SAMSUNG

Samsung Knox 助力啟動量子安全新未來

自 Galaxy S25 旗艦系列起，三星電子積極拓展新型態先進行動安全領域 - 後量子密碼學 (post-quantum cryptography, PQC)。該技術採用進階演算法，預防量子運算對傳統加密方式所帶來的風險。

三星新聞中心將利用本文剖析數位資安的未來發展，揭露三星超前部署的原因。

高瞻遠矚 防患未然

量子運算是現代科技中極具影響力的領域，其無與倫比的問題解決能力，足以掀起翻天覆地的變革。一旦成功駕馭量子電腦，原本複雜的挑戰將立刻迎刃而解，運算效率更較傳統技術呈指數級增長，推動從醫藥到物流等諸多產業的突破。例如，量子演算法能簡化供應鏈流程或提升運輸系統的準點率。

然而，此龐大的運算能力亦伴隨風險。由於當今用於保護資料的特定加密方式可能遭量子演算法破解，因此勢必要建立針對性防護機制，才能保障日後的資料安全。

儘管量子運算預期不會立即全面採用，但及早採取行動是一大關鍵，如此才能防範「先竊取、後解密」的威脅，亦即攻擊者先收集資料，將來再以量子技術進行解密。

重新定義防禦標準

三星正如火如荼地發展 PQC 技術，確保加密資料在進入量子世代後仍舊安全無虞。

為抵擋量子電腦的攻擊，三星謹守由國家標準和科技機構 (NIST)[註一] 所推薦的多項標準。例如，ML-KEM (模組化網格金鑰封裝技術) 演算法採用的網格運算是一種複雜的多維結構，即便是量子電腦也極難破解。該演算法最適合用於保護串聯裝置之間的通訊安全，不僅提供堅若磐石的防禦，還能最佳化效能並盡可能減少資料交換。

NIST 的 PQC 標準可廣泛應用於確保電子資訊安全，涵蓋機密文件到電子商務交易等諸多方面。對三星而言，這便是讓雲端資料免受量子威脅的未雨綢繆之道。

三星的策略方針

因應量子運算等技術的演變，三星將為 Samsung Knox Matrix 導入後量子進階資料防護(EDP)，以旗下領先業界的防護機制將串聯裝置生態圈納入保護傘，守護用戶資料。

當透過三星雲端服務進行個人資料備份、還原或同步時，三星的 EDP 功能可為用戶資料提供端對端加密。

將 PQC 技術整合至 Knox Matrix 後，相當於多一層防護，同時將行動裝置的雲端安全推升至嶄新境界。Knox Matrix 的跨裝置相容性將築起滴水不漏的量子安全防火牆，致力把關三星雲端備份及智慧型裝置、智慧顯示器和數位家電間的資料同步。

該功能將支援首搭載 One UI 7 的全新 Galaxy S25 旗艦系列，為 Galaxy 用戶提供強大的保護措施，抵禦量子電腦招致的威脅。

由三星引領的安全未來

在瞬息萬變的數位版圖中，迎戰潛在威脅不僅是選擇，更是必然。隨著量子運算時代在即，構築具前瞻性的資料安全網更是刻不容緩。

Galaxy S25 旗艦系列是業界首款支援 PQC 雲端資料防護的裝置，為即將到來的量子運算世代奠定極高標準。展望未來，三星將持續引領行動安全產業並打造美好未來，讓消費者安心享受聯網體驗。

註一：NIST 已確立一系列的加密演算法準則，旨在抵禦來自量子電腦的網路攻擊。全新標準因應未來趨勢，載明於 NIST 後量子密碼學（PQC）標準化專案中首批完成的標準。

參考文獻

聯邦資訊處理標準（FIPS）之公開文獻：FIPS 203-模組化網格金鑰封裝技術標準；FIPS 204-模組化網格數位簽章標準；及 FIPS 205-無狀態雜湊數位簽章標準（2024 年 8 月 14 日）。聯邦公報。

摘錄自：https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

國家標準暨技術研究院（2025 年 1 月 2 日）。NIST。

摘錄自：https://www.nist.gov/

NIST 發布前三項後量子加密標準最終版（2024 年）。NIST。

摘錄自：

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards