量子技術基本原理與應用發展

◎廖建興 博士 ・ 王智億

1.前言

2016年8月中國發射了世界第一顆所謂的量子科學實驗衛星「墨子號」(Quantum Experiments at Space Scale，簡稱QUESS)，該衛星於中國酒泉衛星發射中心搭載長征二號丁運載火箭發射升空，是設計於低軌道進行量子科學實驗的衛星，實現世界上首次衛星和地面之間的量子通信，並且首次驗證一對纏結光子被分發到遠距離下仍可以保持纏結的理論預言。墨子號量子衛星主要目的是要進行太空與地面之間量子密鑰分發的實驗，並且將在此基礎上進行實驗廣域量子密鑰網路(quantum cryptography internet)，以為空間量子通訊實用化作準備，除具有科學意義及實用價值外，並期望能在量子太空競賽中掌握主導地位。2017年6月，墨子號首先成功實現將兩個量子纏結光子被分發到相距超過1200公里的距離後，仍可繼續保持其量子纏結(quantum entanglement)的狀態。中國並已是目前世界各國針對量子科技至少為第二大投資發展之大國[1-2,9]。

古典物理的極限使得量子物理得以崛起。由於量子力學的一些特性，使得量子電腦相較於傳統古典電腦在速度上及容量上更具優勢，量子密碼根據量子力學的測量理論使資訊得到更大的安全性，以往只能在科幻片中出現的量子隱形傳輸方式，如今已成為可能。然而，何謂量子？何謂量子力學？何謂量子資訊？何謂量子計算？何謂量子纏結？何謂量子傳送？等，此些便是本文陸續所要探討之問題。同時本文並整理探討在量子基本理論發展演進及量子技術相關之發展研究情形，希使讀者能較有系統地了解量子相關重要理論、技術內涵及發展情形。

2.量子力學理論演進[3]

科學已經能破解所有宇宙和生命的奧秘了嗎？可以說，今天的科學技術只是認知世界的初級階段而已，雖然說比起幾百年前科學證實了地球是圓的(是繞着太陽轉)的階段，其實只進步了一些而已。浩瀚宇宙與極微粒子仍難窺其項背，因此，在探討所謂量子技術(Quantum Technology)之前，可能便要先來探討一下科學仍不及之巨觀與微觀的宗教物理世界究竟為何？佛家講，一粒沙粒裡便有一千個大千世界，又說，色即是空，空即是色，“色”所指的便是一切物質，“空”所指的或便是一切“非物質”(能量波？)。那麼在宇宙邊界外是什麼東西呢？有所謂的“邊界”嗎？一粒沙粒內的大千世界又是什麼東西呢？有所謂的最小粒子嗎？莊子雜篇天下章中，曾有一段有關莊子與惠施有關宇宙的對話，惠施說：「至大無外，謂之大一。至小無內，謂之小一」。“至大無外”是目前宇宙學(Physical Cosmology)對宇宙大小的解釋：宇宙範圍非常大，但是仍然沒有邊界(科學已證明仍膨脹中？)，當然也就沒有所謂“外面”；“至小無內”是基本粒子的定義：基本粒子非常小，沒有任何的內部結構。“至大無外”的宇宙學與“至小無內”的基本粒子(Fundamental Particle)在物理學中其實有緊密的連結。基本粒子學說剛開始是用來解釋最簡單的原子核(nucleus,10^{-15}m)的結構，其由質子(proton)及中子(neutron)

構成，而質子及中子又由夸克(quark)構成(10-^{18}m)，夸克再往下可能便是一股無形的能量了。而原子核與電子(electron)組成了原子(atom，10^{-10}m)、分子(molecule)、星系(galaxy)、星團(cluster)，乃至整個宇宙(universe)。

量子力學(Quantum mechanics)便是研究微觀粒子的運動規律的物理學分支學科，它主要研究原子、分子，以及原子核及基本粒子等結構及性質的基礎理論，其與相對論(Theory of relativity)共同構成了現代物理學的理論基礎。量子力學不僅是近代物理學的基礎理論之一，而且在有關學科和許多近代技術中也獲得廣泛應用。從科學演進而言，量子理論發展時間最早可以追溯到1900年普朗克(Plank），為解決黑體輻射的問題時開始。1925年海森堡(Heisenberg)發表了矩陣力學，之後薛丁格(Schrödinger)發表了波動力學(Wave dynamics)；同年波恩(Born)提出了波函數的機率振幅概念，顛覆古典物理世界的實在觀。1927年海森堡發表了測不準原理(uncertainty principle)，陳述如確定粒子位置(position)，將使其動量(momentum)不確定性增加；相反的，如精確測量粒子動量，將使它的位置的不確定性增加，位置與速度無法同時精確地被定義。。當利用波動理論來描述粒子時，如確定粒子的位置(也就是波的位置)，而與粒子速度有關的動量(所代表的就是波的波長)，將無法被確定。因此，當波傳播時，粒子的位置將不確定到某種的程度，當波長無法清楚的定義時，動量亦將不確定到某種程度。

1935年，愛因斯坦(Einstein)與其在普林斯頓高等研究院的助手波多爾斯基(Podolsky)及羅森(Rosen)等3人當時認為以測不準原理來解釋量子力學並不完備，於是發表了一篇論文，並以署名的三位物理學家名字的第一個字母命名，稱為EPR悖論(EPR paradox)。文章設想了一個思想實驗：假設A、B兩個粒子交互作用後彼此遠離。雖然測不準原理指出：位置越精確則動量越不確定，反之亦然。但我們可以只測量A粒子的動量，而根據守恆定律推算出B粒子的動量；同時我們只測量B粒子的位置，也可得知A粒子的位置。如此一來，我們就可以同時知道兩個粒子的動量與位置，但量子力學卻無法同時表述出這兩個物理量的值，可見它並不完備(incomplete)。薛丁格針對此篇EPR論文，用量子纏結(Quantum entanglement)這個名詞來稱呼此二個產生交互作用的粒子，指出其荒謬之處。然而量子世界中似乎真的存在超距作用。1964年愛爾蘭物理學家貝爾(Bell)提出檢驗量子纏結是否存在的實驗方法(貝爾不等式)。等到1980年代技術成熟以後，許多實驗的統計結果都違反了貝爾不等式，代表量子纏結的確成立，貝爾不等式不成立也意味著愛因斯坦所主張的局域實體論(Local realism)，其預測不符合量子力學理論。至此，量子力學的基本原理已經建立。而隨著量子力學擴散至其他科學與技術領域，促使電晶體、積體電路與雷射等的發明，也促成半導體及光電等產業的蓬勃發展。可以說此一階段量子力學的基本原理發展改變了人們對於物質世界的微觀觀點。

