量子時代的網路安全挑戰

蔡永信

中華民國 111 年 7 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘 要

量子計算主要利用量子位元的3種量子效應(量子干涉、量子疊加與量子糾纏)進行運算，在量子效應下，由於對疊加並糾纏的n個量子位元運算，其效果等於同時對 2^n 個數值運算，達到類似指數級倍數的平行計算加速，因此。量子計算具有一個相當大的計算優勢。

目前的量子電腦技術只能提供不具錯誤校正功能的 NISQ 量子電腦，亦即其量子位元容易在雜訊的干擾下失去應有的資料。各科技公司正在嘗試各種系統模型，及合適的材料與科技，以達到邏輯量子位元的可量化性，最後逐步實現可容錯的通用型量子電腦， 2030 年將有可能是量子電腦達到容錯能力的關鍵時點。

網路安全的四大基石，機密性、身分認證、資料完整性及不可否認性，主要是透過密碼學演算法達成。而量子破密攻擊，將降低目前作為網路安全碁石的密碼學演算法安全性，甚至是將其破解。後量子密碼學係使用現有的電腦與網路，並利用公認無法被量子電腦有效解決的計算難題，發展出可抵抗量子電腦攻擊的公鑰密碼系統，因未改變既有的網路安全架構，僅取代核心密碼演算法，因此能無縫地接軌既有的網路安全機制，被視為是抵抗量子破密攻擊的較佳解決方案。

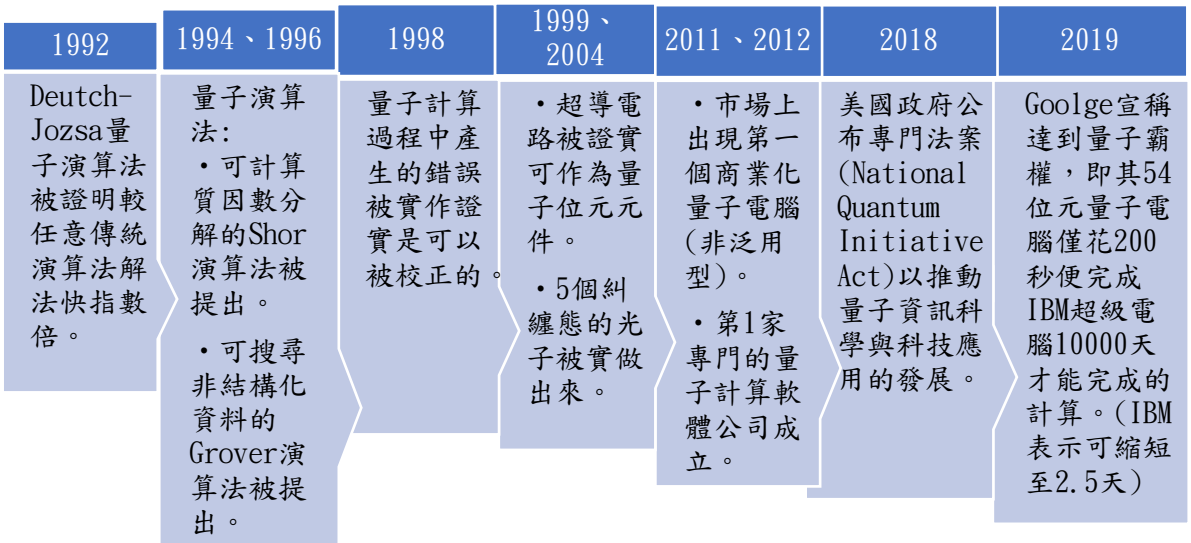
網路安全所需要注意的面向廣泛，尤其是處在量子科技即將起飛的時代，新的變革帶來新的機會，也帶來新的威脅與不確定性，而企業組織由上至下均應以戒慎恐懼的心來面對，而來自高階管理階層的行動支持，將有助於及早訂定行動方針，迎接量子時代更嚴峻的網路安全挑戰。

目　次

壹、量子計算發展簡史

量子計算是指利用量子力學裡的量子效應(Quantum Effects)來進行電腦運算，其理論概念發展主要集中在 1980 至 1990 年間，1980 年美國物理學家 Paul Benioff 證實量子力學(Quantum Mechanics)模型下的圖靈機(Turing Machine)可運作性(Paul Benioff, 1980)，而圖靈機是現今傳統電腦(Classical Computers)計算的理論基礎，等於是證明了微觀物理學中最奇妙的量子力學特性是可運用於電腦計算。之後，蘇聯數學家 Yuri Manin 與英國物學理學家 Richard Feynman 分別提出透過量子計算或是所謂的量子電腦的量子力學特性，能有效地模擬複雜的量子力學系統(Yu. I. Manin (1980)； R. Feynman (1982))，克服傳統電腦至今仍無法有效率地處理的指數級別運算負荷。接著，英國物理學家 David Deutsch 於 1985 年提出泛用型量子電腦(Quantum Computers)理論模型(D. Deutsch (1985))，並推測量子電腦也能應用於非量子力學問題。此後，科學界與企業界開啟了一系列對量子電腦領域的研究與發展(如圖 1)。

圖 1 量子電腦領域的研究與發展史



貳、何謂量子計算

量子計算雖然是利用量子力學中的量子效應進行運算，但其與傳統電腦計算一樣，都是將資訊儲存在位元(Bits)上，再對其進行運算操作，只不過量子計算所使用的是量子位元(Quantum Bits, Qubits)。量子位元實際上是一個具有 2 個量子態(Quantum State)的量子力學系統，利用這 2 個量子態來分別代表二進位制裡的 0 跟 1，而量子態是量子力學裡的物理量，例如，電子自旋性、光子偏極性等。由於量子位元具有量子力學的不確定性(Uncertainty)，物理學上用波函數(Wave Functions)來描述此不確定性，波函數裡的機率振幅(Probability Amplitudes)與量子位元被量測到 0 或 1 的機率有關。量子計算主要利用量子位元的以下 3 種量子效應：

一、量子干涉(Quantum Interference)

量子位元被量測到 0 或 1 的機率，可以透過量子干涉，影響量子態的機率振福大小，就像水波里的波紋交互作用造成波峰與波谷相互抵消，或是波峰與波峰相互增強。

二、量子疊加(Quantum Superposition)

量子位元可以處在 0 跟 1 這 2 個量子態的疊加態($\alpha|0\rangle + \beta|1\rangle$，$\alpha$，$\beta$為機率振幅)，而要確定量子位元的值，則需透過測量該量子位元才能確定，舉日常生活經驗來比喻的話，可想成投擲兩面分別為人頭與數字的銅板，在空中時的銅板朝上的一面猶如人頭與數字的疊加態，只有在落地後，才能確定銅板朝上的一面出現的是人頭或是數字。另外，量子位元測到 0 跟 1 的機率與這 2 個量子態的機率振幅有關，因此當透過干涉改變疊加態的機率振幅時，即操作處於疊加態的量子位元，其效果就等同是同時對 0 跟 1 運算。

三、量子糾纏(Quantum Entanglement)

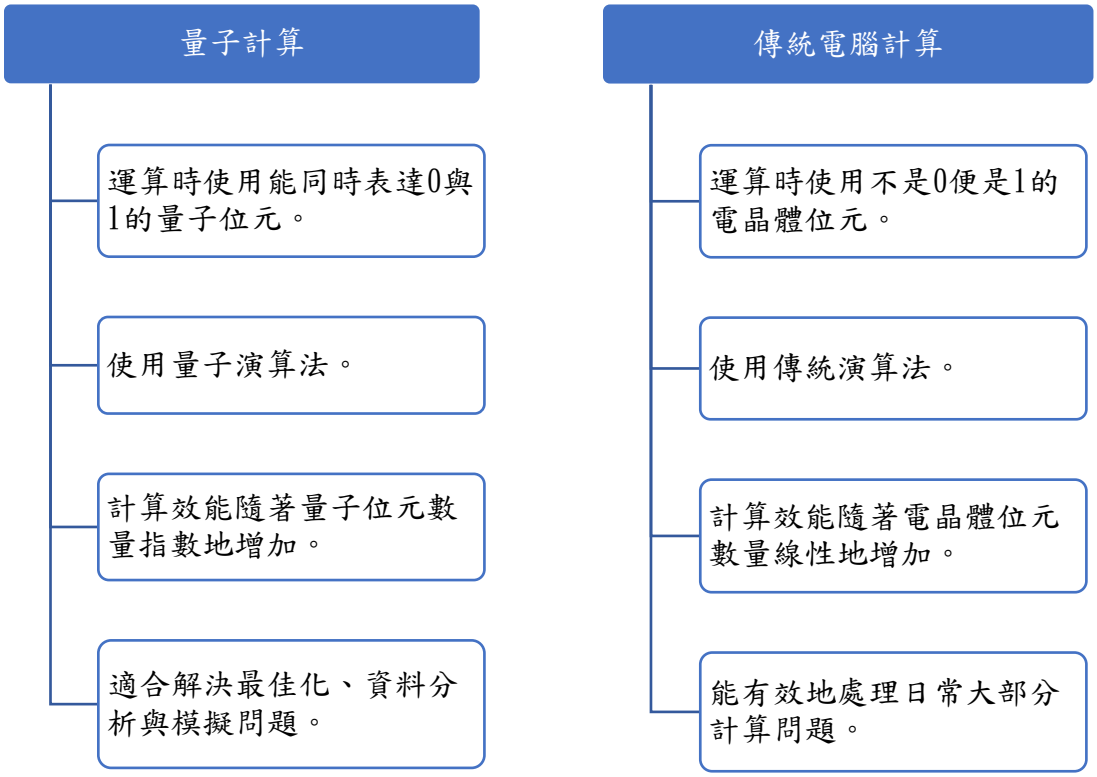
透過將 2 個處於疊加態的量子位元糾纏在一起，可以將其關聯起來，整體視為一個量子力學系統，即操作其中 1 個量子位元，會同時改變另一個量子位元，其效果等於是擴充為同時對4個($2^2 = 4$)量子態(即 00、01、10 與 11)操作，達到指數級的加速效果。

在量子效應下，量子計算具有一個相當大的計算優勢，就是所謂的量子平行性(Quantum Parallelism)，由於對疊加並糾纏的 n 個量子位元運算，其效果等於同時對2^n個數值運算，達到類似指數級倍數的平行計算加速。另一方面，由於量子位元測量出來的結果是依機率振幅相關的機率分布，導致單次的量子計算結果具有不確定性，因此需要精心設計的量子演算法(Quantum Algorithms)，使得同樣運算重覆數次後，出現次數最高的結果能成為正確答案。

參、量子計算與傳統電腦計算的差異

量子計算似乎能帶來強大的運算效能，解決目前仍難以解決的計算問題，但事實上它並非無所不能，它也僅能解決可計算的問題，即傳統電腦能計算的問題，只是其中有些對於傳統電腦計算來說，無法在合理時間內有效率地計算出結果(例如大數字的質因數分解)，但透過量子計算卻能巨幅縮短計算所需時間；而另一方面，量子計算在處理某些計算問題卻會耗費更多時間(例如加減乘除計算)。因此，它與傳統電腦之間應該是處於分工合作的互補角色，依其個別優勢將問題拆解後讓他們各自運算。量子計算與傳統電腦計算的差異可簡單歸納如下圖：

圖 2 量子計算與傳統電腦計算差異



肆、量子計算發展狀況

一、量子計算產業生態系

根據麥肯錫管理諮詢公司 (Mckinsey & Company)2021 年 12 月份發布的報告「量子電腦：新興的產業生態系與使用案例」，從量子計算產業的私募資金投資情形來看，從 2001 年至 2021 年已募得 33 億美元，僅 2021 年量子計算新創公司募得的資金估計超過 17 億美金，是 2020 年募得金額的兩倍，顯見民間投入金額正在加大力度，而其中 70%投向了硬體開發廠商，主要是因為目前硬體技術尚未成熟，仍需大量資金投入研發。實際上，近幾十年來，政府資金透過學術與研究機構已投入超過 330 億美元在量子計算領域。

目前的量子計算產業生態系包含基礎元件製造商、硬體廠商、軟體廠商、雲端量子計算服務供應商與終端應用使用者，整體家數自 2013 年的少數

幾家成長至 2021 年已有超過 200 家相關新創公司，可見量子計算的產業生態系正不斷加速擴展，其中以軟體廠商數量成長最多，且這些新創公司主要集中在加拿大、英國與美國。

為進一步了解各企業在生態系裡扮演的角色，美國波士頓諮詢公司(Boston Consulting Group)將其分成 4 大類(如表 1)，但這些公司在產業生態系中的角色是動態的，界線也是模糊的，專注硬體生產的公司有可能在日後硬體技術成熟後，往軟體與服務層擴大業務(Philipp Gerbert and Frank Ruess (2018))。這 4 大類角色的功能與現有的企業如下：

(一)完整解決方案提供者：從雲端服務到硬體設計一手包辦，通常是全球科技大廠或是資金雄厚的新創公司，包括佔有領先地位的 IBM、最早宣稱達到量子霸權(Quantum Supremacy)的 Google、中國電商巨頭阿里巴巴、全球作業系統巨擘 Microsoft，及 2022 年剛在 NASDAQ 上市的新創公司 Rigetti 等。

(二)硬體與系統提供者：專門研發量子計算最核心也是目前技術瓶頸的硬體系統，如全球晶片霸主 Intel、新創公司 IonQ、Quantum Circuits 及 QuTech 等。

(三)軟體與服務提供者：尋找潛在的應用並將現實世界的問題轉換成量子計算能運行的演算法，如 Zapata Computing、QC Ware、QxBranch 及 Cambridge Quantum 等。

(四)專家實驗室/新創公司：提供企業客戶特殊且專業的解決方案，主要是由研究機構分出的新創公司，如 Q-CTRL、Quantum Benchmark 等。

表 1 各公司在量子計算產業生態系中扮演的角色

	完整解決方案提供者	硬體與系統提供者	軟體與服務提供者	專家實驗室/新創公司
服務層	1.IBM 2.Google 3.Rigetti Computing 4.Microsoft 5.Alibaba Group 6.D-Wave Systems 7.Honeywell 8.Xanadu 9.Qilimanjaro		1.Zapata Computing 2.Cambridge Quantum Computing 3.QC Wave 4.1QBit 5.Riverlane 6.QxBranch	1.Tellus Matrix Group 2.Quantka 3.Entanglement Partners 4.h-bar Quntum Consultants
應用層與系統軟體層				1.Quantum Benchmark 2.Strangeworks 3.Q-CTRL 4.Qindom 5.ProtenQure 6.QbitLogic
系統層		1.IonQ 2.QuTech 3.Intel 4.Quantum Circuits 5.BraneCell 6.TundraSystems Global		SeeQC
量子電腦硬體層				1.Silicon Quantum Computing 2.PsiQ (PsiQuantum) 3.Alpine Quantum Technologies (AQT)

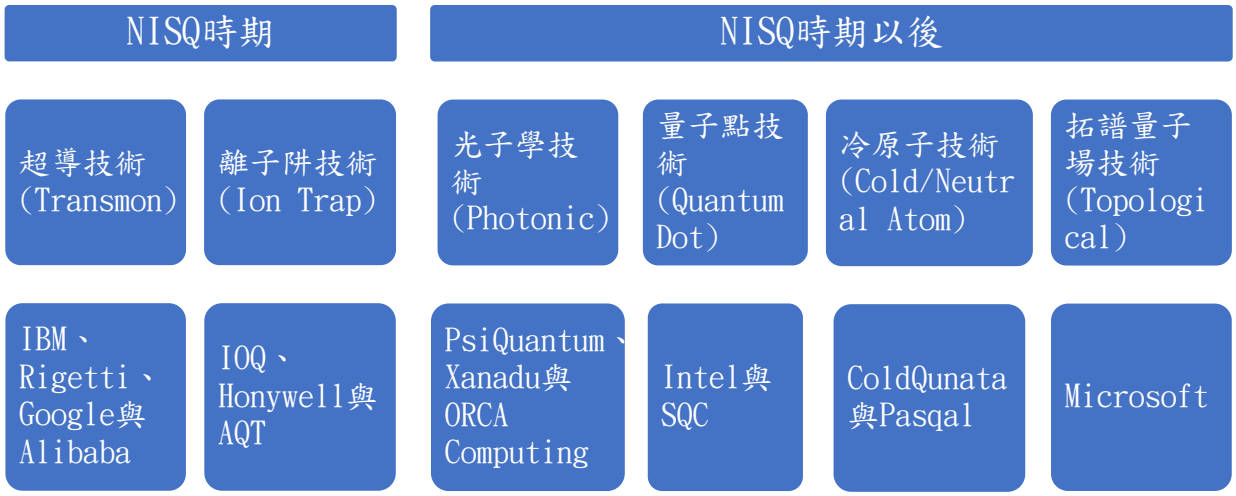
二、量子電腦研發進展

量子電腦是量子計算運行的設備，主流的量子電腦系統模型為量子電路模型(Quantum Circuit Model)或稱為量子閘模型(Gate Based Model)，其中一個極重要的硬體元件便是量子位元。目前實作出的量子位元極易受到各種干擾而喪失應有的狀態(稱為量子退相干，Quantum Decoherence)，因此量子電腦需具備於量子位元發生錯誤時能校正(稱為量子錯誤校正，Quantum Error Correction)的功能，以便確保量子計算的正確性。而為了要達到錯誤校正的

目的，一個無運作錯誤的邏輯量子位元(Logical Qubits)約需要數百至 1 千個實體量子位元(Physical Qubits)來實作，已知的通用型量子電腦最多僅達到 1 百多個實體量子位元規模。根據從事相關研發量子電腦的公司預估，在近幾年內實體量子位元數量僅能達到中等規模，即數百個至 1 千個實體量子位元，所以目前的量子電腦因無量子錯誤校正功能，尚未達到容錯性(Fault Tolerance)，無法保證其計算結果可靠性。換言之，現在正處於所謂的雜訊中等規模量子時期(Noisy Intermidiate-Scale Quantum Era，NISQ Era)(John Preskill (2018))。

因此，各科技公司正在嘗試各種系統模型，及合適的材料與科技，以達到邏輯量子位元的可量化性(Scalability)，最後逐步實現可容錯的通用型量子電腦。這些從事研發的科技公司所支持的量子計算科技正處於百花齊放、百家爭鳴的競爭階段，相關產業科技分析報告將其分成 NISQ 時期與 NISQ 時期以後(即以容錯性為研發重點) 2 大類，包含超導技術(Transmon)、離子阱技術(Ion Trap)、光子學技術(Photonic)、量子點技術(Quantum Dot)、冷原子技術(Cold/Neutral Atom)、拓譜量子場技術(Topological)等 6 種具備發展潛力的量子位元科技(如圖 3)，由此不難看出 IBM、Google 與阿里巴巴等公司以發展 NISQ 量子電腦為目標，再逐漸過渡到容錯性量子電腦，如此一來便能快速取得進入市場的商機，而 Intel 與 Microsoft 等公司則選擇發展具有容錯性前景的技術，期望能建造出容錯性較佳的量子電腦，直取市場主導地位，以便達成後來居上的策略目標。

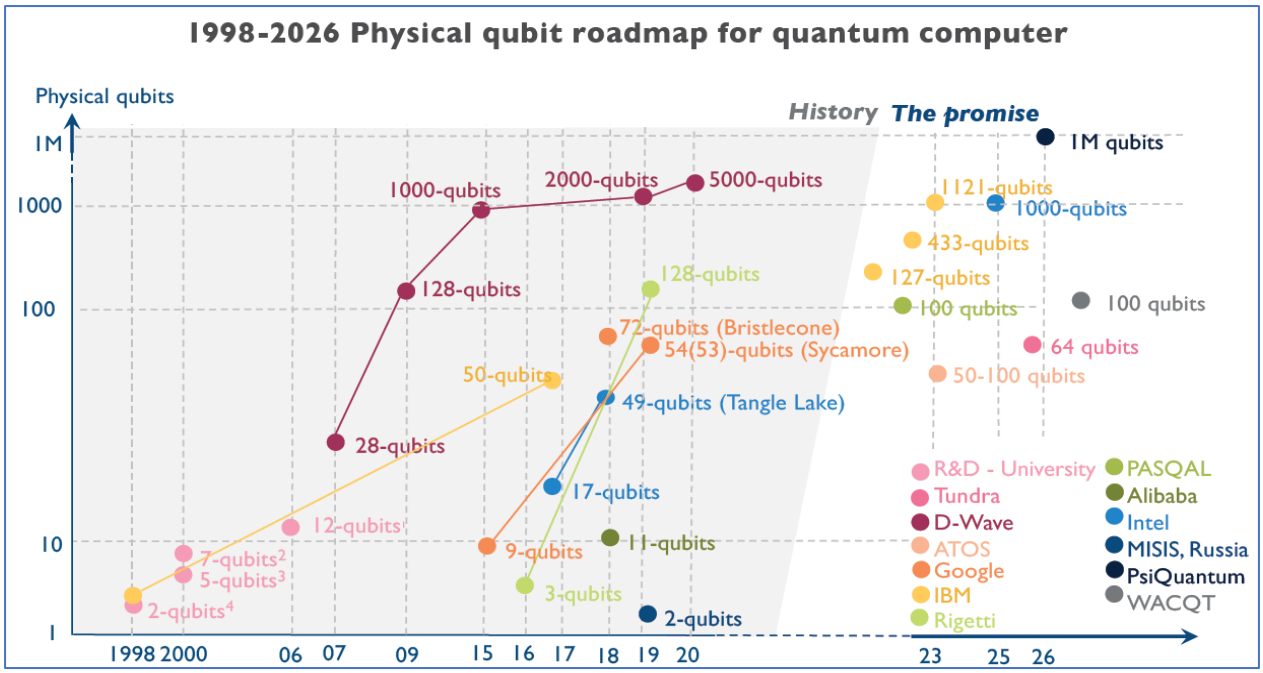
圖 3 具發展潛力的量子電腦科技



參考來源：Philipp Gerbert and Frank Ruess (2018)、OIDA (2020)與 Jean-François Bobier et al.(2021)

至於量子電腦未來研發進展，相關產業調研資訊表示未來十年將有可能是關鍵技術突破發生點，如波士頓諮詢公司依據等效的量子摩爾定律推估，小規模的容錯量子計算(~50 邏輯量子位元)有可能於 2028 至 2039 年實現(Philipp Gerbert and Frank Ruess (2018))。麥肯錫管理諮詢公司分析量子電腦硬體製造商預估的研發期程，認為小規模的容錯量子計算(~100 邏輯量子位元)有可能於 2025 至 2030 年實現(McKinsey & Company (2021))。另依法國市場研究公司 Yole Development 整理出的量子電腦實體量子位元發展期程(如圖 4)及波士頓諮詢公司整理出的量子電腦主要科技公司將陸續完成的發展里程碑(如圖 5)，可發現 2026 年前將達成 100 萬個實體量子位元的可量化性，且軟體發展也將隨著硬體層抽象化加速，邏輯量子位元需要的實體量子位元數也有望減少，再加上 Google 亦野心勃勃地宣布要在 2030 年前發展出量子錯誤校正技術，因此 2030 年將有可能是量子電腦達到容錯能力的關鍵時點。

圖 4 1998-2026 量子電腦實體量子位元發展期程



資料來源：Eric Mounier (2021)

圖 5 量子電腦主要研發公司預計 2030 年前達成的里程碑

2021年

- Honeywell
  - 量子位元品質：Honeywell研發中的量子系統H1，其雙量子位元閘的保真度(Fidelity)較前一年已提升4倍達99.8%。

2023年

- IBM
  - 硬體層抽象化：IBM將釋出預建量子執行期函式庫，讓演算法開發者無需考慮硬體層差異。
- IonQ
  - 量子電腦模組化：IonQ將在資料中心部署模組化的量子電腦並透過網路串接。

