金融業後量子密碼 (PQC) 遷移指引

李依珊‡、左瑞麟 [2]
[1、2] 國立政治大學 資訊科學系
[1]110753501@nccu.edu.tw、[2]raylin@cs.nccu.edu.tw

摘要

量子電腦的發展已是科技界的熱門話題，它的出現顛覆了我們對電腦的想像，量子運算也有望解決我們地球面臨的一些挑戰，包括環境、農業、健康、能源、氣候、材料科學等領域。對於其中一些問題，隨著系統的成長，傳統運算越來越受到挑戰，量子系統將會有超過現今最強大超級計算機的能力，例如現今電腦安全系統中，必定會運用到的加密與電子簽章技術，早在 1994 年時，Peter Shor 發現了一種可用於整數分解的量子演算法，其執行速度會以指數方式快過已知最好的傳統演算法，能夠破解作為現今電子商務安全性基礎的眾多公開金鑰密碼編譯系統，包括 RSA 和橢圓曲線密碼 (Elliptic Curve Cryptography)，有朝一日量子電腦成功製造出來後，攻擊者將能夠破解當今世界上使用的主要公鑰密碼系統，所以我們需要提前準備避免對現今密碼學的破壞性影響。而為了應對量子破密的潛在威脅，美國 NIST 在 2024 年 8 月 13 日公布了歷經 8 年選出的後量子密碼學 (PQC) 標準，其中 3 個新的聯邦資訊處理標準 (FIPS)，分別是 FIPS 203、FIPS 204 與 FIPS 205，第 4 個 PQC 標準將於 2024 年底推出。因此評估採用後量子密碼 (PQC) 來確保數據的安全性，及後量子密碼的遷移計畫已是刻不容緩的工作。

關鍵詞：金融安全、後量子密碼、後量子密碼遷移策略

*通訊作者 (Corresponding author.)

Post-Quantum Cryptography (PQC) Migration Guide for Financial Institutions

Yi-Shan Lee[1], Raylin Tso[2*]
[1, 2]Department of Computer Science, National Chengchi University
[1]110753501@nccu.edu.tw, [2]raylin@cs.nccu.edu.tw

Abstract

The development of quantum computers has become a hot topic in the technology world. The emergence of quantum computers has subverted our imagination of computers. Quantum computing is also expected to solve some of the challenges facing our planet, including the environment, agriculture, health, energy, climate, and materials science. For some of these problems, with the growth of the system, traditional computing is increasingly challenged. Quantum systems will have capabilities beyond today's most powerful supercomputers. For example, in today's computer security systems, encryption and digital signature technologies must be used. As early as 1994, Peter Shor discovered a quantum algorithm that can be used for integer decomposition. Its execution speed will be exponentially faster than the best known traditional algorithms, and it can crack many public key cryptography systems that are the basis of today's e-commerce security, including RSA and Elliptic Curve Cryptography. Once a quantum computer is successfully manufactured, attackers will be able to crack the main public key cryptography systems used in the world today. Therefore, we need to prepare in advance to avoid the destructive impact on current cryptography. In order to deal with the potential threat of quantum cracking, the US NIST announced the Post-Quantum Cryptography (PQC) standard selected after 8 years on August 13, 2024, including 3 new Federal Information Processing Standards (FIPS), which are FIPS 203, FIPS 204 and FIPS 205 respectively. The 4th PQC standard will be launched at the end of 2024. Therefore, evaluating the adoption of Post-Quantum Cryptography (PQC) to ensure data security, and the migration plan of Post-Quantum Cryptography is an urgent task.

