1　引言

量子信息是量子物理与信息科学相融合的新兴交叉学科　　,它诞生于上个世纪 80年代,在 90年代中期引起国际学术界的巨大兴趣　,受到西方各国的高度重视 ,得到迅速发展 ,迄今方兴未艾！

量子计算是量子信息的一个重要分支,　近年来得到了人们广泛的关注。量子计算机是实现量子计算（　quantum computation）的机器。量子计算和量子计算机概念起源于著名物理学家　Richard Feynman, 是他在 1982 年研究用经典计算机模拟量子力学系统时提出的。　1985 年, 量子图灵机（Turing）的模型被 David Deutsch 提出, 通过它的性质的研究,　预言了量子计算机的潜在能力。由于量子计算机依赖于量子力学规律处理信息, 所以它有着经典计算机永远不可逾越的巨大优势。量子计算机不但可以提供更多的比特以及更高的时钟速度, 它还提供了一种基于量子原理的算法的全新计算方法[1]。量子计算机中的信息是用量子逻辑门来进行处理的。量子逻辑门是实现量子计算的基础。为了实现量子计算, 也就是说构建量子计算机, 必须选择与设计合适的物理体系并控制它以实现量子逻辑门。目前, 已经有许多作为执行这些量子计算系统的逻辑门的方案被提出, 而且其中许多方案已经实现。例如, 离子阱 [2]、腔量子电动力学 [3]、核磁共振 [4]、量子点 [5]和基于 Josephson 结的超导体方案 [6]等。

基于 Alan Turing 理论发展起来的现代计算机科学在近几十年中取得惊人的发展 ,计算机硬件能力在　20 世纪 60 年代后的几十年时间里以近似 Moore 定律成长。随着电路集成度的提高　,进一步提高芯片集成度已极为困难。当集成电路的线宽在　011μm以下时 ,电子的波动性质便明显地显现出来。这种波动性就是量子效应。为此　,多数观察家预期 Moore 定律将在 21 世纪前二十年内结束　,人们在考虑替代当前计算机的新途径。物理学方面　　,自 Max Planck 在 1900 年提出量子假说以来　,量子力学给人类生活带来翻天

覆地的变化 ,改变了经典物理学对世界的认知方式。 Moore 定律最终失效问题的一个可能解决办法是采用不同的计算模式 ,量子计算理论就是这类模式的一种。但是直到 1982 年,才由 Benioff 和 Feynman 发现了将量子力学系统用于推理计算的可能 [7]; 1985 年 Deutsch 提出第一个量子计算模型 [8]。由此,量子计算迅速吸引了全世界研究者的注意并成为一门具有巨大潜力的新学科。量子计算是应用量子力学原理来进行有效计算的新颖计算模式 ,它利用量子叠加性、纠缠性和量子的相干性实现量子的并行计算。量子计算从本质上改变了传统的计算理念。本文介绍了量子计算的基本原理、实现量子计算的基本要求、量子计算的根本困难、可能的解决办法 ,以及当前的几个有希望实现量子计算的物理系统。并介绍量子信息技术中量子逻辑门的基本特点、方法以及实现量子门的物理实验进展。

2 量子计算

2.1 量子计算研究简史

Benioff 最早用量子力学来描述可逆计算机。 Feynman 发展了 Benioff 的工作 ,构造了对应各种逻辑门的哈密顿量。 Deutsch 则进一步提出了量子图灵机和通用量子计算机的最初构想 ,随后又提出了量子计算网络 ,并构造了两个量子比特的算法。 Andrew Chi2Chi Yao 证明了任意在量子图灵机上是多项式时间可计算的函数一定存在一个相应的多项式大小的量子电路。

1993 年, Bernstein 等人研究了量子计算复杂性理论 ,对量子算机在数学上给予严格的形式化描述 ,给出了量子图灵机比经典概率图灵机在计算效率上更为强大的证据。