1980年代開始，科學家開啟了將量子力學原理與資訊理論結合的構想。1980年貝尼奧夫(Benioff)提出圖靈機(Turing Machine)可以用量子力學的方式來操作的原理。1982年美國著名物理學家費曼(Feynman)認為圖靈機並不完備，並進而提出可逆計算的量子電腦模型。1985年杜奇(Deutsch)提出量子杜奇-圖靈機的量子電腦模型，並指出任何物理過程原則上都能極佳地以量子電腦來模擬。但是因為量子態的測不準現象及特性，以及量子系統容易

受環境雜訊干擾影響，使得量子電腦在實現困難。1994年蕭爾(Shor)發展並證明出第一套量子演算法：量子因式分解演算法，證明運用量子電腦能有效地進行大數值的因式分解。1996年葛洛弗(Grover)提出可以在巨量雜亂的資料中快速搜尋資料的量子搜尋演算法[4-7]。逐漸掀起了研究量子資訊的熱潮，世界各國的大學和研究機構都紛紛投入到量子計算的研究中，並運用諸如核磁共振(NMR)、深阱離子(Trapped ions)及固態半導體等各式系統來進行量子計算的研究。

另外，如從產業發展角度來看，促使產業進步的科學技術皆是以古典物理學為主。80年代前之量子力學理論發展，促成半導體產業技術的進步。然而，近年來隨著半導體產業在晶片製程之元件尺寸縮小，量子效應已經成為必需面對的難題，使業界遵循了數十年的摩爾定律即將面臨更大的挑戰及極限限制。為了產業未來的持續發展，也為了追求更高速的運算能力，因此促使各國紛紛投入量子技術的發展。

3.量子技術產業創新發展方向

圖1顯示量子技術主要產業創新發展方向，應可分為三個領域方向，即承襲奈米以降之半導體元件技術之量子元件(Quantum components)領域、量子資訊(Quantum information)領域，以及量子通訊(Quantum communications)領域等。在產業上運用量子技術來創新發展。量子元件方面，像是量子疊加態(superposition state)及量子纏結對(或EPR pair)，其對於環境變化非常敏感，所以可以用來製造非常精確而靈敏的量子元件感測器。量子資訊方面主要可分量子計算(Quantum computing)及量子演算法(Quantum algorithms)兩領域，其係一門利用量子力學系統達成資訊處理與計算工作的新興研究學門。主要目的係以量子力學理論為基礎，設計出比古典理論更快速有效的資訊運算與處理方法，並進而發展出實現這些方法的實際量子元件裝置。量子計算概念主要運用量子位元疊加狀態，進行量子平行運算，就是將系統的相態做歸一轉換，當位元數目增加後，我們就可用它來模擬任何量子系統，甚至包含系統與環境的交互作用。希能在未來實現真正的量子電腦都。量子演算法係希能在量子電腦上運行的演算法，它利用了量子相關特性提高計算速度，如前述之Shor演算法及Grover演算法。量子通訊主要可分為量子傳輸(Quantum teleportation)及量子密鑰 (Quantum cryptography)兩領域。量子傳輸係應用純量子隱形傳輸理論的量子通訊；量子密鑰則係將量子理論與傳統通信及加密技術結合的方法，融合了古典與量子通訊方法。

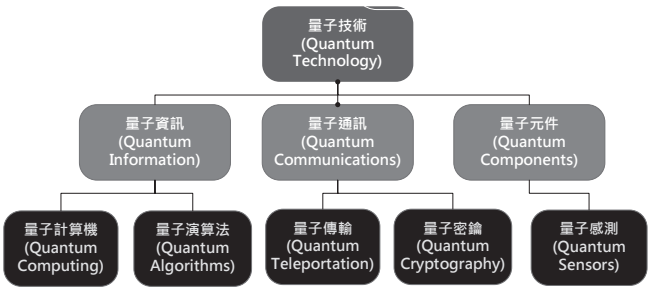

圖1：量子技術主要產業創新發展方向[2]

4.量子資訊及傳輸基礎概論[8]

古典資訊本來就是離散的東西了，但是這與量子資訊(quantum information)不同。在一般的電腦裡，我們用電位的高低代表0與1，進而組成各種資訊。在所謂量子電腦裡，我們用原子的能階來代表資訊的0(標記為|0>)與1(標記為|1>)。一個位元的量子資訊可以是這兩個狀態的線性組合，代表該位元在某一瞬間的狀態稱為同相狀態(coherent states) ，否則如受外界干擾而改變同相位狀態即可稱之為解非同相(decoherence)。量子電腦無論是對系統的時間、振幅、相位的要求均很嚴格。將量子資訊由一處「隱藏」地傳送至遠處，即可謂量子隱藏傳輸(quantum teleportation)。事實上，隨著未來量子電腦而來的革命性改變仍多，在計算方法、通訊方法，以及測量方法上，都會有相當大的改變。總之，在量子電腦及通訊成為事實以前，仍有許多技術需要創新發展，屆時，量子力學將會更加與吾人日常生活息息相關了。

(1)量子位元(quantum bit:qubit)：古典資訊(即目前之0與1數位資訊系統世界)中，位元只能處在一個狀態，非0即1；而在量子資訊中，一個量子位元可同時具有|0>、|1>及其線性的疊加態，由此構成一個量子疊加態(superposition)。狀態疊加假設$\{|n\}$為可能的量子狀態，則$\{\sum_j a_{jk}|k\}$也是一個可能的量子狀態。對應於量子計算，這表示量子電腦可以同時代表(傳統計算機)的許多狀態。狀態疊加時，依各狀態間的相位關係可能出現相長或相消的情形，這是古典計算機Boolean狀態所不具備的特徵稱為干涉性。如果我們用量子力學中之粒子(例如光子)來實現資訊中0與1的兩個狀態(標記為|0>與|1>)，則此種位元稱為量子位元，明顯地，傳統0與1僅為其特例位元狀態而以。如以量子位元來存儲和處理資訊，則稱為量子資訊也。可以說，量子資訊與古典資訊最大的不同在於傳統電腦上用一個二元基底(basis)只能表示出0或1這二種可能狀態，因此在資料儲存量的表現上，量子位元便有其獨特的優勢。

- 單量子位元：若對量子位元進行一次量，只能給出0或1，量子位元的測量後的態為|0>或|1>。因此，從一次測量，吾人只能獲得關於量子位元態的一個位元的資訊。單個量子位元可表示為下式之疊加表示。

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle\Rightarrow|\psi\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle \quad (1)$$
$$\left(|\alpha|^2+|\beta|^2=\frac{1}{\sqrt{2}}^2+\frac{1}{\sqrt{2}}^2=1\right)$$

- 多量子位元：兩個經典位元，有4種可能狀態：00，01，10，11。兩個量子位元有4個計算基態：|00>，|01>，|10>與|11>。兩量子位元的重要量子態是Bell態或EPR對(如後述)，如$(|00\rangle+|11\rangle)/\sqrt{2}\equiv|\beta_{00}\rangle$，兩量子位元之間存在量子關聯。兩量子位元可表示為下式之疊加表示。

$$|\psi\rangle=\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$$
$$\Rightarrow|\psi\rangle=\frac{1}{2}|00\rangle+\frac{1}{2}|01\rangle+\frac{1}{2}|10\rangle+\frac{1}{2}|11\rangle \quad (2)$$
$$\left(|\alpha_{00}|^2+|\alpha_{00}|^2+|\alpha_{00}|^2+|\alpha_{00}|^2=\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=1\right)$$

(2)量子邏輯閘(quantum logic gates)：正如古典之數位邏輯電路一樣，電晶體之設計組合便可組合成為數位邏輯閘(Logic gate)；而古典數位計算機之三種基本邏輯閘為AND，OR及NOT，其可組合而成任何複雜之邏輯關係電路。而量子邏輯閘則由量子位元態所組合而成，其作用是線性的。而用做量子邏輯閘的矩陣限制為只要單量子邏輯閘矩陣U為歸一矩陣(unitary)或稱酉矩陣或么正矩陣（即$U^+U=I$ ）。此歸一性限制係對量子邏輯

閘的唯一限制，任意歸一矩陣則均可標定為有效量子邏輯閘。

- 量子X邏輯閘：作用於單量子位元的量子非邏輯閘，可以圖2之量子非邏輯閘(NOT gate)及(3)歸一矩陣描述。

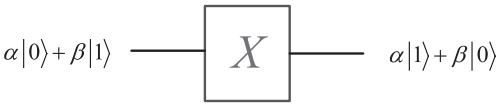

圖2：量子X邏輯閘(NOT)

$$X\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\begin{bmatrix}\beta|0\rangle\\ \alpha|1\rangle\end{bmatrix} \quad (3)$$

- 量子Z邏輯閘：作用於單量子位元的量子Z邏輯閘，可以圖3之Z量子邏輯閘及(4) 歸一矩陣描述。

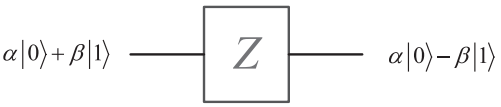

圖3：量子Z邏輯閘

$$Z\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\begin{bmatrix}\alpha|0\rangle\\ -\beta|1\rangle\end{bmatrix} \quad (4)$$

- 量子H邏輯閘：作用於單量子位元的量子H邏輯閘，可以圖4之H量子邏輯閘及(5) 歸一矩陣描述。

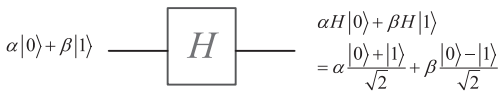

圖4：量子H邏輯閘(Hadamard)

$$H\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}(\alpha+\beta)|0\rangle\\ (\alpha-\beta)|1\rangle\end{bmatrix} \quad (5)$$

- 量子CNOT邏輯閘：作用於單量子位元的量子CNOT控制非邏輯閘，可以圖5之量子邏輯閘及(6.1~2)歸一矩陣描述。假定U是作用在某n個量子位元上的任意歸一矩陣(定義可控U個)，其有單一個控制量子位元及n個目標量子位元。如果控制量子位元為0，則目標量子位元不發生任何變化；若控制量子位元為1，則U邏輯閘作用在目標量子位元上。

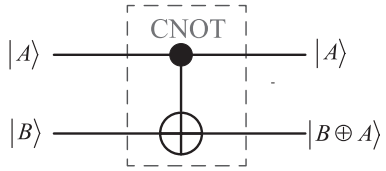

圖5：量子CNOT邏輯閘(Controlled NOT)

$$|AB\rangle\Rightarrow\begin{cases}|00\rangle\Rightarrow(|0\rangle+|1\rangle)\oplus|0\rangle\Rightarrow|00\rangle+|11\rangle\\ |01\rangle\Rightarrow(|0\rangle+|1\rangle)\oplus|1\rangle\Rightarrow|01\rangle+|10\rangle\\ |10\rangle\Rightarrow(|0\rangle-|1\rangle)\oplus|0\rangle\Rightarrow|00\rangle-|11\rangle\\ |11\rangle\Rightarrow(|0\rangle-|1\rangle)\oplus|1\rangle\Rightarrow|01\rangle-|10\rangle\end{cases} \quad (6.1)$$

$$CN\begin{bmatrix}|00\rangle\\ |01\rangle\\ |10\rangle\\ |11\rangle\end{bmatrix}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}|00\rangle\\ |01\rangle\\ |10\rangle\\ |11\rangle\end{bmatrix}=\begin{bmatrix}|00\rangle\\ |01\rangle\\ |11\rangle\\ |10\rangle\end{bmatrix} \quad (6.2)$$

(3)量子電路(quantum circuits)：正如古典數位計算機之三種基本邏輯閘為AND，OR及NOT可組合成任何複雜之邏輯關係電路一樣，量子基本邏輯閘亦可設計組合成任合量子電路。以下即舉貝爾量子電路及三個量子CNOT邏輯閘量子交換電路說明之。