Keywords: Financial Security, Post-Quantum Cryptography, PQC Migration Strategy

壹、前言

量子電腦的發展進度，一直是大家所關注的議題，除了新技術有望助於解決一些問題，新技術也可能摧毀現有的加密系統，所以持續關心國內外發展進程是亦是重要的工作。Google 在量子電腦的發展歷程中取得了許多重要的里程碑。根據 2023.07 的報導，Google 的 Sycamore 量子電腦展示了驚人的運算能力，能夠在 6 秒鐘內完成傳統超級電腦需要 47 年才能完成的任務 [12]。此外，根據 2024.11 的報導，Google 的量子 AI 部門正在使用 Nvidia 的 Eos 超級電腦來加速量子處理器的設計，這將有助於克服現今的硬體限制 [7]。

IBM 於 2022.05 公布了最新的量子電腦發展路線圖，計劃在 2025 年推出超過 4,000 個量子位的系統 [1]。這些系統將結合模組化量子處理器與 Qiskit Runtime 的經典基礎架構，讓使用者可以輕鬆地將量子運算部署在其工作流程中。此外，IBM 計劃在十年內打造出 100,000 個量子位元的量子電腦，這將有助於解決目前超級電腦無法處理的複雜問題。根據 2023.12 的報導，IBM 還推出了第一台模組化量子電腦 IBM Quantum System Two，這是 IBM 以量子為中心的超級運算架構的基礎，這套系統的原型預計將在 2023 年推出與運行 [2]。這些進展顯示出 IBM 在量子電腦領域亦有的巨大潛力。

此外，在近期 2024.10 的報導中，一家美國新興公司 Atom Computing，推出了擁有 1,180 個量子位元的量子電腦，不僅超越了 IBM 神鷹量子電腦的 1,121 個量子位元，甚至德國達姆施塔特工業大學也宣布開發出 1,305 個量子位元的超級電腦 [5]。而國內也在 2024.11 傳出，中央研究院南部院區第 3 期開發的量子科技實驗大樓在當月舉行動土儀式，規劃設置高精密量測實驗室、製程實驗室、光學實驗室、元件分析實驗室等 [10]。誰能成為量子計算的最終霸主，仍然是未解之謎。或許在不遠的將來，將重新定義我們對計算、數據與科技的理解。

貳、國內現行金融機構密碼要求相關法規

量子電腦將以我們無法想像的速度改變世界，隨著量子計算技術的發展，傳統的加密方法可能會被破解。現行國內金融機構資訊安全有關加密系統與數位簽章要求亦皆制定於規範中，初步整理如表一。

表一、金融機構資訊加密與數位簽章相關規範整理

法規	加密要求	數位簽章
金融機構辦理電子銀行業務安全控管作業基準[9]	1. 對稱性加解密系統至少採用 3DES 112bits 以上、AES 128bits 以上或其他安全強度相同之演算法；惟應用於 TLS 時，不得使用 3DES 演算法並建議使用數據認證加密模式(Authenticated Encryption with Associated Data, AEAD) 2. 非對稱性加解密系統應至少採用 RSA 2048bits 以上、ECC 256bits 以上或其他安全強度相同之演算法依協商訊息加密金鑰(如 Diffie-Hellman Key Agreement)	1. 符合我國電子簽章法之數位簽章者 2. 或非我國憑證機構通過 WebTrust 或 ETSI 認可具密碼保護且可應用於法人金融交易簽章之憑證、第七條第二款或第三款安全設計，並使用安全元件 (Secure Element)、可信賴執行環境(Trusted Execution Environment)、安全載具(如動態密碼產生器)或增強防護機制之行動裝置應用程式軟硬體
金融機構辦理快速身分識別機制安全控管作業指引[8]	應採用 AES 128 bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行加密運算，應採用 TLS 1.2 (含)以上之通訊協定並使用 Elliptic Curve Diffie-Hellman Exchange 方式進行金鑰交換	應採用 SHA256 以上或其他安全強度相同(含)以上之演算法進行押碼，及採用 RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行數位簽章
證券期貨市場相關公會新興科技資通安全管控指引[11]	應採用 AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同含以上之演算法進行加密運算，應採用 TLS 1.2(含)以上之通訊協定並使用 Elliptic Curve Diffie-Hellman Exchange 方式進行金鑰交換	應採用 SHA 256 bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同 含以上之演算法進行押碼、加密運算或數位簽章
信用卡業務機	對稱性加解密系統：	應採用可防止蓄意篡改訊息之

