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

- 主要研究領域
  - ✓ 資訊安全 – 確保通訊過程中資料的機密性、完整性與可用性
  - ✓ 密碼學 – 利用數學與計算理論建構可證明其安全性之通訊機制
  - ✓ 網路安全 – 探討如何將安全的密碼學機制應用於現行的網路環境
- 實驗室活動
  - ✓ 密碼學讀書會
  - ✓ 大學部專題競賽
  - ✓ 產學交流與合作

研究方向與成果

Leakage-Resilient Anonymous Multi-receiver Certificate-based Key Encapsulation Scheme

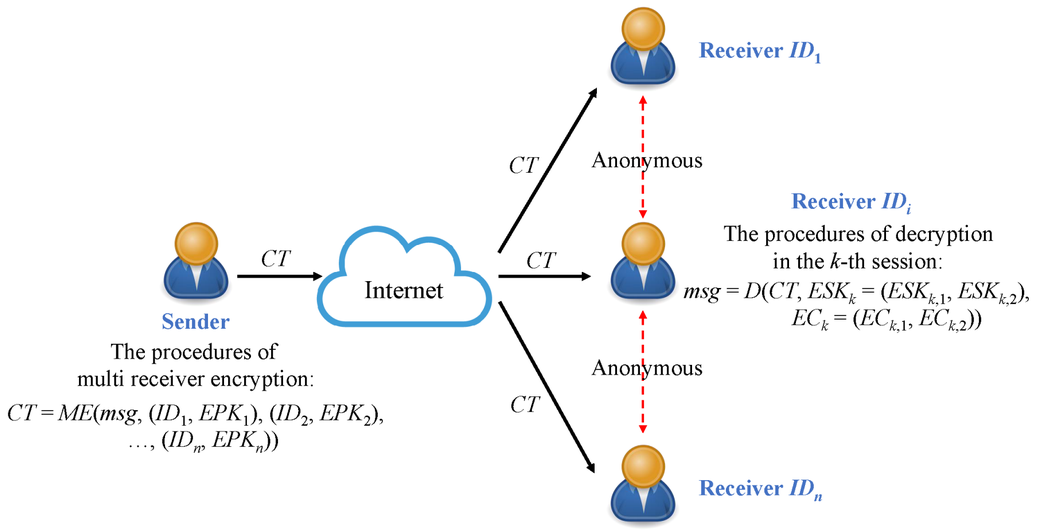

Fig.1 The procedures of anonymous multi-receiver encryption and decryption.

Leakage-Resilient Public Key Signcryption with Equality Test and Its Application

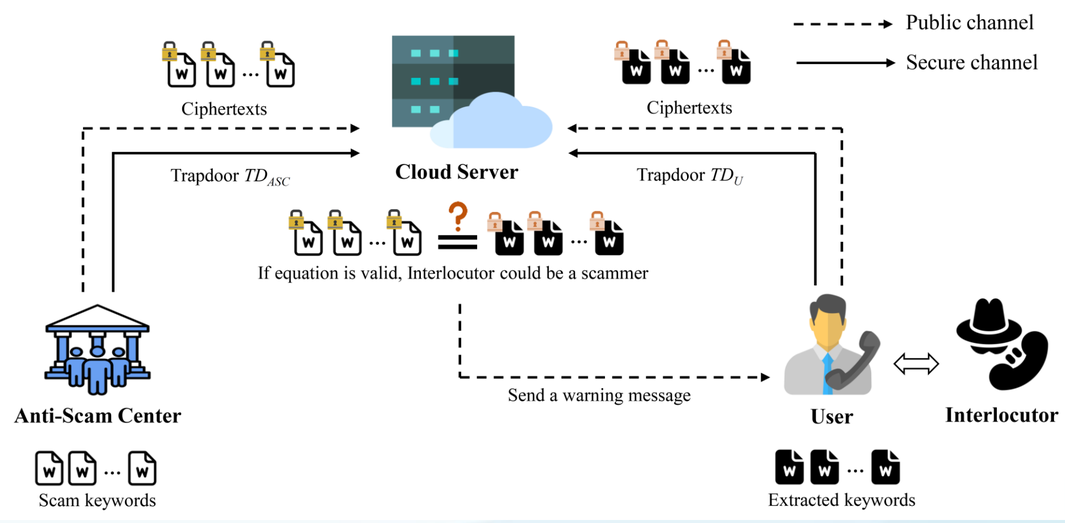

Fig. 2 Building an anti-scam system based on the proposed LR-PKSCET scheme.

