出國報告書（出國類別：出席國際會議發表論文）

出席國際會議 The 2011 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-11) 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：韓國（濟州島）
出國期間：100 年 12 月 11～12 月 14
報告日期：101 年 1 月 19 日

目次

壹、摘要.....3

貳、目的.....4

參、會議論文介紹.....7

肆、過程.....9

伍、心得與建議.....14

壹、摘要

ACSA 是由韓國的學術研究機構 FTRA 所舉辦的大型國際會議。本屆爲第二屆。此次會議共有來自韓國，日本，美國，及土耳其，芬蘭等歐洲各國的研究學者及專家共約 100 人與會。會議的關注議題主要爲密碼學在未來計算(Future computing)方面的應用。

此會議今年是第二次舉辦，尚屬較年輕的一個會議，所以學術地位及其重要性尚未完全被定位及建立。但由出席人數及其盛況，可以看出此會議是相當受到重視的。相信未來此會議將會在資訊安全的領域中佔有重要之地位。

報告人此次共有 4 篇文獻被收錄，兩篇爲合著，另兩篇爲個人著作。和著之論文由和著者發表，因此此次報告者共發表了兩篇論文。除此之外，報告者並另外擔任其中一個議程之議程主席，協助會議之進行。

藉由此次會議之參與，認識了許多國內外之專家學者。藉由發表與之後的討論，除了增加了政大之國際能見度之外，也爲自己開拓了更多未來可能合作之對象。

貳、目的

The 2011 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-11) 是由韓國的學術研究機構 FTRA 所舉辦的大型國際會議。此次之會議地點在韓國濟州島，會議時間爲 2011 年 12/12 至 12/15 共五天。會議的關注議題主要爲密碼學在未來計算(Future computing)方面的應用。未來計算在此包括了無所不在的計算環境(ubiquitous and pervasive computing)，網格計算，雲端計算以及 P2P 計算等科學領域。在這些環境中可能遭遇到的一些安全問題如訊息的機密性，完整性以及認證等等，這些問題如何利用密碼學等相關的技術來解決，以實現一個安全的未來計算環境，就是本次會議的主要議題。詳細的議題如下：

Track 1. Cryptography and Information Security

- Encryption and cryptography
- Block/Stream Ciphers
- Hash Functions
- Mathematical and Algorithmic Foundations of Applied Cryptography
- Design and Analysis of Cryptographic Algorithms and Protocols
- Pairing Based Cryptography for FCS
- Provable Security for Cryptographic Primitives Suitable for FCS
- Information Security with Mathematical Emphasis for FCS
- Public Key Cryptosystems
- Side Channel Attack

Track 2. Security Protocols and Applications

- Authentication and Non-repudiation
- Access Control and Authorization
- Identity and Trust Management
- Database and System Security
- Intrusion Detection, Tolerance and Prevention
- Secure communications
- Information Hiding
- Digital Signatures
- Digital Right Management
- Watermarking and Steganography
- Critical infrastructure protection
- Digital rights management
- Computer Forensics
- Trust computing
- Security for M2M Platform
- Security and privacy issues for intelligent vehicular systems and communications

Track 3. Industrial Security & its Business and Services

- Information assurance
- Emergent challenges in security and assurance
- Theories, methods, tools and techniques in managing security
- Security and privacy standards
- Common Criteria
- Risk evaluation and security certification
- Security in E-commerce and E-business
- Security Policy
- Trust model and management
- Smartphone Security issues
- Security for Open convergence system
- IPTV security services in the BcN
- Security issues for Broadband convergence Network (BcN)

此會議今年是第二次舉辦，尚屬較年輕的一個會議，所以學術地位及其重要性尚未完全被定位及建立。但由會議的出席人數（國際研究學者及專家出席人數約 100 人）及其盛況，相信此會議將會越來越受到重視。

報告人此次共有 4 篇文獻被收錄，兩篇爲合著，另兩篇爲個人著作。詳細資料如下：

1. Certificateless Signatures with Message Recovery

此篇論文爲報告人之個人著作。其內容主要探討免憑證電子簽章的協議設計，以及如何提供訊息回復機制以降低訊息傳輸時所需要之頻寬。

2. A New Way to Generate a Ring: Universal Ring Signature

此篇論文亦爲報告人之個人著作。其內容主要探討如何設計一個電子簽章方案以保護簽章者以及/或簽章擁有者之隱私。此處所指之隱私包括了簽章者之身份訊息以及/或訊息之內容。

