國立政治大學 資訊安全科技研究中心
Information Security Center, National Chengchi University

金融科技應用中的前瞻資安技術開發(1/2)
Development of Advanced Security-technologies for Fintech

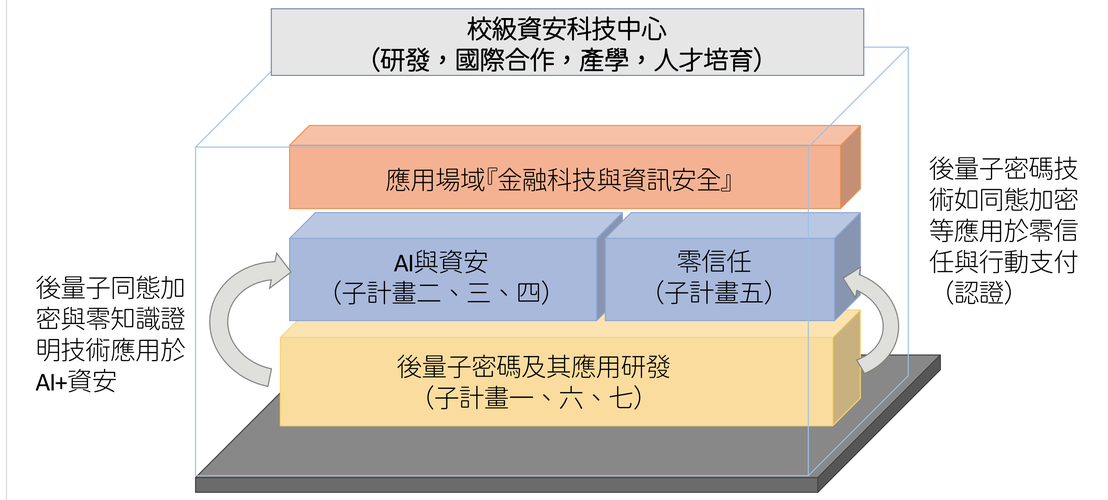
計畫編號：NSTC112-2634-F-004-001-MBK
執行期間：112年06月01日至113年05月31日

1 總計畫

後量子
- 子計畫一 後量子憑證、隱私保護技術、零知識證明及同態加密技術，及其於零信任架構之應用
- 子計畫六 人工智慧與金融科技中之隱私保護技術
- 子計畫七 適用於金融科技之後量子密碼系統設計與分析

AI與資安
- 子計畫二 運用對抗式學習於聯邦推薦系統中進行投毒攻擊與防禦
- 子計畫三 時序資料應用模型的動態型式執行測試與對抗例生成
- 子計畫四 基於語言模型與多模態融合架構之資安事件偵測方法

零信任
- 子計畫五 基於EMV協議的零信任金融框架



資安中心計畫框架

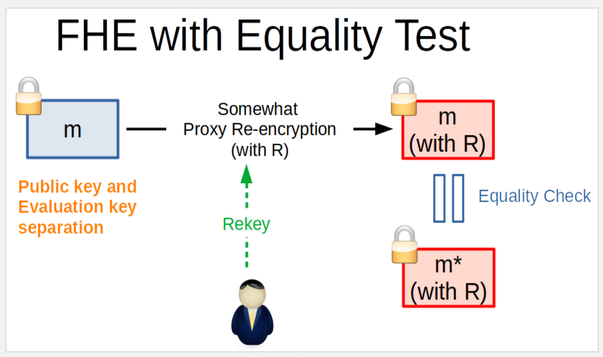
摘要目的

為了解決金融科技業的安全問題，本計畫成立校級資訊安全科技研究中心。該中心專注於研究和開發金融科技的AI與資安、零信任架構、和後量子密碼元件。研究部分將分為七個子計畫，同時探討這三個主要研究領域。透過匯集各方資源和專業知識，該中心可以為金融科技公司提供尖端的安全解決方案，並降低資料洩露和受到網路攻擊的風險，從而確保敏感資料的安全和隱私，以及增進使用者的信任和信心，進而促使金融科技產業的持續成長和創新。

2 後量子領域

研究目的

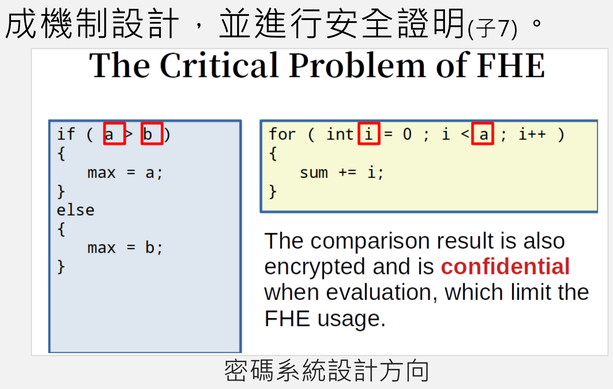
- 研究適用於金融科技之密碼元件及研究全同態加密系統的權限控制機制以及密文比對功能，提昇全同態加密應用上的可能性，期望以密碼學知識解決金融科技中的資安問題。
- 零知識證明協定可加強可搜尋式加密的可靠性，於進行搜尋前讓使用者以零知識證明向伺服器證明其有權限存取所搜尋之檔案，以避免惡意使用者進行阻斷服務攻擊。
- 計畫嘗試開發軟體函式庫，以服務的方式提供其他子項技術來使用。



研究動機

目前成果

- 在後量子隱式憑證的開發上，已設計出隱式憑證之通用架構，並依此架構設計出基於離散對數，基於RSA，及基於q-TESLA的隱式憑證技術。其中，q-TESLA為後量子版本之技術(子1)，
- 將提出一種可以直接對兩個密文進行比較，並得到明文結果的相等性測試。有了這項技術的協助，同態加密便不會再受限於條件控制的缺陷(子6)，
- 已完成新IBEETIA機制之設計與正規安全性分析，此機制可以克服以往IBEETIA無法解決的安全問題，並將集延伸應用至設計基於同源密碼學的基於身分加密。此外，對於隱私保護資料搜尋機制的可否認性研究，目前本團隊已完成機制設計，並進行安全證明(子7)。



密碼系統設計方向

結果與貢獻

1 於112年10月27日建立國立政治大學校級資訊安全科技研究中心

- 協辦「第十四屆金融科技高峰會春季場」
- 邀請瑞士電腦網路安全專家Christian Grothoff 教授至政大進行「GNU Taler 未來支付」講座
- 協辦2024金融資安研習營

2 人才培育

目前累計培育61名碩博士生及1名大專生資安領域專業人才，其中政大之劉子源博士於112年12月畢業，並於112年12月獲得鴻海科技獎、及於113年3月獲得中華民國資訊安全學會『賴溪松教授論文獎』博士論文獎優等獎。

3 學術成就

投稿54篇學術性論文(期刊為28篇、會議為26篇)，已通過為29篇(期刊為10篇、會議為19篇)，其中投稿頂尖會議為4篇；投稿頂尖期刊為13篇，通過3篇：

投稿場合	論文主題	作者	進度	衡量標準
Advanced Engineering Informatics	Knowledge distillation for portfolio management using multi-agent reinforcement learning	陳旻佑; 陳巧莛;黃思皓	已發表 (Aug 2023, 57, 102096.)	• JIF = 4/90 (ENGINEERING, MULTIDISCIPLINARY)
IEEE Transactions on Computational Social Systems	Member-Augmented Group Recommendation With Multi-Interest Framework and Knowledge Graph Embeddings	Lin, S. J., Chen, C. T., Huang, S. H.	已發表 (Jan 2023, PP(99):1-14)	• JCI = 5/32 (COMPUTER SCIENCE, CYBERNETICS)
IEEE Transactions on Dependable and Secure Computing	GDPR-Compliant Personal Health Record Sharing Mechanism with Redactable Blockchain and Revocable IPFS	Lo-Yao Yeh, Wan-Hsin Hsu, Chih-Ya Shen	已接受	• JCI = 5/132(COMPUTER SCIENCE, SOFTWARE ENGINEERING) • JCI = 5/63(COMPUTER SCIENCE, HARDWARE & ARCHITECTURE)

4 產業合作

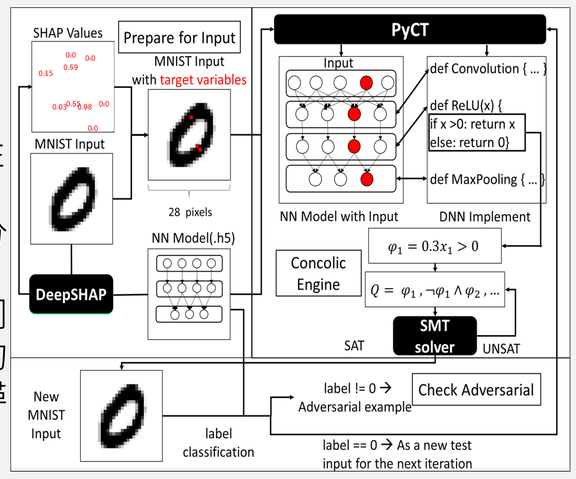
- 協助QSMC量子安全遷移中心在金融領域的後量子技術推廣與後量子遷移
- 與政大金融科技研究中心合作，規劃金融資安相關研討會與資安訓練課程
- 與全球量子技術公司BTQ簽署合作意向書，共同進行後量子密碼的研發
- 與財金資訊股份有限公司簽署合作意向書，並以『基於量子安全之數位支付金鑰管理機制POC試驗案』主題進行洽談中。

3 AI資安領域

研究目的

無論任何系統，整體的資訊安全是重要的。

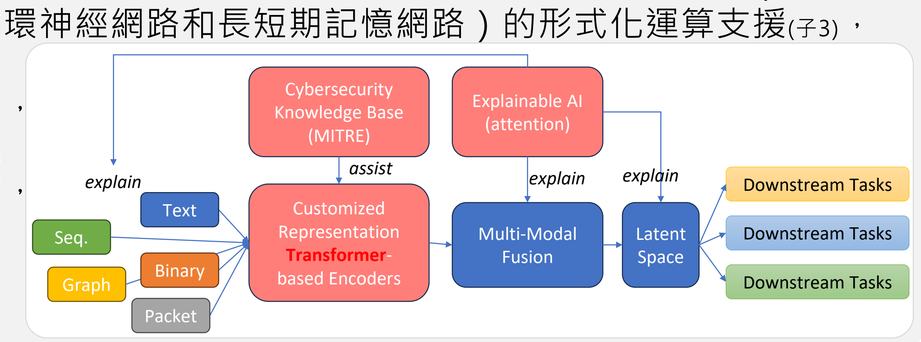
- 在強化AI資安方面，研究兩個面向：
  1. 聯邦推薦系統中的投毒攻擊與防禦。
  2. AI模型的自動化測試，以動態型式驗證技術達成系統性的測試輸入值自動生成，強化AI應用的穩健性。
- 在AI強化資安方面，研究面向為異質性的資安攻擊資料分析（例如：系統事件、封包、程式等）。
- 本研究提出的重要研究議題：不同資料語意的整合與協同分析。我們將採用人工智慧中的語言模型進行不同資料的解讀與嵌入，並在多模態的技術下進行融合，並最終找尋攻擊的樣態並提出可解釋性的結果。



PyCT 2.0 系統架構圖

目前成果

- 提出的基於對抗學習的模型框架應用於聯邦推薦系統中的投毒攻擊與防禦，進一步將此框架擴展至不同場景下的各類推薦系統，以探討模型的穩固性與準確性(子2)。
- 以程式驗證技術落實AI模型應用的白箱檢測，開發基於約束的對抗性示例生成方法並實作新版的PyCT，一個Python動態型式測試工具，目前已涵蓋各種神經網路操作（如浮點運算、連接層運算、卷積、循環神經網路和長短期記憶網路）的形式化運算支援(子3)，
- 此外，建制分散式運算以及儲存平台、搜集足夠的資訊安全文件，訓練具有資訊安全知識的語言模型、利用語言模型進行下游任務，以上的成果可以為資訊安全分析帶來更適切、更為準確、更robust的資安偵測結果(子4)。



語言模型與多模態融合架構之資安事件偵測方法

4 零信任領域

研究目的

- 探討現有移動支付方法面臨的各種安全威脅。
- 預計在金融基礎設施中結合零信任架構的安全解決方案。
- 本計畫所提出的基於零信任的EMV框架與現有的EMV交易協定兼容，可以實現相互驗證及加密，並添加FIDO以防止各種攻擊。

目前成果

- 提出多環境因子驗證機制，透過將人造環境因子引入自然環境中，檢測terminal與手機間之距離，有效地對抗中繼攻擊(子5)。
- 現階段已於實際交易環境中，模擬攻擊者將交易資料relay至遠端進行行動支付的安全性實驗(子5)。
- 後續將提出安全性與效能分析(子5)。
- 將持續進行將FIDO與行動支付結合之零信任金融支付框架研究(子5)。

計畫主持人： 左瑞麟 特聘教授 **子計畫主持人：** 左瑞麟 特聘教授(子一) 蕭舜文 副教授(子四) 紀博文 副教授(子六) **協同研究人員：** 葉羅堯 副教授 曾俊元 副教授 **計畫專任助理：** 鍾加儒 **計畫參與學生人數：** 62
共同主持人： 陳恭 教授 黃思皓 副教授(子二) 楊明豪 副教授(子五) 曾一凡 助理教授(子七) 孫士勝 助理教授 卓信宏 副教授 李育
郁方 副教授(子三) 羅嘉寧 副教授(子五) 許建隆 特聘教授 王仁甫 助理教授