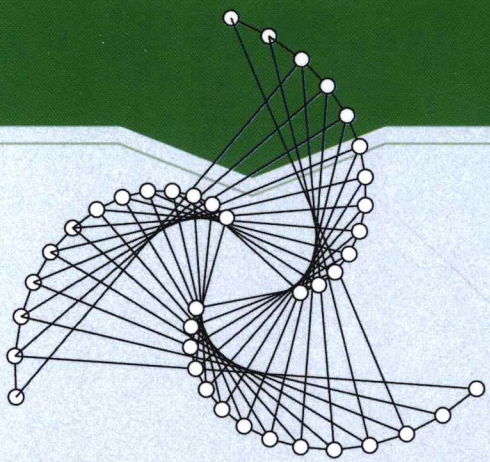
量子签名及应用

LIANG ZI QIAN MING JI YING YONG

温晓军 陈永志◎著



航空工业出版社

量子签名及应用

温晓军　陈永志　著

航空工业出版社

北京

内 容 提 要

本书以课题组近年的研究成果为主体，结合量子签名在国内外的研究进展，经过归纳整理构建了量子签名的框架体系，并探讨了量子签名在电子支付系统和电子选举系统中的应用。

全书分 4 部分（共 9 章）。第一部分（即第 1 章）深入浅出地介绍了量子签名研究所必需的量子力学基础知识；第二部分（即第 2 章）简要地介绍了信息签名的基本知识以及量子签名的研究进展；第三部分（第 3 章~第 7 章）为量子签名协议的设计与分析，主要包括单用户量子签名、多用户量子签名和盲签名、群签名、代理签名等各种特殊用途的量子签名协议的设计及其安全性分析；第四部分（第 8 章、第 9 章）是量子签名在电子支付系统、电子投票系统中的应用。

图书在版编目（CIP）数据

量子签名及应用 / 温晓军，陈永志主编. -- 北京 : 航空工业出版社，2012.7

ISBN 978-7-5165-0006-4

Ⅰ. ①量… Ⅱ. ①温… ②陈… Ⅲ. ①量子论－研究 Ⅳ. ①O413

中国版本图书馆 CIP 数据核字(2012)第 140010 号

量子签名及应用

Liangzi Qianming ji Yingyong

航空工业出版社出版发行

（北京市安定门外小关东里 14 号 100029）

发行部电话：010-64815615 010-64978486

北京忠信印刷有限责任公司印刷 全国各地新华书店经售

2012 年 7 月第 1 版 2012 年 7 月第 1 次印刷

开本：787×960 1/16 印张：12.5 字数：231 千字

印数：1－3000 定价：28.00 元

当今时代是信息时代，信息安全是当今时代世界各国竞争的焦点之一，是信息正常传播的基本保证。信息安全不仅仅关系着国家的军事安全、政治安全，也关系着银行、企业等的经济安全，乃至每一个人的日常生活各方面的信息安全、隐私保护。信息安全的重要性是不言而喻的。目前，电子商务、电子政务正在蓬勃发展，安全的电子支付系统和电子选举系统是其存在和发展的前提。信息签名用以保证信息的真实性、完整性和不可否认性，并实现对通信双方的身份认证，防止消息的冒名伪造或篡改以及发送方或接收方的抵赖。信息签名是信息安全的核心技术之一，也是安全电子商务和安全电子政务所依赖的关键技术之一。然而随着签名技术在电子商务、电子政务领域的深入应用，普通的数字签名已经不能满足一些应用的特殊需要，如无法保障签名者的匿名性、不可追踪性等。正是这些新的需求，推动了签名技术的发展。

