NTOU CSE 資訊工程學系 COMPUTER SCIENCE AND ENGINEERING

實驗室網站

網路安全實驗室
Network Security Laboratory

指導老師：蔡東佐 (tttsai@mail.ntou.edu.tw)

實驗室介紹







本實驗室專注於培育具備扎實資安理論基礎的頂尖人才。我們深信，真正的安全不能僅憑直覺，任何「安全」的宣稱都必須仰賴嚴密的邏輯佐證或數學證明。除了深研理論，我們同樣重視實作與國際視野：透過與鴻海的產學合作，帶學生走進企業、接觸業界的實務問題；也帶領學生遠赴日本札幌參加國際研討會，上台報告研究成果。研究之餘，大家也會聚在一起慶生、聚餐，舉辦尾牙與聖誕交換禮物；這段過程有辛苦，也有歡笑。

職場思維 01
視實驗室為職場前哨戰，重視態度如同重視能力

成長與傳承 02
向學長姐學習、克服任務並在挑戰中進化

開放溝通 03
溝通是關鍵，每個挑戰都是討論與解決問題的機會

實驗室位置 電綜大樓 709 | **老師研究室** 資工系館 507

指導學生之學術與競賽成果

2026

115 學年度國科會大專學生研究計畫 **通過 2 件**
吳慧金、陳敏瑄 | 各 4.8 萬元

第 36 屆全國資訊安全會議 CISC 2026 **最佳簡報獎**
葉婉玲

2025

第 30 屆大專校院資訊應用服務創新競賽｜教育開放資料組 **第一名**
楊沛穎、葉婉玲、陳敏瑄、陳佳誼、康慈軒、呂亭儀 | 獎金 5 萬元

第 30 屆大專校院資訊應用服務創新競賽｜臺北生活好便利創新應用組 **第三名**
陳宥霖、陳敏瑄、楊沛穎、吳慧金 | 獎金 1 萬元

全國大專校院智慧創新暨跨域整合創作競賽｜數位永續科技組 **第二名**
陳宥霖、陳敏瑄、楊沛穎、吳慧金 | 獎金 5 萬元

軟體工程競賽 **佳作**
葉婉玲、陳佳誼、楊沛穎、陳敏瑄

2023

第 28 屆大專校院資訊應用服務創新競賽｜資安創新技術組 **佳作**
葉宥君、黃煒甯、王嘉羽、林昱彤 | 獎金 0.5 萬元

數據驅動創新應用大賽 **亞軍**
李炘杰、陳元瑾、江子安、洪旻昌 | 獎金 15 萬元

數據驅動創新應用大賽 **微軟特別獎**
呂安曦、蘇士堯、張唯仁、王彤 | 獎金 5 萬元

第 33 屆全國資訊安全會議 CISC 2023 **Session Award、最佳學生論文獎**
陳元瑾

112 學年度國科會大專學生研究計畫 **通過 1 件**
王嘉羽 | 4.8 萬元

2022

第 27 屆大專校院資訊應用服務創新競賽｜商業資訊創新應用組 **第二名**
王嘉羽、黃菁蕙、陳伸蓉、盧品樺 | 獎金 3 萬元

全國大專校院智慧創新暨跨域整合創作競賽｜體感互動科技組 **第三名**
王竣樺、葉宥君、石貫志 | 獎金 2 萬元

全國大專校院智慧創新暨跨域整合創作競賽｜體感互動科技組 **佳作**
黃子毓、吳翊楷、曾昱翔 | 獎金 0.5 萬元

第 32 屆全國資訊安全會議 CISC 2022 **最佳論文獎佳作**
曾昱翔、吳承燁



教育開放資料組
第一名



數位永續科技組
第二名



臺北生活好便利創新應用組
第三名


軟體工程競賽
佳作

研究方向與成果

➢ 研究方向 Research Areas

密碼學
Practical Cryptography
公鑰加密與搜尋加密的設計，結合隱私保護計算，同時兼顧檢索效率與資料安全

機器學習與醫學影像辨識
ML & Medical Imaging
深度學習於醫學影像的應用：病灶自動分割、醫學影像分類與輔助診斷系統

AI 模型安全與內容治理
AI & Content Security
研究 LLM Guardrails 實踐，以防範提示注入與誘導攻擊，並以零信任架構確保輸出可控

➢ 研究成果 Research Highlight

Leakage-Resilient Certificateless Public Key Encryption with Equality Test Resistant to Side-Channel Attacks

T.T. Tsai* and J.H. Yang, Computer Networks, vol. 270, Article ID 111485, 2025.

無憑證公鑰加密 (CL-PKE) 免除了憑證管理，並解決了金鑰託管問題；結合等值測試 (Equality Test) 後，測試者不需解密即可比對不同使用者的密文是否對應相同明文。然而，攻擊者可藉由功率分析、電磁輻射、時間分析等旁通道攻擊反覆蒐集洩漏資訊，逐步還原秘密金鑰 (Fig. 1)。本研究提出第一個可抵抗旁通道攻擊的 LR-CL-PKEET 機制 (Fig. 2)：以金鑰更新技術將秘密金鑰拆分為兩部分，於每次運算前進行更新，並在 Generic Bilinear Group (GBG) 模型下證明其具備 IND-CCA 與 OW-CCA 安全性。

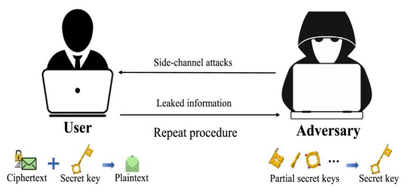


Fig. 1 Recover the secret key by side-channel attacks.

- ✓ 免除 PKI 憑證管理
- ✓ 解決金鑰託管問題
- ✓ 抵抗旁通道攻擊
- ✓ 支援密文等值測試

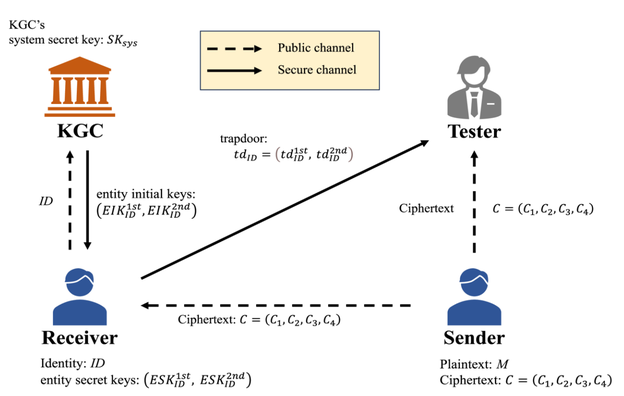


Fig. 2 Framework of an LR-CL-PKEET scheme.

➢ 產學合作 Industry–Academia Collaboration

LLM 多層安全防護系統

產學計畫｜鴻海精密工業股份有限公司 × 國立臺灣海洋大學

針對提示注入、RAG 數據投毒與輸出安全等風險，提出三階段縱深防禦架構 (Fig. 3)，從輸入、推論到知識來源層層把關，建構可稽核、可追溯的 LLM / RAG 安全防線。

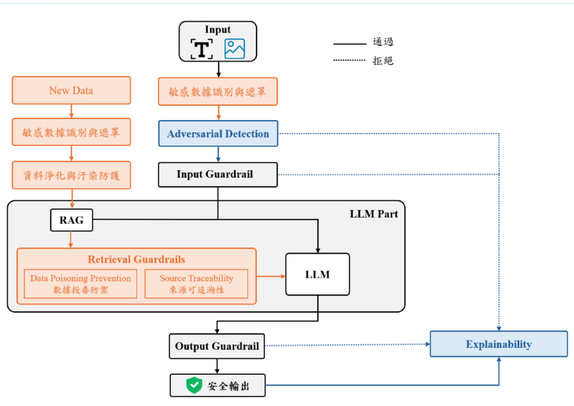


Fig. 3 Three-stage LLM defense-in-depth architecture.

階段一 基礎安全防護
輸入端：權限驗證與語義判斷；輸出端：事實準確性驗證與敏感內容過濾

階段二 進階攻擊防護
多模態輸入處理、對抗性偵測攔截混合型與滲透型攻擊，並導入可解釋性框架

階段三 資料完整性防護
敏感數據的識別與遮罩、資料汙染防護、檢索層防護與來源可追溯

➢ 近期期刊論文 Journal Papers (2024–2026)

1. T.T. Tsai, H.Y. Lin*, T.H. Yu, Y.C. Chen, and Y.J. Ye, "On the construction of a leakage-resilient certificate-based encryption with equality test scheme", Journal of Information Security and Applications, vol. 99, Article ID 104422, 2026.
2. H.Y. Lin, T.T. Tsai*, and Y.C. Wang, "IoT-assisted cloud data sharing with revocation and equality test under identity-based proxy re-encryption", Computers, Materials & Continua, vol. 86, no. 3, Article ID 14, 2026.
3. T.T. Tsai* and J.H. Yang, "Leakage-resilient certificateless public key encryption with equality test resistant to side-channel attacks", Computer Networks, vol. 270, Article ID 111485, 2025.
4. T.T. Tsai, H.Y. Lin, W.N. Huang, S. Kumar, K. Agarwal, and C.M. Chen*, "Anomaly detection through outsourced revocable identity-based signcryption with equality test for sensitive data in consumer IoT environments", IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 6327-6339, 2025.
5. T.T. Tsai*, "Leakage-resilient public key signcryption with equality test and its application", Informatica, vol. 36, no. 2, pp. 429-452, 2025.
6. T.T. Tsai, H.Y. Lin, Y.C. Chen*, and Y.C. Chen, "Leakage-resilient public key encryption with equality test resistant to side-channel attacks", Journal of Information Science and Engineering, vol. 41, no. 1, pp. 195-216, 2025.
7. H.Y. Lin, T.T. Tsai*, and H.L. Wu, "A revocable certificateless sanitizable signature scheme with batch verification", IEEE Access, vol. 12, pp. 143392-143400, 2024.
8. Y.M. Tseng*, T.C. Ho, T.T. Tsai, and S.S. Huang, "AHMRE-SCST: Lightweight anonymous heterogeneous multirecipient encryption with seamlessly compatible system transformation for IoT devices", IEEE Internet of Things Journal, vol. 11, no. 17, pp. 28508-28525, 2024.
9. Y.M. Tseng*, T.T. Tsai, S.S. Huang, and T.C. Ho, "Leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption in heterogeneous public-key system settings", IEEE Access, vol. 12, pp. 28155-28168, 2024.

* corresponding author | 完整論文列表 (共 61 篇)：nsl.cse.ntou.edu.tw/publications