2025年

- PsiQuantum
  - 量子位元可量化性：PsiQuantum將建造出具備100萬個實體量子位元的光子型量子電腦並將其商業化。

2029年

- Google
  - 量子錯誤校正：Google將建造出100萬個實體量子位元的超導型量子位元系統並具備量子錯誤校正能力。

資料來源：Jean-François Bobier et al.(2021)。

伍、量子計算帶來的應用與效益

通用量子電腦的計算能力能較傳統電腦快上指數級倍數，但如上一節所述，目前的量子電腦技術只能提供不具錯誤校正的NISQ量子電腦，亦即其量子位元容易在雜訊的干擾下失去應有的資料。NISQ 量子電腦為了減少雜訊干擾，需維持在超高真空與超低溫，這使得其硬體體積龐大且取得價格與維護成本昂貴，因此 Amazon、Google、IBM、Microsoft 等科技公司將 NISQ 量子電腦的計算能力，以雲端服務的方式提供給有興趣的使用者，如此可透過共享資源的方式，提高經濟規模，降低量子計算使用費用並增加利用率。同時隨著量子電腦硬體與軟體的進步，軟體研發人員無需更換核心的軟硬體設備，便能進一步地尋找有潛力的應用產業與試驗更成熟的量子演算法，或是解決相關的問題，例如如何將大量資料載入量子電腦的記憶體 Quantum ram，QRam)等。

一、產業應用的量子演算法類型

哈佛商業評論 2022 年的一篇文章「量子計算給企業領導者帶來的機會與挑戰」(Jonathan Ruane et al. (2022))指出，未來這些最有可能應用於企業流程(Bussiness Processes)的量子演算法，有些能縮短營運工作時間，提高企業效率，有些則能創造新的商機，其可分為 5 種類型：

(一)量子模擬

根據研究推估，若要透過量子模擬可以真實與快速地計算出化學反應裡重要的 100 個電子間相互作用，約需要 100 邏輯量子節點組成的量子電腦叢集(Markus Reiher et al. (2017))。

(二)線性系統

線性系統方程組經常是工程、金融、化學與經濟領域想解決的數學問題，而量子線性系統演算法(如 Harrow-Hassidim-Lloyd 演算法，HHL 演算法)較傳統演算法可提供指數級倍數的加速。最有前景的應用在於加速深度機器學習裡的類神經網路模型參數收斂，解決因巨量資料與類神經網路層數增加造成的傳統電腦計算效能不足問題。

(三)最佳化

這類演算法是解決在特定情境下，如何選擇最佳方案以達到預先設定好的目標，例如在平衡風險與預期報酬下，決定最佳的退休金投資策略，或者是安排最佳生產策略等。而量子最佳化演算法相較於傳統演算法，更能完善所採取的解決方案，並縮短所需的計算時間。

(四)非結構化搜尋

對於非結構化的資料，即未正規化或排序的資料，要搜尋到特定資料，猶如大海撈針，需要逐一檢視、搜尋資料，平均搜尋次數約為資料量的一半。透過量子演算法(如 Grover 演算法)可以改善搜尋所需步驟，並減少為資料量的平方根。

(五)質因數分解與解密

巨大合數(如 2048 位元以上)的質因數分解若透過傳統的電腦計算，需要幾十億年以上的時間，但是利用量子質因數分解演算法(如 Shor 演算法)可將其中最耗時的步驟以指數級倍數加速，研究發現若配合 2,000 萬個實體量子位元的 NISQ 量子電腦，有機會縮短至 8 小時便能分解出來(Craig Gidney and Martin Ekerå (2021))，有利於破解目前常見的 RSA 公私鑰加密系統。

二、具有前景的應用與效益

相關的產業調查報告普遍認為量子計算隨著技術逐漸成熟，能幫助化工產業、製藥業、金融產業、能源產業及汽車產業等創造新的產值與開創新的商機，其應用的例子與效益如下：

(一)化工產業

1.在製造肥料的固氮反應研究上，透過量子模擬能更完整的模擬生物酶如何達成固氮反應，幫助產業界找到更有效方式製造肥料，降低肥料製造過程的能源消耗與環境汙染。

2.透過量子模擬能更準確地模擬化學分子間作用，可加速研發以蛋白質為基底且友善環境的農藥，及其他友善環境的清潔劑。

(二)製藥業

1.研究顯示，在藥物開發過程中的藥物探索(Drug Discovery)階段，可利用量子模擬與量子機器學習演算法，加速尋找出有效的化合物(Yudong Cao et al. (2018)，Junde Li et al. (2021))。

2.傳統電腦輔助藥物設計(Computer–Aided Drug Design, CADD)會因簡化量子力學效應而造成的低精確度，利用量子計算則可提高精確度，亦即量子 CADD 能應用到更大型與複雜的藥物設計，進而降低藥物實驗成本。

(三)金融產業

1.新創公司 Zapata Computing 和西班牙的銀行 Banco Bilbao Vizcaya Argentaria (BBVA)合作研究量子計算在信用風險評估調整(Credit Valuation Adjustment)的可行應用，而部分專家預期量子風險管理(Quantum Risk Management)將於 2030 年實現。

2.隨著資產管理中的資產組合排列與考量因子增加，其複雜度與計算量也會有指數級倍數的增長，而量子最佳化演算法將有助於提升交易策略最佳化的結果。

3.量子計算可減少風險管理中 Monte Carlo 模擬法運算所需的時間，由原本需要數天的時間減少至幾小時。

(四)能源產業

1.有可能是未來乾淨能源選項的可控核融合(Controlled Nuclear Fusion)技術中，其中一種是利用高功率雷射將雷射反應爐裡的微量核燃料壓縮，產生高溫與高壓，達到融合所需的條件， Google 量子人工智慧實驗室的創立者 Hartmut Neven 認為透過量子計算能力將有助於設計出更有效的反應爐。

2.美國能源部(Department of Energy)已成立 2 個實驗室專門研究量子計算在電網最佳化的應用。

(五)汽車產業

1.量子機器學習將有助於自駕車技術的進步，透過產生合成資料填補不易取得的資料，有利縮短研發週期。

2.量子化學模擬(Quantum–Chemistry Simulations)有助於電動車找出更有效率的電池材料，及改善電池內部設計，提高能量轉換率。

根據波士頓諮詢公司估算量子電腦應用創造的產業價值，以 2030 年為 NISQ 分水嶺，將量子電腦發展劃分為三個時期(如圖 6)，產業價值將由 NISQ 年代的 50 至 100 億美元，倍增約 8.5 倍至量子電腦成熟期的 4,500 至 8,500 億美元，且供應商營收約佔產業價值的 20%。

圖 6 量子電腦發展三階段推估產業應用創造的產值與供應商營收

NISQ年代（2030之前）	容錯量子電腦初期（2030之後）	容錯量子電腦成熟期（2040之後）
• 為量子電腦使用企業創造每年50至100億美元產值。 • 為量子電腦供應商創造每年10至20億美元營收。	• 為量子電腦使用企業創造每年800至1,700億美元產值。 • 為量子電腦供應商創造每年150至300億美元營收。	• 為量子電腦使用企業創造每年4,500至8,500億美元產值。 • 為量子電腦供應商創造每年900至1700億美元營收。

資料來源：Jean-François Bobier et al.(2021)。

陸、量子計算帶來的威脅

量子計算的強大計算能力讓人們對其應用充滿無限想像，但另一方面，國家級駭客組織也正在磨刀霍霍，琢磨如何使用量子電腦入侵有戰略或金融價值的電腦系統，即使在現在尚未取得合適的量子電腦的情況下，駭客仍可在以背地裡蒐集相關加密資料，以便在日後利用量子電腦破解，即所謂的先蒐集後破解攻擊(Harvest Now, Decrypt Later Attacks)。

一、網路安全的基石

綜觀當前網際網路通訊與數位經濟的網路安全，其中以數位資料安全為最核心且最為人所關注，且普遍認為數位資料安全是建構在資訊系統所具備的下列 4 項關鍵基本功能之上 (Deborah Golden et al. (2021))，因此，下列 4 項也是網路安全的基石。

(一)機密性(Confidentiality)：只有獲得授權者才能檢視資料內容。

(二)身分認證(Authentication)：能驗證存取來源的身分。

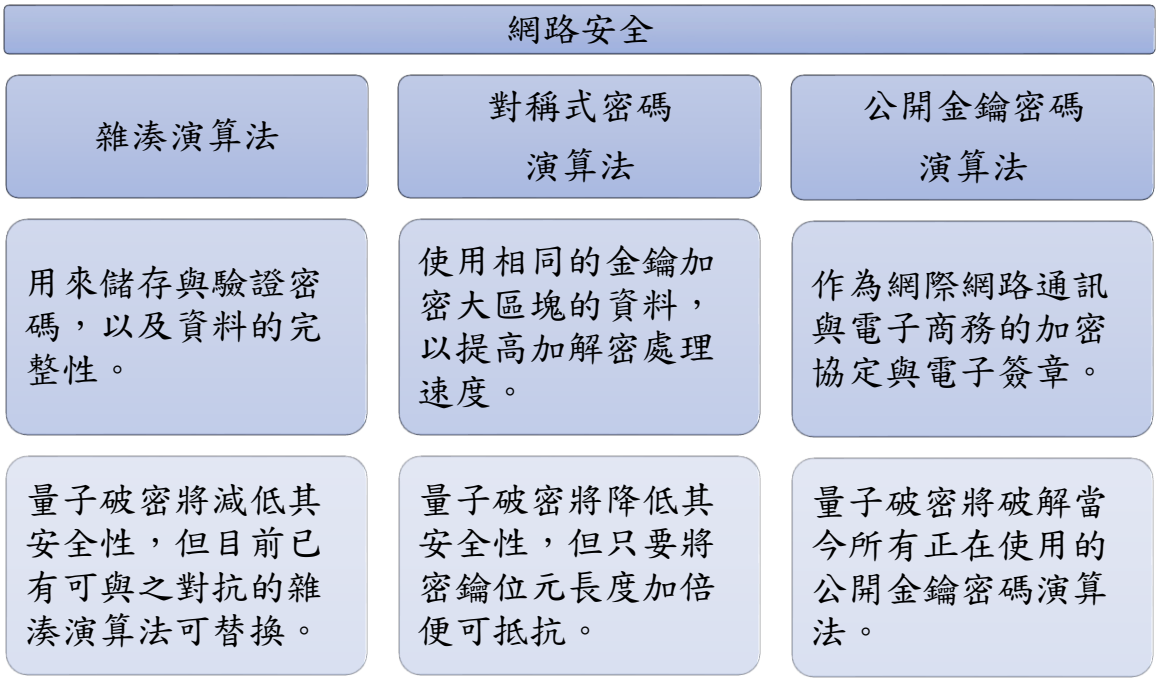
(三)資料完整性(Integrity)：能偵測到未經授權的資料變更。

(四)不可否認性(Nonrepudiation)：送出交易或變更資料者無法否認其行為。機密性是用以確保未經授權下，任何人或系統皆無法存取被保護的資料；身分認證功能則可確定存取者的身分，並依此判斷是否有權存取特定資料；資料完整性是用以偵測資料是否在傳輸途中經過非法的變更，以確保資料未經變造；不可否認性則要確保送出交易或變更資料者，無法否認其行為，避免事後不認帳或無法溯源的情形發生。

二、當下密碼學演算法遭遇的威脅—量子破密

資訊系統要實作前述四項關鍵基本功能，主要是透過密碼學演算法(雜湊演算法、對稱式密碼演算法及公開金鑰密碼(或非對稱式)演算法)，對資料或數位交易內容進行相關的運算而達成。而利用量子電腦強大的運算能力，搭配相關的量子演算法(如 Shor 演算法、Grover 演算法)解算密文，將降低目前作為網路安全基石的密碼學演算法之安全性，甚至是將其破解(如圖 7)，這也就是所謂的量子破密(Quantum Cryptanalysis)攻擊。進一步來說，當駭客在取得具有足夠數量(6000+)邏輯量子位元的量子電腦的情況下，以 Grover 演算法(用來加快非結構化資料搜尋)為基礎，可大幅縮短破解對稱式密碼系統的時間，只有當對稱式密碼系統使用夠長的密鑰時(密鑰的位元數目標準值再加 1 倍)，才可能避免被量子破密；但駭客藉著 Shor 演算法(用於巨大合數質因數分解)為基礎，將可破解現今所有正在使用的公開金鑰密碼系統(非對稱式加密演算法，如 RSA、ECC(橢圓曲線密碼學， Elliptic Curve Cryptography))，屆時其影響層面將比千禧蟲危機(Year 2000 problem)還廣泛，除了動搖整個數位經濟產業，也將影響國家安全。

圖 7 量子破密對密碼演算法的衝擊



參考資料：Deborah Golden et al. (2021)。

三、威脅逐步逼近

美國 Waterloo 大學量子計算研究所創立者 Michele Mosca 教授認為，隨著量子計算技術的成熟(2026 年前將達成 100 萬個實體量子位元的可量化性、2030 年前發展出量子錯誤校正)，2027 年前 RSA-2048 公鑰加密系統被破解的機率為 1/6，而 2032 年前破解的機率則提高到 1/2(Michele Mosca (2018))。甚至 Google 的 CEO Sundar Pichai 在 2020 年的世界經濟論壇上表示，在 2026 年至 2031 年之間，量子電腦將破解目前已知的加密系統。因此，無論是樂觀地預期量子破密威脅造成的衝擊發生在 2031 年，或是悲觀地認為在 2026 年，守護網路安全的巨牆基石已然出現縫隙，令所有資安專家們無法等閒視之。

柒、如何面對量子時代的網路安全

早在量子破密威脅變得如此真實且緊迫之前，各國研究機構內的有識之士便著手開始研究解決對策，如歐盟網路安全計畫(European Network of Excellence for Cryptology，ECRYPT)便在 2006 年於英國舉辦了第 1 次的後量子密碼學(Post–quantum cryptography，PQC)工作坊，並陸續於美國、德國、台灣、法國等地舉辦，探討能夠抵抗量子破密 (Quantum–resistant) 的密碼學，以利用公認量子電腦無法攻克的數學難題，取代現有密碼系統演算法，繼續確保網路安全。又如 2005 年起各國競相實驗並建立的量子加密通訊網路，如美國國防高等研究計畫署(Defense Advanced Research Projects Agency，DARPA)的量子網路、歐洲的量子通訊網路(Secure Communication based on Quantum Cryptography，SECOQC)與中國的金融資訊量子通訊驗證網，使用量子密鑰分配(Quantum Key Distribution，QKD)協定分配密鑰，以利用量子力學特性確保網路通訊安全。

一、量子密鑰分配協定與後量子密碼學的比較

為了避免量子破密攻擊，相關領域的專家學者普遍認可的解決方案有 2 種，分別為：

(一)量子密鑰分配協定解決方案

以硬體方式實作出運用量子力學特性的網路通訊網路與協定，確保通訊傳輸過程未被駭客竊聽，並使通訊雙方產生並分享隨機、安全的密鑰，以該密鑰進行 AES 等對稱式密碼的訊息加解密。

(二)後量子密碼學解決方案

使用既有的電腦與網路而不依靠量子力學特性，利用公認無法被量子電腦有效解決的計算難題，發展出可抵抗量子電腦攻擊的公鑰密碼系統。

量子密鑰分配協定解決方案的優點是，透過量子力學的特性使得駭客組織竊聽通訊都會被發現，從而不論駭客組織的破密能力多麼強大，都能確保資訊傳遞的安全性。但美國國家安全局(National Security Agency/Central Security Service，NSA/CSS)認為它並非是抵抗量子破密攻擊的完整解決方案，缺點如下：

(一)無法驗證傳輸對手的身分。

(二)需要建造額外的特殊傳輸設備。

(三)整個通訊基礎建設需要額外的實體安全保護機制。

(四)不易確保整體安全性與驗證

(五)容易受到阻斷服務攻擊(Denial of Service，DOS)。

因此，除了過高的成本與技術未臻成熟等不利因素外，單靠它無法全面確保上一節提及的網路安全 4 大基石，機密性、身分認證、資料完整性及不可否認性。

另一方面，後量子密碼學解決方案具有的優點為，因其未改變現有的網路安全架構，僅取代核心密碼演算法，因此能無縫地接軌既有的網路安全機制。但其缺點是，無法透過量子電腦實作檢驗後量子密碼安全強度，所以需要透過公開相關演算法讓公眾檢驗，以尋找公認量子電腦無法有效解決的計算難題。

因此，早在 2016 年美國國家標準與技術研究院(National Institute of Standards and Technology，NIST)便舉辦後量子密碼標準草案競賽，目前進入第四輪的候選演算法，分別為 CRYSTALS-KYBER 等 5 個公開金鑰加密演算

法，與 CRYSTALS-Dilithium 等 3 個簽章演算法，並預計在 2024 年前公佈結果，以利各界檢驗安全性並及早擬定轉換計畫。綜而言之，後量子密碼學才是較為有效且經濟的抵抗量子破密攻擊之完整解決方案。

二、過渡時期的緩解措施

根據歷史經驗，過去全世界為了提高資訊安全，共花費了超過 20 年的時間，才轉換至安全性較高的 SHA1 與 AES 加密演算法。如今在後量子密碼系統公開檢驗完成並確立前的空窗期，面對著 2031 年可能發生的量子破密衝擊，仍應及早開始規劃轉換作法並採取緩解措施。

有鑒於此，歐盟旗下的網路安全機構 ENISA(The European Union Agency for Cybersecurity)研究報告指出，若有需要保留 10 年以上的機敏資料，現在就要採取量子破密衝擊緩解措施，以避免先蒐集後破解攻擊，相關建議的緩解措施有 2 種方法，分別如下(Ward Beullens et al. (2021))：

(一)採取混合式加密方式，也就是在傳統加密公鑰加密之外，再多做 1 次後量子加密候選演算法加密，雙重確保資料的安全。

(二)另一種做法是在通訊連線對話密鑰(session key)產生的時候，除了公開金鑰密碼系統之外，並在產生函數內多放入 1 個共享密鑰(Pre-Shared Key，PSK)，這個 PSK 初始時是透過線下(offline)取得的，並在每次連線對話(session)結束後更新這個 PSK。

三、後量子密碼系統轉換作法

由於量子電腦的發展是一個漫長且動態的過程，相關的網路安全標準也將隨之演進，因此，在建置或升級資訊服務系統，又或是採購資訊設備時，需要考慮是否具備加密捷變性(Cryptographic Agility，Crypto-Agility)；換言

之，實作或使用相關的加密協定與標準時，要考量能同時支援多個基礎與進階的加密演算法，以便無需耗費太多人力便能輕鬆地移轉至類似的加密演算法，如此方能有利於後量子密碼移轉(Post-quantum Cryptography Migration)作業。

關於如何進行後量子密碼移轉工作，負責美國金融業者摩根大通銀行(JPMorgan Chase)面對新興科技資訊安全的執行董事 Yassir Nawaz，在 NIST 於 2020 年舉辦的後量子密碼移轉工作坊上，建議全球金融機構進行後量子密碼轉換時，可採行下列 4 階段(Yassir Nawaz (2020))：

(一)資料盤點：透過資料盤點，鑑別出高風險資料

(二)轉換前置作業：建立加密系統使用端與提供端的捷變性，並評估市面可行的後量子密碼系統解決方案，以利後續轉換。

(三)轉換作業：確認並建立後量子密碼標準後，由高風險資料至低風險資料依序開始轉換。

(四)棄用過時加密系統：逐步棄用傳統的加密系統。

捌、結語

網路安全所需要注意的面向廣泛，非三言兩語能道盡，尤其是處在量子科技即將起飛的時代，新的變革帶來新的機會，也帶來新的威脅與不確定性，而企業組織由上至下均應以戒慎恐懼的心來面對。前面所述的資訊系統轉換，尤其需要來自高階管理階層的行動支持，方能順利進行，因此建議企業管理者參考以下 5 項行動方針，帶領組織全員動起來：

- 建立企業內部成員對量子破密的風險意識。
- 採取以加密捷變性為核心的加密系統治理原則。

- 評估組織內部資訊系統是否具備加密捷變性
- 適時了解最新的量子時代資訊安全標準。
- 持續維持好的網路衛生(Cyber Hygine)習慣。

相信只要能依以上 5 項方針確實執行，將有助於企業應對量子威脅，在未來進入量子時代時，更有能力接受更嚴峻的網路安全挑戰。

參考文獻

Paul Benioff (1980), “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines,” Journal of Statistical Physics, 22(5), 563–591.

Yu. I. Manin (1980), “Vychislimoe i nevychislimoe,” Sov.Radio, 13–15.

R. Feynman (1982), “Simulating physics with computers,” Internat. J. Theoret. Phys. 21, 467–488.

D. Deutsch (1985), “Quantum theory, the Church–Turing principle and the universal quantum computer,” Proc. Roy. Soc. London Ser. A 400, 96–117.

Frank Arute et al. (2019), “Quantum supremacy using a programmable superconducting processor,” Nature, 574(7779), 505–10,

John Preskill.(2018). “Quantum computing in the NISQ era and beyond,”. Quantum, 2, p.79.

Philipp Gerbert and Frank Ruess (2018), “The next decade in quantum computing—and how to play”, Boston Consulting Group.

OIDA (2020), “OIDA QUANTUM PHOTONICS ROADMAP”, OSA Industry Development Associates.

Jean-François Bobier et al.(2021). What Happens When ‘If’ Turns to ‘When’ in Quantum Computing? Boston Consulting Group. Available at: https://www.bcg.com/publications/2021/building-quantum-advantage

Eric Mounier (2021). Quantum Technologies 2021 report. Yole Développement. Available at: https://www.i-micronews.com/products/quantum-technologies-2021/?utm_source=PR&utm_medium=email&utm_campaign=PR_QUANTUM_TECHNOLOGIES_YOLE_June2021.

McKinsey & Company (2021), “Quantum computing: An emerging ecosystem and industry use cases”.

Jonathan Ruane et al. (2022), “Quantum computing for business leaders,” HBR. Jan-Feb issue.

Markus Reiher et al. (2017), “Elucidating reaction mechanisms on quantum computers,” Proceedings of the national academy of sciences, 114(29), 7555-7560.

Craig Gidney and Martin Ekerå (2021), “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” Quantum, 5, 433.

Yudong Cao et al. (2018), “Potential of quantum computing for drug discovery,” IBM Journal of Research and Development, 62(6), 6-1.

Junde Li et al. (2021), “Drug discovery approaches using quantum machine learning,” In 2021 58th ACM/IEEE Design Automation Conference (DAC) (pp. 1356-1359). IEEE.

Michele Mosca (2018), “Cybersecurity in an era with quantum computers: will we be ready?,” IEEE Security & Privacy, 16(5), 38-41.

Deborah Golden et al. (2021). Preparing the trusted internet for the age of quantum computing. Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/topics/cyber-risk/crypto-agility-quantum-computing-security.html.

Lucian Comandar et al. (2021). Ensuring Online Security in a Quantum Future. Boston Consulting Group. Available at: https://www.bcg.com/publications/2021/quantum-computing-encryption-security.

NSA/CSS. Post-Quantum Cybersecurity Resources. The National Security Agency/Central Security Service. Available at: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

Ward Beullens et al. (2021). Post-Quantum Cryptography: Current state and quantum mitigation. The European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

Yassir Nawaz (2020). Post-Quantum Crypto Transition for Global Financial Institutions. Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms. NIST. Available at: https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf