科技部工程司
107 年度「量子電腦」專案計畫
徵求公告

壹、前言

隨著半導體技術持續精進，更高速更省電且計算能力更強大的電腦已被陸續開發出來。目前半導體產業龍頭台灣積體電路公司已經使用 7 奈米製程技術進行晶片製造，2019年時將推出第二代 7 奈米製程，預計在 2020 年時 5 奈米製程將會量產，而 3 奈米的晶片亦可預期。然根據台灣積體電路公司張忠謀董事長估計，半導體製程的微縮再往前進將有其不確定性，並因為物理上的限制而遭遇到瓶頸。一顆原子的大小約為 0.1 至 0.5 奈米，製程上就會受限於這個大小，晶片的大小會越來越接近原子尺度，電晶體的運作也越來越無法遵從原本的古典物理與電路理論，因此摩爾定律在不久的將來有可能會失效，因此，我們必須先找出新一代電腦研發的方向及相關應用。

1969 年時學者 Stephen Wiesner 最早提出基於量子力學的計算裝置的概念，緊接著許多學者跟著發表基於量子力學的資訊處理相關研究;在 1982 年時諾貝爾物理學獎得主 Richard Feynman 在一個著名的演講中提出利用量子系統所構成的電腦來模擬量子現象則運算時間可大幅度減少的想法，從而量子電腦的概念應運而生；2012 年諾貝爾物理學獎得主法國科學家 Serge Haroche 與美國科學家 David Wineland 分別提出了突破性的實驗方法，能測量和操控個別量子系統，瑞典皇家科學院即發表聲明指出「量子電腦或許會在本世紀改變我們的日常生活，就像現在的電腦在上個世紀大幅改變人類生活一樣」，因此，以量子為基礎的超高速電腦可預期的會成為下一世代的電腦，並帶動新一波的資訊革命。

以量子為基礎的電腦之所以具有成為下一世代電腦的潛力，主要是因為量子具有量子糾纏（entanglement）及量子疊加（superposition）的特性，當兩個量子交互作用時，就會出現纏結，意思是一個量子會影響遠處的另一個量子，即使兩個量子分開，兩者的連結還會持續一段長時間，而在量子糾纏時，量子就可能進入疊加（superposition）狀態，因此一個量子位元（qubit）可能是0或1，或既是0又是1，這就開啟了新一世代電腦之路，因為量子疊加（superposition）和量子糾纏（entanglement）特性而使得量子運算能具有巨大的量子平行性 (quantum parallelism) 的運算能力，能使量子電腦結合運行量子演算

法(quantum algorithm)具有超快速度來解決現今連功能強大的超級電腦都無法解決的問題。例如 AT&T 貝爾實驗室的 Peter Shor 於 1994 年提出快速完成質因數分解的第一個量子演算法，這在傳統資訊領域裡被認為是無法有效率地計算的一個 NP 問題，其後更延伸應用至離散對數及所有 Hidden Subgroup 問題(包含質因數分解與離散對數問題)。