传统的信息安全是通过经典密码的计算复杂性来实现安全性的，然而伴随着计算能力的不断提高，特别是拥有强大的并行计算能力的量子计算机等将逐步成为现实，经典密码的安全性越来越受到威胁。经典密码的签名方案大多是基于大数因子分解、离散对数、二次剩余等计算复杂性问题，这些方案并不能被证明是无条件安全的。随着计算能力的不断提高，这些签名算法或协议将变得不安全。以 1994 年提出的 Shor 量子并行算法为例，它是一个真正把经典计算复杂性 NP 类问题化为 P 类问题的算法，可以在多项式时间内解决大数因子分解难题。因此，Shor 量子算法可以轻易攻破 RSA，现已证明，Shor 量子算法还可以轻易攻破常用的 DSA 和 ECDSA 等。当然我们可以再去努力寻找新的数学难解问题，并在其基础上构建新的密码系统，但这并非长久之计，新的量子算法的出现又会攻破这些系统。怎样才能从根本上解决问题呢？

我们认为，根本出路就是“以子之矛攻子之盾”，利用量子信息的独特物理性质设计量子密码，使量子计算机及其网络的强大计算能力无用武之地。因为量子密码的安全性由量子信息的物理特性来保证，而不是基于数学上的计算复杂性问题，因而与攻击者的计算能力或计算资源的大小无关，这种安全性通常称为量子密码的“无条件安全性”。另外，攻击者的行为必将对量子态产生

扰动而被发现，这就是量子密码对窃听攻击的可检测性，这种性质是经典密码所不具有的。可见，量子密码具有两个基本特征——对窃听的可检测性和无条件安全性。这两个特征来源于量子系统的内禀属性——海森堡（Heisenberg）测不准性和未知量子态不可克隆性。对窃听的可检测性的基于 Heisenberg 测不准原理（或称“不确定关系”），而无条件安全性则未知量子态不可克隆定理。当然，所谓无条件安全性，并非是指“绝对”的安全，而是指与当前的计算资源无关，即安全性是不以攻击者的计算能力多强为条件的。

自 1984 年 Bennett 和 Brassard 提出著名的量子密钥分配协议——BB84 协议以来，人们在量子保密通信领域取得了巨大的成功，并且在实验上也不断取得进展。除最早研究的量子密钥分配外，量子秘密共享、量子身份认证、信道认证、量子安全直接通信、量子加密等的研究方兴未艾。鉴于信息签名在信息安全中的重要作用，对量子签名的研究也逐渐引起了人们的兴趣和重视。我们认为量子签名是经典数字签名在 “后量子时代”的理想替代者。然而，目前国内外对量子签名协议的设计与分析的理论还在探索中，在量子签名方面的研究论文相对还不多，量子签名的专著更是凤毛麟角。本书的出版将起到抛砖引玉的作用。

本书以课题组近年的研究成果为主体，结合量子签名在国内外的研究进展，经过归纳整理构建了量子签名的框架体系，并探讨了量子签名在电子支付系统和电子选举系统中的应用。为使本书自成体系，在前两章分别介绍了量子力学基础知识和经典信息签名的基础知识。由于本书采用线性代数语言浅显易懂地介绍量子力学基础知识，因此对量子签名感兴趣但无量子力学基础的读者，只要具有一般代数知识就可以读懂本书。而对那些没有密码学及信息签名基础的读者，通过第 2 章的阅读即可很快进入量子签名研究领域。有相应基础的读者可以跳过相关章节。

全书分 4 部分（共 9 章）。第一部分深入浅出地介绍了量子签名研究所必需的量子力学基础知识（第 1 章），作者相信这一章内容对经典密码学、信息安全、计算机通信等领域学者了解量子力学是绝对必要的；第二部分简要地介绍了信息签名的基本知识以及量子签名的研究进展（第 2 章）；第三部分为量子签名协议的设计与分析，主要包括单用户量子签名、多用户量子签名和盲签名、群签名、代理签名等各种特殊用途的量子签名协议的设计及其安全性分析；第四部分是量子签名在电子支付系统、电子投票系统中的应用。

感谢航空工业出版社的同仁为本书的出版付出了辛勤的劳动，本书的出版还得到了深圳职业技术学院学术著作出版基金的支持。此外，本书中部分课题的研究得到了中国博士后基金等项目的资助，在此一并表示衷心的感谢。

