出國報告書（出國類別：出席國際會議）

出席第八屆資訊處理與管理

(ICIPM2013)國際會議心得報告

服務機關：國立政治大學資訊科學系
姓名職稱：左瑞麟（助理教授）
派赴國家地區：韓國（首爾）
出國期間：102 年 3 月 31 日～4 月 4 日
報告日期：102 年 5 月 2 日

目次

壹、摘要

此次赴韓國首爾參加第八屆資訊處理與管理國際會議(ICIPM2013)。資訊安全為其中之一個議題。為擴大參與，本屆與另外兩大會議 –第八屆資訊處理、管理與智能訊息技術國際會議(8th International Conference on Information Processing, Management and Intelligent Information Technology ;ICIPT2013)以及第八屆智能資訊處理國際會議(8th International Conference on Intelligent Information Processing;ICIIP2013)合辦。此次會議共有來自大陸，日本，印度，孟加拉，及台灣等世界各國的專家學者共約 100 多人與會。報告人此次有一篇關於密碼學的被收錄並發表。透過今年之會議參與以及會後交流，除了增加了政大之國際能見度之外，也為自己開拓了更多未來可能的研究方向與合作之對象。

貳、目的

第八屆資訊處理與管理國際會議(The 2013 8th International Conference on Information Processing and Management ;ICIPM-2013) 是由韓國的學術研究機構-收斂訊息技術進階研究所(Advanced Institute of Convergence Information Technology ;AICIT)所舉辦的大型國際會議。此會議此次和另外兩大會議 –第八屆資訊處理、管理與智能訊息技術國際會議((8th International Conference on Information Processing, Management and Intelligent Information Technology; ICIPT2013)以及第八屆智能資訊處理國際會議(8th International Conference on Intelligent Information Processing;ICIIP2013)合辦。參加者因此可以聽到三個會議之所有演講，以增廣見聞。這在近年似乎已是舉辦會議的一個趨勢。此次之會議地點在韓國首爾。會議的關注議題主要為有關資訊處理與管理方面的所有有關理論、開發、應用以及評估等方面。

資訊安全與密碼學是屬於 Information Processing（資訊處理）的領域。本人此次赴 ICIPM 之目的之一就是發表本實驗室近年之成果。此論文之題目為：Security Weakness in a Privacy Preserved Two-Party Equality Testing Protocol（具保護隱私之雙方相等性驗證機制之安全性分析）。此論文之報告是安排在 4 月 1 日下午的議程報告。

參、會議參加經過

會場 Registration

論文報告

在密碼學的研究方面，今年有三篇是屬於公開金鑰密碼學，其他大部分較偏向於數位浮水印，資訊隱藏與多媒體資料的保護等。本人的報告是在第一天的下午。由於國科會計畫是有關同態加密以及其應用方面，此次之報告亦是有關這部分之研究成果。我們發現了之前在 ICGIT2011 報告的研究成果有一些安全性上的問題。這樣的問題可能導致欲隱藏的資訊被洩漏，引此在此會議中將此問題點出來。另外有一篇和同態加密相關的論文是介紹如何利用同態加密應用在資訊擷取上面。個人認為此方案之實用價值頗高。除此之外，台灣科技大學資訊管理學系羅乃維副教授的研究團隊亦在此會議介紹的他們的研究成果，是關於可轉換之多方驗證加密機制(convertible multi-authenticated encryption scheme)方面。

肆、與會心得與建議

ICIPM2013 提供全球資訊領域的專家學者一個研究交流的平台，持續推動資訊處理與管理相關領域的發展。今年參加者，單純以目視估計配合接收論文數量，估計有近 100 人左右與會。會議之參加費用頗高，但相對來說會場的布置與準備卻似乎沒有達到這樣一個價值。與相關領域的專家學者齊聚一堂， 針對密碼與資訊安全的相關議題相互討論，彼此交流，分享成果及實務經驗，固然是參加會議之主要目的。但會場之準備與設備沒有到位的話，整個感覺就有點降低了。這是本次參加會議的

一點負面評價，值得未來舉辦會議時之參考。

伍、攜回資料

The proceedings of the 8th International Conference on Information Processing and Management (ICIPM 會議論文光碟)

六、附件

會議之詳細議題如下：

Topic 1: Information Processing（資訊處理）

• Research/Technical Issues on Convergent Aspects of IT and Ubiquitous Technology
• Hybrid Approaches of Information Technology
• Multimedia, Game, and Culture Technology
• High Performance Data Processing and Digital Content Technology
• High Performance Information System and Communication
• Information Security and Cryptology
• Intelligent Approach on Information Processing
• Bioinformatics and Healthcare
• Network and Communication
• Mobile and Ubiquitous Technologies
• Media, Culture and Communications
• Embedded Systems and Software
• Grid and Distributed Computing
• Smart and Green Computing
• System and Device Design
• Other Issues on Information Processing

Topic 2: Management Information Systems, Business Systems, Service and Finance Systems （訊息系統，商業系統，服務和金融系統管理）

• Traditional Issues on Information Management
• Technical Issues on Information Management
• Future Issues on Information Management
• Recent Issues on Business System, Modeling and Architecture
• Knowledge Management and Secure Information Management

• Convergent Approaches on Advanced Information Management
• Evaluation, Trust and Computational Finance issues
• Social Issues on Information Management
• Management, Service and Business issues on Healthcare
• U-Service issues on Advanced Information Management
• Management Issues on Media, Culture and Communications
• Organizational behaviors
• Human Resource Management
• Information Management for Business Applications
• Computational Finance
• Financial Information System and Service
• Business systems, design, Enterprise Systems, Architecture, Integration
• Service-oriented architecture; Enterprise service bus; Service-component architecture
• Trust issues in business and systems
• Value-based management and systems
• Other Issues on Information Processing