol{v}\rangle}{\||\boldsymbol{v}\rangle\|}\right\|=1$。

定义 2-4　假设 $\mathcal{V}$ 是 $\mathbb{C}^n$ 上的一组向量，如果 $\mathcal{V}$ 的一个子集中的每个向量都是单位向量，且任意两个不同向量之间都是正交的，即 $\langle \boldsymbol{v}_i | \boldsymbol{w}_j \rangle = 0,\ i,j = 1\cdots n,\ i \neq j$，称这个子集是正交的。

一个向量空间的计算基必须是正交的。因此这些向量形成向量空间的生成集，除生成集之外的任何向量都可以写成这些向量的线性组合。

2.1.2.3　外积

两个向量的外积(outer product)就是它们的内积的反乘积。内积的输出是一个复数，而外积的输出是一个矩阵，即

$$|\boldsymbol{v}\rangle\langle\boldsymbol{w}| = \boldsymbol{A}_{i,j} = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} (b_1^* \cdots b_n^*) = \begin{pmatrix} a_1 b_1^* & \cdots & a_1 b_n^* \\ \vdots & \ddots & \vdots \\ a_m b_1^* & \cdots & a_m b_n^* \end{pmatrix} \tag{2-9}$$

外积是利用内积来表示线性算子的一种有效方法。令 $|\boldsymbol{v}\rangle$ 为内积空间 $\mathcal{V}$ 中的一个向量，$|\boldsymbol{w}\rangle$ 为内积空间 $\mathcal{W}$ 中的一个向量，定义 $|\boldsymbol{w}\rangle\langle\boldsymbol{v}|$ 为一个从 $\mathcal{V}$ 到 $\mathcal{W}$ 的线性算子，即

$$(|\boldsymbol{w}\rangle\langle\boldsymbol{v}|)(|\boldsymbol{v}'\rangle) = |\boldsymbol{w}\rangle\langle\boldsymbol{v}|\boldsymbol{v}'\rangle = \langle\boldsymbol{v}|\boldsymbol{v}'\rangle|\boldsymbol{w}\rangle \tag{2-10}$$

这个公式至少有两层含义：其一，将向量 $|\boldsymbol{v}'\rangle$ 通过矩阵映射到 $\mathcal{W}$ 中的一个向量；其二，表示将向量 $|\boldsymbol{w}\rangle$ 与一个复数 $\langle\boldsymbol{v}|\boldsymbol{v}'\rangle$ 相乘。

外积概念的另一个应用是标准正交向量的完备性关系(completeness relation)。令 $|\boldsymbol{v}_i\rangle$ 为内积空间 $\mathcal{V}$ 的一个正交基，则必须满足

$$\sum_i |\boldsymbol{v}_i\rangle\langle\boldsymbol{v}_i| = \boldsymbol{I} \tag{2-11}$$

2.1.2.4　张量积

张量积(tensor product)是一种根据两个较小的向量空间创建一个更大向量空间的操作。假设 $\mathcal{V}$ 和 $\mathcal{W}$ 分别是维数为 m 和 n 的向量空间，$\mathcal{V}\otimes\mathcal{W}$ 是一个 mn 维的向量空间，其中的元素为 $|\boldsymbol{v}\rangle \in \mathcal{V}$ 和 $|\boldsymbol{w}\rangle \in \mathcal{W}$ 的张量积 $|\boldsymbol{v}\rangle \otimes |\boldsymbol{w}\rangle$ 的线性组合。

例如，向量 (1,2) 和 (3,4) 的张量积为

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1\times 3 \\ 1\times 4 \\ 2\times 3 \\ 2\times 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

以上例子是在两个向量空间上进行张量积运算，该运算也可以对向量空间上的线性算子进行。假设 $\boldsymbol{A}:\mathcal{V}\to\mathcal{V}'$，$\boldsymbol{B}:\mathcal{W}\to\mathcal{W}'$，则 $\boldsymbol{A}\otimes\boldsymbol{B}:\mathcal{V}\otimes\mathcal{W}\to\mathcal{V}'\otimes\mathcal{W}'$。假设 $\boldsymbol{A}$ 是一个 $m\times n$ 的矩阵，$\boldsymbol{B}$ 是一个 $p\times q$ 的矩阵，则矩阵表达为