前瞻科技與管理　13 卷 1 期，21-46 頁（2024 年 11 月）
Journal of Advanced Technology and Management Vol. 13, No. 1, pp. 21-46 (November, 2024)
DOI:10.6193/JATM.202411_13(1).0002

後量子密碼標準發展及運用分析

陳君明 *

國立臺灣大學數學系兼任助理教授

摘 要

隨著量子計算技術的迅速發展，現有公鑰密碼系統面臨嚴峻挑戰。本文首先探討公鑰密碼的基本原理和應用，說明這些系統在現代資訊安全中的重要地位。接著解析量子電腦的威脅，特別是未來量子計算在解決特定複雜數學問題上的強大潛力，可能使得現今廣泛使用的公鑰密碼系統如 Rivest-Shamir-Adleman（RSA）和 Elliptic Curve Cryptography（ECC）變得脆弱不堪。本文介紹後量子密碼學的發展，說明美國政府推動後量子密碼演算法標準化之過程，以及演算法使用之數學工具，這些後量子密碼系統可以有效抵禦量子電腦攻擊。本文亦探討後量子密碼遷移及其應用現狀和挑戰，強調政府、企業和學術界需共同合作，制定過渡計劃和策略，確保在量子計算威脅真正到來之前，資訊安全得到有效保障。

關鍵詞：量子計算、公鑰密碼、後量子、抗量子、標準化

* 通訊作者：陳君明
電子郵件：jmchen@crypto.tw
（收件日期：2024 年 9 月 18 日；修正日期：2024 年 9 月 27 日；接受日期：2024 年 9 月 27 日）

Journal of Advanced Technology and Management Vol. 13, No. 1, pp. 21-46 (November, 2024)
DOI:10.6193/JATM.202411_13(1).0002

Development and Application Analysis of Post-Quantum Cryptography Standards

Jiun-Ming Chen*

Adjunct Assistant Professor, Department of Mathematics, National Taiwan University

Abstract

With the rapid development of quantum computing technology, existing public key cryptographic systems face severe challenges. This article first discusses the basic principles and applications of public key cryptography, explaining the important role of these systems in modern information security. It then analyzes the threat of quantum computers, particularly the powerful potential of future quantum computing in solving specific complex mathematical problems, which may render widely used public key cryptographic systems such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) vulnerable. Against this backdrop, the article introduces the development of post-quantum cryptography, explaining the process of the US government promoting the standardization of post-quantum cryptographic algorithms and the mathematical tools used by these post-quantum cryptographic systems to effectively defend against quantum computer attacks. Finally, it explores the current status and challenges of post-quantum cryptography migration and its applications, emphasizing the need for collaboration among government, businesses, and academia to develop transition plans and strategies to ensure effective information security protection before the quantum computing threat truly manifests.

Keywords: quantum computing, public-key cryptography, post-quantum, quantum-resistant, standardization

* Corresponding Author: Jiun-Ming Chen
E-mail: jmchen@crypto.tw

壹、前言

資訊安全的範圍廣大，其中涉及資料加密與身分認證的「密碼學」（Cryptography）是核心且最關鍵的部分。隨著量子計算技術的迅速發展，現有的資訊安全正面臨前所未有的挑戰。量子電腦可能在不遠的未來，破解傳統的公鑰密碼系統（Public-Key Cryptosystem, PKC），從而對全球的資訊安全構成巨大威脅（如圖 1）。面對這一挑戰，科學家和政府機構已經著手開發可抵禦量子攻擊的後量子密碼（Post-Quantum Cryptography, PQC），並制定國際標準。本文將說明 PKC 的基本原理與現狀，分析量子電腦對其帶來的威脅，介紹 PQC 標準的最新進展，並探討如何有效地實現，從傳統密碼系統向 PQC 系統的遷移（Migration）及其在現實世界中的應用。

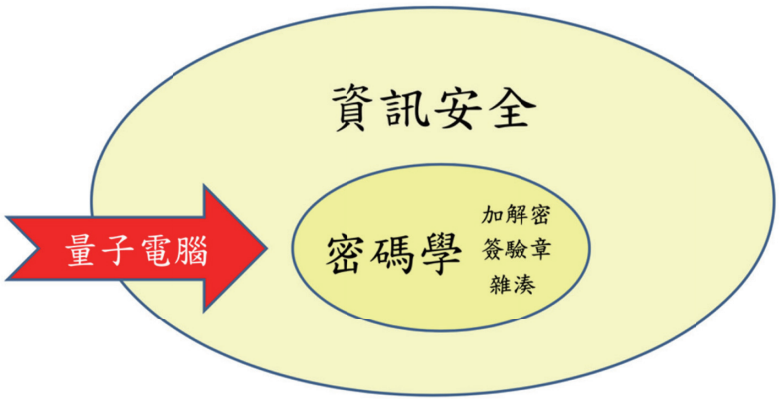

圖 1　量子電腦對資訊安全核心之密碼學的威脅

資料來源：作者自行研究整理。

貳、PKC

密碼系統分為兩大類：對稱（Symmetric）與非對稱（Asymmetric），後者又稱為 PKC。未來量子電腦對二者產生的威脅，有很大差異，因此我們必須先區分二者。兩千年前的凱撒加密（Caesar Cipher）是很好的入門範例，介紹「密鑰」（Key）的觀念。

凱撒加密是一種古老的加密技術，據歷史文獻記載，由古羅馬帝國的凱撒大帝發明使用。如圖 2，「加密」（Encryption）是將每個字母向後推三位，例如 SPY 被加密為 VSB，看起來像亂碼。以當時的背景，方法雖然簡單但有效，訊息在傳送過程中即使被攔截也難以被解讀。凱撒曾經使用這種加密與其將軍們聯繫，確保軍事計畫不會輕易落入敵手。

在凱撒加密中，字母推移量 3 即是密鑰。加密是 + 3，解密即是 – 3。若加密是 – 7，解密即是 + 7。加解密雙方可以同時更換密鑰，若密鑰不同，則將相同明文加密，得到的密文會不同。此即為現代對稱式密碼系統的濫觴，密碼系統之所以能安全保護資料，是因為加解密雙方小心藏好只有雙方知道的密鑰，敵人沒有密鑰就無法將攔截到的密文轉換為可判讀內容的明文。

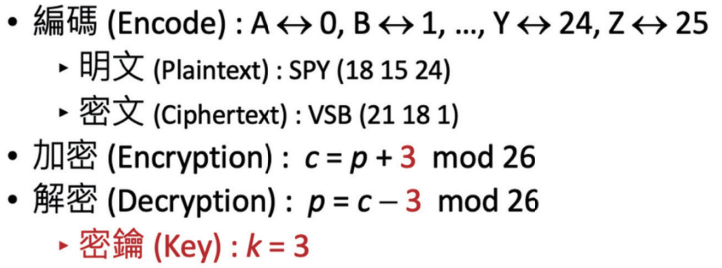

圖 2　凱撒加密

資料來源：作者自行研究整理。

編碼學與密碼學是兩門獨立的學問，有何不同？「編碼」（Encode）是資料格式的轉換，不涉及隱藏資訊，例如圖 2 的編碼是將字母對應至整數。編碼學的主要研究，是使編碼具備「錯誤偵測」（Error Detection）或「錯誤更正」（Error Correction）等功能。圖 2 的加密作用則是隱藏資訊（Conceal Data 或 Hide Information），使傳送的密文看起來像亂碼，敵人無從解讀。密碼學的主要研究，是處於敵人存在的環境中，進行安全通訊。

兩千年來，對稱密碼系統的基本架構不變，如圖 3，紅色表示必須小心隱藏和保護的資訊，藍色表示公開或在傳送過程中可能被敵人攔截或竊聽的資訊。1977 年，美國政府制定 Data Encryption Standard（DES）為對稱密碼系統國家標準。2000 年，美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）經由公開且嚴謹的評比，選出由兩位比利時籍密碼學家設計的 Rijndael 演算法取代 DES，成為新的對稱密碼系統標準 Advanced Encryption Standard（AES）（NIST, 2001）。美國的國家標準，總會成為國際標準，全世界通用。至今 AES 安全無虞，全球廣泛使用。未來量子電腦成熟，對 AES 等對稱式密碼系統略有影響，但不如對 PKC 的安全性影響劇烈。

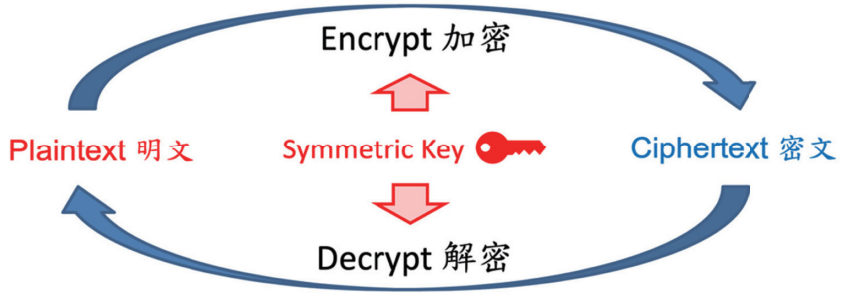

圖 3　對稱密碼系統

資料來源：作者自行研究整理。

Diffie and Hellman（1976）提出 PKC 的概念，使得密碼學的發展由黑暗時期（Dark Age）進入現代化。公鑰和私鑰是非對稱密碼系統的核心概念，它們相互配對，使用於對應的操作。如圖 4，使用者以裝置先隨機生成私鑰，再推導出公鑰。公鑰是公開的，任何人都可以取得；私鑰則是保密的，只有擁有者能夠使用它操作。私鑰可輕易推導出公鑰，

但由公鑰逆推回私鑰則極度困難，以專業術語來說是「計算上不可行」（Computationally Infeasible）。

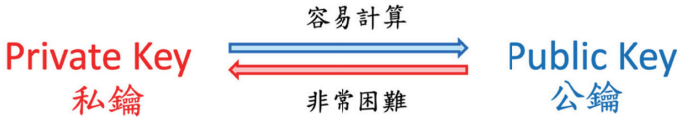

圖 4　私鑰與公鑰

資料來源：作者自行研究整理。

三位麻省理工學院（Massachusetts Institute of Technology, MIT）的學者 Rivest, Shamir, and Adleman（1978）發明 Rivest-Shamir-Adleman（RSA），至今仍為全世界廣泛使用，其安全性基於「質因數分解（Integer Factoring）的困難度」。使用者隨機生成兩個 512 位元的大質數，作為私鑰；兩質數相乘得到 1,024 位元的整數，作為公鑰，此為 RSA-1024。目前實務上使用最多的是 RSA-2048，而 RSA-4096 亦不少見。對於目前的電腦，質因數分解 1,024 位元以上的大整數極度困難。但很不幸，對於未來的量子電腦，質因數分解可能變得很容易，於是 RSA 未來不再具備安全性。

現今其他 PKC 使用另一類型數學工具，其安全性基於「離散對數問題（Discrete Logarithm Problem, DLP）的困難度」，例如橢圓曲線密碼系統（Elliptic Curve Cryptosystem, ECC）。DLP 未來也可能被量子電腦輕易破解。也就是說，沒有任何現有的傳統 PKC 標準，在未來量子電腦成熟時是安全的。

若將 PKC 使用於加解密，如圖 5，是以公開的公鑰對明文加密，傳送密文至生成該公私鑰對（Key Pair）的使用者，由該使用者以保密的私鑰解密，將密文還原為明文。PKC 由於運算量大，加解密效率比對稱密碼系統慢上千倍，因此實務上均不以其加解密大量資料。最普遍的做法是先以 PKC 加密傳送 AES 密鑰，再以雙方均持有密鑰之 AES 加解密欲秘密傳送的資料。也就是說，公鑰加解密使用於密鑰建立。美國的密鑰建立國家標準：SP 800-56A（Barker, Chen, Roginsky, Vassilev, and Davis, 2018）以離散對數為基礎，SP 800-56B（Barker, Chen, Roginsky, Vassilev, Davis, and Simon, 2019）以質因數分解為基礎。

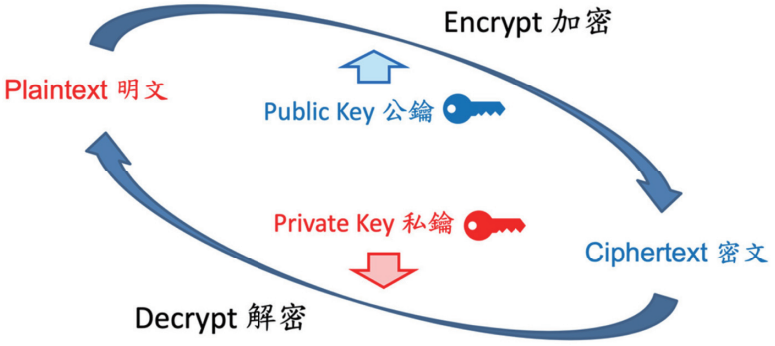

圖 5　PKC 的加解密

資料來源：作者自行研究整理。

數位簽章（Digital Signature）則是將公私鑰的操作順序對調。如圖 6，公私鑰對的持有者，先以保密的私鑰對訊息簽章（Sign），被簽署的可能是合約、訂單或轉帳交易。簽章的運算結果和訊息本身一起公開或傳送，再由其他人以公開的對應公鑰驗章（Verify）；若通過驗章，則認定該訊息是由私鑰持有者正確簽署，在特定應用上與手寫簽名具備相同法律效力。美國最新數位簽章國家標準，規範於 FIPS 186-5（NIST, 2023）。

數位簽章具有多項功能，包括：

（一）完整性（Integrity）：數位簽章可確保訊息在傳輸過程中未被篡改。任何對訊息的改變都會導致簽章驗證失敗，從而提醒接收者訊息可能已被修改；

（二）鑑別性（Authentication）：數位簽章能夠驗證訊息的發送者身分。由於只有持有私鑰的發送者才能生成通過驗章的數位簽章，因此接收者能夠確定訊息來自於真正的發送者；

（三）不可否認性（Non-Repudiation）：數位簽章能防止簽名者事後否認曾經簽署過訊息。由於私鑰是唯一且安全的，因此發送者無法否認其對訊息進行過簽章的事實。

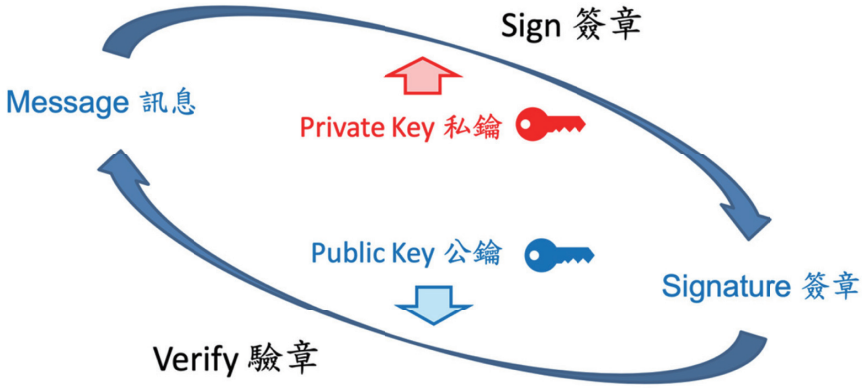

圖 6 數位簽章

資料來源：作者自行研究整理。

比特幣（Bitcoin）、乙太坊（Ethereum）等，基於區塊鏈（Block Chain）技術的密碼貨幣（Cryptocurrency），均依賴數位簽章對交易進行簽署。數位簽章對現有的網路運作，特別是對電子商務的發展，具有至關重要的作用。在電子商務中，數位簽章可確保交易各方（包括消費者和商家）的身分驗證，並可有效防止交易過程中數據篡改，確保交易的安全性與合法性。

臺灣《電子簽章法》（2002）於 2002 年正式生效，為數位簽章的使用提供法律依據。該法案奠定使用和管理數位簽章的基本規範，並確保數位簽章在法律上具有和手寫簽名同等的法律效力。

近期在數位發展部積極推動下，《電子簽章法》（2024）在 2024 年 4 月 30 日經立法院三讀修正通過。此次修法進一步完善了相關規範和標準，旨在提升數位簽章的應用範圍與普及率，進一步促進臺灣數位經濟的發展。

由以上說明可知，PKC 分為加解密和數位簽章兩大類，使用公私鑰的順序不同。未來取代現行 PKC（Barker et al., 2018, 2019; NIST, 2023），可抵禦量子電腦攻擊的新一代 PKC 標準，也將區分為加解密和數位簽章兩大類。

參、量子電腦的威脅

量子計算利用量子力學原理，在特定問題上以超越傳統電腦的速度和效率執行計算，關鍵性質是量子的疊加（Superposition）和糾纏（Entanglement）。

疊加是量子力學中的基本概念，允許量子位元（Qubits）同時存在於多種狀態。它不同於在任何特定時間，只能處於 0 或 1 狀態的傳統位元。由於疊加，量子位元可以同時處於 0 和 1，使量子電腦能處理大量數據並同時執行多個計算。

糾纏是量子力學的另一獨特性質，將兩個或多個量子位元的狀態相互聯繫，不受它們之間的距離影響。當量子位元處於糾纏態，一個量子位元的狀態會立即影響另一個，為量子計算提供強大工具。這種現象使量子位元能夠以高度連動的方式處理資訊，解決複雜問題。

近年來，量子計算的技術持續穩定進展，著名科技公司和研究機構正大力投資於量子計算研究。未來大規模（Large-Scale）通用（Universal）量子電腦成熟，將以超高效率解決目前傳統電腦無法解決的特定問題。

一、Shor 演算法

在 1994 年，貝爾實驗室的 Peter Shor 發表一項開創性的演算法（Shor, 1994, 1997），成為量子計算領域的重要里程碑。該演算法若實作於未來大規模通用量子電腦，將以極高效率破解現今使用的 PKC，例如 RSA、ECC。

RSA 的安全性依賴於質因數分解大整數的「計算上不可行」，ECC 的安全性依賴於 DLP 的計算上不可行，兩問題對於現有的傳統電腦來說，需要天文數字級別的計算量，無法在可接受的時間範圍內解決。

Shor（1994, 1997）演算法利用量子力學的疊加和糾纏，未來可在短時間解決以上計算難題。量子疊加允許量子電腦同時在多個狀態進行計算，而量子糾纏則使得不同量子位元之間能以一種複雜且相互關聯的方式進行互動。這些特性使得量子電腦非常適合用來尋找龐大且複雜之週期函數（Periodic Function）的週期（Period）。在 Shor 演算法中，質因數分解與 DLP 都被轉換成為尋找某個週期函數的週期。這樣的轉換使得量子電腦可以藉由高效的量子傅立葉變換（Fourier Transform）快速找到函數週期。一旦找到週期，質因數分解或 DLP 便可迅速解決。

在 2001 年，IBM 展示史上首次 Shor 演算法的概念證明（Proof of Concept, PoC）實現，以 7 個量子位元的量子電腦，分解 15 為質因數 3×5。該演算法的步驟包括：

（一）疊加：將數字 15 編碼為一個量子狀態的疊加，以表示 15 的所有可能因數值；

（二）量子操作：應用量子操作來操作量子位元，找到與因數分解問題相關的函數週期；

（三）測量：測量量子狀態，將疊加崩塌為與 15 的因數對應之經典狀態。

近年隨著量子電腦的量子位元數增加，可質因數分解的整數也逐漸增大。何時通用量子電腦的量子位元數將達到二、三千或更多，破解現有 RSA 和 ECC，專家們有各種樂觀與悲觀的估計，至今仍然沒有共識。目前最權威的預測來自 Mosca and Piani（2021），為美國官方報告引用，例如 Moody（2022）。圖 7 來自 Mosca 與 Piani 的報告，是量子計算對現有密碼系統之威脅時間預測的統計分析。該報告徵詢 46 位量子計算專家，讓每位專家估計在 5 年、10 年、15 年、20 年和 30 年後，量子電腦破解 RSA-2048 的可能性（Likelihood）。例如 2021 年的 15 年後，亦即 2036 年，有多大的機率，量子電腦可以在 24 小時內破解 RSA-2048 ？6 位專家預測機率低於 5%，12 位預測低於 30%，10 位預測約 50%，13 位預測大於 70%，5 位預測高於 95%。

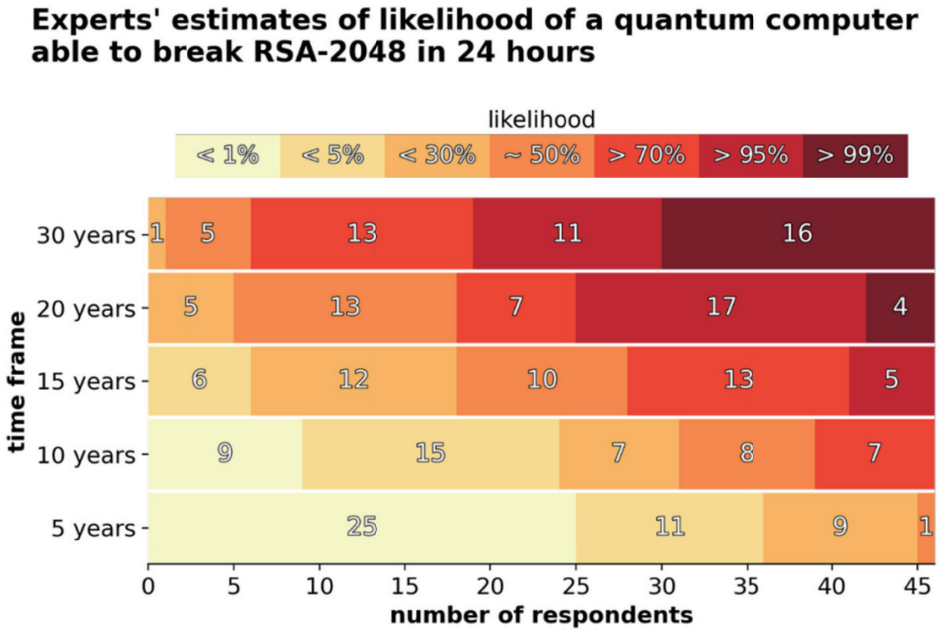

圖 7　專家群預測量子電腦破解 RSA-2048 發生時間

資料來源：Mosca and Piani（2021）。

二、PQC 與 QKD

PQC 又稱抗量子密碼學（Quantum-Resistant Cryptography），是研究和設計既可抵抗現有傳統電腦攻擊，亦能抵抗未來量子電腦攻擊的密碼學領域。這些 PKC 使用不同數學工具，計算難題基礎迥異於質因數分解或 DLP。最具代表性的 PQC 系統類型如下：

（一）基於晶格的密碼學（Lattice-Based Cryptography）；

（二）基於編碼的密碼學（Code-Based Cryptography）；

（三）基於雜湊函數的密碼學（Hash-Based Cryptography）；

（四）多變量密碼學（Multivariate Cryptography）。

其中基於雜湊函數的數位簽章早在 1970 年代末期即開始發展，距今超過 40 年。臺灣學術界投入多變量密碼學的研究超過 20 年，Yang, Chen, and Chen（2004）提出了一種在低成本智慧卡上實現高效簽章的方法，發表於密碼硬體與嵌入式系統水準最高的會議 Conference on Cryptographic Hardware and Embedded Systems（CHES）。

PQC 現今最受重視的領域，則是以晶格（Lattice）為數學工具。實數座標平面上的二維晶格如圖 8，所有實心圓點，亦即所有線性獨立向量 u_1 和 u_2 的整係數線性組合 $n_1u_1 + n_2u_2$，即是由基底 $U = \{u_1, u_2\}$ 生成的晶格。

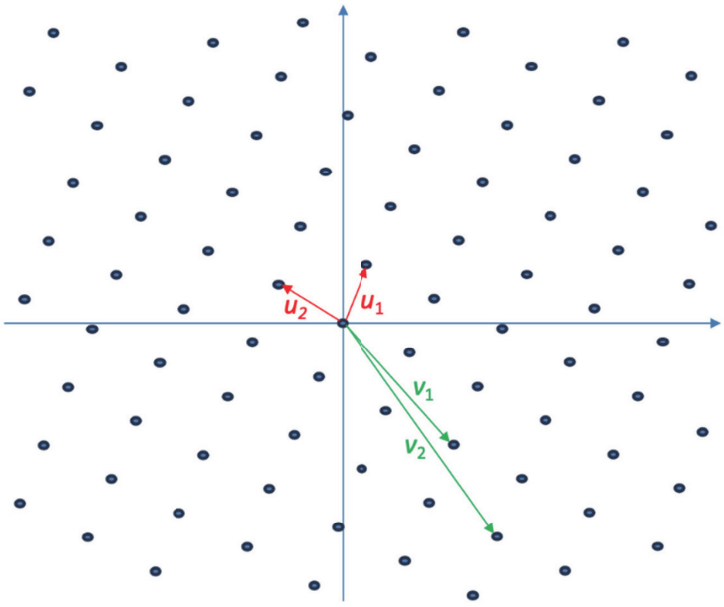

圖 8　二維晶格

資料來源：作者自行研究整理。

基底 $V = \{v_1, v_2\}$ 生成的晶格完全相同，也是這些實心圓點。U 的向量長度短，且彼此的夾角接近直角，是「好的基底」。V 則是「差的基底」。當晶格維度（Dimension）高時，將差的基底轉換為同一晶格之好的基底，無論對傳統電腦或未來量子電腦都極度困難，稱之為基底化約（Basis Reduction）難題。

最短向量問題（Shortest Vector Problem, SVP）也是晶格上的計算難題，目標是找出給定晶格中最短的非零（Non-Zero）向量。在圖 8 中，由於只有二維，若給定差的基底 V，可操作類似輾轉相除法的演算法找到最短非零向量 u_1 或 $-u_1$。但是當晶格維度高時，SVP 極度困難。另一計算難題是最接近向量問題（Closest Vector Problem, CVP）：給定空間中的一點不在晶格上，目標是找到最接近給定點的晶格點。

目前基於晶格的 PQC，安全性都是基於類似上述難題之一。實務上，圖 8 實數座標不適合密碼系統，PQC 大多使用結構化晶格（Structured Lattice），以有限的離散代數結構實現。

相較於 RSA 或 ECC，欲達到以傳統電腦估計的相同安全等級，以上各類型 PQC 系統

若非公私鑰長度較大，即是數位簽章長度明顯較大，使用上較不方便。因此只有當量子電腦的發展已對 RSA 和 ECC 造成隱憂，才會積極轉移至 PQC 系統。

量子密碼學（Quantum Cryptography, QC）領域涉及使用量子力學物理，以特製硬體裝置來保護敏感資訊的機密性。如今最常見的例子，是利用量子物理來分發使用於 AES 等傳統對稱式密碼系統的密鑰，稱為量子密鑰分配（Quantum Key Distribution, QKD）。QKD 利用量子態（如光子的偏振或自旋）傳遞密鑰，其安全性基於量子不可複製原理（No-Cloning Theorem）和測量會改變量子態的特性。此技術已存在，並且與未來用於攻擊密碼系統的量子計算技術有所不同。QKD 的唯一功能是在使用者之間分配密鑰，因此它僅是密碼系統的一部分。

美國國家安全局（National Security Agency, NSA）於 2020 年 10 月 26 日在官方網站上發布一篇聲明（NSA, 2020），列出 QKD 的五大技術限制。聲明最後總結指出：NSA 將 PQC 視為比 QKD 更具成本效益且易於維護的解決方案，NSA 不支持在國家安全系統（National Security System, NSS）中使用 QKD 或 QC 保護通信，並且除非克服這些限制，否則不會認證或批准任何 QKD 或 QC 的安全產品供 NSS 客戶使用。

英國情報與資訊安全最高機構 Government Communications Headquarters（GCHQ）早在 2018 年發布了一篇公告（Schneier, 2018），表明對 QKD 的類似觀點。之後，這篇公告由英國國家網絡安全中心（National Cyber Security Centre, NCSC）撰寫的白皮書 “Quantum Security Technologies” 取代。該白皮書強調，NCSC 不會背書任何用於政府或軍事的 QKD 方案，並指出量子安全密碼學（即 PQC）才是抵禦量子電腦威脅的最佳解決方案（NCSC, 2020）。

德國資訊安全聯邦管理機構（Bundesamt für Sicherheit in der Informationstechnik, BSI）與法國、瑞典、荷蘭的對應機構於 2024 年 1 月 29 日聯合發布 “Position Paper on Quantum Key Distribution”（BSI, 2024），分析 QKD 的局限性和挑戰，旨在幫助決策者和政策制定者對使用 QKD 做出明智判斷。該報告指出，QKD 需要專門的通信基礎設施，且存在許多功能上的限制，只能應用於特定的利基案例。此外，報告強調，為了使組織能夠遷移到量子安全的環境，應優先考慮部署 PQC 技術，因為 PQC 與現有的密碼學技術差異不大。