量子签名是一个正在探索和发展中的研究领域，由于作者学识、水平所限，加之本书成书时间仓促，书中难免存在不妥之处，恳请读者批评指正。

编　者

2012 年 4 月

目　录

第 1 章　量子信息学基础知识

微观粒子具有波粒二象性，它的运动状态、性质、描述方法、运动规律是牛顿经典力学所不能描述和解释的，而**量子力学是我们描述微观粒子运动的一个理论框架和数学结构**。量子力学的诞生，给我们提供了描述微观世界的正确方法，加深了我们对物质世界本质的理解。世界本质上是量子的，经典规律只是量子规律在客观条件下的近似。

20 世纪初到 20 世纪 20 年代逐步形成的量子力学，其数学表现形式有薛定谔（Schrödinger）等提出的“波动力学”，以及海森堡（Heisenberg）等人提出的“矩阵力学”，后来人们证明二者虽然外在形式不同，但实质是完全等价的。特别是后者采用线性代数语言——矢量和矩阵来刻画量子态及其演化，后来狄拉克（Dirac）又引入了狄拉克符号，使人们对量子力学的表述更加简明。本书采用第二种形式介绍量子力学基础知识，具有一般线性代数基础的读者即可读懂本章。

1.1　量子力学的基本概念和原理

1.1.1　量子力学五大基本假设

量子力学的基本假设（或者说基本原理）可以有不同的归纳方法，归纳的条目和每条的内容也不完全一样，但总的内涵没有大的差别。我们依据大多数文献[1-9]的提法归纳为如下五条，并依次称之为公理 1~公理 5。

公理 1. 量子态的描述。

量子力学系统的态由 Hilbert（希尔伯特）空间中的矢量完全描写。

公理 2. 量子态叠加原理（principle of superposition）。

若$|\psi_i\rangle$（i=1,2,3,…）是量子系统的可能状态，则它们的叠加态$|\psi\rangle$也是系统可能的状态

$$|\psi\rangle=c_1|\psi_1\rangle+c_2|\psi_2\rangle+\cdots+c_n|\psi_n\rangle+\cdots=\sum_i c_i|\psi_i\rangle \tag{1-1}$$

公理 3. 力学量算符。

在量子力学中，每一个力学量 F 都用一个线性厄米算符 $\hat{F}$ 表示。

公理 4. 测量力学量算符的取值。

测量力学量 F 的可能值谱就是算符 $\hat{F}$ 的本征值谱；仅当系统处在某个本征态$|u_n\rangle$时，测量力学量 F 才能得到唯一结果 F_n，即本征态$|u_n\rangle$的本征值；若系统处在某一归一化态矢$|\psi\rangle$所描写的状态，测得本征值之一 F_n 的概率是$|C_n|^2$，C_n 是态$|\psi\rangle$按 $\hat{F}$ 的正交归一完备函数系$|u_n\rangle$展开的展开系数

$$|\psi\rangle=\sum_n C_n|u_n\rangle \quad C_n=\langle u_n|\psi\rangle \tag{1-2}$$

公理 5. 量子态的演化原理。

孤立量子系统态矢量随时间的演化遵守薛定谔方程

$$i\hbar\frac{\partial \boldsymbol{\psi}}{\partial t}=\hat{\boldsymbol{H}}\boldsymbol{\psi} \tag{1-3}$$

$\hat{\boldsymbol{H}}$ 是系统的 Hamiltonian，$\boldsymbol{\psi}$ 是态矢量。

在这些基本原理下更深层次的问题，或者说人们对量子力学基本原理的解释和理解（有的文献称之为“量子力学的基本问题”），还存在着这样或那样的不同看法（本书不涉及此问题，对此有兴趣的读者可以参考相关文献[10-13]）。但是，由上述几个基本原理推演出的结论，得到了无数实验事实的验证，因此，量子力学作为一个成功的物理理论，没有人怀疑过它的正确性。