在算法方面， 1994 年, Shor 提出了离散对数问题和大整数质因子分解问题的量子算法 ,证明了这两个重要且复杂的问题属于 BQP 类。 Shor 算法

极大地促进了量子计算的发展 ,使人们第一次清楚地看到了量子计算独具优势的重要应用前景。 从此,世界众多研究小组加入了该研究行列 ,量子计算研究领域取得了许多重大进步 ,如 Jozsa 的因子分解算法 ,Hogg 的约束满足问题算法、 Grover 的数据库搜索算法及求中数和平均数的算法等。 Shor 的另一项同样重要的成果是率先提出了量子纠错码 ,这使得容错的量子计算成为可能。量子计算在密码学领域也取得了迅速的发展 ,自 1984 年提出第一个量子密钥分发协议 BB84 以来,目前已提出的协议就有十几个 [9]。

2.2 量子计算过程

从物理观点看，计算机是一个物理系统，计算过程则是这个系统演化的物理过程。量子计算机是个量子力学系统，量子计算过程就是这个量子力学系统量子态的演化过程。从 “ 计算 ” 的本质上看，它是被称为计算机的物理系统执行的一个物理过程。根据采用的计算设备的不同，这一物理过程可以非常不同。它可以是人脑所完成的 “ 计算 ”、算盘操作的 “ 计算 ” 和电子计算机控制的 “ 计算 ”，等等。不管采用何种计算设备，“ 计算 ” 的一般过程是：首先，输入初始数据，从物理的角度看，这可以解释为在计算系统中制备出一个初始物理态；其次，执行计算，这个过程实际是按照算法规定的步骤，将给定的初始物理态演化成对应输出物理态的过程；最后，输出计算结果，给出问题答案，这可以看作对演化的物理末态进行测量得到所需信息的过程。所以计算过程可归结为：制备物理态，演化物理态，最后对物理态实施测量。当然不同的计算机执行这三个步骤的方式可以非常不同，但本质上都是一样的。从这个意义上说，任何一个物理系统，只要它能提供足够多的不同状态，用来编码信息并能按照算法要求演化，最终能从对末态测量中提取出所需要的结果，这个物理系统就是一个计算机。

量子计算机是服从量子力学规律的计算机，它可以支持新类型的量子算法。如， Shor 算法和 Grover 算法等。任何量子算法的核心都是研究如何

处理量子并行计算，使得以较高的概率测量我们所期望的计算结果。

在量子计算机中， 采用的是量子态编码信息， 其存储量子信息的基本单元是量子位 （qubit）的量子双态系统 （或者说是一个 2 维 Hilbert 空间）。可以将量子计算机看成是由一系列量子逻辑门构成的电路。量子逻辑门对量子寄存器进行操作，实现量子态的转换（即实现对量子寄存器中的数据进行计算、处理）。与“ 计算 ”的一般过程对应，量子计算的过程是：首先，制备出处于叠加、等振幅（等概率）的量子初态；其次，按照算法需要对叠加态不断进行演化（量子门操作，幺正变换）；最后，对最终的叠加态进行测量使其以接近于 1 的概率坍缩到所希望的态，从而给出量子并行计算的输出结果。在量子计算过程中，这种状态的转换是由量子逻辑门实现的，一个量子计算网络能被分解成多个不同的量子逻辑门，因此，量子逻辑门是量子计算机最基本的构造单元之一。对于量子计算系统，因为可以制备出由各个互不相同的态叠加所形成的初始态，量子计算机具有对这些初始态同时进行演化的能力，也即量子计算机可以沿着各条互不相同的路径同时演化初始叠加态，直至获得对应的输出的叠加态 [10]。

2.3 量子计算的物理实现

量子计算的物理实现方案 ，包括离子阱、中性原子、光学、超导约瑟夫森结、腔量子电动力学、液体核磁共振、 Kane 的硅基半导体方案、富勒球、量子点和液氦表面电子等 [11]。实现量子计算机 ,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地隔离 ;另一方面又要求能精确而有效地控制系统的演化 ,即,需要外界控制系统与量子系统之间有很好地耦合。这两者形成了一对矛盾。因此 ,选择什么样物理体系来制作量子计算机要兼顾这两个方面的要求。科学家正努力寻找能实现量子计算的更多的物理系统 ,目前的研究主流集中在下列两个方向 : (1)固态量子计算 ,包括超导系统、量子点系统等 ; (2)基于量子光学的量子计算 ,包括离子阱、腔 QED 系统、线性光学系统、光子晶体、光格子等。

2.4 量子并行计算

与经典计算机相比，量子计算机最重要的优越性体现在量子并行计算上。我们已经知道，量子计算最本质的特征为量子叠加性和相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，并按一定的概率振幅叠加起来，给出量子计算机的输出结果，这种计算称为量子并行计算。例如，在某一时刻，一个二位量子寄存器可同时存储 8个数据，若对该寄存器进行读 / 写操作，一次读 / 写操作可同时对 8个数进行，而同样的操作经典计算机需要 3次才能完成。推广到 n位量子寄存器，一个 n位量子寄存器可同时存储 2的n次方个数，一次读写操作可同时对 2的n次方个数进行读 / 写操作。量子并行处理大大提高了量子计算机的效率，使得其可以完成经典计算机无法完成的工作。量子相干性在所有的量子超快速算法中得到了本质性的利用。因此，用量子态代替经典态的量子并行计算，可以达到经典计算机不可比拟的运算速度和信息处理功能，同时节省了大量的运算资源。

2.5 量子计算应用领域

量子计算的应用主要在下面三个方面 [12]:

(1) 保密通信。由于量子态具有事先不可确定的特性 ,而量子信息是用量子态编码的信息 ，同时量子信息满足 “ 量子态不可完全克隆 (No-Cloning) 定理 ”，也就是说当量子信息在量子信道上传输时，假如窃听者截获了用量子态表示的密钥，也不可能恢复原本的密钥信息 ,从而不能破译秘密信息。因此，在量子信道上可以实现量子信息的保密通信。目前，美国和英国已实现在 46KM 的光纤中进行点对点的量子密钥传送，而且美国还实现在1KM 以远的自由空间传送量子密钥 ,瑞士则实现了在水底光缆传送量子

密钥。此外， A. K.Pati 等人利用量子力学的线性性证明密码攻击者不能破坏量子信息传输的完整性。

(2) 量子算法。对于一个足够大的整数， 即使是用高性能超级并行计算机，要在现实的可接受的有限时间内，分解出它是由哪两个素数相乘的是一件十分困难的工作， 所以多年来人们一直认为 RSA 密码系统在计算上是安全的。然而， Shor博士的大整数素因子分解量子算法表明， 在量子计算机上只要花费多项式的时间即可以接近于 1 的概率成功分解出任意的大整数，这使得 RSA 密码系统安全性极大地受到威胁。因此 , Shor算法的发现给量子计算机的研究注入新活力 ，并引发了量子计算研究的热潮。

(3) 快速搜索。 众所周知，要在经典计算机上从 N个记录的无序的数据库中搜索出指定的记录 ，算法的时间复杂性为 O (N)。因为搜索数据库是在外存进行的，所以当记录数 N 充分大时，搜索工作犹如“ 大海捞针 ”一样的困难与烦琐。 Grover于1997 年在物理学界鼎尖杂志《 Physics Review Letters》上发表了一个乱序数据库搜索的量子算法 ，其时间复杂性为 O($\sqrt{N}$).此量子搜索算法与经典搜索算法相比达到数量级的加速 ，特别适用于求解那些需要用穷举法对付的 NP类问题。

3 量子逻辑门

3.1 经典逻辑门与量子逻辑门的比较 [10]