法規	加密要求	數位簽章
構辦理行動信用卡業務安全控管作業基準[6]	1. 美國國家標準與技術中心(National Institute of Standards and Technology；以下簡稱 NIST)之三重資料加密演算法 (Triple Data Encryption Algorithm；以下簡稱 TDEA 演算法)，金鑰有效長度為 112 位元雙金鑰之三重資料加密演算法 (Two Key Triple Data Encryption Algorithm；以下簡稱 2TDEA)或 168 位元三金鑰之三重資料加密演算法 (Three Key Triple Data Encryption Algorithm；以下簡稱 3TDEA)。 2. NIST 之進階加密標準(Advanced Encryption Standard；以下簡稱 AES 演算法)，金鑰長度為 128、192 或 256 位元。 非對稱性加解密系統： 1. RSA 加密標準 (Rivest、Shamir、Adleman Encryption Standard ；以下簡稱 RSA 演算法)，金鑰長度 1024 位元(含以上)且必須為 EMVCo 組織公告之有效長度。 2. 橢圓曲線數位簽章演算法(Elliptic Curve Digital Signature Algorithm；以下簡稱 ECDSA 演算法)，質數模數為 256 位元(P-256)。	加解密技術，可採對稱性加解密系統進行押碼 (Message Authentication Code, MAC) 或非對稱性加解密系統產生數位簽章 (Digital Signature) 等機制。 (一)對稱性加解密系統應採用下列演算法之一： 1. TDEA 演算法，金鑰有效長度為 112 位元 (2TDEA) 或 168 位元 (3TDEA)。 2. AES 演算法，金鑰長度為 128、192 或 256 位元。 (二)非對稱性加解密系統應採用下列演算法之一： 1. RSA 演算法，金鑰長度 1024 位元(含以上)且必須為 EMVCo 組織公告之有效長度。 2. ECDSA 演算法，質數模數為 256 位元 (P-256)。

參、美國後量子密碼 (PQC) 標準與遷移計畫研究進度

根據美國國家標準暨技術研究院 (NIST) 於 2024 年 8 月 13 日正式發布了三項後量

子密碼 (PQC) 標準，旨在應對未來量子計算可能對現有加密系統帶來的威脅[3]。這三項標準如下表二：

表二、美國國家標準暨技術研究院 (NIST) 發布後量子密碼 (PQC) 標準

標準	名稱	發展演算法	特點說明
FIPS 203	模組格基金鑰封裝機制標準 (ML-KEM)	CRYSTALS-Kyber	適用於一般加密，具有金鑰尺寸小、交換方便且執行速度快
FIPS 204	模組格基數位簽章標準 (ML-DSA)	CRYSTALS-Dilithium	提供數位簽章功能，確保資料完整性與身份驗證
FIPS 205	無狀態雜湊基數位簽章標準 (SLH-DSA)	SPHINCS+	採用不同的數學方法，作為備用方案，增強數位簽章的安全性
FIPS 206	(預計 2024 年底發布)	FALCON	進一步豐富加密工具組的多樣性

NIST 強調，隨著量子計算技術的快速發展，未來可能出現能破解現有加密方法的設備。因此，NIST 鼓勵各界盡早開始轉換至這些新標準，並將其整合到現有系統中，因為全面轉換的過程將需要一定的時間。而如何將現有的加密系統轉換為能夠抵禦量子計算攻擊的新型加密技術，而這個遷移過程涉及多個步驟，包括評估現有系統的安全性、選擇合適的 PQC 演算法、進行測試和驗證，以及最終在生產環境中部署新的加密技術等，這將是一個複雜且需要協作的過程。

美國網路安全暨基礎設施安全局 (CISA)、國家安全局 (NSA) 和美國國家標準與技術研究所 (NIST) 於 2023.08 共同完成一份說明文件 【Quantum-Readiness: Migration to Post-Quantum Cryptography】，這份資料表旨在告知那些支持關鍵基礎設施的組織，有關量子技術能力影響的資訊，並鼓勵透過制定量子就緒路線圖儘早規劃遷移到後量子加密標準[4]。在文件中提出成功的後量子密碼遷移需要時間來規劃和實施，並提供了針對量子計算威脅的全面應對策略，涵蓋了從風險評估到技術實施的詳細步驟，而組織需要跨部門合作，逐步落實建議，以實現安全的量子轉型。以下條列文件中所提到的目標及步驟：