指導學生之學術與競賽成果

- 2023.07.08 指導學生 李炘杰、江子安、洪旻昌、陳元瑾 獲得獎項
  - ✓ 2023數據驅動創新應用大賽 – **亞軍**
- 2023.07.08 指導學生 呂安曦、張唯仁、蘇士堯、王彤 獲得獎項
  - ✓ 2023數據驅動創新應用大賽 – **微軟特別獎**
- 2023.06.02 指導學生 陳元瑾 獲得獎項
  - ✓ 2023第33屆資訊安全會議 – **Session Award**
- 2023.02.01 指導學生 王嘉羽 獲得計畫
  - ✓ 112 學年國科會 – **大專學生計畫**
- 2022.12.16 指導學生 王竣樺、葉宥君、石貫志 獲得獎項
  - ✓ 2022全國大專校院智慧創新暨跨域整合創作競賽之體感互動科技組 – **第三名**
- 2022.12.16 指導學生 黃子毓、吳翊楷、曾昱翔 獲得獎項
  - ✓ 2022全國大專校院智慧創新暨跨域整合創作競賽之體感互動科技組 – **佳作**
- 2022.11.05 指導學生 王嘉羽、黃菁蕙、陳伸蓉、盧品樺 獲得獎項
  - ✓ 2022第27屆大專校院資訊應用服務創新競賽之商業資訊創新應用組 – **第二名**
- 2022.06.18 指導學生 曾昱翔、吳承燁 獲得獎項
  - ✓ 2022第32屆資訊安全會議 – **最佳論文獎佳作**

Journal Papers

1. T.T. Tsai, Y.M. Tseng, and S.S. Huang, “Leakage-resilient anonymous multi-receiver certificate-based key encapsulation scheme”, IEEE Access, vol. 11, pp. 51617-51630, 2023.
2. T.T. Tsai, Y.M. Tseng, and S.S. Huang, “Leakage-resilient certificateless signcryption scheme under a continual leakage model”, IEEE Access, vol. 11, pp. 54448-54461, 2023.
3. H.Y. Lin, T.T. Tsai, P.Y. Ting, and C.C. Chen, “Identity-based proxy re-encryption scheme using fog computing and anonymous key generation”, Sensors, vol. 23, no. 5, pp. 2706, 2023.
4. Y.M. Tseng, T.T. Tsai, and S.S. Huang, “Fully continuous leakage-resilient certificate-based signcryption scheme for mobile communications”, Informatica, vol. 34, no. 1, pp. 199-222, 2023.
5. T.T. Tsai, H.Y. Lin, and H.C. Tsai, “Revocable certificateless public key encryption with equality test”, Information Technology and Control, vol. 51, no. 4, pp. 638-660, 2022.
6. T.T. Tsai, Y.M. Tseng, S.S. Huang, J.Y. Xie, and Y.H. Hung, “Leakage-resilient anonymous multi-recipient signcryption under a continual leakage model”, IEEE Access, vol. 10, pp. 104636 - 104648, 2022.
7. T.T. Tsai, S.S. Huang, Y.M. Tseng, Y.H. Chuang, and Y.H. Hung, “Leakage-resilient certificate-based authenticated key exchange protocol”, IEEE Open Journal of the Computer Society, vol. 3, pp. 137-148, 2022.
8. T.T. Tsai, H.Y. Lin, and H.C. Chang, “An efficient revocable identity-based encryption with equality test scheme for the wireless body area network”, Journal of Sensors, vol. 2022, Article ID 1628344, 2022.
9. H.Y. Lin, T.T. Tsai, H.R. Wu, and M.S. Ku, “Secure access control using updateable attribute keys”, Mathematical Biosciences and Engineering, vol. 19, no. 11, pp. 11367-12379, 2022.
10. H.Y. Lin, T.T. Tsai, P.Y. Ting, C.C. Chen, “An improved ID-based data storage scheme for fog-enabled IoT environments”, Sensors, vol. 22, no. 11, pp. 4223, 2022.
11. Y.M. Tseng, S.S. Huang, T.T. Tsai, Y.H. Chuang, and Y.H. Hung, “Leakage-resilient revocable certificateless encryption with an outsourced revocation authority”, Informatica, vol. 33, no. 1, pp. 151-179, 2022.
12. T.T. Tsai, Y.H. Chuang, Y.M. Tseng, S.S. Huang, and Y.H. Hung, “A leakage-resilient ID-based authenticated key exchange protocol with a revocation mechanism”, IEEE Access, vol. 9, pp. 128633-128647, 2021.