下面我们就从这五条基本原理出发，深入浅出地介绍量子力学基本概念和基础知识，这些预备知识对研究量子签名来说是必备的。

1.1.2 Hilbert 空间与态矢量

（1）Hilbert 空间（Hilbert space）的数学概念

一个完备的内积空间称为 Hilbert 空间，简记为 $\boldsymbol{H}$ 空间。

内积空间(inner-product space)：定义了内积运算的矢量空间称为内积空间。由于量子力学中所用到的空间，是复数域上的 Hilbert 空间，下面给出复数域上矢量空间中内积运算的定义：

内积运算：复矢量空间上的内积定义为一种映射——按顺序任取矢量空间中的两个矢量 $\boldsymbol{\psi}$ 和 $\boldsymbol{\varphi}$，总能得到一个数 c 与之对应，记作

$$(\boldsymbol{\psi},\boldsymbol{\varphi})=c$$

其中内积具有如下性质：

① $(\boldsymbol{\psi},\boldsymbol{\varphi})=(\boldsymbol{\varphi},\boldsymbol{\psi})^*$；（$c^*$表示 c 的复共轭，即设 $c=a+b\mathbf{i}$，则 $c^*=a-b\mathbf{i}$，其中 $\mathbf{i}=\sqrt{-1}$ 为复数单位，a、b 为实数。可见内积运算与两个因子的次序有关。）

② $(\psi,\varphi+\xi)=(\psi,\varphi)+(\psi,\xi)$；（分配律）

③ $(\psi,\varphi c)=(\psi,\varphi)c$；（$c$ 是数，φc 表示数 c 与矢量 φ 的数乘运算）

④ 对任意矢量 ψ，$(\psi,\psi)\geqslant 0$ 是实数，且若 $(\psi,\psi)=0$，则 ψ 必为零矢量。

由第④条性质，我们可以定义矢量 ψ 的模（norm）或称矢量长度（length）为

$$\|\psi\|=\sqrt{(\psi,\psi)}$$

内积空间的完备性（completeness）：空间中任何在 Cauchy 意义下收敛的序列 $\{\psi_1,\psi_2,\psi_3,\cdots\}$ 的极限也必须在本空间中。在 Cauchy 意义下收敛的意思是：对给定任意小的实数 ε，有正整数 N 存在，当正整数 $m,n>N$ 时，有

$$(\psi_m-\psi_n,\psi_m-\psi_n)<\varepsilon$$

（2）态矢量与波函数

根据上节**公理 1** 可知，**量子力学系统的态由 Hilbert 空间中的矢量完全描写**，我们称表示量子态的矢量为**态矢量**（state vector），而由态矢量张起的这个 Hilbert 空间称为**态矢空间**。

Dirac 引入一个称为 $|\cdot\rangle$ **右矢**（ket vector）的符号（有的资料也称之为“刀”）表示态矢量。一个具体的态矢可以用 $|\psi\rangle$ 表示，ψ 是表征具体态矢的特征量或符号，如本书中经常出现的 $|\varphi\rangle$，$|0\rangle$，$|+\rangle$，$|+y\rangle$ 等都表示量子态。Dirac 还引进 $\langle\cdot|$ 为**左矢**（bra vector，有的资料也称之为“刃”），左矢 $\langle\psi|$ 为右矢 $|\psi\rangle$ 的**共轭矢量**（conjugate vector）。注意在右矢空间的数乘 $|\psi\rangle c=|\psi c\rangle$ 对应到左矢空间应为 $\langle\psi c|=c^*\langle\psi|$。若用大家熟知的线性代数中的列矢量、行矢量来表达态矢量，右矢 $|\psi\rangle$ 可表示为 Hilbert 空间中的一个列矢量，而对应的左矢 $\langle\psi|$ 可用将上述列矢量作转置后再取复共轭而得到的行矢量来表示。

引入 Dirac 符号后，两个态矢量 $|\psi\rangle$ 和 $|\varphi\rangle$ 的内积可以记为 $\langle\psi|\varphi\rangle$，即 $\langle\psi|\varphi\rangle=(\psi,\varphi)=c$，如果内积 $\langle\psi|\varphi\rangle=0$，则称两态矢量 $|\psi\rangle$ 和 $|\varphi\rangle$ **正交**，否则称它们是非正交的。

态矢量 $|\psi\rangle$ 常常要求是**归一化**的矢量，即它的模 $\|\psi\|=\sqrt{\langle\psi|\psi\rangle}=1$。

正像欧几里得空间（位形空间）中一个矢量可以用不同的坐标系（如直角坐标系、球坐标系等）表示一样，Hilbert 空间的态矢量也可以用不同的“坐标系”表示。在量子力学中称表示态矢的具体“坐标系”称为**表象**（representation）。态矢用定义在某个区域 Ω 上的平方可积复值函数表示，就称为态矢的**坐标表**

象。在坐标表象中，常省去 Dirac 符号，直接用这个可积复值函数表示态矢量。在单光子情况下，这个函数可记为 $\psi(\vec{x})$，$\vec{x}$ 就是光子的坐标。$\psi(\vec{x})$描述单光子的物质波，所以又称**波函数**（wave function）。除坐标表象外，常见的还有动量表象、$\hat{\sigma}_x$表象、$\hat{\sigma}_y$表象、$\hat{\sigma}_z$表象，等等，表象理论的介绍详见 1.1.4 节。

例：在某表象中有两个态矢量$|\psi_1\rangle$、$|\psi_2\rangle$可表达为列矢量

$$|\psi_1\rangle=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}\qquad |\psi_2\rangle=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}$$

试计算每个态矢量的模以及这两个态矢量的内积。

右矢$|\psi_1\rangle$、$|\psi_2\rangle$对应的左矢$\langle\psi_1|$、$\langle\psi_2|$可分别表达为

$$\langle\psi_1|=\left(|\psi_1\rangle^{\mathrm{T}}\right)^*=\left[\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}^{\mathrm{T}}\right]^*=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}$$

$$\langle\psi_2|=\left(|\psi_2\rangle^{\mathrm{T}}\right)^*=\left[\begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}^{\mathrm{T}}\right]^*=\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}$$

式中，上标 T 表示矩阵或矢量的转置。所以

$$\langle\psi_1|\psi_1\rangle=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}=1$$

同理，$\langle\psi_2|\psi_2\rangle=1$。因此两个态矢量的模分别为$\|\psi_1\|=\sqrt{\langle\psi_1|\psi_1\rangle}=1$，$\|\psi_2\|=\sqrt{\langle\psi_2|\psi_2\rangle}=1$。

矢量$|\psi_1\rangle$与$|\psi_2\rangle$的内积为

$$\langle\psi_1|\psi_2\rangle=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\mathrm{i}\end{pmatrix}=0$$

同理，可算得$|\psi_2\rangle$与$|\psi_1\rangle$的内积为$\langle\psi_2|\psi_1\rangle=\langle\psi_1|\psi_2\rangle^*=0$。可见$|\psi_2\rangle$与$|\psi_1\rangle$是正交的。

态矢量或波函数，它的物理意义在于能对它描述的系统实施测量的结果概率分布作出预言。我们可以理解态矢量是获得这个态历史过程的记录，包含着制备这个态过程中使用的宏观仪器、选定的参数值、经过一套操作程序等全部信息。指定量子系统的一个态就是指定这个系统的组分，制备过程中使用的仪器、操作程序和选择的参数等。比如从电子枪出发，通过屏上一条缝的电子态就由发射电子、屏上窄缝等指定，而不同于从两条缝通过的电子态。如果两个量子系统在制备过程中相关条件都相同，就可认为这两个系统处在相同的量子态。所以我们说态矢完全描述了量子系统。

（3）基矢

一个矢量空间中可以有多组完全集，所谓完全集，是指一个线性无关的矢量集合$\{|v_1\rangle,|v_2\rangle,|v_3\rangle,\cdots,|v_n\rangle\}$，矢量空间的任意矢量$|\varphi\rangle$都能表示为这个完全集中矢量的线性叠加，即

$$|\varphi\rangle=\sum_{i=1}^{n}a_i|v_i\rangle \tag{1-4}$$

的形式，其中a_i是一组复数。如果完全集中每一个矢量$|v_i\rangle$都是归一化的，且各矢量又是两两相互正交的，这样的完全集称为这个空间的一组**基矢**，n称为矢量空间的**维数**。基矢组$\{|v_1\rangle,|v_2\rangle,|v_3\rangle,\cdots,|v_n\rangle\}$的正交归一性可以表示为

$$\langle v_i|v_j\rangle=\delta_{ij}=\begin{cases}1 & \text{当}i=j\text{时}\\ 0 & \text{当}i=j\text{时}\end{cases} \tag{1-5}$$

式中，$i,j=1,2,3,\cdots,n$。

例：量子信息中最常用的是二维 Hilbert 空间中的量子系统（所谓“量子比特”），具体的如电子的自旋，光子的偏振等，二维 Hilbert 空间可记作 $\mathbf{C}^2$。作为特例，下面讨论二维 Hilbert 空间的基矢，$\mathbf{C}^2$ 最常用的一组基矢表示为$|0\rangle$和$|1\rangle$，这样二维 Hilbert 空间中任意态矢$|\psi\rangle$可表示为

$$|\psi\rangle=a|0\rangle+b|1\rangle \tag{1-6}$$

式中，a,b 为复数，且 $\|a\|^2+\|b\|^2=1$。如果二维正交基矢$|0\rangle$和$|1\rangle$分别用列矢量$\begin{pmatrix}1\\0\end{pmatrix}$和$\begin{pmatrix}0\\1\end{pmatrix}$表示，即令$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$，$|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$，则任意态矢$|\psi\rangle$在此基矢下可表示为列矢量

$$|\psi\rangle=a|0\rangle+b|1\rangle=a\begin{pmatrix}1\\0\end{pmatrix}+b\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}a\\b\end{pmatrix} \tag{1-7}$$

二维 Hilbert 空间除了用$\{|0\rangle, |1\rangle\}$基矢外，也可以用$\{|+\rangle, |-\rangle\}$基矢表示，其中

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), \tag{1-8}$$

式（1-6）表示的态矢量$|\psi\rangle$在$\{|+\rangle, |-\rangle\}$基矢中表示方式为

$$|\psi\rangle=\frac{\sqrt{2}}{2}(a+b)|+\rangle+\frac{\sqrt{2}}{2}(a-b)|-\rangle。 \tag{1-9}$$

量子信息中习惯称$\{|0\rangle, |1\rangle\}$为**计算基矢**（computational basis），$\{|+\rangle, |-\rangle\}$为**物理基矢**（physical basis）。

1.1.3 算符（算子）

（1）算符

算符（operator，或译“算子”）在量子物理中对应于一种对量子态的操作（或说“运算”），作用在量子态上的操作将改变量子态。一般地，如果运算 $\hat{F}$ 作用到态矢上，结果仍然是一个态矢，即有

$$|\varphi\rangle=\hat{F}|\psi\rangle, \tag{1-10}$$

则 $\hat{F}$ 就是一个算符。

（2）线性算符

若 $a, b\in$ 复数域 $\mathbf{C}$，$|\phi\rangle$，$|\varphi\rangle$ 是 Hilbert 空间的两个任意矢量，任何满足下式的运算 $\hat{L}$ 称为线性算符（linear operator），

$$\hat{L}(a|\phi\rangle+b|\varphi\rangle)=a\hat{L}|\phi\rangle+b\hat{L}|\varphi\rangle。 \tag{1-11}$$