新聞稿


# 意法半導體推出後量子密碼學解決方案，為嵌入式系統提供量子抗性

*後量子密碼學新演算法已整合於通用微控制器、安全微控制器及車用微控制器中*

**【臺北訊，2025年4月8日】—** 服務橫跨多重電子應用領域之全球半導體領導廠商意法半導體（STMicroelectronics，簡稱ST；紐約證券交易所代碼：STM）推出了硬體加密加速器及相關軟體庫，適用於通用微控制器和安全微控制器，為未來嵌入式系統提供抗量子攻擊的防護。

隨著量子電腦在研究測試中逐漸超越傳統電腦，產業已開始為量子電腦進入主流應用做準備。新的政府規範正在標準化後量子密碼學（Post-Quantum Cryptography，PQC），並採用依賴數學問題的技術，這些問題對量子電腦來說難以解決。至今推出的 PQC 標準已採用屢獲殊榮的 Keccak 演算法，這是一種由意法半導體專家發明、具有高度抗性的雜湊演算法。

因應現行標準的資安要求，市場已迫切需要合適的解決方案，協助產品開發人員依據現行最佳實務建立防護機制，並隨著技術水準的演進，持續強化抵禦能力。意法半導體的全新解決方案，現已整合於 STM32 開發人員可使用的 X-CUBE-PQC 軟體函式庫中，亦適用於內建 SHA-3 硬體加速器的 Stellar 車用微控制器。此外，ST 亦針對安全微控制器推出新的軟體函式庫與硬體 IP，支援 Common Criteria 與 FIPS 140-

3 標準，並涵蓋 ML-KEM、ML-DSA 及 XMSS/LMS[1] 等 PQC 演算法。

意法半導體安全平台總監 Jacques Fournier 表示，「量子電腦預計將在金融、科學研究、地球觀測等領域帶來顯著優勢，但同時，它們也可能突破目前日常設備中使用的某些密碼學技術。意法半導體是首家在其所有產品系列中提供量子抗性功能的公司，並為所有客戶、所需的安全等級，提供對應的解決方案。」

意法半導體推出的後量子密碼學資產已準備就緒，幫助客戶將量子抗性技術應用於其產品的關鍵安全功能，如韌體更新、安全啟動及身份驗證機制。

欲了解更多有關意法半導體在後量子密碼學（PQC）領域的成果，請點擊此處。



**關於意法半導體**

意法半導體擁有 50,000 名研發與製造專業人才，掌握完整的半導體供應鏈，並營運多座先進晶片製造廠。作為垂直整合製造商（IDM），我們與超過 20 萬家客戶及數千家合作夥伴緊密合作，開發創新產品、解決方案與生態系統，以回應市場需求並迎接產業挑戰，同時推動永續發展。我們的技術支援更智慧的交通應用、更高效的能源管理，以及大規模雲端連網自主裝置的應用。公司正積極邁向碳中和目標，涵蓋範疇 1 和範疇 2 的直接與間接排放，以及產品運輸、商務差旅與員工通勤的範疇 3 排放，並計劃在 2027 年底前全面採用 100% 再生能源。欲了解更多資訊，請造訪 www.st.com。

[1] ML-KEM（即 CRYSTALS-Kyber，FIPS-203）、ML-DSA（即 CRYSTALS-Dilithium，FIPS-204）以及 LMS/XMSS（Leighton-Micali Signature / eXtended Merkle Signature Scheme）為用於非對稱加密與數位簽章的正式標準化 PQC 演算法，並獲得包括美國國家標準與技術研究院（NIST）與網際網路工程任務小組（IETF）等機構的推薦。