張慶瑞專欄。

後量子密碼竟沒有量子？

文・圖／張慶瑞

2024年五月數位發展部成立「後量子資安產業聯盟」，許多人都困惑為什麼「量子資安聯盟」都還沒成立，就先成立「後量子資安聯盟」了？一般人由於對量子的陌生與畏懼感，另外也怕被嘲笑落伍與無知，並不敢問這個問題。在量子時代，各種奇怪的量子術語如雨後春筍出現，量子密碼學、量子加密、後量子密碼學、量子安全加密、量子證明加密、抗量子加密、量子安全等都是量子通訊與資安的方法，但正常人聽到『量子』兩字後都是滿頭問號，更何況是量子XX？這些名詞中，最容易混淆的就是量子密碼（Quantum Cryptography, QC）與後量子密碼（Post-Quantum Cryptography, PQC）這對難兄難弟，一個量子，一個是算法，一個物理為主，一個則以數學為主。PQC的出現更早於QC，所以量子密碼學界常見的笑話是「為什麼量子密碼（QC）都不存在，就開始研究後量子密碼（PQC）？」，還有一個類似笑話，「後量子密碼中竟沒有量子？」

要了解QC與PQC的差異，必先了解現在使用的古典密碼（Classical Cryptography, CC）。二戰時，各國的電報都會利用密碼本加密，收到同盟電報後就用密碼本解密，所以就算被攔截，敵人也無法了解含意。CC的訊息加密是依賴複雜數學，CC，PQC與QC的差別也在於不同來源與使用方法。

東西方由於文字特性不同，發展出不同加密方式。西方的拼音字母，用數學的一對一映射法即可加密，最出名的就是凱撒密碼。例如love，字母向右位移3個位置，就變成oryh，收訊者只要將轉換順序再左移3個位置，就了解原意。《福爾摩斯探案》中「跳舞小人」的暗號與密碼也是一對一映射的加密法。摩斯電碼將英文字母或數字，換成由「-」及「.」的組合來代表，由於永不變換，許多人並不認為是一種加密。

中國最早加密文書是姜子牙的陰符與陰書，陰符使用形狀大小各異的物件來代表不同意思，例如「大勝克敵符」，長1尺；「破陣擒將符」，長9寸等。陰書則採用『一合而再離，三發而一知』，把資訊分成三份，書寫在三枚竹簡上後分開運送。到達目的地再將三枚竹簡合而為一，讀取完整訊息。傳送過程中即使被敵方捕獲，由於只有部分資訊被截而不致洩漏。

中國古代加密方式有：

一、替代法：每一字元都換成另一字元或符號，類似於西方的凱薩密碼。

二、藏頭與藏尾法：藏頭與藏尾詩也是一種加密，但也可以藏在詩中任何位置上。例如『誰解**我**心愁，陽明**喜**重遊，觀音**歡**賞海，獨缺**你**同遊。』各句的第三字傳達『**我喜歡你**』的密文。

三、標示法：在平淡無奇的文書中，利用約定位置來傳達密文。標示方式也可以利用紙張上的摺痕，或先約定好的特定位置來溝通。

四、反切碼：戚繼光用「反切」來進行編碼，通常以兩首詩詞來加密。第一首是**聲母**詩，『柳邊求氣低，波他爭日時。鶯蒙語出喜，打掌與君知。』詩詞中的15個字分別編號為1-15。第二首則代表**韻母**，『春花香，秋山開，嘉賓歡歌須金杯，孤燈光輝燒銀缸。之東郊，過西橋，雞聲催初天，奇梅歪遮溝。』，詩歌的36字按順序編號為1-36。當時發聲有八種聲調，也依序編號為1-8。例如傳送密文的編號是“12-36-2”，12是聲母「蒙」字，36是韻母「溝」字，2是聲調的二聲。則“12-36-2”就很容易解讀為「謀」字。「反切」加密的優點是每次戰前可以隨時變化所用詩詞。

五、字驗法：打戰前約定好一首五言律詩，以唐代杜甫的《春望》為例。『國破山河在，城春草木深，感時花濺淚，恨別鳥驚心。烽火連三月，家書抵萬金，白頭搔更短，渾欲不勝簪。』如果軍隊在糧食將盡，前方從密碼本中查出「請糧料」的編碼是第九，而《春望》中的第九字是「**木**」。於是請糧將領就將「**木**」字寫到普通公文書牒中，並在「**木**」字上加蓋官章。指揮所收到公文後，看到蓋官章的「**木**」字，就知道急需糧食補給。每次作戰前，指定一首律詩作為密鑰，前後方據此進行加密通訊。

六、字謎法：將文字的內容打亂或隱射，即使被截取也無法了解內容。武則天時，徐敬業請駱賓王寫首童謠給裴炎：『一片火，兩片火，緋衣小兒當殿坐。』裴炎看後非常高興，立即回封信，只寫了「青鵝」兩字。官方截獲後大思不解，武則天卻猜出「青」就是「十二月」，「鵝」是「我自與」。意指裴炎告訴徐敬業可在十二月起兵叛變，我會於城中做內應，裴炎因此被殺，武則天並出兵擊敗徐敬業和駱賓王。武則天如果破解不了密文，駱賓王也不會因此不知所終，甚至可以做出更多超越「請看今日之域中，竟是誰家之天下」的驚世之作。駱賓王童謠中的兩片火就是炎，而緋衣就是裴，小兒當殿坐則是指裴炎的兒子要當皇帝，而使得裴炎立即同意參與叛變。這種中文特有加密後來演變成燈謎。

近來密碼專家分析135萬人的ATM密碼大數據資料後，發現有三種主要型態，(1)ABAB，例如0505, 1919 等；(2)使用者的生年，例如19xx，20xx等；(3)使用者的特殊日子，例如生日用1025、0916等。這可能因為銀行定期要求改變密碼，多次強迫疊代後就迴歸到這三大類的密碼誤區。

數學加密法在設定ATM四位密碼便不會迴歸到三大愚蠢組合區，例如使用四次方程式f(x)= (x-2)(x-1)(x+1)(x+3) 作為設定ATM密碼的多項式，當第一次設定密碼時代入6，就產生4579，要換密碼時就改成代入5，也就變成3468，容易使用而且不易破解。目前CC所使用的數學複雜度遠超過多項式，但基本原則就是要簡單加密而困難破解。CC可分為兩大類：對稱密碼術和非對稱（公鑰）密碼術。對稱加密常用於網路通訊端對端加密與手機硬體加密中，許多ATM卡、金融卡中也使用。非對稱加密則有主要有兩種：(1)採用ECC（橢圓曲線密碼學）作為數位簽章機制，例如區塊鏈與比特幣中。(2)採用 RSA 加密來確認使用者身分，例如政府自然人憑證以及金融體系中。目前RSA與ECC密碼都有容易檢驗而古典電腦無法破解的特性，但到2030年前後，量子電腦可能每試兩次就可破解一次，因此CC便將崩潰。對稱密碼就像個人信箱的開或關都是同一把鑰匙，非對稱密碼則提供公鑰給所有會員，但是又為每個會員打製一把專屬私鑰。就像圖1，在公共信件室內的個人信箱，任何有公鑰的人都可以進出公共信件室，放東西在任何信箱中，但只有私鑰可以打開個人信箱取出物件。

秀爾量子演算法（Shor algorithm）雖可破解RSA密碼，但目前仍沒有量子電腦可用來破解CC。但因為「現在收集、稍後解密」（Harvest now, decrypt later, HNDL）的資安顧慮，必須開始改變現用密碼。專家就提出格密碼學（Lattice-based cryptography）等數學方法來開發量子電腦也無法破解的PQC。美國NIST在2016年便啟動PQC標準化進程，2024年選定CRYSTAL-Kyber作為密鑰封裝機制（KEM），及另外三種加密方式，CRYSTAL-Dilithium，SPHINCS+和FALCON，作為用於數位簽章演算的國家標準。2024年八月更宣布聯邦資訊處理標準（FIPS），把上述四種依序重新命名為FIPS 203（ML-KEM）、FIPS 204（ML-DSA）與FIPS 205（SLH-DSA），第4個標準FIPS206（FN-DSA）將於年底推出。FIPS 203是通用加密類型，而其他三種則屬於數位簽章的主要標準。將全球密碼系統由CC換為PQC需要很長時間與龐大資源，NIST粗估僅美國聯邦機構至少就要71億美元，而全球移轉的開銷將更為驚人。預計到2035年，可以先將有長期資安顧慮的系統都轉移到PQC加密體系。

QC 與 PQC 完全無關，PQC利用數學難題來開發防禦量子電腦攻擊的加密方

圖1：(A) 對稱密碼就像是信箱的開與關都用同把鑰匙，發送雙方都可以打開信箱存取資訊，但也容易被有心者偷走與破解。特務007用私鑰開啟7號信箱，但駭客手上也有7號信箱鑰匙。(B)非對稱密碼就像只要有公鑰，任何人都可以使用信件室，但只有私鑰可以打開個人信箱取得訊息，保密性高且不易洩漏。由於除了私鑰，還多一把公鑰，非對稱密碼也稱為公鑰系統。特務007用公鑰打開信件室，駭客手上只有公鑰，但沒有007的私鑰，仍然無法竊取資料。插圖為大同大學何明果校長繪製。

案，QC則是利用量子物理來保障通信安全。古典通訊和量子加密通訊都使用光子傳遞訊息，但古典通訊中的訊號是由大量光子共同組成，也因為統計效應而消失量子特性。QC是編碼在單光子的量子態上，根據不可複製特性，如果有人竊取並試圖讀取訊息，量子態的改變會被發現。QC是用量子糾纏來加密，但訊息傳遞速度並不會超過光速。CC的安全保證來自古典電腦無法破解密鑰，QC則有量子糾纏特性保障安全。量子通訊結合量子力學和資訊理論的特點，量子金鑰分發（QKD）受到物理定律的嚴格保護，可以防止竊聽提供絕對的通訊安全。目前QC的瓶頸在於糾纏光子的輸送損耗，只能在約百公里內有效傳送，長距離必須透過中繼器來加強訊號。量子網路的中繼器有三種，量子中繼器，可信任中繼器與安全中繼器，由於「全量子網路」仍未出現，因此目前實施的是量子網路與古典中繼器的混合式系統。

「古典密碼學」依靠數學的複雜性，「量子密碼學」利用量子力學，而「後量子密碼學」則是專指有能力抵禦量子電腦攻擊的困難數學。下表中列出CC，QC與PQC的特性對照，並試圖釐清QC與PQC只是名字類似，但兩者其實毫無關係。

《老子》提到「國之利器不可以示人」，《周易》也記載「君不密則失臣，臣不密則失身，幾事不密則害成，是以君子慎密而不出也。」而韓非子的《說難》中則說：「夫事以密成，語以泄敗。」 資訊洩密會導致事情失敗，即使是無心之失，也會危及安全。『機不密，禍先行』，但真正問題是這世界上真有永遠保密的資訊嗎？維基解密（WikiLeaks）的出現或許就已告訴大家，『事無不可對人言』的誠實政策才是保密最佳方案。

由於數位網路世界中互動頻繁，互相勾心鬥角，竊取資訊謀取私利，保密變成維護權益

表1：古典密碼（Classical Cryptography），量子密碼（Quantum Cryptography）與後量子密碼（Post-Quantum Cryptography）特性說明對照表：

名稱	古典密碼（CC） Classical Cryptography	量子密碼（QC） Quantum Cryptography	後量子密碼（PQC） Post-Quantum Cryptography
加密原理	使用如大質因數分解，離散對數或橢圓曲線離散對數的數學「難題」來加密，超級電腦無法在合理時間內破解密文。	利用量子定律加密，主要是使用物理學的原理。量子密碼受到保護，即使量子電腦的運算能力無法改變物理定律。	防禦量子電腦攻擊，主要是發展格密碼學等量子電腦也困難破解的數學加密。
保密性	古典電腦需要數千年才能破解，除非駭客能竊取金鑰，否則是安全的。	根據量子力學，量子通道無法在不被偵測到情況下被任何人竊聽與攔截。	利用複雜演算法保障可靠度，但並不保證未來通用型量子電腦無法破解。
硬體設計要求	現有通用硬體設施即可	需使用特殊的量子硬體。	不需要增加複雜的硬體。
傳遞網路	適用於所有數位通訊介質，包括RF無線網路和光通訊。	目前僅適用於自由空間或是光纖上的光通訊。	適用於所有數位通訊介質，包括RF無線網路和光通訊。
中繼器	使用現有的數位中繼器技術。	三種類型的中繼器在發展：可信任中繼器、安全中繼器和量子中繼器。	可使用現有的數位中繼器技術。
硬體網路設施	使用目前的行動裝置通訊。	需要新的硬體和通訊基礎設施，成本將更高。	與目前的行動裝置通訊相容。
加密方式與主要算法	利用數學與電腦，有多種加密版本使用於各種不同用途上。主要有凱撒密碼，AES，RSA，ECC等。	利用光量子糾纏有保密功能，不需要另發展數位簽章。目前由於技術所限，僅傳送量子金鑰，而QKD有BB84, E91等。光量子傳播量足夠時，將可出現量子安全直接通信。	利用數學與電腦，目前正開發基於格密碼學等問題的多種加密版本，也可做為數位簽章。目前有CRYSTAL-Kyber,CRYSTAL-Dilithium，FALCON和SPINCS+等。
適用場所	教育，低保密與快速加密。	重要金融與國防資料，需要有量子通訊設施	需要高保密環境及有較佳之電腦相關設備
挑戰與發展	發展成熟，需要密鑰管理且安全性相對差。	發展初期，硬體設備昂貴且糾纏光子無法長距離傳遞。	全球標準化進行中，目前相對安全。

的必要手段。企業或政府目前都使用CC的AES或RSA來保護資料，古典電腦需要數千年才能破解大數分解和離散對數上的難題，除非駭客能竊取加密金鑰，否則加密文件是安全的。所以也有人說，資訊保密其實是信任數學。現在的量子科技與密碼學就像卡通影片『湯姆貓與傑利鼠』，當老鼠變聰明，貓也就只好厲害起來，市場需求是一切進步的動力。許多大型企業擔心『現在收集、稍後解密』的資安攻擊，所以密碼必須立即遷移到PQC，因為有些機密是需要永久保密，如果不使用PQC保護，即使在未來洩密，後果仍將不堪設想。NIST 2024年正式啟動PQC後，QKD的必要性已經引起專家的質疑，除了目前QC硬體設施昂貴外，另外只傳送金鑰而不能傳送完整信息也似乎是殺雞用牛刀。

「後量子密碼」不僅是為了量子時代的資訊安全，而更是要保護現在資訊的永久安全和隱私。「後量子密碼」利用數學複雜性上來加長量子電腦的破解時間，其實與量子特性並無關係，所以正名為「後古典密碼」或是「抗量子密碼」，甚至「進階數學密碼」更名符其實。新的PQC雖然可以抵抗Shor演算法的破譯，但尚未證明在更新的量子演算法及通用量子電腦攻擊下仍無法破解。未來量子密碼與後量子密碼的貓與老鼠互動遊戲仍將持續，量子跟古典間的競合，將是未來盛宴的主角。PQC是數學上的加密防禦，而QC則通過物理手段提供量子的安全保障，因此也有人提出量子安全直接通信（Quantum secure direct communication, QSDC）方案，將PQC與QC混合，在短距離用QC做量子通信，而利用PQC在安全中繼站內自動收發，完美結合古典與量子才是未來科技的發展方式。有詩為證曰：『平盤算卦聲聲撞，籌子多維粒粒敲，量力自然成萬物，鑄成矩陣沸天霄』。

張慶瑞 小檔案

1979 年畢業於臺大物理學系，1988 在加州大學聖地牙哥分校取得物理博士學位，1989 年二月進入臺大服務，曾經擔任臺大副校長並代理校長。

張教授從事微磁學數值研究與自旋傳輸機制，已發表 280 篇以上專業論文並獲得 28 個專利。他是美國物理學會（APS）與國際工程學會（IEEE）會士。曾擔任亞洲磁性協會理事長，及臺灣磁性協會理事長暨臺灣物理學會理事長。近來曾主持 NTU-IBM 量子計畫，積極加速培養新興跨領域人才。近期推動量子計算相關研究，應用於新材料、新藥物合成，與財務金融領域，並創建臺灣量子電腦暨資訊科技協會，擔任理事長。於 2022 年擔任中原大學物理系講座教授並兼任校級量子資訊中心主任。