三、PQC 的迫切性

Year to Quantum（Y2Q）亦稱為 Q-Day，是指未來量子電腦破解 RSA 或 ECC 等傳統 PKC 的日期。雖然 Y2Q 不至於立即發生，轉移至 PQC 卻有勢在必行的急迫性。

“Harvest now, decrypt later”（現在收集，日後解密）或 “Catch now, break later”（Cybersecurity and Infrastructure Security Agency [CISA], 2023）是一種監控策略，截獲並長期存儲目前無法解讀的密文，等待可能的解密技術突破，使其在未來可讀取。少數國家級大型情報機構已經開始大量儲存密文，等待 Y2Q 的來臨。對於被敵人儲存的密文，沒有任何機會挽救，唯一因應之道是早日採用 PQC。

量子計算專家 Michele Mosca 提出 XYZ 風險模型（Risk Model），如圖 9：如果 $X + Y > Z$，亦即「資訊保密期限」（X）加上「PQC 標準化並採用」（Y）的時間，比「大規模通用量子電腦實現所需時間」（Z）更長，就該憂慮出現的問題。

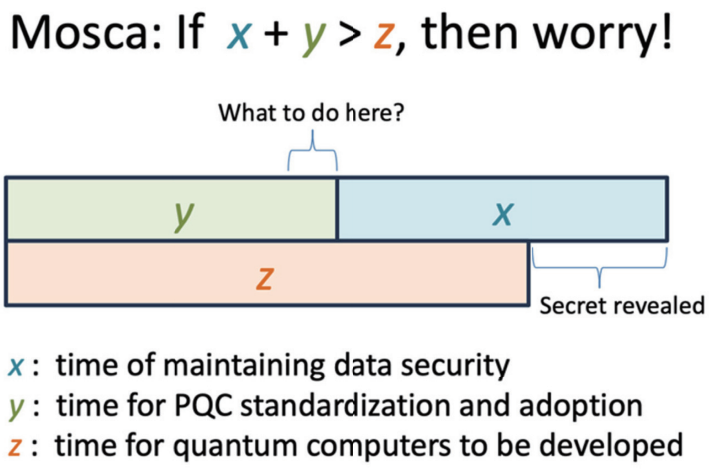

圖 9　XYZ 風險模型

資料來源：Mosca（2015）。

舉例來說：*X* 和 *Y* 都是 10 年，*Z* 是 16 年，乍看之下沒問題，10 年後的保密裝置已具備 PQC，可抵抗量子電腦攻擊。但是 9 年後，亦即圖 9 中 “What to do here?” 期間建置的保密裝備，尚未具備 PQC，只能使用 RSA 或 ECC 等現有 PKC。該期間產製的密文在 7 年內會被量子電腦破解，保密期限頂多 7 年，少於預設的 10 年，這就導致問題。

由以上說明可知，只有當 $X + Y \leq Z$ 時，才可確保萬無一失。由於量子電腦技術成熟的時間 *Z* 對所有人都是相同的，不同應用則有不同的保密期限 *X*。對於保密期限較長的應用，PQC 的準備時間 *Y* 必須越短，過渡至 PQC 的需求也越加急迫。

最後，根據過去經驗，全面更換特定類型的密碼系統，總是曠日費時，例如從對稱式加解密 DES 到 AES、從雜湊函數 MD5 或 SHA-1 到 SHA-2，都歷時多年。現今 PKC 的使用既多且廣，全面轉移至 PQC 很可能也是 10 年以上的漫長過程，宜及早開始。

肆、PQC 標準

在資訊科技（Information Technology, IT）領域，美國的國家標準經常成為國際標準，全世界通用。密碼系統標準亦不例外，自 1970 年代制定對稱式加密標準 DES 起，美國政府主導制定的密碼標準總是成為全球通用的標準。1997 ~ 2000 年，NIST 主導 AES 標準甄選競賽，邀請全世界頂尖密碼學家參與，經由公開且嚴謹的兩輪評選程序，從 15 項來自全球的演算法投稿中，選出由 2 位比利時專家設計的 Rijndael，成為取代 DES 的新一代對稱加密標準。

此後 NIST 亦以甄選競賽的形式，廣發英雄帖邀請全球專家參與，制定雜湊函數 SHA-3、輕量級（Lightweight）對稱加密 Ascon 等標準。美國 PQC 標準制定亦由 NIST 主導，以競賽形式進行（NIST, n,d,-b）。

一、NIST 制定 PQC 標準

NIST 於 2016 年的 PQCrypto 國際會議中宣布，將進行 PQC 標準的甄選（Moody, 2016）。投稿於 2017 年 11 月截止，共收到 82 項提案，包括 59 項公鑰加密（Public-Key Encryption, PKE）演算法和 23 項數位簽章演算法。其中 69 項提案文件完整，進入第一輪評選。

2019 年 1 月，26 項 PQC 演算法進入第二輪評選。2020 年 7 月，NIST 公布第三輪名單，包含 7 項決選者（Finalists）和 8 項候補者（Alternatives）。

2022 年 7 月，NIST 公布第三輪評選結果，從 15 項演算法中選出 4 項作為 PQC 標準，其中包括：

（一）1 項 PKE 演算法：CRYSTALS-Kyber（Kyber）；

（二）3 項數位簽章演算法：CRYSTALS-Dilithium（Dilithium）、FALCON 和 SPHINCS$^+$。

KYBER、Dilithium、FALCON 是基於晶格（Lattice-Based），SPHINCS$^+$ 是基於雜湊函數（Hash-Based）。

PKE，又稱為密鑰封裝機制（Key Encapsulation Mechanism, KEM），有 4 項此類型的演算法進入第四輪評選，分別為：BIKE、Classic McEliece、HQC 和 SIKE。其中，基於超奇異同源（Super-Singular Isogeny）的 SIKE 已被成功破解，剩下的三項候選演算法則是基於編碼理論（Code-Based）。

目前選出的三項 PQC 數位簽章標準，簽章的長度較大，對於一些應用可能較不方便。NIST 因此另闢戰場，主導 “Additional Digital Signature Schemes” 評選，目標是選出簽章長度小的數位簽章標準，40 項演算法進入第一輪。

2023 年 8 月 24 日，NIST 公布以下三項 PQC 標準草案，徵求回饋意見：

（一）FIPS 203：ML-KEM（Module-Lattice-Based Key-Encapsulation Mechanism Standard），原 Kyber；

（二）FIPS 204：ML-DSA（Module-Lattice-Based Digital Signature Standard），原 Dilithium；

（三）FIPS 205：SLH-DSA（Stateless Hash-Based Digital Signature Standard），原 SPHINCS$^+$。

其中 FIPS 是「聯邦資訊處理標準」（Federal Information Processing Standard）的縮寫。2024 年 8 月 13 日，NIST 公布 FIPS 203、204、205 三項 PQC 標準的最終版本（NIST, 2024a, 2024b, 2024c）。

2024 年 11 月 12 日，NIST 的 PQC 標準制定團隊公布一份內部報告（Internal Report, IR）NIST IR 8547 草案，明訂 RSA 和 ECC 自 2030 年開始淘汰，2035 年起禁止使用（Moody, Perlner, Regenscheid, Robinson, and Cooper, 2024）。

二、CNSA 2.0

商用國家安全演算法套件（Commercial National Security Algorithm Suite, CNSA）是由 NSA 頒布的一組密碼演算法，旨在保護美國 NSS 中的機密訊息，直至最高機密級別（Top Secret Level）。

CNSA 1.0 包含 RSA、ECC 等現有 PKC。CNSA 2.0 公布於美國國防部網站（NSA, 2022, 2024），摒除未來可能被量子電腦破解的 PKC，並納入 PQC 標準 FIPS 203 與 FIPS 204，如表 1 所示。

表 1　CNSA 2.0

Algorithm	Function	Specifcation	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS 197	Use 256-bit keys for all classifcation levels
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS 203	Use Category 5 parameter, ML-KEM-1024, for all classifcation levels
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any case, including signing firmware and software	FIPS 204	Use Category 5 parameter, ML-DSA-87, for all classifcation levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classifcation levels. LMS SHA-256/192 is recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classifcation levels

資料來源：NSA（2024）。

基於雜湊函數的 PQC 數位簽章可分為有狀態（Stateful）與無狀態（Stateless）兩大類。前者需要記錄並避免重複使用已使用過的私鑰，必須在使用時保存額外紀錄。後者則無此限制，使用上較方便，也符合長期以來數位簽章的使用概念。

CNSA 2.0 用於簽署韌體或軟體的是有狀態數位簽章 LMS 和 XMSS，規格定義於 NIST 公布的 SP 800-208（Cooper, Apon, Dang, Davidson, Dworkin, and Miller, 2020）。值得注意的是，基於雜湊函數的無狀態數位簽章標準 FIPS 205，雖然與 FIPS 203 和 FIPS 204 同時獲選並於 2024 年正式發布，但未收錄於 CNSA 2.0，且不得於 NSS 中使用（NSA, 2024）。

CNSA 2.0 於 NSS 的實施進度，規範於圖 10，條列如下：

（一）軟體和韌體簽署：CNSA 2.0 的過渡應立即開始，2025 年前測試且成為選項，2030 年前成為預設且成為首選，2030 年後全面專屬使用；

（二）網頁瀏覽器／伺服器和雲端服務：CNSA 2.0 在 2025 年前測試且成為選項，2033 年前成為預設且成為首選，2033 年後全面專屬使用；

（三）傳統網絡設備（例如虛擬私人網路 [Virtual Private Network, VPN]、路由器）：CNSA

2.0 在 2026 年前測試且成為選項，2030 年前成為預設且成為首選，2030 年後全面專屬使用；

（四）作業系統：CNSA 2.0 在 2027 年前測試且成為選項，2033 年前成為預設且成為首選，2033 年後全面專屬使用；

（五）專業設備（例如受限設備、公開金鑰基礎建設 [Public Key Infrastructure, PKI] 系統）：CNSA 2.0 在 2030 年前測試且成為選項，2033 年前成為預設且成為首選，2033 年後全面專屬使用；

