TO: ICCL

出席 Asiacrypt'05 2005, India

國際學術會議手扎

(Dec. 04-08, 2005)

中央警察大學 王旭正

Dec. 02, 2005

這個行程是有些緊湊的，開始於 11 月下旬的一個週末，理事長知會我，將代表學會參加 Asiacrypt 2005(於印度，Madras，現已改稱 Chennai)全英名為（Chennai, India)。在近二星期的工作時間，我即趕辦啟程得必備的相關程序申請，包括對當地環境的查詢及了解、預約飛機航班、住宿問題的預定，至印度簽證的申請、工作崗位的請示出差與我的課程班級得提早調整調課等，諸多事物得在這段時間內完成。所有的工作，中間無論有多少插曲，使得進度因此延緩，但終究在出發前(12/02 出發，因稍晚的機位訂位已滿，無法在預定的 12/03 啟程)的前一天， 12/01 完成與確認所有的工作。於 12/02 上午 0740 搭乘馬來西亞航空（Malaysia Airline）經吉隆坡（Kuala Lumpur）轉機至印度的 Chennai。

到 Chennai 時已是當晚當地時間下午 0900，當時的天候正巧碰到暴風雨(Tropical Storm)襲擊該市造成機場漏水，街道也淹大水。飛機在降落時重飛了 3-5 次以上，過程之驚險，是我多次出國搭機裡，難忘的「驚魂」經驗。**機長的飛航專業佩我折服，各行業的專業果然是令人敬重的最好表現形式，此事令我想到同樣的道理，做研究亦是講究專業／真理／實學，這些技能/認知是讀書人挺天立地的利器，有了他們，何懼之有！亦因此可得人敬重。**

從機場出境，由印度的接待單位派專員接機，有趣的是，機場週邊亦淹水，實在慘不認睹，專員光腳過水來接我，我亦禮尚往來的脫下鞋子，光著腳回敬他

（因為只有光著腳鴨子，起褲管才能順利渡過水患的通路），至停車場搭車離去。此事大概也為個人的國外出差經驗記下難忘的一筆。知道嗎，從機場至下榻的旅館，過程的情景，不敢相信我竟成為報導中的人物之一了：記得在前些月裡，從台灣的報章雜誌，報導印度淹水時的取景資料，見到路人、行車擠在路上，寸步難行，洪流滾滾望水興嘆的一幕。想說的是，在到達印度當晚，我竟亦成為那幕中的主角（配角／路人甲、乙…..），實在令人玩味。也完全體會 Chennai 在暴風雨過境的情景，不知道隔天的報紙會不會像台灣一般報導某一城市／地區淹水，然後市長／地區官員們開被「唸」，要下次改進。告訴一個事實，那就是翻開報紙，沒有，完全沒有。哈，我猜四個字「司空見慣」可以解釋，或許亦可以這麼說，台灣其實還算幸福，「福氣啦！」

12/02 當晚，很累，測測網路環境後，在毫無多少意識下，進入無知覺狀態，睡著了！

Dec. 03, 2005

到達 Chennai 的第二天(由於飛機航班的原因，我是 12/02 即來到此地)，即開始做會議行程的了解與安排。會場內的布置是在 Ball-room 的國際會議廳，值得一提的是參加了多次的國際研討會，這是第一次看到在住宿（亦為會議所在地的旅館）地方，有著「重兵」駐紮，經詢問這是為保護會議住宿的安全所佈署，出入門的重要據點，設有安全門做金屬探測與人身檢查，對於如此的「招待」真不知是「幸福」亦是「不便」，不過後者在熟悉了幾位武裝人員後，我已能以常客的身分自由進出了，我想此時應算是幸福，享受如「高級長官」般的待遇。

此時，戶外仍是飄著細雨，記得 12/02 的暴風雨嗎？我想此時已快過該風雨的肆虐，相信下午時，應很快的「撥雲見日」，也象徵此會議即將從明日(12/04)正式開始。

Dec. 04, 2005

12/04 的確早上的天空較前二天的陰霾，露出了難得的開朗曙光。從旅館望外亦看到這個城市的一些活動力。也興起了至旅館周遭走動的念動，早上拿了該市的 Map 好好的研究一番，赫然發現，原來所住宿的地點是該市重要的現代化建築，住在此，當地居民皆視以「高級身份」。不過對我而言，其實只是身在異鄉，只得依會議地點，選擇最近的地點，以免迷失了方向，所以倒也自在了些，沒有啥多少身份的提升，我還是我，中華民國台灣在印度的一個土地上站著。下午，即開始了會議的前奏，PM0200~0500，一場關於「**Pairing Cryptosystem**」的 Tutorial。所有的會議參加者在此時似乎一湧而上地出現在會場。哇，人擠人，也許該說，會議接待處有些小，所以突顯了此現象。我極力地注意是否除了我以外，還有來自台灣其他單位代表，但今天毫無所獲。若看到類似面孔，例如日、韓、馬民族亦或普通話的對岸，是多些親切，但大夥溝通的仍是共同的語言，英文，在 Prof. Tanja Lange 的演講中，我特別環視所有參加的人員，當然我看到近 1/3 (or more)印度籍的年輕學生。我想我可體會此種情形，如同 2003 年台灣舉辦「Asiacrypt 2003」，我們亦發動所有學生來共襄盛舉，此情此景，在印度我看到台灣的翻版。只是臉孔變成了印度學生的樣子而已。