量子计算机中，信息的基本单元是量子比特（ qubit）即量子位，信息的基本操作元件是量子逻辑门（ quantum logic gate)。量子比特是信息的载

体，量子比特的信息经量子逻辑门操作处理后，最后得到计算结果。

量子信息处理是对编码的量子态进行一系列幺正演化，量子逻辑门就是对量子比特的最基本的幺正操作。而量子计算则是通过量子逻辑门来控制和操作量子态的演化和传递，进行量子信息处理的。故幺正性是量子逻辑门的唯一要求，任何满足幺正性的矩阵都能表征一个量子逻辑门。而所有的量子逻辑门都是可逆操作，　不伴随信息的擦除　（输入信息的丢失），在理论上也就不存在热耗散的极限，从而杜绝了经典计算机从根本上就无法解决的热耗散严重影响器件正常功能的问题。

经典计算机电路由连线和逻辑门构成，连线用于在线路间传送信息，而逻辑门负责处理信息，把信息从一种形式转换为另一种。显然，逻辑门是经典逻辑电路的最基本单元。量子计算机的量子电路由量子连线和量子逻辑门构成，量子连线不一定对应物理上的接线，而可能是对应一段时间或一个从空间的一处移动到另一处的物理粒子，如光子。量子连线用于在量子电路间传送量子信息，而量子逻辑门负责处理量子信息，把量子信息从一种量子态演化为另一种量子态。显然，量子逻辑门是量子逻辑电路的最基本单元。与经典线路不同，量子线路不允许出现回路。另外，量子逻辑门的操作要求是可逆的，而经典计算机中的逻辑门都是不可逆的，故在量子逻辑门中不能直接推广。研究表明　，单量子比特旋转门和双量子比特控制非门是基本量子门，利用它们可以组成所有的可逆操作，实现各种各样的运算。量子逻辑门按其作用的量子比特的数目可分为单比特、二比特和三比特逻辑门等。

3.2　量子逻辑门

3.2.1　单比特门 [1]

量子逻辑门的操作可以用对量子比特的　Hilbert 空间基矢的作用定义。量子逻辑门的本质是对量子比特实施最基本的幺正操作。如果一个幺正操

作演化基矢态为

$$\left.\begin{aligned}|0\rangle &\to |0\rangle \\ |1\rangle &\to e^{i\omega t}|1\rangle\end{aligned}\right\} \tag{1}$$

这个幺正操作就是一个单比特门，即一位门。记基 $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$，$|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$，这个门操作就可用一个幺正矩阵

$$P(\theta)=\begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix} \tag{2}$$

表示，其中 $\theta=\omega t$。

当 $P(\theta)$ 分别作用到 $|0\rangle$ 和 $|1\rangle$ 时，有

$$P(\theta)|0\rangle=\begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}=|0\rangle,$$

$$P(\theta)|1\rangle=\begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\e^{i\theta}\end{bmatrix}=e^{i\theta}\begin{bmatrix}0\\1\end{bmatrix}=e^{i\theta}|1\rangle,$$

所以这个门操作还可以用投影算子形式表示为

$$P(\theta)=|0\rangle\langle 0|+e^{i\theta}|1\rangle\langle 1| \tag{3}$$

注意到 $|0\rangle$、$|1\rangle$ 满足正交归一化条件，可以得到：

$$\left.\begin{aligned}P(\theta)|0\rangle&=|0\rangle\langle 0|0\rangle+e^{i\theta}|1\rangle\langle 1|0\rangle=|0\rangle\\ P(\theta)|1\rangle&=|0\rangle\langle 0|1\rangle+e^{i\theta}|1\rangle\langle 1|1\rangle=e^{i\theta}|1\rangle\end{aligned}\right\} \tag{4}$$

由于 P 操作改变两个基底态的相对位相，P 门称为位相门。

适用于单个量子位的量子状态变换的单比特量子逻辑门有：

单位门（恒等变换）：$I=|0\rangle\langle 0|+|1\rangle\langle 1|$，不采取任何操作，其矩阵为 $I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，即单位矩阵。

X 门(求非变换)：$X=|0\rangle\langle 1|+|1\rangle\langle 0|$，其作用为 $X|0\rangle=|1\rangle, X|1\rangle=|0\rangle$，

对应着经典逻辑非门——NOT 操作，故 X 门又叫“非”门，它的矩阵表示为 $X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$。

