国家科学技术学术著作出版基金
NFAPST

量子保密通信协议的设计与分析

温巧燕 郭奋卓 朱甫臣◎著

科学出版社
www.sciencep.com

国家科学技术学术著作出版基金资助出版

量子保密通信协议的设计与分析

温巧燕　郭奋卓　朱甫臣　著

科学出版社

北京

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，并提出一些与之紧密相关的新研究课题. 全书分四部分(共 8 章). 第一部分为量子保密通信研究所需的量子力学基础知识(第 1 章); 第二部分为量子密码协议的设计，主要包括量子密钥分发与身份认证、量子秘密共享、量子加密、量子安全直接通信 (第 2~5 章); 第三部分为量子密码协议的分析(第 6 章); 第四部分为量子隐形传态以及与量子保密通信密切相关的量子纠错码(第 7、8 章). 重点从密码学的角度阐述了量子密码协议的设计与分析.

本书既可作为对量子保密通信感兴趣的读者的入门教材，也可作为量子保密通信领域研究工作者的参考用书，适合于密码学、信息安全、信息与通信系统、信号与信息处理、物理学、数学及相关学科的高年级本科生、研究生、教师和科研人员阅读参考.

图书在版编目(CIP)数据

量子保密通信协议的设计与分析/温巧燕, 郭奋卓, 朱甫臣著. —北京：科学出版社, 2009

ISBN 978-7-03-024837-4

Ⅰ.量… Ⅱ.①温… ②郭… ③朱… Ⅲ.① 量子-保密通信-通信协议-设计②量子-保密通信-通信协议-分析 Ⅳ.TN918.8

中国版本图书馆 CIP 数据核字(2009) 第 103083 号

责任编辑: 王丽平 杨 然 / 责任校对: 刘小梅

责任印制: 钱玉芬 / 封面设计: 王 浩

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

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 6 月第 一 版 开本: B5(720×1000)

2009 年 6 月第一次印刷 印张: 19 1/4

印数: 1—2 500 字数: 369 000

定价: 58.00 元

(如有印装质量问题, 我社负责调换〈环伟〉)

前　言

人们的生活离不开交流和沟通. 从电报、电话等通信工具的出现, 到通信网、互联网的飞快发展, 人们相互间的交流越来越便利, 需要交换的信息也与日俱增. 在特定情况下, 人们往往只想让期望的人看到自己发送的信息, 而不希望其他人也得到这些信息. 这一点在军事领域和商业领域尤其突出, 一条军事机密的泄漏可能会导致战争的失败, 一条商业机密的公开可能会给公司带来巨额经济损失. 随着人们对信息保密的要求日益提高, 保密通信研究也在不断发展和壮大, 其基本目的就是确保用户间的秘密消息能够在公开信道中可靠地传输.

在保密通信中, 通常称消息发送者为 Alice, 接收者为 Bob, 而窃听者为 Eve. 为了达到保密的目的, Alice 在发送消息前先利用加密密钥, 根据一定的加密算法将要发送的消息 M(即明文) 加密, 得到密文 C, 然后把密文 C 通过公开信道传输给 Bob. Bob 收到这些信息后可以用相应的解密密钥和解密算法由密文 C 恢复出明文 M, 从而得到 Alice 的真实消息. 一般地, 由于窃听者 Eve 不知道相应的解密密钥, 即使她窃听到传输的密文 C, 也不能恢复出明文消息 M. 这就是保密通信的基本原理, 其安全性取决于密钥的安全性. 现代密码体制主要包括对称密码体制和公钥密码体制两类, 它们在应用中各有特点. 对称密码体制常用来直接对明文消息进行加密和解密, 速度快且对选择密文攻击不敏感; 公钥密码体制则主要用于密钥分发及数字签名等. 因此在实际应用中一般采用混合密码系统, 即用公钥密码体制在通信者之间分发会话密钥, 然后用会话密钥通过对称密码体制来对通信消息进行加密.

大多数经典密码体制的安全性是建立在计算复杂性基础上的. 也就是说, 窃听者要想破译一个密码系统, 需要在有限的时间 (即秘密消息的有效期) 内解决某个计算难题. 而根据计算复杂性假设, 这种任务通常在当前人们的计算能力下很难实现. 这正是经典密码体制的安全性基础. 但是, 随着分布式计算和量子计算的发展, 这种密码体制的安全隐患越来越突出. 以 1994 年 Shor 提出的量子并行算法为例, 它能在多项式时间内解决大数因子分解难题. 一旦这种算法能够在量子计算机上付诸实施, 现行很多基于此类难题的公钥密码体制将毫无安全性可言.