（六）自定義應用程式和舊有裝置：到 2033 年前升級或更換。

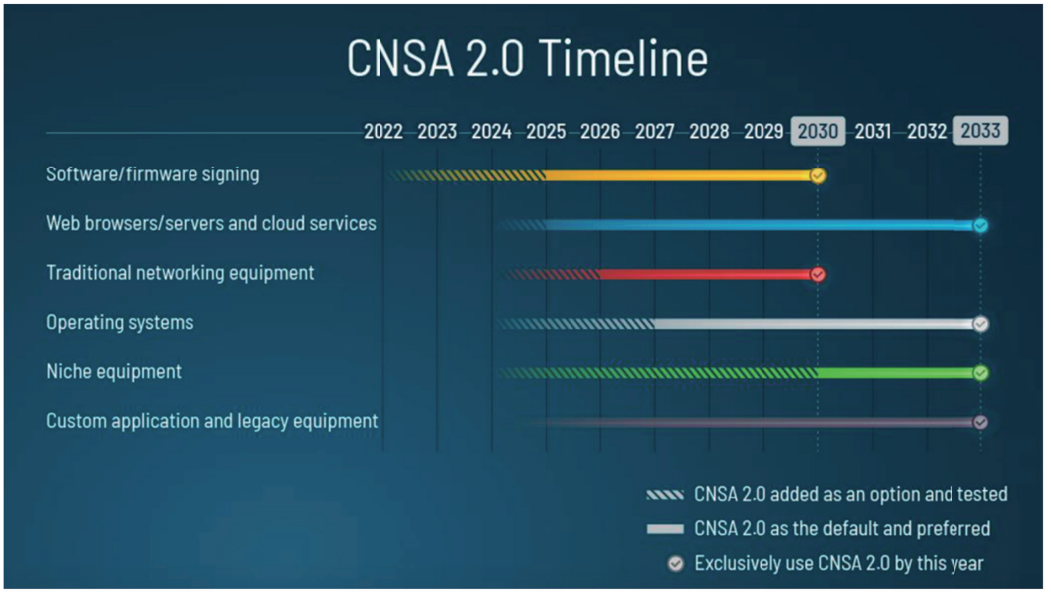

圖 10　CNSA 2.0 時間表

資料來源：NSA（2024）。

三、代數晶格密碼套件（Cryptographic Suite for Algebraic Lattices, CRYSTALS）

2017 年底，CRYSTALS（n.d.）網頁上線，介紹 Kyber 和 Dilithium 兩項演算法，參與 NIST 主導的 PQC 標準制定競賽。CRYSTALS-Kyber 獲選為 FIPS 203，CRYSTALS-Dilithium 獲選為 FIPS 204。該團隊設計的這兩項演算法不僅最先獲選為 NIST 制定的 PQC 標準，亦被 NSA 納入 CNSA 2.0，無疑是 PQC 競賽的最大贏家。

「Crystals」單字的本義為「晶體」。Kyber 來自《星際大戰》（*Star Wars*）故事中的虛構晶體，該晶體被絕地武士和西斯用來運用原力並製作代表性的武器，為光劍（Lightsaber）提供能量，是光劍刀刃的重要組成部分。另一方面，在《星際迷航》（*Star Trek*）故事中，Dilithium 是一種虛構的結晶礦物，作為星艦運作和超光速旅行的能量來源，其稀缺性和重

要性經常成為《星際迷航》劇集的核心情節。CRYSTALS 團隊的主要成員是《星際大戰》和《星際迷航》的影迷，以這兩部作品中的晶體名稱為其兩項演算法命名。

Kyber 和 Dilithium 的設計團隊 CRYSTALS Team 共有 12 位成員：

1. Roberto Avanzi, ARM Limited（DE）；
2. Shi Bai, Florida Atlantic University（US）；
3. Joppe Bos, NXP Semiconductors（BE）；
4. Jintai Ding, Tsinghua University（CN）；
5. Léo Ducas, CWI Amsterdam（NL）& Leiden University（NL）；
6. Eike Kiltz, Ruhr University Bochum（DE）；
7. Tancrède Lepoint, Amazon Web Services（US）；
8. Vadim Lyubashevsky, IBM Research Zurich（CH）；
9. John M. Schanck, Mozilla（US）；
10. Peter Schwabe, MPI-SP（DE）& Radboud University（NL）；
11. Gregor Seiler, IBM Research Zurich（CH）；
12. Damien Stehle, CryptoLab Inc（FR）。

以上名單依照姓氏字母順序排列，最晚加入團隊的是美籍中裔丁津泰（Jintai Ding）教授。丁津泰於中國取得學士與碩士學位，再於美國耶魯大學深造獲得物理博士學位，長年任教於美國俄亥俄州的辛辛那提大學數學系。Kyber 演算法的密鑰建立技術觸及丁津泰已申請的專利，NIST 付費取得專利授權，所有依照 FIPS 203 正式版演算法實作的產品皆不需再付授權費。

Kyber 和 Dilithium 的安全性，皆是基於模晶格（Module Lattice）上的計算難題。對於所有 NIST 定義的安全級別，Kyber 和 Dilithium 所需操作是雜湊函數 Keccak 的變體、以固定質數 q 定義之有限體 Z_q 加法和乘法，以及多項式商環（Quotient Ring）$Z_q[x] / (x^{256} + 1)$ 的數論變換（Number Theoretic Transform, NTT）。

簡單來說，Kyber 和 Dilithium 操作 255 次數（Degree）的多項式：

$$c_{255}\, x^{255} + c_{254}\, x^{254} + \ldots + c_1\, x + c_0$$

其中整係數 c_i 介於 0 與 $q - 1$。Kyber 使用質數 $q = 3{,}329 = 13 \times 2^8 + 1$，Dilithium 使用質數 $q = 8{,}380{,}417 = 2^{23} - 2^{13} + 1$。

「容錯學習」（Learning with Errors, LWE）是晶格上的計算難題，當晶格維度高時，對量子電腦和傳統電腦都是「計算上不可行」，許多 PQC 系統的安全是基於 LWE 或其變體的難度。圖 11 的 s 和 e 是短向量，與矩陣 $\mathbf{A}$ 皆由使用者生成，其中 $\mathbf{A}$ 的每個元素皆在很大的範圍內。計算 $t = \mathbf{A}\, s + e$，公布 t 和 $\mathbf{A}$ 作為公鑰。當敵人只知道公鑰 t 和 $\mathbf{A}$，欲解出私鑰 s 為極度困難，此即是 LWE 難題。不難推導，LWE 與 CVP 高度相關。

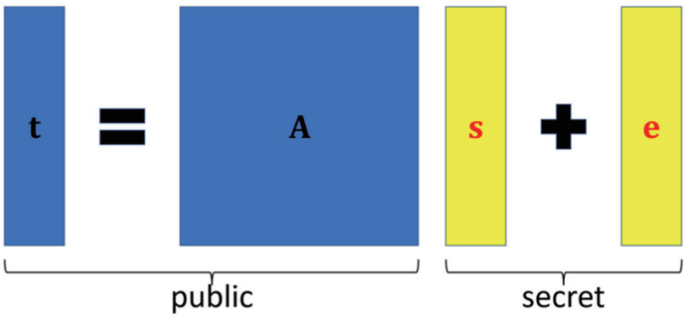

圖 11 LWE 難題

資料來源：作者自行研究整理。

LWE 等式 $\mathbf{A}s + e = t$ 與常見的方程組 $\mathbf{A}s = t$ 明顯不同：

$$\begin{bmatrix} 14 & 15 & 5 & 2 \\ 13 & 14 & 14 & 6 \\ 6 & 10 & 13 & 1 \\ 10 & 4 & 12 & 16 \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 262 \\ 374 \\ 258 \\ 336 \end{bmatrix} \quad (1)$$

在此範例中，操作高斯消去法（Gaussian Elimination）可輕易解得答案 $s = (0, 13, 9, 11)$。但若等式中有未知短向量 e 作為誤差，則解題難度大幅增加。

Kyber 與 Dilithium 的難題假設是模容錯學習（Module Learning with Errors, MLWE），安全性以此問題的計算難度為基礎。在圖 11 中，Kyber 和 Dilithium 操作的向量和矩陣，每個元素都在多項式商環 $Z_q[x] / (x^{256} + 1)$ 之中，可視為係數在 Z_q 中的 255 次多項式。

簡單來說，向量 t 和 $\mathbf{A}$ 是 LWE/MLWE 類型 PQC 的公鑰，s 是私鑰。求解 s 無法轉換成可由量子電腦迅速破解的問題。

以下是多項式商環 $Z_{17}[x] / (x^4 + 1)$ 上的小型範例：

$$\mathbf{A} = \begin{pmatrix} 6x^3 + 16x^2 + 16x + 11 & 9x^3 + 4x^2 + 6x + 3 \\ 5x^3 + 3x^2 + 10x + 1 & 6x^3 + x^2 + 9x + 15 \end{pmatrix} \quad (2)$$

$$t = (16x^3 + 15x^2 + 7 \quad 10x^3 + 12x^2 + 11x + 6)$$

欲尋找係數小的短向量 s 和 e 使得 MLWE 等式 $As + e = t$ 成立，並不容易。事實上，此範例的答案是（t、s、e 均視為轉置的行向量）：

$$s = (-x^3 - x^2 + x, -x^3 - x)$$
$$e = (x^2, x^2 - x) \quad (3)$$

Kyber 和 Dilithium 使用的質數 q 大得多，多項式次數也高達 255，求解 MLWE 的計算複雜度以指數型暴增。即使對未來的量子電腦，破解 Kyber 和 Dilithium 背後的 MLWE 難題均為計算上不可行。

四、FIPS 203 ML-KEM 及應用

CRYSTALS-Kyber 獲選並制定為 PQC 標準 FIPS 203（NIST, 2024b）之後，以 Module-Lattice-Based Key-Encapsulation Mechanism（ML-KEM）為其正式名稱，官方將不再使用其原名 Kyber。它是基於 MLWE 難題假設，滿足 Indistinguishable under an Adaptive Chosen-Ciphertext Attack（IND-CCA2）安全性質的 KEM。

ML-KEM 的建立，包括兩大步驟。首先是 PKE，包含公私鑰對生成、加密、解密三個功能。再來經過 Fujisaki-Okamoto 轉換形成 KEM，包含密鑰生成、封裝、解封裝三個功能。圖 12 是 ML-KEM 的封裝與解封裝流程圖。

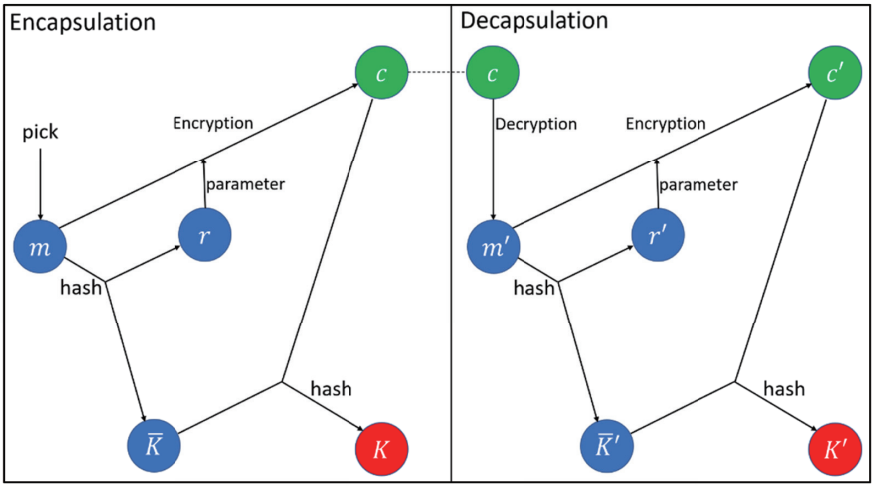

圖 12　ML-KEM 封裝、解封裝流程圖

資料來源：作者自行研究整理。

ML-KEM 除了滿足安全性的要求，設計上亦著重運算效率，適用於各種應用。實務上這種高效性很重要，因為它使該演算法能夠在計算能力有限的設備上有效運行。應用範圍包括：

（一）安全通信：應用於安全通信協議，建立用戶之間的加密通道；

（二）資訊保護：可用於在敏感數據儲存解決方案中，封裝對稱加密的密鑰；

（三）整合至現有框架中：可以整合到現有的密碼基礎設施中，增強其對抗量子攻擊的安全性。

五、FIPS 204 ML-DSA 及應用

CRYSTALS-Dilithium 獲選並制定為 PQC 標準 FIPS 204（NIST, 2024a）之後，以 Module-Lattice-Based Digital Signature Algorithm（ML-DSA）為其正式名稱，官方將不再使用其原名 Dilithium。它是基於 MLWE 和「模最小整數解」（Module Smallest Integer Solution, MSIS）難題假設，滿足 Existential Unforgeability under Chosen Message Attack（EUF-CMA）安全性質的數位簽章演算法。

圖 13 是簡化版的 ML-DSA 變數關係圖。ML-DSA 不但滿足安全性的要求，設計上亦著重效率，此為其獲選並納入 CNSA 2.0 的主要原因。應用範圍包括：

（一）安全交易：可應用於各種數位交易，藉由數位簽章確保真實性和完整性；

（二）區塊鏈技術：可融入區塊鏈系統，為協議和合約提供強大的安全功能；

（三）軟體分發：可驗證軟體更新和數位內容，確保來自可信來源且未被篡改。

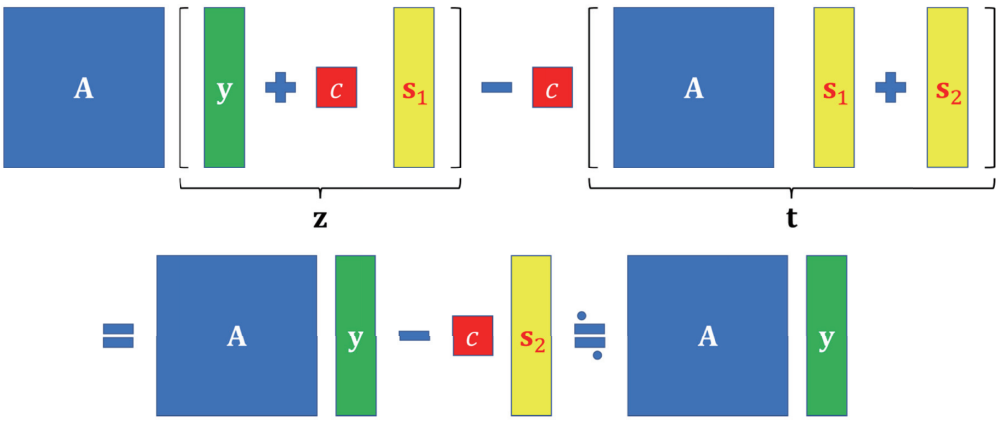

圖 13　ML-DSA 變數關係圖

資料來源：作者自行研究整理。

伍、PQC 遷移及運用

PKC 的使用極為普遍，必須費心的不是為 PQC 尋找新應用，而是將現有 RSA、ECC 等 PKC 全部以 PQC 取代，抵抗未來量子電腦攻擊。從 PQC 演算法標準制定，到實務運用，仍有一段不短的距離。首先，密碼演算法通常不是單獨使用，而是組合於協定（Protocol）之中混合運用，因此常用的網路協定必須納入 PQC 標準。其次，組織或企業使用的 IT 系統可能龐大，即使 IT 管理人員也未必清楚何處使用 PKC，進而進行更換，可能需要新開發的「密碼發現」（Cryptographic Discovery）工具協助確認 PKC 之所在。再者，對應資料敏感程度排定更換 PKC 順序、供應鏈中哪些 PQC 產品適合採用，都必須審慎評估、擬定計畫執行。

全球最積極從事 PQC 遷移的國家，無疑是美國。除了 NIST 主導 PQC 標準制定，美國

總統更以簽署並頒布「國家安全備忘錄」（National Security Memorandum, NSM）一錘定音，風行草偃，由上至下推動 PQC 遷移。

一、PQC 協定

Open Quantum Safe（OQS）專案是一個由開源社群推動的重要計畫，主要目標是協助和促進電腦科學領域從傳統密碼學轉向 PQC 的過渡（OQS, n.d.）。OQS 專案包含兩項主要工作：命名為 liboqs 的開源程式庫，以及稱為 OQS-Provider 的整合協定與應用，所有相關的程式碼都公開於 Github 平臺。OQS 的最早發布可以追溯到 2018 年 4 月。2024 年 5 月發布的 0.10.0 版本進一步完善了各項程式實作。官方宣布，從 2024 年開始，OQS 將加入 Linux 基金會，並成為 Linux PQC 聯盟的一員。

liboqs 程式庫主要以 C 語言實作，除各種密碼系統的軟體實作外，更包括應用程序介面（Application Programming Interface, API）、測試平臺以及效能評比。同時，liboqs 也提供其他語言的包裝，例如 Python、Java 和 Rust。

OQS-Provider 作為整合工具，可以向後呼叫 liboqs 函式庫執行所需運算，並可以與現行的多項網路協定溝通，包括傳輸層安全協定（Transport Layer Security, TLS）、OpenSSH 協定、X.509 憑證標準，以及安全多用途網路郵件擴充（Secure Multipurpose Internet Mail Extensions, S/MIME）等。此外，liboqs 也被整合在許多其他的應用與環境中，例如 Microsoft PQC VPN、Thales eSecurity Go wrapper、Cisco、Debian 與 IBM Cloud 等。

執行 TLS 協定時，使用者會聯繫伺服器，並且協商出欲使用的密碼套組（Suite），此過程若與 PQC 無關，則 OQS-Provider 不會對協定進行修正。舉例而言，若此次連線決議採用 RSA，則遵照原本的 TLS 協定進行連線程序。反之，若使用者與伺服器決議用到 PQC，OQS-Provider 將會遵循以下三項網際網路工程任務組（Internet Engineering Task Force, IETF）頒布的標準與草稿，對協定進行修正。

（一）Hybrid key exchange in TLS 1.3；

（二）Internet X.509 Public Key Infrastructure: Algorithm Identiflers for ML-DSA；

（三）RFC 5208: Public-Key Cryptography Standards（PKCS）#8: Private-Key Information Syntax Speciflcation Version 1.2。

二、密碼敏捷性與金融機構 PQC 遷移

NIST 於 2020 年 7 月舉辦 PQC 遷移會議，該會議的主題之一，是配合 PQC 遷移之密碼敏捷性（Crypto Agility）（NIST, 2020）。在密碼協定設計中，密碼敏捷性是指能夠在多個密碼原型（Crypto Primitive，指低層級密碼演算法）之間進行切換的能力。具有密碼敏捷性的系統可以選擇使用哪種原型組合來實現特定的標準。如果一個安全系統的密碼演算法或參數可以輕易替換並且至少部分自動化，則被認為是密碼敏捷的。PQC 遷移提高人們對密碼敏捷之重要性的認識。