Z 门（相位移动操作）：$Z=P(\pi)$，即 $Z=|0\rangle\langle 0|-|1\rangle\langle 1|$，其作用是改变态 $|0\rangle$ 和 $|1\rangle$ 的相对位相 π，即 $Z|0\rangle=|0\rangle, Z|1\rangle=-|1\rangle$，它的矩阵表示为 $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$。

Y 门：我们可以定义 Y 操作门 $Y=ZX$，其作用为 $Y|0\rangle=-|1\rangle, Y|1\rangle=|0\rangle$，注意到 $ZX=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$，所以 Y 操作可以用矩阵表示为 $Y=i\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$

Hadamard 旋转门：$H=\frac{1}{\sqrt{2}}[(|0\rangle+|1\rangle)\langle 0|+(|0\rangle-|1\rangle)\langle 1|]=\frac{1}{\sqrt{2}}(X+Z)$，其作用为 $H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-1\rangle)$，用矩阵表示为 $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$。

3.2.2 二比特门

作用到两个量子位上的所有可能的幺正操作构成二比特量子逻辑门，即二位门。在二位量子逻辑门中，最有意义的是控制 - U 门（Control U-gate），可表示为 $|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U$，其中，I 是一个量子位的恒等操作，U 是另外一个一位门。第一量子位称为控制位，第二量子位称为目标位。控制 -U 门对目标位的作用，决定于控制位处于 $|0\rangle$ 态还是 $|1\rangle$ 态。当控制位处于 $|0\rangle$ 时，第二量子位执行逻辑恒等操作，保持不变。当控制位处于

$|1\rangle$ 时，第二量子位执行逻辑非门即 X门操作。由此又可将此二位门表示为 $|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes X$ 。控制-非门（Control NOT-gate）的作用为 $|00\rangle\rightarrow|00\rangle,|01\rangle\rightarrow|01\rangle,|10\rangle\rightarrow|11\rangle,|11\rangle\rightarrow|10\rangle$，因此，当且仅当第一量子位处于态 $|1\rangle$ 时，才对第二量子位执行一位门运算（ U变换）。对于两量子位的态矢空间的基底 $|00\rangle,|0\ 1\rangle,|1\ 0\rangle,|1\ 1\rangle$，控制 NOT门（C-NOT门）的作用可以用矩阵表示为

$$C_{NOT}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \tag{5}$$

3.2.3 三比特门

作用到三个量子位上的所有可能的幺正操作构成三比特量子逻辑门，即三位门。在三位量子门中最重要的一个就是 3 位控制 - 控制-U 门，可表示为 $|0\rangle\langle 0|\otimes I+|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U$ ，即它有二个控制位，第一、二量子位为控制位，第三量子位为目标位。两个输入的量子位（控制位）控制第三个量子位（目标位）的状态，两控制位不随门操作而改变。当且仅当两个控制位同时处于态 $|1\rangle$ 时，才对第三量子位执行 U变换，使目标位改变，否则保持不变。

在三位量子门中，对第三量子位 U 取逻辑非时，就得到了经典的 Toffoli 门——经典通用门。 Toffoli 门的作用是：

$$
\begin{cases}
|000\rangle \to |000\rangle \\
|001\rangle \to |001\rangle \\
|010\rangle \to |010\rangle \\
|011\rangle \to |011\rangle \\
|100\rangle \to |100\rangle \\
|101\rangle \to |101\rangle \\
|110\rangle \to |111\rangle \\
|111\rangle \to |110\rangle
\end{cases}
\tag{6}
$$

这个门的矩阵表示是：

$$
T = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}
\tag{7}
$$

3.2.4　量子计算的通用逻辑门——　**Deutsch**门

我们知道，任何满足幺正性的矩阵都能表征一个量子逻辑门。　Deutsch 早在 1989 年就考虑了用量子逻辑门来构造计算机的问题，　他将经典 Toffoli 门推广到量子情况，得到了　Deutsch 门。Deutsch 门是一个 三位控制 - 控制 - R 门，即当且仅当前两个量子位都处在态　$|1\rangle$ 时，才对第三位态施加一个　R 变换。其中

$$
R = -iR_x(\theta) = -i\begin{bmatrix}
\cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\
i\sin\frac{\theta}{2} & 2\cos\frac{\theta}{2}
\end{bmatrix}
\tag{8}
$$

θ 角是满足　θ/π 等于无理数的任意角度　。

可以证明　Deutsch门能够实现经典　Toffoli 门的作用。Deutsch还进一步证明任意　n 位 Hilbert 空间的所有幺正变换，　其计算网络都可以由这个门重

复使用构造出来，所以这个门对量子计算是通用的。他还发现几乎所有的三比特量子逻辑门都是通用逻辑门。通用逻辑门的含义是指，通过该逻辑门的级联，可以以任意精度逼近任何一个幺正操作，也就是由这个通用量子逻辑门可以实现任何量子门操作。

在 Deutsch 提出了通用三位量子门之后， 1995 年， IBM 研究实验室的 Divincenzo 证明 Deutsch 门可以用两位门实现。 紧接着，纽约大学的 Tycho Sleator 和因斯布鲁克大学的 Harald Weinfurter 提出两量子位的量子门对于量子计算是可以通用的。 后来，Deutsch 又进一步证明， 差不多任意 2-位门或 n-位门 $(n \geq 2)$ 对量子计算都是通用门组。之后 Barenco 等人又证明通用量子门还可由经典多位门和量子一位门构成 [1]。

虽然人们已经证明了量子门的通用性，但是如何将这样的量子门连接起来进行通用的量子计算还是一个问题。 Deutsch 说道：即使有足够数量的“通用量子门”可供使用，迄今为止，仍然没有证明，对于想利用它们进行计算的人有什么用途。因为这些门首先要组装成量子计算网络，才能用于执行需要的计算。但是这种组装并不等于执行运算。 1993 年， Yao 证明了 Deutsch 类型的通用量子门网络能够模拟通用量子图灵机并能达到任意精度 [13]。

3.3 量子逻辑门的物理实现及进展 [14]

由于最基本的逻辑门就是受控的两量子位的物理系统，在两量子位系统之间根据一个位的状态条件对另一个位实现所需要的幺正演化、控制两量子位之间的转动就足以构造出能执行任意复杂的量子计算网络。因此，量子逻辑门的实现是量子计算的关键。

目前，构造量子逻辑门的实验方案主要有以下几种：

3.3.1 离子阱方案

量子逻辑门的最初离子阱方案是由 Cirac提出，它是在特定构形的电极

上加上静电场、交变电场或磁场的适当组合，将带电离子稳定地囚禁于高真空的一种装置。利用这种装置将离子冷却至质心运动状态的基态，从而使离子处于用来表征量子信息的 qbit上，并通过辅以的特定操作， 实现量子逻辑门。该方案由于与外界的相互作用极弱，因而，由环境所引起的消相干效应可忽略不计； 另外，由于处于阱中的 n个超冷离子是排成一行的，因而可实现 n 位的量子逻辑门。而连接 n 位量子逻辑门的“ 导线 ”就是 n 个超冷离子在阱中的集体振荡。

但由于离子冷却的难度很大，因而很难推广至多个超冷离子的制备。与此同时，人们不断地提出其它的可能实现方案， 1998 年， Poyatos提出不用超冷离子也能实现量子逻辑门的方案，即所谓的“ 热 ”离子方案。其基本思想是在对量子位的操作中只依赖于离子的内态，而与外态无关，即无论外界处于何种状态，离子都能进行任意的量子操作。 2000 年， Cirac 和Zoller提出了一种新的基于椭圆型离子阱构形的方案， 该方案避免了多个离子之间的库仑排斥的影响，易于集成。但真正的实现该方案，在技术上仍存在着很大的难度。

3.3.2 腔量子电动力学方案

在单原子、单光子水平实验的技术基础上， 1995 年，Barenco 和Sleator 等人同时提出实现两量子位控制转动操作的腔 QED方案。在该方案中，量子位由高 Q 微波腔内的量子化电磁场和两能级原子充当。当原子通过腔场时原子和腔场作用的时间，决定了腔场的态及原子的运动速度，从而实现了所需要的条件量子相移门与控制非门。

