數位發展部數位產業署 廣告

後量子密碼安全檢測技術人才培育課程

隨著量子技術快速發展，傳統加密演算法將逐步退出市場，美國 NIST 已公布後量子加密標準（FIPS 203/204/205），全球正加速邁向 2030 年前的全面遷移，企業若無提前建立測試與導入能力，將可能錯失第一波後量子時代轉型機會。

本課程專為企業量身打造，透過後量子密碼的旁通道分析與錯誤注入技術的深入講解與實作訓練，讓晶片業者能更快理解資安需求、提前發現設計漏洞、縮短開發周期，並與資安業者加速建立有效協作；同時協助資安業者快速掌握晶片與工具串接細節，提升測試效率、減少溝通障礙。課程內容亦對應 ISO/IEC 17825 國際標準規範，旨在培育專業檢測人才、強化企業產品可信度，協助企業順利進入合規需求的國際供應鏈。

學員獲得
- 最新後量子安全檢測技術
- 掌握國際標準檢測作業流程

企業獲得
- 強化產品韌性與競爭力
- 搶先國際合規市場門票

內容	時間
報到	13:00-13:30
國際標準與旁通道分析簡介 後量子加密簡介與 NIST 標準現況 後量子加密應用場景與安全挑戰 旁通道分析(SCA)基本概念 錯誤注入(FI)基本概念	13:30-14:20
休息	14:20-14:30
後量子密碼檢測實務與驗證 ISO/IEC 17825 標準導入與合規驗證實作 後量子晶片測試實例操作	14:30-15:20
休息	15:20-15:30
企業導入與國際合規實務 實驗室測試流程與檢測準備 廠商產品送測與準備要點	15:30-16:30

對象：半導體或資安產業人士
時間：115 年 7 月 16 日(四) 下午 13:30-16:30
地點：新竹同業公會 201 會議室(新竹市東區展業一路 2 號)
費用：免費
報名連結：https://ievents.iii.org.tw/EventS.aspx?t=0&id=3175
聯絡窗口：廖先生　02-6607-8934　jianweiliao@iii.org.tw

報名 QR code

指導單位：數位發展部數位產業署　　**主辦單位：財團法人資訊工業策進會**
協辦單位：臺灣中小企業資訊安全協會

後量子密碼旁通道安全檢測

免費預檢測服務

功耗與電磁訊號分析

- 捕捉密碼運算時的功耗與電磁洩漏
- 標準分析PQC演算法執行特徵

硬體金鑰還原

- 利用旁通道資訊還原密碼
- 評估旁通道洩露程度

國際法規測項連接

- 對應ISO & FIPS 140-3等標準
- 提升產品信任，強化市場說服力

開辦檢測人才培育課程

課程內容亮點

- PQC旁通道(SCA)分析理論
- 錯誤注入(FI)基本概念

學員獲得

- 最新後量子安全檢測技術
- 掌握國際標準檢測作業流程

企業獲得

- 強化產品韌性與競爭力
- 搶先國際合規市場門票

指導單位:數位發展部數位產業署
主辦單位:財團法人資訊工業策進會
協辦單位:台灣中小企業資訊安全協會
檢測聯絡資訊:

課程時間: 2026/07/16 (四) 13:30~16:30
課程地點: 新竹市東區展業一路2號201會議室
課程報名連結: