# 科技部 111 年度「量子科技專案計畫」說明附件(草案)

# 研究面向一：通用量子電腦硬體技術

壹、 計畫背景及目的

量子電腦是透過量子位元的邏輯閘運作來達成通用型的運算。雖然量子電腦還在發展的前期，但因可廣泛且高速地解決傳統電腦難以有效運算的各式複雜及龐大的問題，也因此更受大家矚目。隨著量子位元數量及邏輯閘結構維度的大幅提高，量子位元的保真度(fidelity)及彼此的連結性(connectivity)都變得相當關鍵。考慮我國在半導體晶片製程、IC 設計與封裝技術具備良好基礎和大量專業人才，固態量子技術將是我國優先投入的選項。研究面向一─通用量子電腦硬體技術，其範圍涵蓋固態量子技術(以**半導體、超導體或其他固態材料為基礎所建構**量子位元為主體之相關技術)，亦包含可積體化、晶片化並具有可擴充性之非固態系統之量子位元技術，並區分為「材料技術」、「量子位元」、「控制/量測電路與系統整合」三大方向。本計畫目標發展此三大方向的關鍵技術，以利建構具運算能力之量子電腦。

貳、 研究議題範疇

計畫研究議題將包含(但不限於)下列相關研究項目:

一. 材料技術：

具有長同調時間(coherent time)以及高保真度的量子位元是量子電腦運作的基石，而同調時間與保真度卻與量子位元的材料及其介面品質息息相關。以固態量子位而言，材料技術涵蓋：超導材料製程技術、高純度矽-28 之合成技術與前驅物開發、低雜質絕緣層製程技術、以及其他可提升量子位元同調時間與保真度之材料與元件技術。具有開發成為新型態量子位元潛力之材料與技術亦包含於本研究項目。

二. 量子位元設計與製作技術：

量子位元除了具有長同調時間與高保真度，具有高連結性的多量子位元系統以及具有可積體化、晶片化以及擴充性亦是實現量子電腦運作的關鍵。本研究議題涵蓋：高保真度與長同調時間之量子位元設計與元件製作，以及多位元量子位元系統設計與製作。量子位

元之材料系統包含超導體與半導體等固態系統，亦包含非固態系統(如離子井等)但具備可積體化、晶片化以及擴充性之量子位元系統。

三. 量子位元周邊控制電路與系統整合：

量子電腦的運作是建立在可靠的多量子位元之寫入、控制與讀取的操作。然而，隨著量子位元數目的增加，其周邊控制的次系統電路之積體化設計，尤其是具備低溫環境操作以及各式量子位元與次系統之間的系統整合亦成為重要環節。本研究議題涵蓋：低溫互補式金氧半(cryo-CMOS)元件與電路設計(多通道 ADC、DAC、FPGA 及 GPU 等)、各式量子位元介面電路、次系統與各式量子位元間的整合介面及可行性架構研究、多位元/多通道之量子次系統連結架構之設計與製作、以及關鍵元件(如濾波、放大器等)與分析系統(微波源、網路分析儀及頻譜分析儀等)之開發。

# 研究面向二：光量子技術

壹、計畫背景及目的

光量子科技包含光量子運算與量子通訊。此二者具有許多共同之關鍵硬體技術（如光源、光學元件與偵測器等）。光量子運算具有室溫操作、不易受干擾(低噪)、不需真空環境、可直接與光纖網路連結等優點。但光量子位元難以限制保存在一固定位置，且光子並不會直接進行交互作用，是早期主要障礙。目前世界上光量子運算的技術進展相當快速，新創公司甚至宣示要推出高達百萬個光量子位元，以及以光量子位元為基礎的雲端運算平台。

量子通訊可以透過傳遞量子資訊以及量子密鑰分發(Quantum Key Distribution, QKD)協定來提升訊息傳遞的安全性，也可以利用量子技術(如利用量子糾纏特性)來提升資料傳輸效率。光子傳播的介質可以是光纖網路，也可以在自由空間或甚至衛星量子通訊。量子密鑰分發於 50 年前在美國貝爾實驗室得到概念性驗證後，至今世界先進國家已開始整合開發商轉的分發協定。雖然目前世界上量子密鑰分發網路的發展已有一定的成熟度，但分發協定這類與安全性相關的技術仍待國內自主開發與設計。另一方面，光在介質中傳遞難以避免受到衰減及雜訊干擾，實際量子網路常需要設置量子中繼器來增加量子資訊傳遞的距離以達成遠距糾纏，而技術上亦可使用量子錯誤更正或量子糾纏純化法來維持量子特性。

為強化我國之光量子技術及其涵蓋之關鍵技術，研究面向二—光量子技術涵蓋光量子運算以及量子通訊之硬體與軟體技術，藉此建立我國自主開發之光量子運算平台與量子通訊技術，以及與光量子相關之關鍵元件製作能力。

貳、研究議題範疇

計畫研究議題包含(但不限於)下列相關研究項目：

一. 光量子運算

光量子運算主要是由量子光源、光子線路(photonic circuit)以及單光子光偵測器所構成。本研究議題涵蓋：量子光源，包含單光子源、糾纏光子源、光量子態產生源(壓縮態、連續變數態)等；光子線路則是根據不同的演算法設計，需可積體化為光量子晶片，以及可重置(reconfigurable)之光學元件；單光子偵測器則必須具有高效率、低雜訊以及高響應速度。

二. 量子通訊

量子通訊硬體技術亦包含光源與偵測器，依據長距離或短距離的應用，其光源與偵測器的要求規格亦不同；量子通訊軟體技術則是包含量子密鑰分發以及量子錯誤更正等技術。本研究議題包含量子通訊之硬體與軟體技術，涵蓋：量子光子源、高純度/高效率糾纏光子光源、光量子態產生器、具高探測效率/低暗計數之單光子偵測模組、具高儲存效率與長儲存時間之量子記憶體、晶片化密鑰位元收發模組、量子密鑰分發、量子糾纏純化等。

# 研究面向三：量子科技軟體技術

壹、計畫背景及目的

量子電腦被預期可執行一些比傳統演算法更有效率的演算法，如量子因數分解演算法、量子搜尋演算法等。此外，量子退火、量子絕熱和量子概算最佳化等利用量子力學的效應(如量子疊加態、量子穿隧效應)的演算法，隨著系統演化，將可得到傳統演算法無法作到的效果。應用這些量子演算法來處理實務上的問題，將會帶來新的計算科學革命。

然而，量子狀態容易因環境的干擾而散失同調性，且量子邏輯閘操作難以完美，將衍生更多雜訊。量子電腦如要實現一種有意義的量子計算（例如因數分解演算法），每個邏輯閘的錯誤率勢必要遠低於 $10^{-10}$。此等級的錯誤率僅靠物理方法實現仍極具挑戰性，因此需要利用量子錯誤更正碼的技術來保護量子態，藉此使量子運算能得到近似於理想的容錯量子計算(fault-tolerant quantum computation)。

而當量子位元數量規模逐漸增大後，以量子電路來描述要進行的量子運算將變得太複雜而不可行，將需進一步發展較高階的量子程式語言。可預期未來如量子計算機結構與量子作業系統等領域也將慢慢成形。因此本計畫也擬投入量子程式語言開發，藉此吸引更多研究者投入。

除此之外，目前普遍預期量子電腦會挑戰現今密碼系統的安全性。後量子密碼學即是開發能夠抵抗量子電腦攻擊的傳統演算法。後量子密碼學經過約二十年的研究已相對成熟，發展出許多具安全性的密碼系統(包含加密、簽章等)，並具備實務應用。然而隨著未來軟硬體技術的演進，仍有進一步研發的必要性。

目前量子電腦硬體發展雖尚未能實現預期的強大運算能力，然而應用量子科技軟體技術的發展卻刻不容緩。研究面向三—量子科技軟體技術將涵蓋演算法、軟體介面、程式語言、量子密碼學與後量子密碼學、以及量子模擬器與量子計算應用，藉此培育我國未來量子科技軟體技術高階人才，待量子電腦硬體技術更加成熟後，將可迅速接軌我國量子科技之全面發展。

貳、研究議題範疇

計畫研究議題包含(但不限於)下列相關研究項目：

一. 量子演算法

包含量子概算最佳化演算法、適用於雜訊中等規模量子電腦之量子演算法、Shor 演算法的高效實施、量子糾錯碼與容錯量子計算、高效能的古典數據量子化編碼和量子可觀察量讀取、及其他量子演算法基礎研究。

二. 量子電腦程式語言設計與使用者介面開發

包含量子程式語言的設計、量子程式的驗證與測試、及有效率的量子程式編譯器。使用者介面設計，主要涵蓋使用者與量子電腦、軟體或應用等互動的介面設計。

三. 量子密碼學與後量子密碼學

包含密碼學的後量子安全性、實用後量子密碼學、設備無關量子密碼學、量子多方安全計算與委任量子計算、及其他量子密碼基元與任務的基礎理論研究。

四. 量子啟發應用計算

包含量子電路的最佳化、量子化學能階結構分析、量子金融、量子機器學習、量子新藥與材料模擬、量子運輸管理、量子可逆電路合成演算法、量子退火、及其他量子啟發應用計算。