- 貝爾量子電路：貝爾狀態(Bell state)量子電路主要由量子H邏輯閘及量子CNOT控制非邏輯閘組合而成，可以

圖6之量子邏輯閘組合成量子電路。本電路可產生二位元量子纏結對(或稱貝爾狀態對及EPR對)(容後述)。二位元共四種之量子纏結對如(7)式所推導。

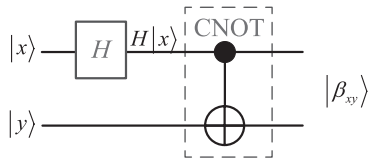

圖6：貝爾狀態(Bell state)量子電路

$$|AB\rangle\Rightarrow\begin{cases}|00\rangle\Rightarrow\dfrac{|0\rangle+|1\rangle}{\sqrt{2}}\oplus|0\rangle\Rightarrow\dfrac{|00\rangle+|11\rangle}{\sqrt{2}}\equiv|\beta_{00}\rangle\\ |01\rangle\Rightarrow\dfrac{|0\rangle+|1\rangle}{\sqrt{2}}\oplus|1\rangle\Rightarrow\dfrac{|01\rangle+|10\rangle}{\sqrt{2}}\equiv|\beta_{01}\rangle\\ |10\rangle\Rightarrow\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\oplus|0\rangle\Rightarrow\dfrac{|00\rangle-|11\rangle}{\sqrt{2}}\equiv|\beta_{10}\rangle\\ |11\rangle\Rightarrow\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\oplus|1\rangle\Rightarrow\dfrac{|01\rangle-|10\rangle}{\sqrt{2}}\equiv|\beta_{11}\rangle\end{cases}\quad(7)$$

- 三個量子CNOT邏輯閘量子交換電路：以包含有三個量子CNOT邏輯閘的量子線路為例(如圖7)，線路中的每條線不一定對應物理上的導線，它可能是時間流向，或許是從某處傳送到另處的物理粒子(如光子)。其實際效果是交換了兩個量子位元。

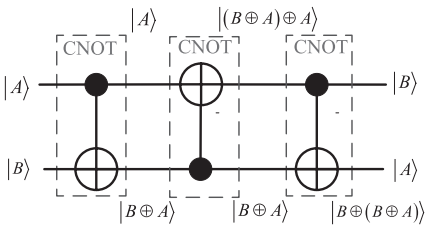

圖7：三個量子CNOT邏輯閘量子交換電路

(4)量子平行處理(Quantum Parallelism)特性：量子電腦速度為何能如此快速呢？原來它的每一個位元都是同時有|0>及|1>存在而疊加在一起的。因此，從初始值開始，便同時代表了所有可能的狀態。所有可能的情況都一次計算完成了，此即是Deutsch所稱的量子平行處理。換言之，打個簡單譬喻，各種高低音樂器的和諧共鳴所組成的交響樂便是，當演出前，各種樂器先就調好各自的音準及狀態，當指揮一舉手便讓各自樂器依序依譜演出，共同發出美妙之交響樂曲。Deutsch並強調：量子並行性是量子電腦發揮其計算潛力的根源。

- Deutsch問題：黑盒子$x\rightarrow f(x)$,x=0,1；$f(x)$=0,1，若想知道此黑盒子究竟是constant(即$f(0)=f(1)$)或balanced(即$f(0)\neq f(1)$)，則古典計算方式需要兩次。以圖8之量子平行性評估電路為例，假定用量子黑盒來評估計算$f(x)$功能，是否能“一次性地”並行判斷此黑盒之狀態？若作用在第二個量子位元y上的是|0>，則第一個量子位元x將不變(f(|0>))；若第二個量子位元y上的是|1>，則第一個量子位元x將反轉(flip)(f(|1>))(類似於前述之CNOT受控非邏輯閘概念)，參(8.1)及(8.2)式。若作用在第一個量子位元x上的是$(|0\rangle+|1\rangle)/\sqrt{2}$，則輸出將變為$|f(0)\rangle/\sqrt{2} or |f(1)\rangle/\sqrt{2}$，無法“一次性地”並行判斷，參(8.3)及(8.4)式。

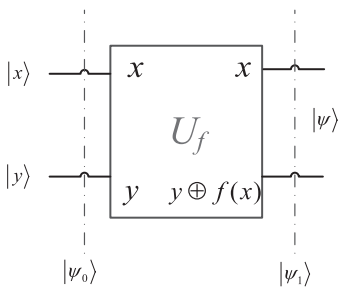

圖8：量子平行性評估電路

$$U_f:|x\rangle|y\rangle\to|x\rangle\cdot|y\oplus f(x)\rangle$$
$$if\ |x\rangle=|0\rangle,|y\rangle=|0\rangle\Rightarrow|\psi_0\rangle=|x\rangle\cdot|y\rangle=|0\rangle\cdot|0\rangle=|0\rangle\Rightarrow|\psi_1\rangle=|f(0)\rangle \quad (8.1)$$

$$if\ |x\rangle=|0\rangle,|y\rangle=|1\rangle\Rightarrow|\psi_0\rangle=|x\rangle\cdot|y\rangle=|0\rangle\cdot|1\rangle=|1\rangle\Rightarrow|\psi_1\rangle=|f(1)\rangle \quad (8.2)$$

$$if\ |x\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right),|y\rangle=|0\rangle\Rightarrow|\psi_0\rangle=|x\rangle\cdot|y\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdot|0\rangle \quad (8.3)$$
$$\Rightarrow|\psi_1\rangle=\frac{1}{\sqrt{2}}\left(|f(0)\rangle+|f(1)\rangle\right)=\frac{1}{\sqrt{2}}|f(0)\rangle or\frac{1}{\sqrt{2}}|f(1)\rangle$$

$$if\ |x\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right),|y\rangle=|1\rangle\Rightarrow|\psi_0\rangle=|x\rangle\cdot|y\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdot|1\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$
$$\Rightarrow|\psi_1\rangle=\frac{1}{\sqrt{2}}\left(|f(0)\rangle+|f(1)\rangle\right)=\frac{1}{\sqrt{2}}|f(0)\rangle or\frac{1}{\sqrt{2}}|f(1)\rangle \quad (8.4)$$

圖9顯示量子平行性評估電路(Deutch's演算法)，式(9)顯示黑盒之通式表示式：$|\psi_2\rangle=|x\rangle\cdot\left((-1)^{f(x)}\left(|0\rangle-|1\rangle\right)/\sqrt{2}\right)$，式(10.1)~(10.3)顯示輸入二位元皆經過H量子邏輯閘轉換後之各個階段狀態之變化情形。假定用量子黑盒來評估計算$f(x)$功能，即能"一次性地"並行判斷此黑盒之狀態，$|\psi_3\rangle=\pm\left(f(0)\oplus f(1)\right)\cdot\left(|-\rangle\right)$。