3. New Convertible Ring Signatures Based on RSA

此篇論文爲報告者及指導之博士班學生黃凱彬之和著論文。報告者爲黃凱彬。此論文之內容主要探討如何利用 RSA 來設計出可轉換環簽章(convertible ring signature)的協議。

4. A Secret Sharing Scheme for EBTC using Steganography

此論文爲報告者與其他國內外研究者之和著論文。論文作者依序爲 *Cheonshik Kim, Dongkyoo Shin, Dongil Shin, Raylin Tso*（左瑞麟）*, Ching-Nung Yang*（楊慶隆）。前三位爲韓國籍之學者，楊慶隆教授則爲國立東華大學資訊工程系兼研究所之教授。此論文之內容主要探討如何利用視覺密碼達成秘密分散。

另外，除了參加會議發表論文之外，報告者亦參與了會議之主持工作，擔任其中一個議程之議程主席。詳細資料如下：

Date: 12/11

Time: 16:30 - 18:30

Session 2-E: ACSA 2011

(Room: 301-A)

(Chair: Raylin Tso)

- Beyond Lightning: A Survey on Security Challenges in Cloud Computing

Chunming Rong, Son Nguyen, Martin Jaatun

- Practical Parallel Key-Insulated Encryption with Multiple Helper Keys

Yanli Ren, Shuozhong Wang, Xinpeng Zhang

- An efficient CP-ABE scheme with constant size ciphertext

In Tae Kim, Nghiem Xuan Hung, Seong Oun Hwang

- Identity Based Construction for Secure and Efficient Handoff Authentication Schemes in Wireless Networks

Yinghui Zhang, Xiaofeng Chen, Hui Li, Jin Cao

參、會議論文介紹

針對此次會議，就我有參與的部分，節錄以下印象較深，較爲重要之研究，或個人較有興趣之演講。

1. Secure and Efficient Data Retrieval over Encrypted Data Using Attribute-Based Encryption in Cloud Storage By *DONGYOUNG KOO, JUNBEOM HUR, HYUNSOO YOON*
   這篇的重點在於利用基於屬性的加密演算法(attribute-based encryption) 來達成安全的資料擷取，而另一方面，又能同時保障資訊的隱私。
2. An ID-based Online/Offline Signature Without Random Oracle for Wireless Sensor Network By *Zhiwei Wang, Wei Chen*
   無限感測網路的特徵就是電源的供給，計算量及儲存空間皆有限。如何在這樣的環境中利用公開金鑰密碼系統一直是個非常重要的研究。本篇的重點在於社寄出了可利用在無限感測網路中的Online/Offline Signature。除此之外，本篇的重點在於公鑰系統是屬於基於身份的公鑰系統。另外，其安全性不需要利用到random oracle，是屬於更爲安全的證明方式。
3. Improved Hashing onto Elliptic curves over F_3m for Pairing-based Cryptosystems By*Young In Cho, Nam Su Chang, Chang Han Kim, Seokhie Hong*
   由於基於配對(pairing-based)的密碼的盛行，而大部分此方案又需利用到Mapping to Point 的雜湊函數，因此，如何設計一個有效率的雜湊函數就是此論文的重點。
4. An Efficient CCA-Secure Cryptosystem Over Ideal Lattice from Identity-Based Encryption By *Yang XiaoYuan, Wu LiQiang, Zhang MinQing, Chen XiaoFeng*
   基於ideal lattice的密碼被稱之爲後量子密碼(post quantum crytography)，也就是量子計算機也無法破解的密碼。本篇的重點在利用ideal lattice及基於身份的密碼設寄出滿足CCA安全的密碼系統。
5. Beyond Lightning: A Survey on Security Challenges in Cloud Computing By *Chunming Rong, Son Nguyen, Martin Jaatun*
   本篇論文算是一篇關於雲端運算安全的相關研究調查的論文。介紹雲端運算可能遇到的一些安全問題，但並沒有提出他的解決方案。算是提出了一些open problem.
6. Practical Parallel Key-Insulated Encryption with Multiple Helper Keys By *Yanli Ren, Shuozhong Wang, Xinpeng Zhang*
   金鑰孤立的公開金鑰密碼(key-insulated encryption)的基本概念是使用者的私密金鑰會隨著時間而改變，而使用者的公開金鑰卻不隨之更改。此篇文章利用多個helper keys來達成此種密碼系統。
7. An efficient CP-ABE scheme with constant size ciphertext By *In Tae Kim, Nghiem Xuan Hung, Seong Oun Hwang*
   CP-ABE是Ciphertext-Policy Attribute-Based Encryption的縮寫，也就是基於密文規則的屬性基加密方案。本篇文章提出了具有constant size 的密文的CP-ABE加密系統。

8. Identity Based Construction for Secure and Efficient Handoff Authentication Schemes in Wireless Networks By *YINGHUI ZHANG, XIAOFENG CHEN, HUI LI, JIN CAO*
認證系統一般皆須經過handshake的階段，此篇文章利用基於身份(identity based)的性質設計出了handoff authentication的方案。
9. Escrowable Identity-based Authenticated Key Agreement Protocol with Strong Security By *LIANG NI, GONGLIANG CHEN, JIANHUA LI*
大部分的excrowable identity-based 金鑰交換系統接僅提供 partial forward secrecy，此論文提出了更安全的方案，可以達到perfect forward secrecy, ephemeral secrets reveal resistance，並且提出了嚴格的安全性證明。
10. Removing Escrow from Ciphertext Policy Attribute-Based Encryption B**y** *Junbeom Hur, Dongyoung Koo, Seong Oun Hwang, Kyungtae Kang*
CP-ABE加密系統和基於身份的密碼系統一樣，具有金鑰託管(key escrow)的問題，此篇論文即在介紹一個新的CP-ABE加密系統，可以解決金鑰託管的問題。
11. A Novel User Authentication and Key Agreement Scheme with Smart Cards over Insecure Networks By *Chun-Ta Li, Cheng-Chi Lee*
此篇論文介紹如何利用弱通行碼達成認證與密鑰分配的問題。
12. A Study on One-Time Password Authentication Scheme in Mobile Environment By *HongGi Kim, ImYeong Lee*
此篇論文針對可適用於mobile environment的一次通行碼認證系統作一個介紹。
13. A novel user authentication scheme with anonymity for wireless communications By *Niu Jianwei, Li Xiong*
認證一般皆需要利用到使用者的個人身份等資訊，此論文提出了可保障匿名性的認證系統。
14. Adaptively Secure Anonymous Identity-based Broadcast Encryption in the Standard Model By *Leyou Zhang, Qing Wu, Yupu Hu*
此論文提出了具匿名性的以及基於身份的廣播式加密演算法，其特徵在於可以在standard model下證明其具有adaptively secure的安全性。

肆、過程

(一) 12 月 11 日(星期日)

中午左右開車和學生黃凱彬赴桃園國際機場,由於我們此次並沒有買到直達濟州島之復興航空班機,因此只好先搭國際線航班至韓國首爾的仁川機場,再買韓國國內線的機票赴濟州島。我們一行首先搭乘下午 3:15 之長榮航空 BR160 班機至韓國首爾。飛行時間約兩小時又三十分鐘,因此到達首爾仁川機場時已經是晚上七點了。之後三步 併兩步的趕搭地鐵赴金浦機場,再衝至韓亞航之櫃臺買到濟州島之機票,幸運的趕上了即將起飛之班機,因爲這班如果沒趕上,到達濟州島後將無巴士可坐。

到達濟州島已晚上 10:00pm 了,趕上了最後一班巴士開往樂天飯店,光巴士又坐了進一個小時,最後終於到達住宿的飯店。結束了一天匆忙的行程。

本次會議住宿之飯店(Lotee Hotel Jeju)外觀

(二) 12 月 12 日(星期一)