- 建立量子準備路線圖：建立專門的項目管理團隊，針對量子計算對現有加密技術的威脅進行應對規劃。

    1. 成立專業團隊來領導量子遷移工作。

2. 對組織內部現有密碼技術進行詳細調查。
3. 針對不同系統的量子威脅風險，分級制定優先處理順序。
4. 制定逐步實施計劃，包括時間表和資源分配。

- 建立加密清單：全面盤點所有依賴量子脆弱技術的資產。
  1. 使用自動化工具定位並識別加密技術的應用範圍，包括協議 (如 TLS、VPN)、硬件設備和軟件。
  2. 統整資產管理與身份管理系統中的數據，確認依賴現有加密技術的應用程式。
  3. 根據風險和影響，建立清單，將需要重點關注的系統列為優先遷移對象。
- 與供應商合作：確保外部供應商對量子威脅的應對計劃與組織同步。
  1. 要求供應商提供產品中密碼算法的詳細清單，確定是否含有量子脆弱的技術。
  2. 與供應商協商，要求未來產品支持 NIST 批准的 PQC。
  3. 在新合同中明確規範供應商的 PQC 遷移責任。
  4. 討論現有系統的升級路徑，減少對過時加密技術的依賴。
- 管理供應鏈量子準備：協調供應鏈中使用的所有加密技術，確保統一的 PQC 遷移步驟。
  1. 辨識供應鏈依賴的高風險量子脆弱系統。
  2. 確保供應商與供應鏈中其他合作方同步進行 PQC 升級。
  3. 為遺留系統 (legacy systems) 設計升級或替代方案。
  4. 對於自建技術，確定是否需要進行內部重新設計。
- 與雲服務供應商協調：保障雲服務的安全性與未來兼容性。
  1. 確保雲服務供應商明確提供其支持 PQC 的計劃時間表。
  2. 評估供應商的服務架構，以確認對現有加密技術的依賴程度。
  3. 制定未來配置更新的計劃，確保雲環境無縫遷移至 PQC。
- 進行風險評估：了解量子威脅對現有系統的具體影響。
  1. 將加密清單中的系統輸入風險評估流程。
  2. 分析每個系統的數據敏感性、長期保密需求以及量子威脅暴露風險。
  3. 優化資源分配，集中力量處理高優先級項目。
- 測試與實施過渡技術：在正式部署 PQC 前，測試過渡解決方案(如混合加密)。
  1. 評估現有的過渡技術，如 Classic McEliece 或 NTRU。
  2. 在低風險環境中試驗混合加密模式，確保與舊系統的兼容性。
  3. 持續監控 NIST PQC 標準的發布進度，根據最新建議調整測試範圍。
- 規劃全面遷移：制定全面且實用的遷移計劃，覆蓋技術和管理層面。
  1. 確保系統升級符合 NIST PQC 標準。

2. 制定培訓計劃，提升內部團隊的 PQC 知識與技能。
3. 預留資金，支援可能的硬件升級與軟件重寫需求。

- 監控與更新：持續追蹤量子計算與 PQC 技術的最新進展。
  1. 建立長期的技術監控機制，追蹤量子計算進展。
  2. 更新組織的密碼政策，確保與國際最新標準一致。
  3. 定期審查並測試已部署的 PQC 系統，確保安全性與性能。

肆、國內金融機構後量子密碼遷移步驟指引

金融機構在資本市場中扮演著資金流動的中介角色，能有效將資金從儲蓄者轉移到需要資金的企業和個人，促進經濟增長對於國家的經濟穩定和發展至關重要，因此應該加速規劃後量子密碼的遷移計畫，以應對未來可能出現的安全挑戰。在遷移到後量子密碼 (Post-Quantum Cryptography, PQC)，需要採取系統化和漸進的策略，以確保現有系統的安全性和穩定性。以下是金融業在實施後量子密碼遷移時的策略與方法步驟：