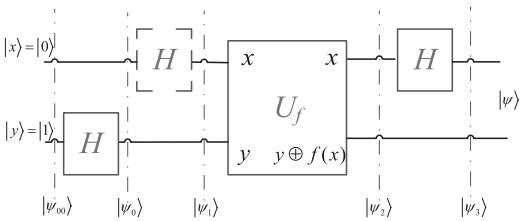

圖9：量子平行性評估電路(Deutch's演算法)

$$U_f:|x\rangle|y\rangle\to|x\rangle\cdot|y\oplus f(x)\rangle$$
$$|\psi_{00}\rangle=|x\rangle\cdot|y\rangle=|0\rangle\cdot|1\rangle \quad (9)$$
$$|\psi_0\rangle=|\psi_1\rangle=|x\rangle\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$
$$\Rightarrow|\psi_2\rangle=|x\rangle\cdot\frac{1}{\sqrt{2}}\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)=|x\rangle\cdot\left((-1)^{f(x)}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)$$

$$if\ |x\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\Rightarrow|\psi_1\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=|+\rangle\cdot|-\rangle$$
$$\Rightarrow|\psi_2\rangle=\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\right)|-\rangle$$
$$\Rightarrow\begin{cases}f(0)=f(1)\Rightarrow|\psi_2\rangle=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\left(|+\rangle\right)\cdot\left(|-\rangle\right)\\ f(0)\neq f(1)\Rightarrow|\psi_2\rangle=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\pm\left(|-\rangle\right)\cdot\left(|-\rangle\right)\end{cases} \quad (10.1)$$
$$\Rightarrow|\psi_3\rangle=\pm\left(f(0)\oplus f(1)\right)\cdot\left(|-\rangle\right)$$

$$if\ |x\rangle=\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\Rightarrow|\psi_1\rangle=\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=|+\rangle\cdot|-\rangle$$
$$\Rightarrow|\psi_2\rangle=\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle-(-1)^{f(1)}|1\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$
$$\Rightarrow\begin{cases}f(0)=f(1)\Rightarrow|\psi_2\rangle=\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\left(|-\rangle\right)\cdot\left(|-\rangle\right)\\ f(0)\neq f(1)\Rightarrow|\psi_2\rangle=\pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\pm\left(|+\rangle\right)\cdot\left(|-\rangle\right)\end{cases} \quad (10.2)$$
$$\Rightarrow|\psi_3\rangle=\pm\left(f(0)\oplus f(1)\right)\cdot\left(|-\rangle\right)$$

$$|\pm\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\pm|1\rangle\right)\Rightarrow\begin{cases}f(0)=f(1)\to|+\rangle(\text{constant})\\ f(0)\neq f(1)\to|-\rangle(\text{balanced})\end{cases} \quad (10.3)$$

(5)量子不可複製(nonclonability)定理：量子不可複製定理可定義為不存在任何物理過程可以精確複製任何未知的量子態。不可複製原理是量子資訊的基礎。量子資訊在通道中傳輸，不可能被第三方複製而竊取資訊，而不對量子資訊產生干擾，此原理亦是量子密碼學的基石。圖10顯示量子不可複製性電路驗證。左圖為古典邏輯複製電路，透過XOR邏輯閘，可產生邏輯複製結果；右圖為類似左圖之量子邏輯"複製"電路，透過CNOT量子邏輯閘，無法產生邏輯複製結果。

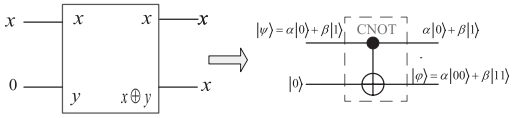

圖10：量子不可複製性電路驗證

(6)量子纏結(quantum entanglement)及隱藏傳輸：將未知量子態(量子位元)傳送到遠處而不傳送量子態的物理載體，謂之量子纏結。1935年愛因斯坦等三人所發表之EPR悖論之思想實驗，旨在說明量子力學的理論中，必然存在「隱藏變數」，否則會有超光速的通訊，違反了狹義相對論，這思想實驗涉及一個稱為「量子纏結」的現象，1964年愛爾蘭物理學家貝爾(Bell)提出檢驗量子纏結是否存在的實驗方法回應EPR悖論。這篇論文為後世提供了驗證是否存在隱藏變數的方法，亦即驗證粒子的屬性到底是預先設定好，抑或如量子力學所理解般要到測量時才可確定。而後覆經物理學家多次實驗結果顯示，量子力學地位仍未受EPR悖論挑戰，站不住腳的反而是局域實體論(local realism)。根據量子力學預測，量子纏結並不受距離限制。前述之中國發射「墨子號」量子實驗衛星，業已證明相隔1200公里貝爾纏結態測試，乃目前距離最遠的一次嘗試。到時候。

圖11即顯示一量子隱藏傳輸電路(Quantum teleportation)，其中$|\beta_{xy}\rangle$即為圖6之貝爾狀態量子產生電路(可為$|\beta_{00}\rangle$、$|\beta_{01}\rangle$、$|\beta_{10}\rangle$或$|\beta_{11}\rangle$任一Bell狀態)。貝爾狀態及各階段之未知$|\psi\rangle$變化情形，分如(11.1)~(11.4)所述。假設此三量子位元之量子纏結電路，第一個位元$|\psi\rangle$即為未知之量子狀態可透過本量子隱藏傳輸電路傳送至遠處，並還原獲得。第二及三位元即為EPR對，分屬於發送者及接收者。假設發送者為Alice，而接收者為Bob，則：

- Alice和Bob各自擁有EPR對的一個纏結粒子。
- Alice對處於未知量子態粒子和她的纏結粒子$|\psi\rangle$進行量子測量，獲得4個可能經典結果00,01,10,11中的一個。
- Alice將測量的結果傳送給Bob依據Alice的資訊對他手中的EPR粒子做相應操作，便可恢復出原始的量子態。

總之，如將原物質的資訊分成古典資訊和量子資訊，則接收者在獲得這兩種資訊後，就可以得出原物質量子態的完美複製結果。其中，最關鍵的地方是量子資訊部分的傳送，發送者甚至對這部分量子資訊一無所知。因此，量子資訊部分的傳送，是接收者利用一對糾纏光子態，透過將其中的一個光子複製到原物質的量子態上，而提取原物質的資訊，並非由發送者傳送給接收者，從而保證資訊的完整性。

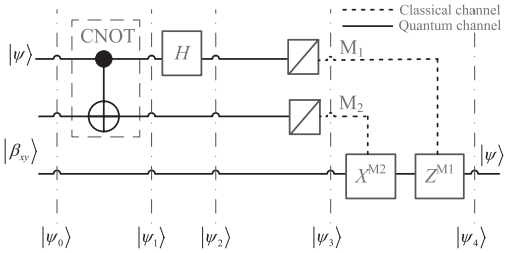

圖11：量子隱藏傳輸電路

$$|\beta_{00}\rangle$$

$$|\psi_0\rangle=|\psi\rangle\cdot|\beta_{00}\rangle=(\alpha|0\rangle+\beta|1\rangle)\cdot\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$$

$$=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|00\rangle+|11\rangle))$$

$$|\psi_1\rangle=|\psi_0\rangle\cdot CN=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|10\rangle+|01\rangle))$$

$$|\psi_2\rangle=|\psi_1\rangle\cdot H=\frac{1}{\sqrt{2}}\left(\frac{\alpha(|0\rangle+|1\rangle)}{\sqrt{2}}(|00\rangle+|11\rangle)+\frac{\beta(|0\rangle-|1\rangle)}{\sqrt{2}}(|10\rangle+|01\rangle)\right)$$

$$=\frac{1}{2}(\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+\beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle))$$

$$=\frac{1}{2}(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta\,0\,))$$

$$|\psi_3(M_1M_2)\rangle=\begin{cases}\psi_3|00\rangle=(\alpha|0\rangle+\beta|1\rangle)\\ \psi_3|01\rangle=(\alpha|1\rangle+\beta|0\rangle)\\ \psi_3|10\rangle=(\alpha|0\rangle-\beta|1\rangle)\\ \psi_3|11\rangle=(\alpha|1\rangle-\beta|0\rangle)\end{cases}\qquad(11.1)$$

$$|\beta_{01}\rangle$$

$$|\psi_0\rangle=|\psi\rangle\cdot|\beta_{01}\rangle=(\alpha|0\rangle+\beta|1\rangle)\cdot\frac{(|01\rangle+|10\rangle)}{\sqrt{2}}=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|01\rangle+|10\rangle)+\beta|1\rangle(|01\rangle+|10\rangle))$$

$$|\psi_1\rangle=|\psi_0\rangle\cdot CN=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|01\rangle+|10\rangle)+\beta|1\rangle(|11\rangle+|00\rangle))$$

$$|\psi_2\rangle=|\psi_1\rangle\cdot H=\frac{1}{\sqrt{2}}\left(\frac{\alpha(|0\rangle+|1\rangle)}{\sqrt{2}}(|01\rangle+|10\rangle)+\frac{\beta(|0\rangle-|1\rangle)}{\sqrt{2}}(|11\rangle+|00\rangle)\right)$$

$$=\frac{1}{2}(\alpha(|0\rangle+|1\rangle)(|01\rangle+|10\rangle)+\beta(|0\rangle-|1\rangle)(|11\rangle+|00\rangle))$$

$$=\frac{1}{2}(|00\rangle(\alpha|1\rangle+\beta|0\rangle)+|01\rangle(\alpha|0\rangle+\beta|1\rangle)+|10\rangle(\alpha|1\rangle-\beta|0\rangle)+|11\rangle(\alpha|0\rangle-\beta|1\rangle))$$

$$|\psi_3(M_1M_2)\rangle=\begin{cases}\psi_3|00\rangle=(\alpha|1\rangle+\beta|0\rangle)\\ \psi_3|01\rangle=(\alpha|0\rangle+\beta|1\rangle)\\ \psi_3|10\rangle=(\alpha|1\rangle-\beta|0\rangle)\\ \psi_3|11\rangle=(\alpha|0\rangle-\beta|1\rangle)\end{cases}\qquad(11.2)$$

$$|\beta_{10}\rangle$$

$$|\psi_0\rangle=|\psi\rangle\cdot|\beta_{10}\rangle=(\alpha|0\rangle+\beta|1\rangle)\cdot\frac{(|00\rangle-|11\rangle)}{\sqrt{2}}=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle-|11\rangle)+\beta|1\rangle(|00\rangle-|11\rangle))$$

$$|\psi_1\rangle=|\psi_0\rangle\cdot CN=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle-|11\rangle)+\beta|1\rangle(|10\rangle-|01\rangle))$$

$$|\psi_2\rangle=|\psi_1\rangle\cdot H=\frac{1}{\sqrt{2}}\left(\frac{\alpha(|0\rangle+|1\rangle)}{\sqrt{2}}(|00\rangle-|11\rangle)+\frac{\beta(|0\rangle-|1\rangle)}{\sqrt{2}}(|10\rangle-|01\rangle)\right)$$

$$=\frac{1}{2}(\alpha(|0\rangle+|1\rangle)(|00\rangle-|11\rangle)+\beta(|0\rangle-|1\rangle)(|10\rangle-|01\rangle))$$

$$=\frac{1}{2}(|00\rangle(\alpha|0\rangle-\beta|1\rangle)+|01\rangle(-\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle+\beta|1\rangle)+|11\rangle(-\alpha|1\rangle-\beta|0\rangle))$$

$$|\psi_3(M_1M_2)\rangle=\begin{cases}\psi_3|00\rangle=(\alpha|0\rangle-\beta|1\rangle)\\ \psi_3|01\rangle=(-\alpha|1\rangle+\beta|0\rangle)\\ \psi_3|10\rangle=(\alpha|0\rangle+\beta|1\rangle)\\ \psi_3|11\rangle=(-\alpha|1\rangle-\beta|0\rangle)\end{cases}\qquad(11.3)$$

$$|\beta_{11}\rangle$$

$$|\psi_0\rangle=|\psi\rangle\cdot|\beta_{11}\rangle=(\alpha|0\rangle+\beta|1\rangle)\cdot\frac{(|01\rangle-|10\rangle)}{\sqrt{2}}=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|01\rangle-|10\rangle)+\beta|1\rangle(|01\rangle-|10\rangle))$$

$$|\psi_1\rangle=|\psi_0\rangle\cdot CN=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|01\rangle-|10\rangle)+\beta|1\rangle(|11\rangle-|00\rangle))$$

$$|\psi_2\rangle=|\psi_1\rangle\cdot H=\frac{1}{\sqrt{2}}\left(\frac{\alpha(|0\rangle+|1\rangle)}{\sqrt{2}}(|01\rangle-|10\rangle)+\frac{\beta(|0\rangle-|1\rangle)}{\sqrt{2}}(|11\rangle-|00\rangle)\right)$$

$$=\frac{1}{2}(\alpha(|0\rangle+|1\rangle)(|01\rangle-|10\rangle)+\beta(|0\rangle-|1\rangle)(|11\rangle-|00\rangle))$$

$$=\frac{1}{2}(|00\rangle(\alpha|1\rangle-\beta|0\rangle)+|01\rangle(-\alpha|0\rangle+\beta|1\rangle)+|10\rangle(\alpha|1\rangle+\beta|0\rangle)+|11\rangle(-\alpha|0\rangle-\beta|1\rangle))$$

$$|\psi_3(M_1M_2)\rangle=\begin{cases}\psi_3|00\rangle=(\alpha|1\rangle-\beta|0\rangle)\\ \psi_3|01\rangle=(-\alpha|0\rangle+\beta|1\rangle)\\ \psi_3|10\rangle=(\alpha|1\rangle+\beta|0\rangle)\\ \psi_3|11\rangle=(-(\alpha|0\rangle+\beta|1\rangle))\end{cases}\qquad(11.4)$$

5.量子技術實現挑戰[2,8]

由於量子態粒子的測不準現象特性，以及量子系統容易受環境雜訊干擾影響，使得通用之量子電腦及傳輸之實現困難。然而，量子電腦的實現量子資訊與計算是一個嶄新且重要的領域，代表下一代資訊處理的根本方法，實驗上也不斷有一些重要的突破。但目前的技術距離普遍運用的階段尚有相當大的距離，仍有許多問題等待克服，例如量子位元及量子邏輯閘之設計製造實現及其多狀態下之穩定控制方式及特定量子位元的量測能力問題，可運算同調時間(Coherent time)過短問題，及量子系統之資訊輸出問題等。本部分即整理說明三種相關之實現(implementation)技術基本想法內涵。

- 深阱離子(Trapped ions)：儲存在線性深阱中的離子集合提供了構建量子電腦方案之一，其每個量子位元(每個離子一個)由一對(one pair)離子的內部狀態組成。深阱中的所有離子具有相同的電荷並彼此排斥，因此任何一個離子透過此種靜電排斥運動，可轉移到深阱中的其他離子，致引起所謂聲子(phonons)的各種集體運動。單一離子之運動可以藉由引導雷射脈衝(laser pulse)到此特定離子，以實現一量子位元。帶電離子之間的庫侖排斥力(Coulomb repulsion)產生了在一對量子位之間實現CNOT邏輯閘的物理機制。量子資訊係在不同特定量化模式聲子(振動態)離子之間傳輸轉移，此為量子資料匯流排重要基礎。聲子的存在或不存在影響了離子之能量位階，根據控制離子(control ion)的狀態，允許目標離子(target ion)對光做出不同反應。在能實現量子邏輯閘之前，聲子模式(phonon mode)必須初始化於純量子狀態。美國及歐洲等地的相關研究機構及專家之實驗

工作成果早已經展示一串四個離子以上之量子糾纏現象；而儲存在離子內部基態的量子位元之去相干時間(Decoherence time)業已證明可達數千秒以上時間。儘管此類型構建之離子深阱量子電腦無基本的規模大小限制，一般認為10個以上之量子位元可能便較難以實現。

- 核磁共振(Nuclear magnetic resonance, NMR)：在NMR核磁共振量子電腦中，磁場中原子核的兩個自旋態(spin state)可用於實現量子位元的兩個狀態。分子(molecules)中的不同原子可用以區隔，所以一個分子可以實際用來實現量子電腦，其每個原子核則提供為單一個量子位元。在NMR實驗中，單分子無法產生足夠強的信號以供觀察。因此，其必須牽涉大量之分子，使其有足夠大綜合之磁感應信號以供感測。此些分子通常在於溶劑中。在NMR量子電腦中，分子為運算的基本單元，將分子液體裝在封閉試管內(此液體所含的分子數約為1018)，每一分子中的原子核具有個別的自旋態，可以做為量子位元的兩個狀態；不同原子自旋間又有耦合作用，如施加適當之雷射脈衝便可以控制其間的行為。利用這種作用可以做為量子邏輯運算閘，而運算結果可由自旋態改變所放出的無線電訊號量得。一些並可用來實現解決Deutsch的問題，其便是計算兩個不同輸入的函數數值，以及允許比較此兩個值。此種比較之達成是僅使用單一個功能評估實現及同時應用於兩個輸入。美國相關研究機構及專家早已建立了具有多達七個以上之量子位元的液態NMR量子電腦。
- 固態方法(Solid state approaches)：由於液態NMR的限制，美國相關研究機構專家提出另一種方法，即是於矽晶中埋置一系列磷原子，並將其上疊加一層絕緣層，其上面並設置有類似的電極陣列，每個電極可以對其下面的原子施加電壓。就像在NMR中一樣，經由顯露於足夠能量無線電波上，此原子核的旋轉狀態可被翻轉(flip)。然而，這些無線電波將可翻轉每個原子核。磷原子具有單一個電子在其外殼中，可以某一複雜方式與原子核旋體(spin)相互作用。對原子施加電壓便會改變需求能量，以解決原子核及電子自旋兩者所需，因此，其改變了翻轉原子核所需的無線電波的頻率。所以，通過向特定電極施加電壓，並將陣列暴露於新頻率便可以解決單一個原子核所需。超導體(superconductivity)的量子現象也可用於構建量子電腦。最先進的固態技術便是所謂量子點(quantum dot)，其基本上是一個半導體深阱(trap)，保有足夠離散數量之電子。一些歐洲及美國相關研究機構專家已提出使用量子點，以作為構建量子電腦之基礎。

6.量子技術發展[1-3]

1980年代量子技術發展較成熟後，許多實驗的統計結果都違反了貝爾不等式，代表量子纏結的確成立，貝爾不等式不成立也意味著愛因斯坦所主張的局域實體論(Local realism)預測不符合量子力學理論。至此，量子力學的基本原理已經建立。而隨著量子力學擴散至其他科學與技術領域，促使電晶體、積體電路與雷射等的發明，也促成半導體及光電等產業的蓬勃發展。可以說此一階段量子力學的基本原理發展改變了人們對於物質世界的微觀觀點。1980年代開始，科學家開啟了將量子力學原理與資訊理論結合的構想。逐漸掀起了研究量子資訊的熱潮，世界各國的大學和研究機構都紛紛投入到量子計算相關

的研究中，並運用諸如核磁共振(NMR)、深阱離子(Trapped ions)及固態半導體等各種技術來進行量子計算的實現研究。

如從產業發展角度來看，促使產業進步的科學技術皆是以古典物理學為主。雖然80年代前之量子力學理論發展，促成半導體產業技術的進步。誠如1965年英特爾公司(Intel)的創辦人之一摩爾(Moore)便觀察預測矽晶片上的電晶體的數目與運算能力約每18個月成長為原來之2倍，直到矽晶片在縮小化的過程中到達本身物理的上限為止(目前有預估2020年即趨於飽和！)，這就是著名的摩爾定律(Moore Law)。由此推估之，較諸次微米(Sub-micron)更小之奈米(10^{-9}m)製程技術，以及微機械與電機之整合技術及成熟(如MEMS微機電感應器)應皆是已然成熟或指日可待之發展目標。試想如依照此種發展趨勢關係，從2000年迄今2016年將近10個1.5年(18個月)的時間，所以處理器的速度經過15、6年大約已經翻了2^{10}(=1024)倍了。但整個產業的技術基礎還是根據古典物理的原理，並未大量運用到純粹的量子特性。然而，近年來隨著半導體產業在晶片微影製程中元件尺寸的不斷縮小，量子效應將成為必需面對的難題，使業界遵循了數十年的摩爾定律即將面臨更大的極限挑戰。為了產業未來的持續發展，也為了追求更高速的運算能力，因此促使各國紛紛投入量子技術的發展。

量子原理的運用並已不再拘限於學術界之科研工作。近年來，國際資訊大廠(如Google等)亦積極投入並展開專利布局。量子電腦還普遍被視為是未來的技術，量子電腦將是在幾年後就會實現的技術。量子技術的重要性與其可能對社會及產業帶來的巨大衝擊，已促使各國政府甚至民間資訊大廠大量投入量子資訊及相關量子技術研發。世界各國都已經積極的投入量子技術的研究，除了美國、歐盟、英國及日本等傳統科技大國外，對岸中國並已投入相當之人力資源進行相關之量子技術及實用化研究開發。而小城市國家如新加坡等亦都投入了相當的研究資源，顯示全球的量子競賽已然展開。中國於2011年便開始啟動量子衛星研製計劃，又於2013年啟動光纖量子通訊網絡工程。目前並建置北京至上海(全長2000餘公里)，一可擴展廣域光纖量子通訊網絡，可用於各安全傳輸領域。中國並計劃於2030年建置全球化量子通訊網絡，墨子號量子實驗衛星之發射成功，便是實現此一目標之重要基礎。歐盟的量子宣言(Quantum Manifesto：A New Era of Technology)提出一旗艦級長期計畫，預期聯合歐洲各國在教育、科學、工程與創新的產業發展，實可作為台灣相關科技發展規劃的借鏡。然而，可能因為多數資訊領域的專家學者並不熟悉基礎量子力學基本物理原理，台灣在量子資訊領域方面發展似乎出現阻滯現象，而在相關研究上出現因境，亦即在科學與工程之間出現難以跨越之鴻溝。因此，或可考慮以大型專案計畫形式，並與先進國家進行國際合作，跨領域結合自然科學領域及工程領域專家學者，共同進行量子技術跨領域研究及相關人才培養；並將量子原理與應用的學習推廣至工程領域各學門中，以滿足未來量子產業中極需要的相關技術人才。

7.結論

古典物理的極限使得量子物理得以順勢崛起。本文已循序整理探討相關量子之基本理論發展演進及量子技術相關之發展研究，應可使讀者以較有系統方式了解量子相關重要理論、技術內涵及發展情

形。如從產業發展角度來看，過去促使產業進步的科學技術皆是以古典物理學為主。1980年代前之量子力學理論發展，促成半導體產業技術的進步。然而，近年來隨著半導體產業在晶片製程之元件尺寸縮小，量子效應已經成為必需面對的難題，使業界遵循了數十年的摩爾定律即將面臨更大的挑戰及極限限制。由於量子態粒子的測不準現象特性，以及量子系統容易受環境雜訊干擾影響，使得通用之量子電腦及傳輸之實現困難，1980年代後，科學家開始將量子力學原理與資訊理論相結合，遂逐漸掀起了量子資訊研究及實現的熱潮，世界各國的大學和研究機構都紛紛投入到量子計算相關的研究中，並運用諸如核磁共振、深阱離子及固態半導體等各種技術來進行量子計算的實現研究。

由於量子力學的特性，使得量子電腦相較於傳統古典電腦在速度上及容量上更具優勢，量子密碼根據量子力學的測量理論使資訊得到更大的安全性，量子隱形傳輸方式如今已成為可能。因此，為了產業未來的持續發展，也為了追求更高速的運算能力，已驅使各國紛紛投入量子技術的發展。量子電腦的實現量子資訊與計算是一個嶄新且重要的領域，代表下一代資訊處理的根本方法，實驗上也不斷有一些重要的突破。雖然目前的技術距離普遍運用的階段尚有相當大的距離，仍有許多問題等待克服，然而，台灣在此方面的參與及投入程度似乎仍落後先進國家許多，希望藉由本文的介紹，拋磚引玉，能讓更多相關領域專家能對此量子技術及實作應用研究等產生興趣及共同努力，以期日後我國能於此新興領域儘速在世界占有一席之地。

8.參考文獻

[1]http://news.xinhuanet.com/photo/2016-08/16/c_1119396090.htm

[2]https://panx.asia/archives/56665

[3]https://zh.wikipedia.org/wiki/量子力學入門

[4]P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, Santa Fe, NM, USA.

[5]P.W.Shor,“Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM J. Comput. 26, pp. 1484-1509 (1997); arXiv:quantph/9508027v2

[6]L. K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” The Proceedings 28th Annual ACM Symposium on the Theory of Computing, pp. 212 (1996).

[7]L. K. Grover, “Quantum Mechanics Helps in Searching for a Needle in a Haystack,” Phys. Rev. Lett. 79, pp. 325-328.

[8]M. Adeeb R. Ghonaimy, “A Tutorial on Quantum Computation and Communication,” The 2006 International Conference on Computer Engineering and Systems, pp. 5-7, Nov. 2006.

[9]https://theinitium.com/article/20160816-dailynews-mozi-quantum/