值得注意的是, 经典密码体制中有一种算法具有无条件安全性, 那就是一次一密乱码本 (one-time pad, OTP). 假设 Alice 要发送的消息是 m, 其长度为 n, OTP 要求 Alice 和 Bob 共享有 n 长的随机密钥 k. 这种情况下, Alice 计算 $c = m \oplus k$(其中 $\oplus$ 代表模 2 加) 得到密文 c, 并把它发送给 Bob. 当 Bob 接收到密文后, 计算

$m = c \oplus k$ 得到明文. 可以看出在 k 未知的情况下, 这样给出的密文相当于同样长度的任何可能的明文消息的加密, 所以该加密体制具有无条件安全性 (这一点已经被 Shannon 从信息论角度所证明). 但是, OTP 的安全性建立在密钥的安全性之上, 它要求使用与消息等长的、随机的、不可重用的密钥. 那么怎样才能在通信者之间安全地分发密钥呢? 显然不能用 OTP 来分发, 因为它在分发密钥的同时需要消耗相同长度的密钥, 这将毫无意义. 在实际使用中, 仍然是通过公钥密码体制在通信者之间建立密钥, 然后再用 OTP 传输消息. 上面已经提到, 公钥密码体制的安全性已经受到各种先进算法强有力的挑战. 因此, OTP 的无条件安全性并不能真正实现.

怎样才能让一个密码体制抵抗上述各种先进的算法, 进而实现真正意义上的保密通信呢? 我们可以努力去寻找新的难解问题, 并在其基础上构造新的密码系统. 但这不是长久之计, 因为量子运算的并行性必将赋予未来的量子计算机超乎想象的计算潜能. 我们有理由相信, 随着量子计算算法的深入研究, 这种潜能很可能会演变成一个个将各种难解问题化难为易的先进算法. 因此, 这种寻找新难题的方法并不能解决经典保密通信所面临的根本问题.

那么还有没有其他办法呢? 答案是肯定的. 通过上面的分析我们知道, 一套完整的密码系统包括密钥的安全分发和消息的保密传输两大部分. 对于后者, OTP 已经能够达到无条件安全性. 我们还需要找到一种安全的密钥分发方法, 这样就能由它和 OTP 构成一套在安全性上趋近完美的保密通信系统. 随着量子密码的出现, 这个困扰人们已久的问题迎刃而解.

量子密码是密码学与量子力学相结合的产物, 不同于以数学为基础的经典密码体制, 其安全性由量子力学基本原理保证, 与攻击者的计算能力无关. 根据量子力学性质 (测不准原理与不可克隆定理), 窃听者对量子密码系统中的量子载体的窃听必然会对量子态引入干扰, 从而被合法通信者发现. 合法通信者能够发现潜在的窃听, 这正是量子密码安全性的本质. 此外, 根据量子力学原理, 如果用户间通过纠缠态建立了量子信道, 他们可以利用隐形传态协议进行保密通信. 这种通信不需要在公开信道中传输任何与所发送消息有关的信息, 因此也能够实现真正意义上的保密通信. 总之, 量子保密通信具有得天独厚的优势并逐渐成为信息安全新技术中的一个重要研究分支.

自从 1984 年 IBM 公司的 Bennett 和 Montreal 大学的 Brassard 提出第一个量子密码协议 ——BB84 协议以来, 国内外对量子保密通信的理论和实验研究都取得了很大进展. 作者及其课题组多年来一直从事量子保密通信的理论研究, 在量子密码协议、量子隐形传态及量子纠错码等相关方向取得了一系列成果. 本书以这些研究成果为基础, 结合国内外学者在量子保密通信领域的最新研究进展和作者对该领域研究问题的认识, 经过仔细归纳整理而成. 据作者所知, 本书是国内外首部重

点讨论量子保密通信协议设计与分析的专著, 有以下几个显著特点: 一是从密码学角度, 把量子密码协议的分析提升到与协议设计相同的高度, 并做重点论述. 其目的就是希望改变当前量子密码研究中普遍 "重设计而轻分析" 的现状, 使设计和分析工作相互促进, 协调发展. 二是参考文献全面, 对几个主要研究内容, 从首次出现该类协议到其最新进展的各个发展阶段, 从不同的物理原理实现到相同原理下效率的提高, 从双 (三) 方到多方甚至到网络, 从低维到高维, 从理论到实验都给出了比较全面典型的参考文献. 对量子保密通信其他的一些研究内容, 如量子签名、量子指纹、量子投币等也附了相关参考文献. 希望这些有助于相关的研究者快速对量子保密通信研究有一个全面的了解. 三是对几个主要内容展示最新研究进展的同时, 对其研究做了进一步的展望, 指出若干目前需要解决的关键问题及目前研究比较薄弱的重要研究课题. 此外, 对全书所用到的量子力学基础知识用线性代数语言进行了系统介绍, 采用向量和矩阵来刻画量子态及其演化, 这使得具有一般代数基础的学者就能读懂本书.

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与身份认证; 第 3 章研究量子秘密共享; 第 4 章研究量子加密; 第 5 章研究量子安全直接通信; 第 6 章研究量子密码协议的分析; 第 7 章研究量子隐形传态; 第 8 章研究与保密通信密切相关的量子纠错码.

