抗量子電腦之端對端安全通訊應用服務

本院覽號	公告日期	智財權狀態
32T-1131129	2025-01-15	know-how

摘要

「抗量子電腦之端對端安全通訊應用服務」涵蓋底層支援後量子密碼的端對端加密模組、安全通訊協定、前端應用(Android/iOS/Desktop)及後端服務。此技術建立了三個重要特點幫助確保目前與未來機敏資料通訊的安全需求： 1. 設計密碼安全協議支援後量子密碼加密機制，能對抗即使目前加密資料被側錄蒐集、以及未來量子電腦的計算力威脅，依然能達到保護傳輸之機敏資料避免遭到破解的目的。 2. 建構系統框架彈性組合使用多種優選的密碼演算法、密鑰長度，做到自主調整後續密碼安全協議運作組件升級或汰換。 3. 提供完整的實作堆疊，並組合出可信任的軟體物料清單，確保系統部署運作時綁定使用自行建構的關鍵核心組件。

技術優勢

- 設計密碼安全協議支援後量子密碼加密機制，能對抗即使目前加密資料被側錄蒐集、以及未來量子電腦的計算力威脅，依然能達到保護傳輸之機敏資料避免遭到破解的目的。
- 建構系統框架彈性組合使用多種優選的密碼演算法、密鑰長度，做到自主調整後續密碼安全協議運作組件升級或汰換。
- 提供完整的實作堆疊，並組合出可信任的軟體物料清單，確保系統部署運作時綁定使用自行建構的關鍵核心組件。

應用範圍

- 組織機關或企業之安全通訊服務
- 機敏訊息或檔案推送服務
- 抗量子電腦加密應用

創作人

李政池

中央研究院
ACADEMIA SINICA