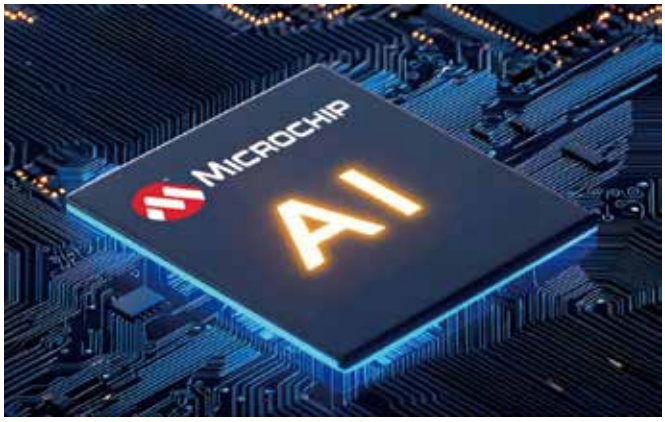
2026 年的 Edge AI：

打造更智慧、更即時回應的邊緣智慧系統

■作者：Nilam Ruparelia/
Microchip Technology Edge AI 事業部副總監

前言



隨著 AI 持續快速發展，2026 年正逐漸成為 Edge AI 發展的重要里程碑。歷經多年以雲端為核心的 AI 訓練與推論快速演進後，產業正迎來一個關鍵轉折點。越來越多高效能 AI 運算開始從雲端移轉至網路邊緣，部署於必須兼顧低延遲、低功耗、有限連線能力及成本限制的各類系統之中。

這並非只是技術上的漸進式演進，而是工程師設計新一代產品、系統與基礎設施時，在分散式智慧架構上的重大轉變。

以高能量電力開關中的電弧故障 (Arc Fault) 偵測為例，尤其是住宅、商業與工業場所常見的室內斷路器。此類應用最大的挑戰，在於必須及時偵測可能發生的電弧故障，迅速使斷路器跳脫，以避免火災發生。然而，傳統傳統以門檻值為基礎的判斷方式，在充滿電氣雜訊的環境中往往容易產生大量誤判，導致實務上難以採用。若改採 AI 為基礎的觸發偵測方法，則可在維持極低漏判率的同時，大幅降低誤判率，打造更實用且更有效率的安全防護系統，最終提升人員安全。

Edge AI 對系統設計代表什麼？

Edge AI 是指將人工智慧運算直接部署於資料來源所在的設備，或靠近資料來源的位置進行處理，而非完全依賴遠端雲端資料中心。當 AI 推論更貼近資料產生的位置時，系統便能獲得即時反應能力、更完善的資料隱私保護，以及降低對持續網路連線的依賴。

這些能力使系統能在毫秒等級完成決策，而非等待數秒鐘才能取得結果，這已成為許多工業與嵌入式應用不可或缺的設計需求。

從工廠自動化到安全關鍵監控系統，即時模式辨識與決策能力已成為系統設計的重要考量。因此，系統必須具備能在本地端運作的智慧，能夠理解環境脈絡，並在雲端連線中斷或不穩定時，仍能維持穩定的運作效能。

推動 Edge AI 發展的工程設計因素

促使工程師採用 Edge AI

的原因，主要來自數項同時發展的重要趨勢。

1. 延遲與可預測性

延遲一直是真實世界即時系統的重要限制因素。當 AI 模型直接在 Edge 端執行，而非依賴雲端運算時，可完全消除資料往返雲端所造成的網路延遲。對於語音指令辨識、即時異常偵測，以及高精度控制迴路等應用而言，可預測且一致的反應時間已不再只是加分項，而是系統設計的基本要求。

以前述電弧故障偵測為例，延遲與可預測性對於安全系統的重要性不言而喻。然而，其他應用領域同樣面臨類似需求。例如，協助型機器人的語音人機介面，或機場自助服務機 (Kiosk) 的手勢操作介面，若系統反應速度過慢或每次反應時間不一致，都會明顯影響使用體驗。因此，在這類應用中，將 AI 推論直接部署於設備端，往往是產品成功的關鍵。

2. 功耗與能源限制

嵌入式平台通常受到嚴格的功耗與能源限制。若要在固定的能源預算內完成 AI 推論，必須在運算能力、演算法效率以及硬體選擇之間取得平衡。因此，工程師在設計時必須確保系統能長時間維持高效率運作，同時符合分散式系統常見的供電能力與封裝限制。

3. 資料隱私與安全

將 AI 運算保留於本地端，可大幅減少敏感資料透過網路傳輸的需求，進而降低資料隱私與資訊安全風險。對於涉及個人資料、營運資訊或安全關鍵資料的系統而言，在設備端完成 AI 推論，可有效降低資料外流風險，同時仍能提供具價值的分析結果。

例如，一套可偵測並統計飯店客房、會議室或餐廳內人數的智慧感測系統，能提供許多有價值的營運分析資訊。然而，只要存在任何個人隱私遭到侵犯的疑慮，就可能使整個應用難以被市場接受。因此，所有資料皆在設備端完成分析、不需上傳雲端的系統架構，便成為此類應用得以落實的重要關鍵。

4. 資源效率與可擴充性

當系統部署規模達到數千甚至數百萬個終端設備時，若所有原始資料都傳送至雲端，再由中央系統執行 AI 推論，所產生的通訊成本與運算負擔將相當可觀。Edge AI 可在設備端先完成資料篩選、轉換與決策，只需將重要的分析摘要或警示資訊回傳至中央系統，大幅降低網路頻寬需求與雲端運算負載。

推動設計創新的 Edge AI 應用

目前，各產業的 Edge AI 已逐漸從概念驗證 (Pilot Program) 邁向大規模量產部署，並開始改變傳統的系統設計方式。

工業系統

預測性維護與異常偵測如今可直接在設備端完成，不僅能降低非預期停機時間，也能即時調整設備運作狀態，而無須依賴遠端分析平台。

汽車與運輸

車內乘員偵測正逐漸成為 Edge AI 的重要應用之一。此類系統必須能即時且可靠地偵測車內是否有乘客，包括遺留在後座的兒童，同時不依賴雲端連線。透過設備端 AI，系統可利用影像、雷達或聲學資料持續進行監測，在保障個人隱私的同時，也能確保系統具備可預測且一致的反應時間。這類設計著重於安全性、低功耗以及安全的本地端資料處理能力，並能完整整合至車輛的嵌入式系統架構中。

消費性電子與 IoT 設備

能在本地端理解語音、手勢及周遭環境資訊的智慧設備，不僅可提供更流暢自然的使用

圖說：應用領域 – 消費性電子

圖說：應用領域 – 基礎設施與能源

體驗，也有助於延長電池續航力，同時提升資料隱私保護。

基礎設施與能源

電網、公用事業及智慧城市中的分散式設備，可透過本地端 AI 即時進行負載平衡、偵測危險電弧故障 (Arc Fault)，並最佳化系統效能，而不致造成通訊網路過度負荷。

從上述各種應用可以看出一項共同趨勢：系統對即時智慧的需求愈高，AI 就愈需要部署在接近資料來源的位置。

2026 年及未來 的 Edge AI 設計考量

將 AI 導入 Edge 端雖然帶來許多優勢，但也增加了系統設計的複雜度。除了硬體設計與系統部署之外，AI 的開發還需要建立完整的資料蒐集與模型訓練流程，而且這不僅是開發初期的工作，更需要在產品生命週期中持續進行。為了建立有效的 AI 模型，工程團隊必須蒐集足夠多元且具有代表性的資料，並透過反覆驗證與調整持續改善模型品質。這樣的開發流程，與傳統嵌入式系統開發有著明顯不同。

然而，當資料蒐集與模型訓練成為工程開發流程的一部分後，許多企業發現，不僅能打造更具實用性的 AI 系統，也能降低整體開發成本，進一步提升產品價值。

除了資料策略之外，工程師還需面對記憶體容量有限、異質運算架構，以及如何將模型訓練與高效率 AI 推論部署串接起來的開發工具鏈等挑戰。因此，一套完整的 Edge AI 開發流程，除了必須分析系統在真實運作環境下的效能表現、驗證 AI 模型在各種限制條件下的行為之外，也需要將 AI 開發流程與既有的嵌入式軟硬體架構緊密整合。

在此情況下，運算平台架構與開發生態系的選擇便顯得格外重要。具備完整效能選擇、完善安全機制以及長期產品供應能力的平台，可協助設計人員兼顧目前產品需求與未來產品規畫。此外，整合最佳化、效能分析 (Profiling) 及除錯功能的開發流程，也能協助工程團隊加快產品上市時程。

結論

2026 年的 Edge AI 已不再只是熱門關鍵字，而是打造新一代智慧系統的重要設計策略。對於需要快速反應、在有限資源下穩定運作，並希望在不增加網路與中央基礎設施負擔的情況下提供差異化效能的系統而言，Edge AI 已成為不可或缺的關鍵技術。