目前量子電腦均成為世界各國產官學競相投入發展之重要領域，歐洲地區已有超過 20 個國家投入量子資訊與量子科技的研究，並分別提出了相關的大型計畫，歐盟委員會於 2016 年 5 月發表了量子宣言(Quantum Manifesto)。宣言中提出「第二次量子革命正在世界各地展開，各國皆期望藉此行動在科學、工業和社會等方面能取得革命性的進步」，因此號召歐洲國家共同發起量子電腦旗艦計畫，目前已獲得許多歐洲產業、研究機構以及科學家們的支持，此旗艦計畫已於 2018 年啟動，目的在使歐洲於這場量子電腦技術革命中能夠保持領先地位，主攻通信、計算、傳感及模擬這四個方面的量子技術；美國於 2000 年即把量子電腦的發展列為國家科技戰略目標之一，2009 年白宮國家科技委員會提出聯邦量子資訊科學展望白皮書，2016 年白宮科技政策辦公室又提出了“美國先進量子資訊科學：國家的挑戰與機會”報告書，再次強調發展量子資訊科學的重要性；另外，美國國家科學基金會(National Science Foundation, NSF)於 2016 年就將量子科技應用定位其未來發展與投資的五個主軸之一；英國政府先前即成立了量子科技戰略顧問委員會擬定了國家量子技術戰略，更於 2013 年成立英國國家量子科技計畫，幫助量子行業在英國紮根；又於 2015 年提出英國國家量子科技策略投入資源培育量子科技人力資源，預備為未來的勞動力提供高級技能，以實現量子科技能為英國帶來利益；澳洲、加拿大、日本、新加坡等國也將量子科技、量子計算與資訊列為補助重點之一，設立國家級的卓越中心和相關研究單位；另外，中國大陸在量子科技上的投資與研究表現後來居上，處於全球領先地位，中國已將量子資訊列為國家自然科學基金優先資助領域，並成立多個量子資訊與計算研究機構，如中國科學院的量子資訊重點實驗室，中國科技大學量子通信與量子計算實驗室，教育部量子資訊與量測重點研究室，原子分子與奈米科學中心的量子資訊研究，北京清華聯合成立量子信息與測量重點實驗室等。2016 年中國國務院發布《國家創新驅動發展戰略綱要》點出十大產業技術體系創新，其中

在發展引領產業變革的顛覆性技術方面，提出大陸應要積極開發量子資訊等技術。在量子通訊發展方面，大陸於 2016 年 8 月發射世界首顆量子通訊實驗衛星墨子號，並計畫在 2030 年建成全球化的量子通訊網路。此外，世界三大科技產業巨頭 Google、IBM 及 Intel 亦投入大量資源研發量子電腦及量子元件，Google 使用超導體製程已於 2018 年 03 月 05 日對外展示了具備 72 個量子位元的量子處理器；IBM 亦使用超導體製程並於 2017 年 11 月 11 日在華盛頓舉行的 IEEE 工業計算峰會上發佈具備 50 個量子位元的量子電腦，而 Intel 除了投資開發超導體量子位元，在 2018 年 1 月的 CES 上發表 49 量子位元的超導測試晶片，另外還研究矽晶自旋量子位元的技術，其遠比超導體量子位元來得小聚擴充性，三大巨頭肩併肩的朝量子霸權邁進。而我國具有領先全球的半導體產業優勢及資訊通信(ICT)產業聚落，在世界各國均投入量子電腦研發的此時，更應積極整合產業優勢推動我國量子電腦之研發，例如使用矽半導體量子點製程研發量子位元，和目前半導體製程標準的互補性氧化金屬半導體(CMOS) 技術相容，因此提供了我國使用相同的矽半導體製造技術來製造量子位元晶片的願景，藉此連結即將到來的量子電腦科技世代，並打造下一個世代的電腦。

量子電腦具有指數級強大功能的運算速度，其發展結果註定會從根本上改變我們的生活、社會和經濟，目前世界各國均投入大量資源研發量子電腦，所以我國需急起直追，而在量子電腦研發項目中，量子運算和量子演算法的發展對於現行的安全通訊機制造成了極大的衝擊，目前普遍用於網際網路資料傳輸數位簽章以及的非對稱性加密演算法，其安全性主要是建立在一些難解的數學問題(one-way function)，其中非對稱式加密演算法就是以整數的質因數為基礎的分解問題，而離散對數問題則是 Diffie-Hellman 演算法的基礎。另外 Elliptic Curve 演算法則與前兩者同屬於 Hidden Subgroup 問題，上述三個演算法是目前最廣為使用的非對稱性加密演算法，但都已經有對應可以破解的量子演算法被提出，此外，安全保密的通訊不僅在軍事、國防、金融、國家與社會安全等領域非常重要不可或缺，在當今的經濟和日常通訊等方面也日漸重要，量子電腦的發展對於現行的Internet網路密碼系統之安全性產生了威脅，但同時，基於量子物理的特性，量子力學也提供了一套絕對安全的(無條件安全的; unconditionally secure)量子通訊機制，稱為量子密鑰分發為量子

(Quantum Key Distribution, QKD)。1984年由 C. H. Bennett 與 G. Brassard 兩位學者共同提出 BB84 協定是最早的量子密鑰分配協定，隨著 BB84 協定的提出，許多先進國家的研究團隊，紛紛投入量子密鑰分配的研究，除了 BB84 外，已有不少量子密鑰分配協定先後被提出(例如: B92、E91…等)，除此之外，量子密鑰分配系統也從實驗階段慢慢進入了應用階段，國外預計將有商用設備問世。因此，量子電腦、量子演算法及可以提供安全的量子通訊，還有可結合我國最具優勢的半導體產業的量子元件和物理，將作為科技部推動國內量子電腦發展初期探索及研發量子電腦的重要項目

目前我國在量子電腦與量子資訊系統這方面的研發散佈在各大學及研究單位，這或許也是正當世界各先進國家積極推動量子資訊科技的工程應用發展時，國內目前相關的研究似乎仍侷限在基礎研究領域的主要原因之一，因此若想要有進一步的實質進展，需建立一個跨領域整合型且集結各方量子資訊與量子科技的研發能量、形成強鏈結性的研究團隊，進而使大家能互相討論、分工、支援、向發展量子電腦科技及培育量子電腦科技人才之目標邁進，這樣才有可能讓世界看到台灣在量子電腦領域的發展，以及達成在台灣發展量子電腦與量子科技產業的終極目標。

貳、 計畫目標

一、整合國內產學研資源研發發展量子電腦，跟上國際腳步，讓世界各國看見台灣在量子電腦領域的發展成果。

二、善用我國現有之半導體產業研發資源及能量以達成推動國內量子元件及物理、量子演算法、量子電腦及量子通訊之研究發展的目標，並利用半導體量子點及 3D 異質整合技術，實現大尺度規模的量子電腦處理器，以連結即將到來的量子電腦科技世代，孕育下一個世代的電腦。

三、推動產學研界在量子電腦和量子資訊系統技術上之研發能量，並開發適用於量子電腦和量子資訊系統之相關技術平台與元件。

四、推動與產業界共同建立合作聯盟發展及培育量子電腦之研發人才。

參、計畫內容與重點研究項目

一、計畫內容

(1) 本專案計畫之總計畫內容必須陳述整體計畫目標，提出具體的研發雛型架構、計畫指標及計畫技術藍圖，目標為開發具有前瞻性及創新性的量子電腦相關項目，並需明確敘述規格指標及相關產業的應用，以建立我國在量子電腦領域競爭優勢為主要目的，並提出具體合作績效。

(2) 各子計畫書中應具體說明國內外相關產業現況並深入分析技術優勢與研究之必要性，並著重於量子電腦研發的創新性及前瞻性。詳細訂定各年度里程碑、查核點、評量指標及技術發展藍圖，以作為評審或查核之依據，計畫結束後進行成果發表及展示。

(3) 本專案計畫重點研究項目需進行相關主題的學術探討及應用效益評估，內容需聚焦於量子元件及物理、量子演算法、量子電腦及量子通訊之相關研究項目其中一項或跨項目整合。

(4) 本專案計畫以達成探索我國量子電腦之發展重點為首要目標，初期規劃五年，前兩年至少需達成量子元件及物理、量子演算法、量子電腦及量子通訊等之其中一個或跨項目整合架構及成果雛形或模擬成果，並期許能與產業有具體合作事項；第三年至少達成初步成果；第五年結束前至少需完成計畫預期之成果指標，並建立產學研共享資料技術平台與合作應用。前述規劃完成之項目，應於總計畫及子計畫之計畫書內分別詳細述明。

(5) 本專案計畫鼓勵與國內外學術或產研單位合作研究開發，計畫團隊可逕行與相關單位接洽合作事宜，並簽訂合作備忘錄，同時需規劃具體研究成果並共同辦理成果發表會。

二、重點研究及預期效益

本專案計畫之重點探索發展項目包含(1)量子元件與物理、(2)量子演算法、(3)量子電腦及(4)量子通訊四個項目；研究團隊著重於跨領域之整合，並訂定明確指標規格及定位核心技術之技術成熟度(Technology Readiness Level, TRL) (請填寫附件 3)及成果指標說明(請填寫附件 4)。

(一)計畫內容必須聚焦下列量子電腦相關研究項目中一項目或跨項目整合：

1. **量子元件與物理:**

目前國內已具有相關低溫量測與量子位元樣品製作技術，因此可以結合我國最具優勢的半導體產業打造量子位元及其製程

研發，同時，需精進半導體低溫微波操控技術與單自旋量測技術；矽半導體量子點量子電腦吸引人的特點是完整的製造過程與標準 CMOS 技術兼容，提供了使用相同的矽半導體製造技術實現大規模量子電腦處理器的願景，研究團隊需參考國際標竿動態，自訂具競爭力且具體的達成目標。

2.量子演算法及程式：

繼 International Business Machines Corporation（IBM）於 2017 年 03 月 提出量子資訊軟體套件 QISKit (Quantum Information Software Kit)後，Microsoft 也於 2017 年 12 月發布了量子開發套件(Quantum Development Kit)的免費預覽版本，其中包括 Q＃程式語言、量子計算模擬器以及其他資源。因此可針對這兩大量子軟體開發套件嘗試編寫量子電腦應用程式，並可以使用 IBM Cloud 的量子電腦實際進行運算模擬，本研究議題至少能建構量子電腦資訊系統雛形，並培育撰寫量子程式及演算法之人才。研究團隊需參考國際標竿動態，自訂具競爭力且具體的達成目標。

3.量子電腦

1994 年時 Peter Shor 提出量子質因數分解演算法後，證明量子電腦速度遠勝傳統電腦。目前已經有許多量子電腦的相關研究，例如 N. Cody Jones 等學者在 2012 年時提出量子電腦架構；此外，除了理論，也有不少學者著力於利用各種量子系統來實現量子電腦，例如美國學者 Matt Reynolds 在 2017 年時完成量子電腦模擬器；另一方面，世界科技產業也紛紛致力於發展量子電腦，Microsoft 在 2017 年 9 月公布兩款量子電腦模擬器，Google、IBM 及 Intel 也已分別建置 72 個、50 個及 49 個量子位元的量子電腦處理器，期望能取得量子霸權搶先攻佔市佔率。因此，目前的量子電腦發展仍處於研發階段，與真正能普及的通用型量子電腦仍有距離，因此本項目期許研究團隊能致力於發展量子電腦，研究團隊需參考國際標竿動態，自訂具競爭力且具體的達成目標。

4.量子通訊測試平台及安全傳輸率：

本研究議題須能掌握對量子密鑰分發技術之研發與裝置設備的自我製造能力實作，以及建置量子通訊、量子安全保密通訊

中的量子密鑰分發系統的主要關鍵技術，包括量子訊號的產生、發送與接收、量子訊號的編碼與量子訊號的同步化控制，其中，量子訊號的編碼方式與所採用的量子密鑰分發協定息息相關，因此，所使用的編碼方式將決定整個量子密鑰分發系統的實作架構。目前實作上常見的有極化偏振態(polarization)編碼法、差分移相(differential phase shift) 編碼法、糾纏態(entanglement)編碼法等。研究團隊需參考國際標竿動態，自訂具競爭力且具體的達成目標。

(二)計畫內容須跨項目整合相關研究項目：

申請本專案計畫需聚焦於「量子元件及物理」、「量子演算法」、「量子電腦」及「量子通訊」之其中一項目或跨項目整合發展，同時必須建立產學研共享資料技術平台以便後續推動產業合作應用。

肆、計畫申請與審查

一、計畫申請注意事項

(一)本專案計畫需以英文計畫書申請。

(二)計畫書需陳述五年計畫規劃藍圖(roadmap)及執行內容，並具體說明年度成果與後續產業化成效，且鼓勵與產業界合作。請於計畫書內陳述與合作企業及法人單位實質合作之規劃項目與內容。