方滨兴院士、蔡吉人院士、冯登国研究员和杨义先教授对本书的出版给予了极大的支持, 在此表示深深的感谢. 全书的编写工作得到了实验室师生的积极配合, 特别是量子密码研究小组的刘太琳博士、杨宇光博士、杜建忠博士、林崧博士、陈秀波博士、孙莹博士、王天银博士、宋婷婷硕士等给予了全力协助和密切配合, 在此一并对他们表示衷心的感谢.

高飞副教授、秦素娟博士后提供大量资料并参与了部分章节的编著工作, 在此说明并表示感谢.

本书的出版得到了国家科学技术学术著作出版基金的资助. 此外, 本书主要成果来自课题组受资助项目: 国家高技术研究发展计划 ("863" 计划) (编号: 2006AA01Z419)、国家自然科学基金项目 (编号: 90604023, 60373059, 60873191)、现代通信国家重点实验室基金项目 (编号: 9140C1101010601) 等, 在此特别表示感谢.

由于水平有限, 时间仓促, 书中难免存在不妥之处, 恳请读者批评指正.

作　者

2009 年 1 月 16 日

目　录

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 [1~7].

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, 见表 1-1.

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 ($\|\psi\rangle$ 的转置再复共轭)
$\langle\phi \mid \psi\rangle$	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
A^*	矩阵 A 的复共轭
A^{T}	矩阵 A 的转置
$A^\dagger$	矩阵 A 的厄米共轭, $A^\dagger=(A^{\mathrm{T}})^*$
$\langle\phi\|A\|\psi\rangle$	向量 $\|\phi\rangle$ 和 $A\|\psi\rangle$ 的内积, 或者 $A^\dagger\|\phi\rangle$ 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一个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 L 就是一个集合 $L=\{a_1,a_2,a_3,\cdots,a_n\}$, 满足: ① 任取 $a_i,a_j\in L$, 都有 $a_i+a_j\in L$; ② 任取复数 $c\in\mathbf{C}$, $a_i\in L$, 都有 $c\cdot a_i\in L$, 则称 L 为复向量空间, L 中元素称为向量. 复向量空间 L 上的内积定义为一种映射: 对于任意的一对向量 $a_i,a_j\in L$, 都有一个复数 $c=(a_i,a_j)$ 与之对应, 称为 a_i 和 a_j

的内积, 它具有如下性质:

$$\left.\begin{aligned}&(a_i,a_i)\geqslant 0\\&(a_i,a_j)=(a_j,a_i)^*\\&(a_l,c_1a_i+c_2a_j)=c_1(a_l,a_i)+c_2(a_l,a_j)\end{aligned}\right\}\tag{1-1}$$

上述定义了内积的复向量空间 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 空间中的列单位向量描述, 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 空间中的行单位向量描述.

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个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 $|\phi_1\phi_2\rangle$.

1.1.2　完备正交基

一个 n 维 Hilbert 空间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 $|u\rangle\in L$, $|u\rangle=\sum_{i=1}^{n}a_i|v_i\rangle$, 其中每一个 $a_i\neq 0$ 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 $\sqrt{\langle v_i\mid v_i\rangle}$) 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由空间的任意一组基构造一组完备正交基.

例如, $\mathbf{C}^2$ 的一组基是

$$|v_1\rangle=\begin{pmatrix}1\\0\end{pmatrix},\quad |v_2\rangle=\begin{pmatrix}0\\1\end{pmatrix}\tag{1-2}$$

因为 $\mathbf{C}^2$ 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, 且每一个的模都为 1, 所以 $\{|v_1\rangle,|v_2\rangle\}$ 是 $\mathbf{C}^2$ 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 $\mathbf{C}^2$ 的另一组常见完备正交基是

$$|v_3\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},\quad |v_4\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\tag{1-3}$$

因为 $\mathbf{C}^2$ 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:

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

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 σ_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 σ_z 和 σ_x 的本征向量都构成 $\mathbf{C}^2$ 的一组完备正交基, σ_y 的本征向量是否也构成 $\mathbf{C}^2$ 的一组完备正交基呢? 答案是肯定的. 习惯上把由 σ_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 2 量子比特状态的张量积. 例如, 2 量子比特可处于态 $|0\rangle \otimes |1\rangle \equiv |0\rangle|1\rangle \equiv |01\rangle$, 具体为

$$|0\rangle \otimes |1\rangle \equiv |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{1-5}$$

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, 2 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 2 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, 2 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, 2 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

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1-6}$$

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, 本书也没有做最终统一.

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 (1-7) 所示关系, 则称 $\hat{F}$ 为线性算子, 其中 c_1, c_2 是复数.

$$\hat{F}(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1\hat{F}|\psi_1\rangle + c_2\hat{F}|\psi_2\rangle \tag{1-7}$$

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

$$\hat{F}_1\hat{F}_2|\psi\rangle = \hat{F}_1(\hat{F}_2|\psi\rangle) = \hat{F}_1|\phi\rangle \tag{1-8}$$

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

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.