在条件量子相移门中，需要对两量子位作如下的操作变换

$$|a,b\rangle \rightarrow \exp(i\phi\delta_{a,1,}\delta_{b\,1}),|a\;\;b\rangle \qquad (9)$$

其中， $|a\rangle$， $|b\rangle$ 分别代表两量子位的基矢，而 $\delta_{a,1}$ ， $\delta_{b,1}$为通常的克隆尼克符号。条件量子相移门在两个量子态都处于 1 时，产生一个 ϕ 角相移，而在其它态时均保持不变。 1995 年， Mandel 和Wolf 证明，连续地改变 δ

从正值到负值或者从负值到正值，　可以实现 ϕ 角在 0 ~ 2π 之间的连续变化。

之后， Giovannetti等证明，腔与原子体系不仅可以实现控制—非门、条件量子相移门、单量子 bit 的任意操作，而且还可以实现 Toffoli 门， Deutsch 门和进行量子纠错编码，使腔与原子体系进行多位量子逻辑计算真正成为现实。 2000年以后，新一代的腔量子电动力学实验取得了突破性进展。应用这些新的技术，有望在不久的将来，实现更多的量子信息的处理器件和建立未来的光量子网络。

3.3.3　固态量子体系方案

1999 年， Nakamura等人利用超导约瑟夫结第一次实现了固态量子逻辑门。在实验中，超导约瑟夫结起两个重要作用：　（1）实现单个库珀对在其中的隧道过程；（2）使能级出现免交叉效应。因而能在宏观的超导箱中实现一个二能级的量子体系。随后，　Makhlin 等首先讨论了单个库珀对的量子逻辑操作。 2001 年，赵志等人证明，使用超导量子干涉，也可实现量子逻辑操作。

在固态量子体系方案中，　另一个可能实现量子逻辑门的体系是量子点。量子点是把半导体材料中几百个原子组成纳米尺度的小岛——量子点，或把半导体材料中的单电子视为量子点，将它们所处的基态和激发态看作一个二能级量子体系，操纵量子点状态之间的变化，即可实现量子逻辑门。

3.3.4　核磁共振方案

核磁共振技术是目前量子信息技术使用最为频繁的实验手段，已提出的各种量子算法都能在几个量子　bit下进行验证。在这一技术中，操作并非作用在某个单独的粒子或分子的自旋上，而是作用在　1023数量级的系综的自旋态上。因而，它实质上是一个宏观系综。由于它是宏观系综，因此，几乎不受外部环境对它的影响。但宏观系综原则上是没有量子特性的，只有纯粹的量子系综才具有量子纯态的特征，因而对它存在着较大的争议。

从目前所提出的所有实现量子逻辑门方案及实验来看，固态量子体系

的实验进展不如离子阱和腔量子电动力学的实验进展　　,从各方面的研究报告统计可以证实。但由于固态量子体系方案，特别是量子点方案能镶嵌在固体材料中，因而，吸引了一大批的理论和实验学家　　,并利用半导体纳米技术,使得在不久的将来量子点方案的实现成为最为可能实现的方案。