透過將 AI 部署於更接近資料產生的位置，工程師正重新定義分散式系統所能實現的能力，也為各行各業建立更即時、更高效率且更安全的智慧系統新標準。 CTA

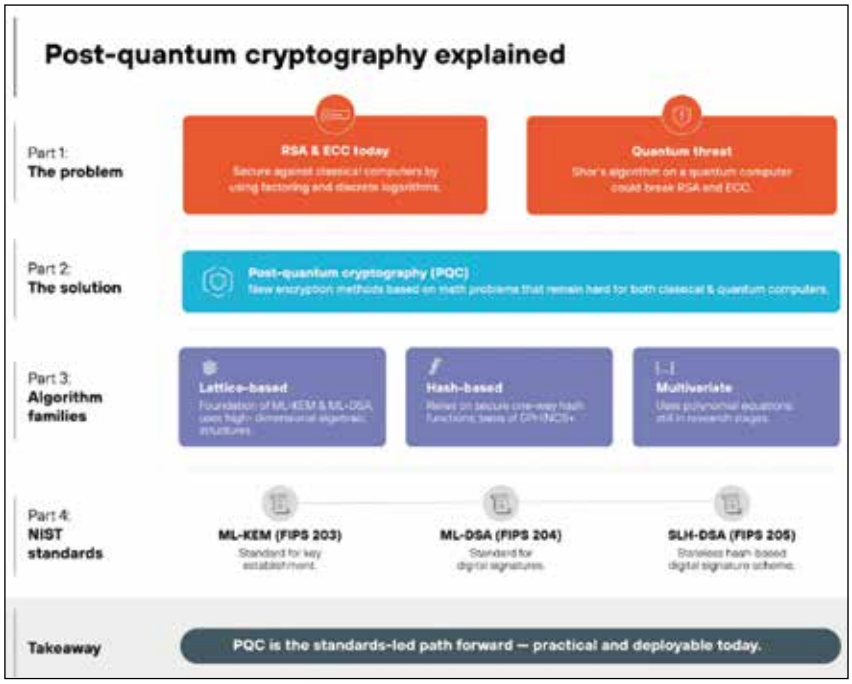
迎戰量子時代：金融科技的防禦與轉型藍圖

■文：任芷萍 Anita Ren

2026 年 6 月中旬，全球資安、金融與高科技製造業接連迎來兩場重磅政策撞擊。先是台灣金融監督管理委員會 (金管會) 於 6 月 18 日正式發佈《金融業後量子密碼遷移參考指引》；緊接著在 6 月 22 日，美國總統簽署第 14412 號行政命令《保護國家免受先進密碼學攻擊》(Securing the Nation Against Advanced Cryptographic Attacks)。

這兩項在四天內密集出台的國家級法規，宣告了一項無可爭議的事實：後量子密碼 (Post-Quantum Cryptography, PQC) 已正式揮別學術論辯，全面躍升為全球供應鏈與金融科技 (FinTech) 最迫切的基礎建設工程。

圖 1：PQC vs. 量子密碼學 —— 基於數學的軟體解決方案 vs. 基於物理的量子彈性硬體要求的比較



資料來源：https://www.paloaltonetworks.com/cyberpedia/pqc-standards

2026 年數位金融的底層主權防線

這場變革的底層邏輯，源於美國國家標準暨技術研究院 (NIST) 在 2024 年發佈的三項後量子密碼標準 (FIPS 203/204/205)，正式將 ML-KEM、ML-DSA 與 SLH-DSA 納入聯邦資訊處理標準。到了 2026 年，這場技術革命的指針已走向「強制合規與主權防禦」的深水區。

根據國際資調機構的最新數據，全球 PQC 市場規模在 2026 年已達 22 億美元，並預計以接近 38% 的年複合成長率 (CAGR)，在 2033 ～ 2034 年前飆升至近 300 億美元！這項驚人的產值爆發背後，代表著密碼學已不再只是軟體層面的翻修，而是演變成一場向下解構半導體晶片硬體、向上重組跨國系統整合商 (SI) 架構、並仰賴人工智慧與加速計算 (Accelerated Computing) 全面進行效能補償的產業海嘯。

從金融科技的視角來看，現代數位金融體系的基石——無論是行動支付、網銀傳輸、數位憑證、高頻交易、零信任架構 (Zero Trust Architecture)，還是自動化機器身份驗證 (mTLS)，其安全根基完全建立在傳統非對稱加密演算法 (如 RSA 或 ECC) 之上。

2026 上半年關鍵時間線：全球政策的剛性交匯

當量子計算的威脅從理論走向剛性時間表，金融機構若未能及時完成密碼架構的重新編排，其所面臨的將不是單一系統的外洩，而是整個金融生態系數位信任體系的總體崩潰。

從華盛頓的戰略合規到台北的金融防線，2026 上半年的政策時程表以極高的密度向前推進，迫使金融機構與金融科技業者將「量子安全」排入近五年的核心資本支出預算中。

美國：行政命令與「量子鐵幕」的築起

美國在 2026 年 6 月 22 日簽署的第 14412 號行政命令，其影響範圍遠超美國聯邦機構本身，而是透過《聯邦採購法規》(FAR) 與國防工業體系 (DIB) 的剛性制約，在國際科技產業與跨境金融清算體系間築起一道不容迴避的「量子鐵幕」。