1. 評估風險與現狀分析
   - 盤點加密資產：識別並列出所有使用現代加密算法的系統、應用和數據流。這包括數據庫、應用服務器、網絡通信、備份和存儲系統等。
   - 風險評估：評估現有加密系統在量子計算機出現時的風險，確定哪些系統和數據最需要保護。
2. 設立專責團隊
   - 設立專項小組：成立專門的小組，包括加密專家、IT 專家和業務代表，負責遷移計劃的制定和執行。
   - 建立與核心業務溝通機制：成員對組織與業務組織應有一定認識，能適時與相關業務成員溝通，掌握計畫執行進度與情形，並確保各部門之間的信息共享和協作。
   - 供應鏈協作：與供應商和合作夥伴進行溝通，確保他們將後量子安全性納入考量，並協助了解其產品如何支持遷移計畫，確保整個供應鏈都能夠適應新的安全標準。
3. 制定遷移計劃
   - 設定目標和里程碑：確定遷移計劃的具體目標和里程碑，設定明確的時間表和資源分配。
   - 計畫分階段遷移：適度分階段遷移，避免衝擊業務系統運作，以降低實施過程中的風險。
4. 選擇合適的後量子加密算法
   - 算法評估：研究並評估各種後量子加密算法，選擇適合金融業應用場景的算

法，如基於格的加密算法(如 CRYSTALS-Kyber)。參考 NIST(國家標準與技術研究院)的後量子加密算法標準化進程。

- 實驗和測試：在實驗環境中測試選定的後量子加密算法，評估其性能、安全性和可操作性。

5. 系統調整與優化
   - 系統兼容性檢查：檢查現有系統與選定的後量子加密算法的兼容性，識別需要修改和更新的部分，確保能夠支持新選擇的後量子加密算法。
   - 考慮混合加密方案：在過渡期間，同時使用現有加密算法和後量子加密算法進行雙層加密，確保順利過渡。
6. 培訓和意識提升
   - 員工培訓：對員工進行後量子加密技術的培訓，確保他們了解新技術的應用和運用方法。
   - 安全意識提升：提升整個組織的安全意識，強調遷移到後量子加密的重要性和必要性。
7. 測試與驗證
   - 試點測試：在小範圍內進行試點測試，以驗證新系統和算法的有效性和穩定性。
   - 反饋與修正：收集反饋並根據測試結果進行必要的調整。
8. 實施和部署
   - 分階段部署：按照遷移計劃及試點測試結果，分階段部署後量子加密算法，逐步替換現有的加密系統，並在全組織內推廣新系統及算法。
   - 監控和調整：在部署過程中進行實時監控，根據反饋和性能數據進行調整，確保遷移過程順利進行。
9. 持續改進和更新
   - 定期評估：定期評估後量子加密系統的性能和安全性，並持續追蹤後量子密碼技術的發展和新興威脅，根據最新的安全威脅和技術進步進行更新和改進。
   - 合規性檢查：確保新系統符合金融業的相關法律法規和行業標準，進行定期的合規性檢查和審計。

金融業在遷移到後量子密碼時，需要採取系統化、全面且漸進的策略。通過評估現有加密基礎設施、設立專責團隊、制定遷移計劃、選擇合適的後量子加密算法、系統兼容性檢查調整與優化、進行員工培訓和意識提升、試點測試與驗證、分階段實施和部署，以及持續改進和更新，以有效地過渡到後量子加密技術，確保在量子計算時代來臨時依然保持高度的數據安全性。

伍、結論

本指引探討了量子運算發展對金融業密碼學安全的影響，並提供了金融機構遷移至後量子密碼 (PQC) 策略與實施步驟。隨著量子技術的快速進步，傳統公鑰加密系統如 RSA 和 ECC 可能面臨無法抵禦量子攻擊的風險，因此，儘早規劃 PQC 遷移對於維持金融安全至關重要。透過本研究，我們回顧了美國 NIST 最新公布的 PQC 標準 (FIPS 203、FIPS 204、FIPS 205)，並分析其適用性。金融機構應採取系統化的方法，包括：風險評估、資產盤點、供應鏈協作、技術測試與驗證、逐步實施 PQC，以及持續監控與調整，以確保過渡期間業務運營的穩定性和安全性。

此外，針對國內法規與國際標準的比較，我們發現現行金融機構的密碼技術標準仍然以傳統加密演算法為主，對於 PQC 的具體規範尚待發展。因此，金融監管機構應及早制定遷移指引，以引導業界安全過渡至後量子密碼技術。總結而言，本研究強調了 PQC 遷移的迫切性與挑戰，並提供可行的技術策略。未來研究可進一步探討 PQC 在實際金融場景中的部署細節，如效能優化、混合加密方案，以及與現有安全架構的兼容性，確保金融體系在量子時代的安全穩健發展。

參考文獻

[1] Kate Liu, “IBM 公布最新實用量子發展路線圖：2025 年推出超過 4,000 量子位的系 , ”IBM Taiwan, https://taiwan.newsroom.ibm.com/2022-05-10-IBM-2025-4,000 (accessed Dec. 2024).

[2] Kate Liu, “新一代 IBM 量子處理器「蒼鷺」Heron 與 IBM Quantum System Two 亮 , ”IBM Taiwan, https://taiwan.newsroom.ibm.com/2023-12-20-IBM-Heron-IBM-Quantum-System-Two (accessed Dec. 2024).

[3] NIST, “NIST releases first 3 finalized Post-Quantum Encryption standards”, NIST.gov, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (accessed Dec. 2024).

[4] NIST, “Quantum-Readiness: Migration to Post-Quantum Cryptography”, CISA.gov, https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf (accessed Dec. 2024).

[5] PanSci, “從離子阱到拓樸量子位元：量子計算的未來還有多少可能?,” 泛科學, https://pansci.asia/archives/377925 (accessed Dec. 2024).

[6] 中華民國銀行商業同業公會全國聯合會, “信用卡業務機構辦理行動信用卡業務安全

控管作業基準”, 植根法律網, https://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040390041061000-1070409 (accessed Dec. 2024).

[7] 季晶晶, “Nvidia 襄助 Google 設計量子運算處理器 進行科技業的長期賭注,” 聯合新聞網, https://udn.com/news/story/6811/8369031 (accessed Dec. 2024).

[8] 金融 FIDO 聯盟, “金融機構辦理快速身分識別機制安全控管作業指引,” 植根法律網, https://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040390021002700-1120425 (accessed Dec. 2024).

[9] 金融業務電子化委員會, “金融機構辦理電子銀行業務安全控管作業基準,” 中華民國銀行商業同業公會全國聯合會, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjcppDGhYaKAxXwh68BHVVYCgkQFnoECAwQAQ&url=https%3A%2F%2Fwww.ba.org.tw%2FFileDownload%2FDownload%3FFileId%3D5ede5db7-e60b-4748-b6cc-bd5bd9d4dbcb%26FileName%3D%25E9%2599%2584%25E4%25BB%25B61_%25E9%2587%2591%25E8%259E%258D%25E6%25A9%259F%25E6%25A7%258B%25E8%25BE%25A6%25E7%2590%2586%25E9%259B%25BB%25E5%25AD%2590%25E9%258A%2580%25E8%25A1%258C%25E6%25A5%25AD%25E5%258B%2599%25E5%25AE%2589%25E5%2585%25A8%25E6%258E%25A7%25E7%25AE%25A1%25E4%25BD%259C%25E6%25A5%25AD%25E5%259F%25BA%25E6%25BA%2596.pdf&usg=AOvVaw25g148o2DkUiESB-D8ivKy&opi=89978449 (accessed Dec. 2024).

[10] 陳政偉, “中研院南院量子大樓動土 打造國家研究基地,” 中央通訊社, https://www.cna.com.tw/news/ahel/202411220250.aspx (accessed Dec. 2024).

[11] 臺灣證券交易所, “證券期貨市場相關公會新興科技資通安全管控指引,” 臺灣證券交易所法規分享知識庫, https://twse-regulation.twse.com.tw/m/LawContent.aspx?FID=FL098969 (accessed Dec. 2024).

[12] 錢玉紘, “Google 量子電腦大進展！超級電腦花 47 年的運算，它只要 6 秒，霸權之爭結束了?,” 數位時代, https://www.bnext.com.tw/article/76065/google-quantum-computer-supercomputer? (accessed Dec. 2024).