會議的議場在飯店旁約 5 分鐘車程之地點,爲了節省經費,所以我們決定走路至會議議場。由於一路風光景色優美,所以一路上並不覺得累。約花了 30 分鐘之後到達會議中心,註冊後提了資料然後開始閱讀。我的第一篇論文**(A New Way to Generate a Ring: Universal Ring Signature)**是在今天第一個議程的第一篇發表,因此早早的就進入了會議室準備。報告完後接受題問,然後聆聽其它的報告。中午和韓國籍的 *Cheonshik Kim* 教授以及東華大學的楊慶隆教授一起用餐。下午的兩個議程都是邀請演講。第一場的演講題目爲 **On the Trends and Challenges in Green Information and Communication Technology and Samples of Some of our Related Research Results**,演講者爲 ***Prof. Mohammad S. Obaidat***

所屬：*Computer Science and Software Engineering, Monmouth University, USA*。

第二場的演講題目爲 **Overlaying Communication Infrastructure For Heterogeneous Multiagent Distributed Intelligence**，演講者爲 ***Prof. Habib F. Rashvand***

所屬：*School of Engineering, University of Warwick, United Kingdom*

邀請演講結束後還有最後一個議程，由我負責主持。報告者的內容主要偏向雲端運算的安全性介紹以及一些公開金鑰密碼的相關研究。晚上在參加完歡迎晚宴後再和 *Cheonshik Kim*，楊慶隆教授等一起走回飯店。

會議議場 International Convention Center Jeju (ICC JEJU)

Invited Talk 1

Reception

Reception

(三) 12 月 13 日(星期二)

早上和前一天一樣，走路至會議中心。我的第二篇論文(**Certificateless Signatures with Message Recovery**)在早上的第一個議程報告。針對我的研究，有學者提出了其實用上的可能性。因爲不需要憑證，所以沒有憑證驗證等等的問題。另一方面，由於提供了訊息回復的機制，所以可以減少所需傳輸的訊息量。由於我只提供了理論研究上的可行性，並沒有真的實做出來，因此，有學者認爲如果實做出來並經過測試的話，將會更有價值。

下午是另外兩場的邀請演講。第一場的演講題目爲 **WiMAX? A Case Study on Minimizing Construction Cost for IEEE 802.16j Multi-hop Relay Networks**。演講者爲

Prof. Han-Chieh Chao，也就是我們國內非常著名的學者，宜蘭大學的趙涵捷校長。趙校長此次演講的內容主要在介紹國內 WiMAx 的現況以及他們實驗室的一些成果。第二場的演講題目爲 **The challenges and practices on Cloud Security**，演講者爲大陸的學者，杭州科技大學(*Huazhong University of Science and Technology)*的金海(***Hai Jin)***教授。雲端運算是現在非常熱門的話題，但其安全性又不可以被忽視，所以這篇演講就是在介紹雲端運算所可能遇到的安全威脅以及金海教授他們的對策。

晚上在樂天飯店舉辦晚宴。

本人在會場報告

晚宴

晚宴

(四) 12 月 14 日(星期三)

早上是實驗室學生黃凱彬同學的報告，這一個議程結束後，我們終於有了一點時間可以進行觀光的行程。美其名爲觀光，其實就是在附近的景點繞一繞，然後照一些相片做紀念。之後又再趕飛機，從濟州島飛到首爾，再從首爾坐 19:45 長榮航空 BR159 的班機回台灣，到達桃園機場時已經是晚上近 11:00 了。結束了四天充實的會議行程。

伍、心得

心得

由於經費的原因，所以無法全程參與會議，必須提前一天回國，是參與此次會議較爲遺憾的地方。另外，過去參加會議都是自己一個人，但這次由於實驗室學生也有論文發表，所以可以一起同行。帶著學生一起參加會議，責任較爲重大。原本擔心學生第一次參加此大型之國際會議，會緊張或由於語言的隔閡而不敢和其他國外學者溝通。沒想到我們實驗室的這位同學非常放得開，積極主動的和國外學者聊天，打交道。雖然他的英文還有極大的空間需要努力，但他的勇氣卻是非常值得鼓勵的。也相信經由這一次的經驗，未來他一定也可以獨立參加國際會議了。

參加此次會議對我個人而言也有許多收穫，除了認識了許多國內外的朋友之外，也找到了許多議題可以在未來研究。此外，在國際合作方面，除了論文的共同研究之外，也和其他學者約好未來共同承辦或參與一些國際會議的舉辦。