圖 2：美國第 14412 號行政命令重點概述

資料來源：https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/；筆者整理製作

白宮在行政命令公告中明確宣示：「大型量子電腦的到來，特別是落入敵手時，將對現行廣泛使用的密碼安全系統構成重大威脅。敵手正在積極收集並儲存美國的敏感資訊，等待未來量子電腦成熟後再行解密。因此，美國必須立即強化敏感數據、關鍵基礎設施與數位經濟的密碼防禦。」

該命令明確規範了兩大戰略檢驗點：

- 2030 年底前：所有關鍵資產與聯邦供應商，必須全面完成量子安全的金鑰交換機制升級。
- 2031 年底前：完成所有數位簽章系統的全面替換，未能實作標準 PQC 的供應商將面臨被排除於美國政府採購清單之外的風險。

對此，全球雲端基礎設施與網路安全龍頭 Cloudflare 的 PQC 遷移技術團隊隨即發表聲明回應：白宮這項全新的行政命令正式將 PQC 遷移定調為美國的國家政策。對於所有向聯邦政府提供服務的科技供應商而言，實作後量子密碼不再是一個可有可無的「安全加分項」，而是繼續在美國市場做生意的「剛性准入條件」。

台灣：從跨部會指引到金融防禦前線

台灣在這一波全球遷移浪潮中並未缺席。數位發展部在 2025 年 4 月推出台灣首版《後量子密碼遷移指引》後，資策會執行長范俊逸在 2026 年 5 月

的台灣資安大會上特別示警：量子電腦足以破解現行加密演算法的「Q-Day」預計將提前至 2030 年左右。

凡涉及非對稱加密或數位簽章的系統，均可能在受威脅影響的範圍之列。組織必須趁此遷移機會，重新檢視密碼機制與協定，全面提升資安韌性。因應此威脅，金管會依據「金融資安韌性發展藍圖」，於 2026 年 6 月 18 日正式向全台金融機構發佈《金融業後量子密碼遷移參考指引》。

這份規範正式將金融基礎設施的底層全面替換期限設定在 2035 年前，並訂定了清晰的三階段打底與實作藍圖：

■2026 ～ 2027 年政策指引與防線打底：金融機構須在內部建立治理架構，由董事會或高階管理層指定權責主管，並完成第一輪加密資產盤點 (CBOM，密碼軟體清單)，著手強化加密敏捷性基礎。

■2027 ～ 2029 場域試辦與跨機構測試：啓動核心基礎設施升級。由證交所、財金公司及聯卡中心等「樞紐機構」先行，運作跨機構協作機制，並於特定金融場域進行 PQC 演算法的雙軌驗證與壓力測試。

■2035 年前高風險系統中長期遷移：依據量子風險評分與系統複雜度進行分期分流切換，全面汰換 RSA 與 ECC 等量子脆弱演算法，達成金融生態系的全面量子安全。

金融科技的深層衝擊：雙重危機與生態系連鎖反應

金管會一針見血地指出金融業目前面臨的治理難題：盤點工作不應追求一次性作完，而應以風險導向，建立加密資產清單 (CBOM)，避免未來第二次、第三次遷移時要從頭再來。金融業應掌握國際密碼標準發展，循序推動關鍵系統盤點、風險評估及遷移準備，降低潛在風險。林裕泰處長所提及的風險，主要包含兩大金融科技界公認的底層危機：

■「先獲取後解密」(Harvest Now, Decrypt Later,

圖 3：《金融業後量子密碼遷移參考指引》建議推動時程

資料來源：https://www.fsc.gov.tw；筆者整理製作

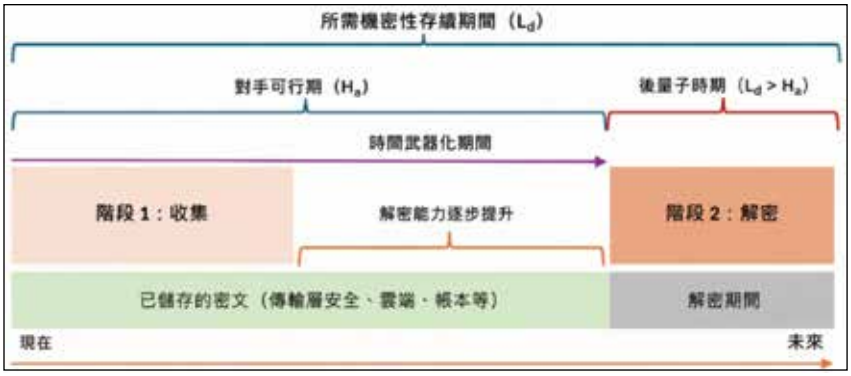
HNDL)：駭客現階段雖受限於硬體，無法立刻破解傳輸內容，但正透過網際網路節點大量側錄並儲存金融機構、證券交易、跨境清算系統間的加密封包。一旦 2030 年前後實用化量子電腦問世，這些涉及歷史客戶隱私、大額資金流向、國際戰略合約的機密資料將在瞬間被迫裸奔。這意味著長生命週期的金融資產，在 2026 年就已經處於「被預先攻擊」的狀態。

■「現在信任、未來偽造」(Trust Now, Forge Later, TNFL)：由於傳統數位簽章與憑證在量子算力面前變得脆弱，駭客未來可以輕易偽造具有法律效益的電子簽章與虛擬銀行憑證。若不提早佈建 PQC 機制，未來的自動化金融指令、區塊鏈智能合約驗證將完全失靈，破壞整體金融市場的「非否認性」(Non-repudiation) 基礎。

金融服務高度仰賴跨機構生態系的交織，例如一次簡單的跨行轉帳，後端就涉及個別銀行、網銀前端 App、財金公司、聯卡中心以及第三方服務供應商 (TSP)。這種高度依存的生態系意味著「安全取決於最弱的一環」。

若整條金融科技傳輸鏈中，有任何一個非銀行業者的 API 節點未能同步完成 PQC 裝配，整條傳輸鏈結就會出現致命的安全破口，這也迫使資訊進口商與跨國系統整合商必須提供立即的架構解決方案。

圖 4：「先獲取後解密」攻擊的時間線，突顯了密文收集、不斷增長的解密能力與敵對力量超過機密性生命週期之間的差距



資料來源：https://www.mdpi.com/2673-4001/6/4/100

硬體底層的重塑：半導體產業的運算革命

當法規將 PQC 從「研發選項」變成「剛性需求」，這股壓力立刻沿著供應鏈回溯到台灣最核心的半導體產業。對於 IC 設計、硬體安全模組 (HSM) 以及晶圓代工業者而言，PQC 的導入絕非僅是軟體改版，它帶來的是硬體晶片架構的物理極限挑戰。

國際車用半導體龍頭恩智浦 (NXP Semiconductors) 晶片資安架構技術主管在技術研討會上坦言：目前絕大多數設計中且正要部署的晶片解決方案，其使用壽命都會遠遠超過 2030 年。為確保系統在整個生命週期內的長效安全，我們必須從現在開始，將 PQC 視為晶片硬體架構設計的基礎必備元素。對於晶片廠商而言，這直接關係到產品的生命週期與存續，否則在量子電腦成熟那天將毫無防禦能力。

1. 記憶體與頻寬的「膨脹危機」

傳統的 ECC 金鑰大小通常只有 256 位元 (bits)，然而 NIST 所標準化的 PQC 演算法 (如 ML-KEM)，其金鑰與密文大小動輒達到數千位元組 (Bytes)，暴增數十倍之多。在先進製程下，SRAM 的微縮難度 (Scaling Wall) 遠高於邏輯電路。安全核心內 SRAM 面積暴增 8 ～ 10 倍，會直接擠壓到晶片其他功能模組的空間，大幅拉高每顆晶片的晶圓製造成本與不良率風險。在物聯網 (IoT) 邊緣端或車聯網 (V2X) 晶片中，傳輸一個 3.3KB 的 ML-DSA

簽章，會導致晶片內部匯流排 (AXI/AHB) 必須連續霸佔數十個至數百個時脈週期進行內部搬移，造成嚴重的內部頻寬堵塞與訊號延遲。

2. 算力黑洞與功耗挑戰

密碼學涉及極為龐大且複雜的多項式矩陣運算。如果缺乏硬體加速，純靠軟體在微控制器 (MCU) 的 CPU 核心上執行，將導致系統運算時間拉長數百倍。頻繁的邏輯閘切換會使動態功耗急遽上升；而如果晶片內 SRAM 空間不足，被迫將中間運算資料置換到晶片外的 DRAM，其存取功耗更會暴增 100 到 1,000 倍，這對依靠電池供電的邊緣物聯網裝置無疑是災難。

為了在限制嚴苛的硬體環境下實現 PQC，全球半導體界與安全 IP 大廠目前主要採用以下硬體加速解決方案：

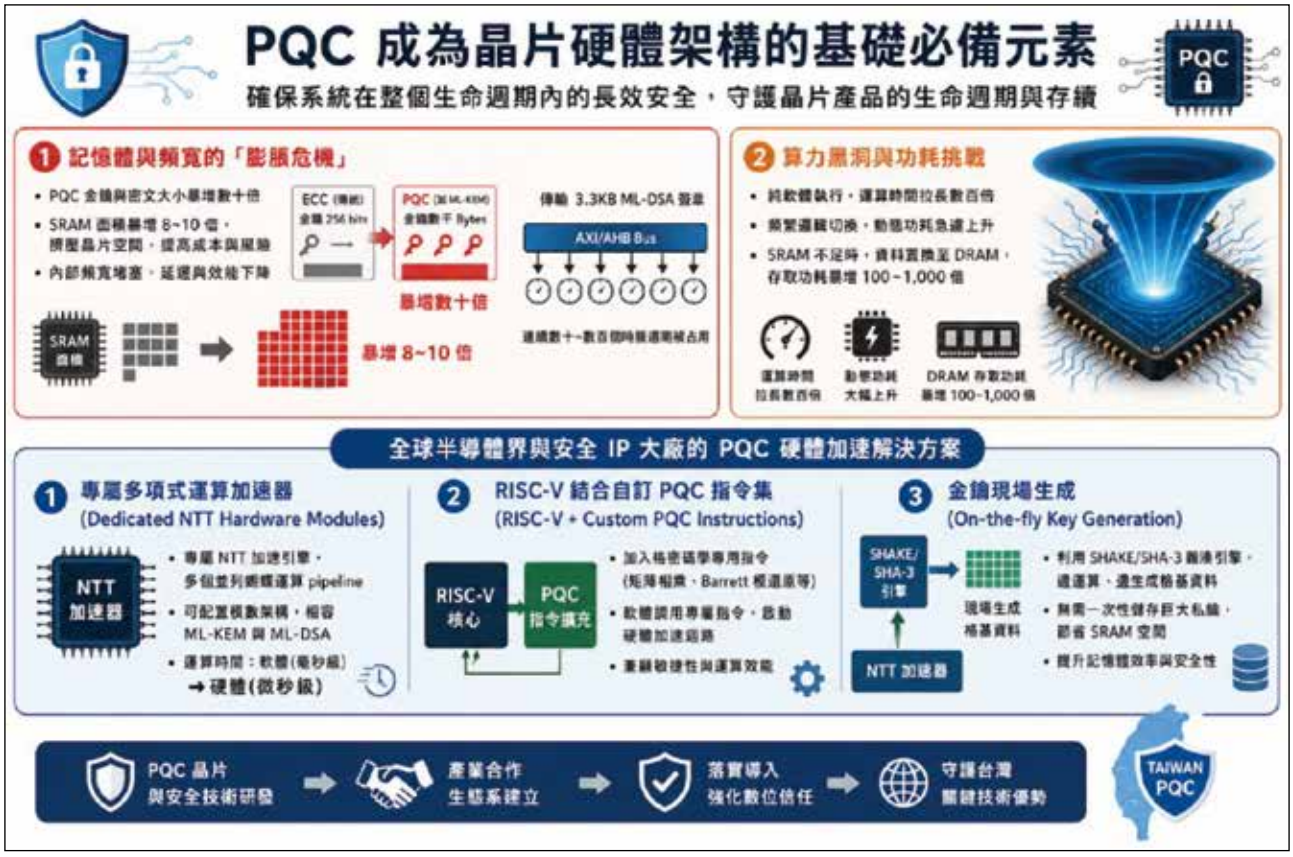
1. 專屬多項式運算加速器 (Dedicated NTT Hardware Modules)：

在晶片內直接設計專屬的硬體 NTT 加速引擎，配置多個並列的蝴蝶運算 pipeline。由於 ML-KEM 與 ML-DSA 所使用的質數模數不同，硬體加速器被設計成可配置模數的架構，單一硬體電路即可相容兩種演算法，將運算時間從軟體的毫秒級縮短至硬體的微秒級。

2.RISC-V 結合自訂 PQC 指令集：

在標準的 RISC-V 處理器核心旁，加入專門針對格密碼學設計的向量擴充指令 (如矩陣相乘、Barrett 模還原演算法)，軟體只需調用專屬的組合語言指令，就能啓動底層硬體加速迴路，兼顧了敏捷性與運算效能。

圖 5：PQC 晶片安全新挑戰與解決方案



資料來源：筆者整理製作

3. 金鑰現場生成 (On-the-fly Key Generation)：

為了節省 SRAM 空間，硬體加速器不再一次性將巨大的私鑰完全展開儲存在記憶體中，而是利用內建的 SHAKE/SHA-3 雜湊函數引擎，在需要用到特定矩陣列時「邊運算、邊現場生成」對應的格基 (Lattice Base) 資料。

鴻海研究院執行長暨後量子資安產業聯盟 (PQC-CIA) 召集人李維斌，在產學發表會上，點出了台灣半導體在地緣政治下的防禦定位：「隨著量子計算技術的進步，傳統加密技術面臨前所未有的挑戰，後量子加密技術已成為保障高科技製造安全的重要防線。台灣在其中擁有關鍵角色，後量子資安產業聯盟將持續推動 PQC 晶片與安全解決方案研發，協助我國企業落實 PQC 導入，強化整體供應鏈的數位信任基礎。」

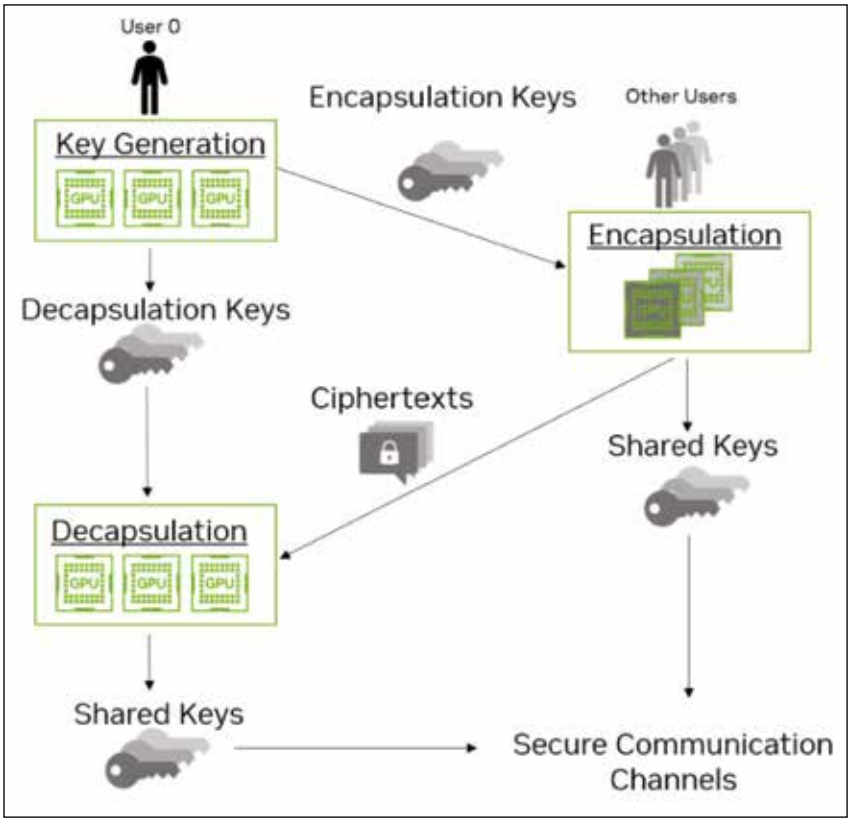
雲端與資料中心的效能救星：NVIDIA 的加速密碼學與超大規模部署

當 PQC 從邊緣端走向超大規模 (Hyper-scale) 雲端資料中心與金融交易高頻伺服器時，激增的密碼運算流量立刻成為傳統 CPU 的算力黑洞。引入複雜的 PQC 計算會嚴重拖慢傳輸層安全性協定 (TLS) 的握手速度，進而威脅到高吞吐量雲端基礎設施與高頻交易系統的穩定性。

為解決資料中心全面 PQC 化後的效能驟降危機，晶片龍頭 NVIDIA 推出了專為 GPU 加速後量子密碼工作負載打造的軟體開發套件——NVIDIA cuPQC SDK。NVIDIA 的資深密碼學運算核心團隊在 cuPQC 的架構發佈白皮書中揭露：量子計算的到來迫使全球密碼學景觀發生根本性改變。這種向新型抗量子演算法的遷移，對高吞吐量與低延遲環境 (如電信、金融服務及雲端基礎設施) 帶來了極其嚴苛的硬體效能挑戰。

NVIDIA cuPQC SDK 旨在利用 GPU 的大規模並行處理能力，將安全性與實用性完美縫合，協助全球組織在不犧牲業務系統效能的前提下，無縫切換至下一代安全協定。」專屬晶片與通用 GPU 的技術分工在後量子密碼學的落地實踐中，專屬硬體加速晶片 (ASIC/FPGA) 與通用 GPU (如 NVIDIA cuPQC) 代表了兩種截然不同的計算哲學；前者追求「極致的專用與低能耗」，後者則專注於「大規模並行與軟

圖 6：標準批次金鑰封裝機制可利用 GPU 進行加速和平行化



資料來源：https://developer.nvidia.com/blog/introducing-nvidia-cupqc-for-gpu-accelerated-post-quantum-cryptography/

體敏捷性」。

落地實踐的樞紐：SI 的金融架構重組

在半導體廠與晶片巨頭提供底層算力、政府提供法規指引後，真正負責在軟硬體交界處將這兩者縫合在一起、推動金融機構核心系統安全落地的，就是系統整合商 (SI)。由於 PQC 封包體積大幅膨脹、運算資源需求暴增，舊有的軟體防火牆、反向代理伺服器 (Reverse Proxy) 與負載均衡器 (Load Balancer) 若沒有經過系統整合商的整體架構重組，直接硬切換的結果就是引發全公司網路集體斷線與系統崩潰。

台灣在地金融 SI 大廠針對系統實務落地給出關鍵性修補與重構建議：金融機構與企業架構高度複雜且碎片化，企業應建立「加密敏捷性」(Cryptographic Agility) 評估指標，強化系統切換演算法的能力，在系統自然演進與汰換的歷程中，逐步導入混合式過渡 (Hybrid) 架構，才能確保業務不中斷。

為協助金融機構安全度過遷移陣痛，系統整合商與組織架構師必須依據以下兩大技術支柱，具體重構既有資訊軟體系統：

■支柱一：如何具體落實金融加密資產盤點 (CBOM) CBOM 是仿照軟體物料清單 (SBOM) 的概念，專門針對系統內所有加密演算法、金鑰、憑證、協定與加解密組件的結構化清單。落實 CBOM 盤點並非人工翻查程式碼，而是需要建立自動化、標準化的維運流程。

■支柱二：既有軟體系統中「密碼敏捷性」架構規劃如果系統在盤點後發現需要更換演算法，卻必須重寫程式碼，

表：NIST PQC 演算法比較

資料來源：美國國家標準暨技術研究院 (NIST)，筆者整理製作

代表系統缺乏「密碼敏捷性」。重構既有系統時，應採用「解耦、模組化、可配置」的架構設計。

2026 年之後的全球金融科技新秩序

工業電腦與系統大廠也積極卡位這波硬體轉型。例如工業電腦大廠新漢 (NEXCOM) 在 2026 年的世界行動通訊大會 (MWC 2026) 上，正式發表了全新一代 PQC 邊緣運算資安平台，將抗量子防禦網從雲端中心機房，透過系統整合商與軟硬體協同，一路延伸佈建到金融臨櫃、企業邊緣端與 6G 電信基地台。

2024 年，NIST 給出了演算法的終極標準；2026 年，美台兩國政府拍板了剛性的合規時間表。後量子密碼遷移已經跨越了純粹的資安防護範疇。從金融科技的視角審視，這是一場由地緣政治法規與金融監理全面發動、經由系統整合商在軟硬體交界處進行架構重組、結合 NVIDIA GPU 進行超大規模算力補償、最終落腳於半導體晶片底層矽智財 (IP) 革命的跨界立體聯防。

對全球金融科技產業、系統商、半導體大廠以及金融機構來說，PQC 已不再是一個帶有科幻與長遠色彩的風險選項，而是一項正在發生、牽動數千億元全球數位基礎建設更迭的強制性工程專案。

未來五至十年的數位信任保衛戰，將取決於金融機構本身的密碼敏捷性架構、IC 設計廠的硬體加速晶片量產速度、以及資料中心對加速密碼學軟體棧的適配能力。在這場全面洗牌的過程中，掌握全球晶片製造命脈與軟硬體整合關鍵節點的台灣，無疑正站在這場量子風暴最核心的戰略制高點。

(筆者現為 FinTech 從業工作者) CTA

恩智浦攜手大聯大世平與成功大學推動 Edge AI 機器人應用開發力

恩智浦半導體 (NXP) 再度攜手半導體零組件及研發支援通路商大聯大世平集團，參與由國際工程與科技學會 (IET) 台北分會主辦，國立成功大學工程科學系與國立成功大學敏求智慧運算學院合作的「Race to Robot — NXP Edge AI 應用工作坊」，以「從構想到開發」為題，於 7 月 24 日在國立成功大學旺宏館舉辦，吸引全台 13 所大專校院近 60 名學生參與，透過機器人應用開發為核心，引導學生從真實問題發想使用者情境。

本次活動透過恩智浦 i.MX 93 FRDM 作為主要開發平台，內建 NPU 可支援低功耗 Edge AI 推論，並整合多元感測介面，可廣泛應用於智慧視覺、自主移動、環境感知等機器人場景，讓學生能以業界級裝置進行系統設計，並在恩智浦與大聯大世平集團工程師的引導下，逐項檢視系統架構、感測整合與 Edge AI 推論流程等關鍵設計，進一步強化解決問題與系統整合的能力。

參與「Race to Robot — NXP Edge AI 應用工作坊」的學子，分別來自國立成功大學、國立清華大學、國立臺灣科技大學、國立臺北科技大學、國立虎尾科技大學、南臺科技大學、國立中央大學、國立中興大學、元智大學、國立高雄大學、國立雲林科技大學、國立彰化師範大學及國立臺中科技大學等 13 所大專院校。

恩智浦並偕同大聯大世平集團，評選表現優異的團隊並頒發獎學金。本次共有 5 組隊伍獲獎，得獎作品分別為國立成功大學的「社區防淹水預警站」、國立成功大學「人形機器人的小腦」、國立臺灣科技大學「RoachHunter-93」、國立成功大學「睡眠感測床墊」、以及國立清華大學「步步高昇」。