(三)本部將於107年4月19日於國立成功大學及107年4月23日於國立台灣大學舉辦量子電腦研發專案計畫徵求之研討會及說明會。

(四)本專案計畫之主持人與共同主持人資格必須符合本部補助專題研究計畫作業要點之規定。

(五)(1)計畫應為單一整合型五年期之型式，將總計畫及各子題之執行方式及經費等計畫內容整合成一份計畫書，並由總計畫主持人之服務機關提出申請。

(2)本計畫研究團隊需含主持人及共同主持人共三人以上，並皆列入本部專題研究計畫件數計算，且按本部規定支領主持費。

(六)(1)本專案計畫期以落實產學研密切結合之目標，故鼓勵計畫團隊邀請業界及法人單位參與規劃及執行，請於計畫書內檢附相關附件1或附件2且依序置於計畫書表CM03研究計畫內容最後。

(2)計畫書中須規劃研究項目及應用項目，說明計畫 roadmap及其核心技術研究之技術成熟度(附件3)及成果指標說明(附件4)。

(3)申請書採用本部一般專題研究計畫之英文計畫書格式，其中表 CM03 研究計畫內容頁數需以不超過 80 頁為限。

(七)計畫依本部專題計畫申請方式於線上提出申請，每件計畫每年補助金額以不超過 2500 萬元為原則。

(八)全程執行期限自107年8月1日起至112年7月31日止。

(九)計畫類別請勾選「一般型研究計畫」、計畫歸屬請勾選「工程司」、學門代碼請勾選 E9858 (量子電腦專案計畫)，以利作業。

二、計畫申請時程

計畫自公告日起接受申請，申請人依本部補助專題研究計畫作業要點，研提計畫申請書(採線上申請)，申請人之任職機構須於 107 年6月15日星期五前函送本部(請彙整造冊後專案函送)，逾期不予受理。

三、計畫審查

審查作業包括初審及複審，如有必要將安排計畫主持人簡報計畫內容。

四、其它

(一)本計畫屬專案計畫，無申覆機制。

(二)其它未盡事宜，依本部專題研究計畫作業要點及其它相關規定辦理。

伍、 計畫考核

一、本專案計畫之計畫主持人及共同主持人需依據專長及所提之計畫書內容，開設與「量子元件及物理」、「量子演算法」、「量子電腦」及「量子通訊」之課程，此課程可規劃為一般學期課程及短期課程(學期中或寒暑假)，並列入計畫實地訪查、期中考核及成果考核項目。請將規劃之課程填寫於附件5中，並置於計畫書表 CM03 研究計畫內容最後。

二、本專案計畫需每年需辦理一次成果發表會並繳交成果報告，每半年本部將進行實地訪查及期中考核。

三、本部將每年進行實地審查此專案計畫執行情形，執行團隊必須定期呈報計畫執行進度與成果，並辦理成果發表會及出席各項審查會議，各執行團隊須定期展示該計畫所開發之技術或系統成果。

四、本專案計畫每一年皆會根據研究成果進行追蹤、查核與考評，審查結果將列為下一年度調整經費的參考依據。

五、計畫全程(五年)結束時所繳交之結案報告需包括學術理論、關鍵技術、優質論文發表、與產業合作成果、重要專利或其它實體產品之說明及提供。

六、計畫執行之第 4 年及第 5 年會將考核計畫成果對產業創新之實質貢獻，解決關鍵問題並提升產業競爭力之情形。

七、執行團隊須配合本部進行計畫考核、執行成果發表、推廣應用及交流、記者會及研討會等工作推動。

陸、專案推動小組

專案召集人：

徐碩鴻司長　科技部工程技術研究發展司

E-mail：shhsu@most.gov.tw

電話：(02)2737-7524

傳真 :(02)2737-7673

量子電腦專案計畫承辦人：

張哲浩副研究員 科技部工程技術研究發展司

E-mail：thchang@most.gov.tw

黃博信博士　　科技部工程技術研究發展司

E-mail：phhuang@most.gov.tw

電話：(02)2737-7525

傳真：(02)2737-7673

量子電腦專案計畫助理：

陳威傑先生　科技部工程技術研究發展司

E-mail：wjchen@most.gov.tw

電話：(02)2737-7374

傳真 :(02)2737-7673