美國最大金融機構摩根大通集團（JPMorgan Chase & Co.）在該會議提出「全球金融機

構 PQC 轉型」（Post-Quantum Crypto Transition for Global Financial Institutions）報告（NIST, 2023），探討全球金融機構的 PQC 轉型，特別聚焦於摩根大通集團。它說明替換密碼基礎設施的主要組件以確保可信度、可靠性和互操作性的複雜性和挑戰。報告強調以資料為中心和基於風險的轉換方法、提升密碼政策、藉由密碼敏捷性推動採用 PQC，以及參與安全協定標準化的重要性。它詳細說明 PQC 轉換的時間表（如圖 14）、考慮事項、密碼敏捷性的挑戰以及對密碼系統使用者和提供者的要求。金融機構需要適應不斷演變的密碼系統標準，以在後量子運算時代增強安全性。

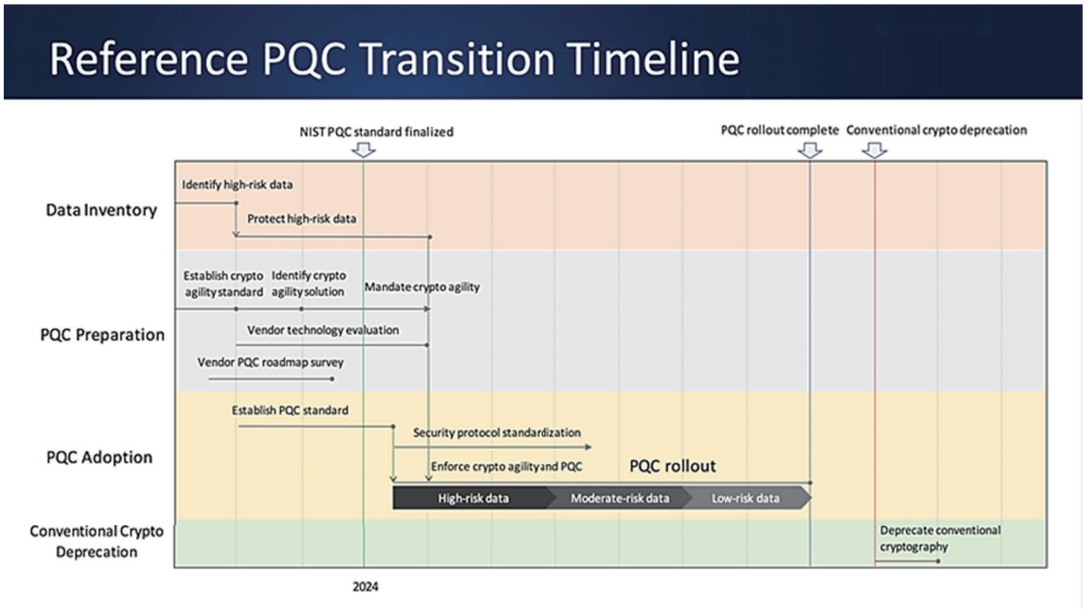

圖 14　摩根大通 PQC 轉型時間表

資料來源：NIST（2023）。

圖 14 時間表中有個關鍵年分：2024 年 PQC 標準定案。在此之前，有許多準備工作。首先是資料盤點（Data Inventory），識別高風險資料。PQC 的導入必須循序漸進，不該同時全面進行，高風險資料應優先以 PQC 保護。其次應建立密碼敏捷標準、識別密碼敏捷解決方案、在 PQC 標準確立後強制密碼敏捷。再來應進行供應商技術評估、供應商 PQC 路線圖調查。2024 年起依序對風險高、中、低資料推行 PQC，強制執行密碼敏捷。完成 PQC 布建之後，陸續淘汰傳統 PKC 系統、廢止其使用。

三、NSM 10

NSM 10 於 2022 年 5 月 4 日由拜登總統頒布（The White House, 2022），是一項旨在確保美國在量子運算領域保持領導地位，同時應對量子技術進步對密碼系統造成重大風險的戰略指示。本備忘錄概述一套綜合方法，以利用量子運算的潛力促進創新和經濟增長，同時保護國家安全和關鍵基礎設施。

NSM 10 的政策目標之一，是維持美國在量子資訊科學（Quantum Information Science, QIS）領域的競爭優勢。量子運算有望革新各領域，包括材料科學、製藥、金融和能源。該備忘錄強調，美國持續的技術和科學領導地位將顯著取決於其在量子運算和 QIS 方面的進步。

雖然量子運算提供許多好處，但它也帶來重大的風險，特別是對密碼系統。未來足夠先進的量子電腦，稱為密碼相關量子電腦（Cryptanalytically Relevant Quantum Computer, CRQC），可能破壞目前使用的許多 PKC。這種能力可能會危及民用和軍用通信、破壞關鍵基礎設施的監督和控制系統，以及破壞大多數基於網路的金融交易之安全性協議。

為減輕這些風險，NSM 10 指示聯邦機構啟動一項連續數年的過程，將脆弱的電腦系統遷移至 PQC。這涉及以下幾個關鍵步驟：

（一）密碼系統清單：機構必須對其目前的密碼系統進行全面清點，以識別漏洞，並優先考慮遷移到 PQC 解決方案的系統；

（二）標準的發展：備忘錄要求制定 PQC 標準。這項任務主要分配給 NIST，該機構負責創建和發布這些標準；

（三）合作與協調：NSM 10 強調政府機構、行業和學界之間合作的重要性。這種合作努力對於推進量子運算技術和開發強固的密碼標準至關重要；

（四）機密附件：備忘錄包含機密附件，涉及與量子運算相關的敏感國家安全問題。該附件提供額外的指導和指示，以確保保護重要的國家安全利益；

（五）NSM 10 的實施涉及幾個聯邦機構，每個機構都有特定的角色和責任。關鍵機構包括國防部、國土安全部、國家安全局和國家情報總監辦公室。這些機構負責監督遷移到 PQC，並確保遵守備忘錄中概述的指示；

（六）NSM 10 的成功實施預計將產生重大的經濟和戰略影響。藉由在量子運算方面保持領導地位，美國可以推動各領域的創新，引領新發現和進步。此外，轉移到 PQC 將增強關鍵基礎設施的安全性和韌性，保護其免受具有先進量子能力的對手之潛在威脅。

總結來說，NSM 10 闡述一套積極主動的戰略方法，旨在解決促進量子運算進步和減輕密碼系統相關風險的雙重挑戰。藉由明確的行動計劃並強調合作，NSM 10 目標是確保美國在量子技術方面保持領先地位，同時保護其國家安全和經濟利益。

四、NSA-CISA-NIST 聯合事實說明

美國網路安全與基礎設施安全局（CISA）、NSA 和 NIST 於 2023 年 8 月共同發布「量子就緒：遷移至後量子密碼學」（Quantum-Readiness: Migration to Post-Quantum Cryptography）聯合事實說明（Factsheet），為美國各機構，特別是支援關鍵基礎設施的機構，提供為量子運算的影響做好準備的準則（CISA, 2023; CISA, NSA and NIST, 2023）。重點包括：

（一）量子就緒路線圖：鼓勵各組織制定路線圖（Roadmap），以遷移至 PQC 標準。這涉及規劃和早期準備，以減輕與量子能力相關的風險；

（二）密碼系統清單：建議對現有的密碼系統進行全面盤點，以識別漏洞並優先考慮遷移至 PQC 系統；

（三）供應鏈考量：機構應評估其供應鏈，以瞭解與密碼系統相關的依賴關係和風險。與技術供應商討論 PQC 至關重要；

（四）技術供應商的參與：機構應與其技術供應商密切合作，以確保他們為遷移至 PQC 做好準備。這包括討論時間表、支援和實施策略；

（五）技術供應商的責任：供應商應藉由提供必要的更新、工具和指導，協助客戶在遷移過程中採用 PQC 解決方案。

這份事實說明旨在提高意識，並鼓勵採取積極措施，以確保平穩過渡到 PQC，從而保護關鍵基礎設施和敏感資訊免受未來量子威脅。

五、NIST SP 1800-38

美國 NIST 的 PQC Team 制定 PQC 國家標準，而 NIST 的國家網路安全卓越中心（National Cybersecurity Center of Excellence, NCCoE）則主導執行「遷移至後量子密碼」（Migration to Post-Quantum Cryptography）專案 （NIST, n.d.-a）。此專案啟動遷移實務之開發，從現今 PKC 平穩轉移至 PQC。

該專案包含兩項工作流程。密碼發現工作流程專注於使用密碼盤點工具，使組織能夠瞭解密碼系統如何保護重要數據和數位系統的機密性和完整性。發現工作流程還研究密碼系統清單如何支援風險管理和優先順序決策，以決定在何處實施利用 NIST 的 PQC 演算法標準的技術。互操作性（Interoperability）和效能（Performance）工作流程回答 PQC 演算法標準如何在 TLS 和安全外殼（Secure Shell, SSH）等通訊協定，以及硬體安全模組（Hardware Security Module, HSM）運作的問題。

該專案撰寫 NIST SP 1800-38（Newhouse et al., 2023），此特別出版文件於 2023 年 12 月發布草案，分為 ABC 三冊。此特別出版文件之目的，在於使各界警覺並瞭解遷移至後量子演算法所涉及的問題，以及盡快做好遷移的準備工作。

SP 1800-38A（Newhouse et al., 2023）為執行摘要，主要闡述整份指南發布的動機、遭遇的挑戰，以及對應的解決方法。此文件列出該專案的聯盟成員，如圖 15。

Consortium Members	
Amazon Web Services, Inc. (AWS)	JPMorgan Chase Bank, N.A.
Cisco Systems, Inc.	Microsoft
Crypto4A Technologies, Inc.	National Security Agency (NSA)
CryptoNext Security	PQShield
Dell Technologies	Samsung SDS Co., Ltd.
DigiCert	SandboxAQ
Entrust	Thales DIS CPL USA, Inc.
IBM	Thales Trusted Cyber Technologies
Information Security Corporation	VMware, Inc.
InfoSec Global	wolfSSL
ISARA Corporation	

圖 15　NCCoE 遷移至 PQC 專案聯盟成員

資料來源：Newhouse et al.（2023）。

SP 1800-38B（Newhouse et al., 2023）則搜羅各種方法與架構，著重於描述 NIST 構建後量子遷移流程的內容以及原因，包括風險分析方法、安全控管方法，以及隱私管制方法。文中將量子攻擊與風險劃分為三個主要來源：程式碼撰寫與開發流程、作業系統和應用程式的執行與程式庫呼叫、網路連線與協定。藉由對這三個方面的檢測，輔以風險分析與量化，可以得出不同項目對於遷移至 PQC 之急迫性，NIST 亦鼓勵各行業與機構依照自身現況訂定遷移計畫。

SP 1800-38C（Newhouse et al., 2023）彙整大量不同的實際應用情境下，PQC 系統的互操作性（Interoperability）以及效能（Performance）的測試結果。應用情境涵蓋各項主流協定，包括 SSH、TLS、Quick UDP Internet Connections（QUIC）和 X.509，以及 HSM 對於後量子演算法的支援程度。藉由商業夥伴以及於 IETF 黑客松（Hackathon）之中，對各項產品的描述與測試，NIST 對於遷移至 PQC 系統抱持樂觀，認為在 SSH 和 TLS 方面的挑戰可以克服。雖然衍生協議如 QUIC 的可用程度尚不如預期，但會有後續合作夥伴對其增援。同時，NIST 也認為在效能方面，Kyber 作為密鑰建立的標準演算法，與當前橢圓曲線技術具有競爭力，即使混合使用，也符合大部分的運用情境。

陸、結語

現今資通訊與網路科技廣泛使用 PKC，未來會被量子電腦破解，宜未雨綢繆。美國政府與產學界積極合作，不但已制定可防禦量子計算威脅的 PQC 標準，亦已著手規範政府機構與國家基礎建設全面轉移至 PQC。金融和電信，可能是最快跟進的產業。提供雲端服務的大型網路公司，如 Google、Microsoft、Amazon 等，更早已投入建置 PQC。歐洲各科技先進國迎頭趕上，支援 PQC 標準的產品如雨後春筍般上市。

臺灣學術界早在 20 年前即已參與 PQC 研究，過渡至 PQC 的實務工作亦當不落人後。臺灣的國安與國防之保密裝備研發單位，早在 2003 年即已知曉 Shor（1994, 1997）演算法對傳統 PKC 之威脅，並理解抵抗量子計算攻擊之 PKC 的存在，但當時尚不需採取任何行動。自 2016 年美國 NIST 啟動 PQC 標準制定競賽起，臺灣的國安與國防即高度關注，並與學術界及產業界合作，隨時掌握最新進展。2024 年 8 月 NIST 的 PQC 標準定案，國安與國防的 PQC 遷移亦進入新階段，準備導入 PQC 至保密裝備，滿足實務工作需要。

臺灣一般政府單位與民間企業的 PQC 遷移積極程度，則與國安與國防相去甚遠。原因不外乎：缺乏動機、缺乏方法。

資安產品的採購，是不會增加營收的開銷，風險意識不足便沒有動機為 PQC 投入額外的費用與工作。美國是由上至下推動 PQC，政府高層訂定強制性的 PQC 遷移政策，各單位均必須遵守。臺灣也需要藉由法遵增進 PQC 遷移的效率，例如由金管會制定規範，各金融單位遵行。

臺灣目前已有不少企業及機構聽聞 PQC 的重要性，但不知從何著手。美國 NIST NCCoE 執行 PQC 遷移專案，並發布 SP 1800-38 等指引文件，作法及文件內容均值得臺灣借鏡。

參考文獻

《電子簽章法》，2002 年 1 月 16 日，院臺經字第 0910080314 號令發布。

《電子簽章法》，2024 年 5 月 15 日，總統華總一義字第 11300039241 號令修正。

Barker E., Chen L., Roginsky A., Vassilev A., and Davis, R., 2018, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* (NIST SP 800-56A Rev. 3). doi:10.6028/NIST.SP.800-56Ar3

Barker E., Chen L., Roginsky A., Vassilev A., Davis R., and Simon S., 2019, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography* (NIST SP 800-56B Rev. 2). doi:10.6028/NIST.SP.800-56Br2

Bundesamt für Sicherheit in der Informationstechnik, 2024/1/29, "Position Paper on Quantum Key Distribution," *SQuaD*, https://www.squad-germany.de/en/position-paper-on-quantum-key-distribution/ (accessed September 1, 2024).

Cooper D. A., Apon D. C., Dang Q. H., Davidson M. S., Dworkin M. J., and Miller C. A., 2020, *Recommendation for Stateful Hash-Based Signature Schemes* (NIST SP 800-208). doi:10.6028/NIST.SP.800-208

CRYSTALS, n.d., "Cryptographic Suite for Algebraic Lattices," https://pq-crystals.org/ (accessed September 1, 2024).

Cybersecurity and Infrastructure Security Agency, 2023/8/21, "CISA, NSA, and NIST Publish Factsheet on Quantum Readiness," https://www.cisa.gov/news-events/alerts/2023/08/21/cisa-nsa-and-nist-publish-factsheet-quantum-readiness (accessed September 1, 2024).

Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, 2023/8/21, "Quantum-Readiness: Migration to Post-Quantum Cryptography," https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF (accessed September 1, 2024).

Diffie W., and Hellman M., 1976, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 22(6), 644-654. doi:10.1109/TIT.1976.1055638

Moody D., 2016, "Post-Quantum Cryptography: NIST's Plan for the Future" https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf (accessed September 1, 2024).

Moody D., 2022, "The Beginning of the End: The First PQC Standards," https://pkc.iacr.org/2022/slides/moody.pdf (accessed September 1, 2024).

Moody D., Perlner R., Regenscheid A., Robinson A., and Cooper D., 2024, *Transition to Post-Quantum Cryptography Standards* (NIST IR 8547 [Initial Public Draft]). doi:10.6028/NIST.IR.8547.ipd

Mosca M., 2015/4/3, "Cybersecurity in a Quantum World: Will We Be Ready?" https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/

presentations/session8-mosca-michele.pdf (accessed September 1, 2024).

Mosca M., and Piani M., 2021/1, "2021 Quantum Threat Timeline Report," *Global Risk Institute*, https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/ (accessed September 1, 2024).

National Cyber Security Centre, 2020/3/24, "Quantum Security Technologies," https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (accessed September 1, 2024).

National Institute of Standards and Technology, n.d.-a, "Migrating to Post-Quantum Cryptography," https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (accessed September 1, 2024).

National Institute of Standards and Technology, n.d.-b, "Post-Quantum Cryptography: Overview," https://csrc.nist.gov/Projects/post-quantum-cryptography (accessed September 1, 2024).

National Institute of Standards and Technology, 2001, *Advanced Encryption Standard* (AES) (FIPS 197). doi:10.6028/NIST.FIPS.197-upd1

National Institute of Standards and Technology, 2020/10/7, "Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms," https://www.nccoe.nist.gov/get-involved/attend-events/virtual-workshop-considerations-migrating-post-quantum-cryptographic (accessed September 1, 2024).

National Institute of Standards and Technology, 2023, *Digital Signature Standard (DSS)* (FIPS 186-5). doi:10.6028/NIST.FIPS.186-5

National Institute of Standards and Technology, 2024a, *Module-Lattice-Based Digital Signature Standard* (FIPS 204). doi:10.6028/NIST.FIPS.204

National Institute of Standards and Technology, 2024b, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (FIPS 203). doi:10.6028/NIST.FIPS.203

National Institute of Standards and Technology, 2024c, *Stateless Hash-Based Digital Signature Standard* (FIPS 205). doi:10.6028/NIST.FIPS.205

National Security Agency, 2020, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (accessed September 1, 2024).

National Security Agency, 2022/9, "Announcing the Commercial National Security Algorithm Suite 2.0," https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF (accessed September 1, 2024).

National Security Agency, 2024/4, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF (accessed September 1, 2024).

Newhouse W., Souppaya M., Barker W., Brown C., Kampanakis P., Manzano M., McGrew D., Dames A., Soukharev V., Lafrance P., Hu A., Hook D., Garcia R., Gervis E., Kim E., Lee

C., 2023/12/19, *Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography* (NIST SP 1800-38), https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1) (accessed September 1, 2024).

Open Quantum Safe, n.d., "Home," https://openquantumsafe.org/ (accessed September 1, 2024).

Rivest R. L., Shamir A., and Adleman L., 1978, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 21(2), 120-126. doi:10.1145/359340.359342

Schneier B., 2018/8/1, "GCHQ on Quantum Key Distribution," *Schneier on Security*, https://www.schneier.com/blog/archives/2018/08/gchq_on_quantum.html (accessed September 1, 2024).

Shor P. W., 1994, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Los Alamitos, CA: IEEE Computer Society Press, 124-134. doi:10.1109/SFCS.1994.365700

Shor P. W., 1997, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, 26(5), 1484-1509. doi:10.1137/S0097539795293172

The White House, 2022/5/4, "National Security Memorandum on Promoting United States Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems," https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed September 1, 2024).

Yang B.-Y., Chen J.-M., and Chen Y.-H., 2004, "TTS: High-Speed Signatures on a Low-Cost Smart Card," in M. Joye and J.-J. Quisquater (Eds.), *Cryptographic Hardware and Embedded Systems─CHES 2004*, Berlin, Germany: Springer. pp. 371-385. doi:10.1007/978-3-540-28632-5_27