4　结束语

量子信息学是一种时尚的科学　，具有强大、高效的计算工具和神奇的隐形传态魔法以及精确无比的量尺　,而量子计算是量子信息的一个重要分支。目前量子计算的理论框架已经基本形成，其研究已经取得日新月异、令人叹为观止的进步，但最终要实现有一定实用价值的量子计算与量子计算机,还存在着许多理论与技术上亟待解决的问题。　例如,如何制备足够数量的量子逻辑门　,其量子状态易于叠加且　U变换准确,如何使量子位扩展　,即实现多量子位纠缠　,组成量子门网络　,如何更好地解决消相干预量子纠错问题　　,即解决量子态与外界隔离的问题　　,延长相干时间　,有效克服或避免量子态与外界环境相互作用而导致的量子耗散和退相干现象对计算结果的干扰等问题;另外,寻找更新的量子算法的问题也需要解决。　在目前量子计算机还未进入实际应用的情况下　,量子计算的研究重点包括　：a) 计算的物理实现。提高量子体系中相干操控的能力　,实现更多的量子纠缠状态。　b) 研究新的量子算法。目前还有很多经典算法无法解决的难题　　,研究新的能解决这些难题的量子算法是一个重要方向。　c) 增强现有量子算法的实用性和扩展现有量子算法的应用范围，如将量子 Fourier　变换的应用推广到解决隐含子群问题以及更广的范围，将Grover 算法体系扩展到二维和多维搜索域等　[9]。2009年11月，世界首台通用编程量子计算机于美国面世。美国国家标准技术研究院的科学家们让量子通信网产业不再遥远。我们有理由相信随着理论与技术的成熟，随着更多的专家与学者加入该领域的研究，量子通信与量子计算

一定会取得突飞猛进的发展，并且对未来科学技术以及人类的发展与进步起到巨大的推动作用，人类进入量子信息时代的梦想一定会实现！

致　谢

在本文即将结束之际，我要由衷地感谢，在我撰写论文的过程中，曾帮助过我的师长与同学．首先，要感谢指导教师苏晓琴教授．在一个多月的学习和写作过程中，苏老师给予我极大的关心和帮助．苏老师治学严谨，学识渊博．在学术和为人上都为我树立了榜样．在苏老师的悉心教导下，我的课题能够得以顺利的开展，并取得了一些阶段性的成果．在此，我向苏老师表示最诚挚的感谢．我还要感谢与我一同写毕业论文的同学．正是我们共同努力，一起探讨，才使研究有所成果．

参考文献

[1] 苏晓琴 .量子信息之量子隐形传态 [M]. 北京：中国科学技术出版社 .2007.45~72.

[2] Cirac J I, Zoller P. Quantum computations with cold trapped ions[J]. Phys. Rev. Lett., 1995, 74: 4091~4094.

[3] Barenco A, Deutsch D, Ekert A, Conditional quantum dynamics and logic gates[J]. Phys. Rev. Lett., 1995, 74: 4083~4086

[4] Gershenfeld N A, Chuang I L. Bulk spin-resonance quantum computation [J]. Science, 1997, 275: 350~356.

[5] Pazy E, Biolatti E, Calarco T, et al. Spin-based optical quantum computation -via pauli blocking in semiconductor quantum dots[J]. Europhys. Lett., 2003, 62: 175~181.

[6] Makhlin Y , Schon G, Shnirman A. Quantum state engineering with Josephson-junction devices[J]. Rev. Mod. Phys.,2001, 73: 357~400.

[7] Feynman R P. Simulating physicswith computers[J]. In te rna tio na lJou rna l of Theo re tica l Phys ic s, 1982, 21 (6&7) : 467~488.

[8] Deutsch D. Quantum theory, the Church2Turing p rincip le and the universal quantum computer[J]. P roce eding s o f the Roya l So c ie ty of London Se rA, 1985,A400: 97~117.

[9] 郑建国 , 覃朝勇 . 量子计算进展与展望 [J]. 计算机应用研究 ,2008,25（3）:641～645.

[10] 苏晓琴, 王金来 , 聂合贤 , 等. 量子计算与量子逻辑门 [J]. 运城学院学报, 2009, 27(05)：14~18.

[11] 周正威 ,黄运锋 ,张永生 ,郭光灿 .量子计算的研究进展 [J]. 物理学进展, 2005, 25（4）：368～385.

[12] 李继容 . 量子计算的研究与应用 [N] . 软件时空 ,2006.

[13] 戴葵, 宋辉, 刘芸, 等. 量子信息技术引论 [M] . 长沙：国防科技大学出版社, 2001. 71~107.

[14] 潘平 . 量子逻辑门及其研究进展 [J]. 四川理工学院学报, 2005, 18（03）：102～105.