在下午近三小時的演講，Speaker Prof. Tanja Lange 從最簡單的概念說起，從在密碼領域的出現，與其它密碼的關係，一起帶到其原始的數理基礎、概念。整場會議，我看到數學文字/符號在會場中翩翩飛舞，這場精采的數學秀，也吸引會場與會學者、學生的目光，摒氣凝神的欣賞這場學術發表，沒有人睡著耶！或者說想睡著的人不會來！據估計，該場演講在會場中約有 150~200 人與會。(有些學者將在 12/05 正式的 Paper Presentation 才出現），故本次的 Asiacrypt 2005 應約有超過 200 人與會，此時此刻期待明日 12/05 的會議重要研究論文發表/報告的粉墨登場。

Dec. 05, 2005

12/05(星期一)，到達印度第三天，是 Asiacrypt 2005 的正式報到/開始。開幕致詞由大會的 Program Chair Prof. Bimal Roy 進行本次會議的說明。在致詞內涵中，提及本會議的傳承過去的優良與精緻、投稿量共 237 篇，僅收錄 37 篇加以刊載，維持 Asiacrypt 歷年來的高水準演出。事實上 IACR(International Association for Cryptographic Research)在 Asiacrypt 上共有 3 項國際會議主軸,分別為 Crypto(八月,美洲/美國)、Eurocrypt(五月,歐洲)與 Asiacrypt(十二月，亞洲)，其中的 Crypto 每年固定於 IACR 總部(Santa Barbara, CA, USA)舉行，其它則巡迴至該洲的各國舉辦。在此次的 Asiacrypt 2005 中，印度為主辦國，我極力的翻了又翻，發現印度本國投稿後得以刊載的文章共 1.5 篇，表列如下：

1、paper 1： "A Near-Practical Attack Against B Mode of LIBB"

Author list：Joydip Mifra (India)

2、paper 2： "New Applications of Time Memory Data Trade offs"

Author list：Jin Hong (Korea) and Palash Sarkar (India)

藉此，想借題發揮的是 Asiacrypt 2005 在台灣，我們亦有一篇文章(Made in Taiwan)得以刊載如下:。

"Untraceable Fair Network Payment Protocols with Off-line TTP"

Author list: Chin-Hung Wang

若較之此次的印度作者論文發表,當年我們的成功演出亦毫不遜色的能得以入圍高水準會議的發表，象徵我國在研究上的一種成就與肯定!今天的會議行程，首先由 Prof. Bart Preneel 進行演講，題目：

HASH STRUCTURE DEVELOPMENT AND APPCICATIONS 。

此題材應是這一、二年來最受囑目的資訊安全重點項之一。因為 2004 年 Crypto2004 的 Prof. Xiaoyun Wang(王小雲教授)提出 MD5 可以提高破解的機率之後，HASH 議題即引起廣泛的討論。在講演內容對於 HASH 的重要與應用，Prof. Bart Preneel 整理出幾項：表列如下：

1. **Digital signature, Destroy the algebraic structure**
2. **Construction of MAC, Stream and block cipher applications**
3. **Payment systems (for example micro-payment, etc)**
4. **Pseudo-random string generation/key derivations**
5. **Confirmation of knowledge/commitment**
6. **Protection of password**
7. **Information authentication: protect authenticity of hash result**
8. **Redundancy: hash result appends to data before encryption**

對 HASH 的議題，相信仍會持續發燒一陣子。若國內研究學者有興趣，此方面研究應有多些機會可在國際會議展成果。接下來的會議論文發表場次為

「**SIGNANURES**」，

「**ALGEBRA AND NUMBER THEORY**」與

「**INFORMATION AND QUANTUM THEORY**」，

其中筆者覺得值得再一提的是其中的一篇 **“Do All Elliptic Curves of the Same Order have the Same Difficulty of Discrete Log?**”與 **“Quantum cryptography”** 的研究。前者是作者在假定一些合理前提下，試著定位 Elliptic Curve Cryptosystem 在眾所皆知的 Discrete Log problem 下的困難度討論。演講者用細膩的筆觸，投影至會議。此舉的介紹，讓在場人員印象深刻(當然議題本質即具吸引力）。另外是 Quantum 的研究，已是近些年來，在物理、計算機裡發光發熱的理論/實驗

題材。故在會場內會較有吸引力，參與者抱持著想知道有什麼“新鮮事”被開發出來了。國內對此亦在積極投入，對於新興議題的投入，若能掌握先機，相信要展露我國的密碼/安全研究能力是很有機會成功的，藉此筆者提一點觀察與淺見，僅作參考。

整天下來，筆者在過去幾年在一些國際場合所接觸的幾位教授也參與此次 Asiacrypt 2005 諸如 Profs. Eiji Okamoto, Kwangjo Kim, Ed Dawson 等人。筆者與幾位握手致意,談論些 IACR 的密碼會議的形式與趨勢。這些教授亦分別是 IACR 裡重要的國際決策核心，例如 IACR Asiacrypt Steering Committee Meeting 即在 12/05 晚上討論 Asiacrypt2008 的主辦國。經過熱烈討論後 Singapore 勝出，將主辦 Asiacrypt2008(此消息來自 Prof. Kwangjo Kim 會後透露)。我國雖然已舉辦 2003 的活動(Asiacrypt 2003)，然若有機會當再爭取更多大型與具指標意義的國際會議，這些國際活動應能積極派員投入/觀摩，或鼓勵學者/研究人員投稿參與，如此才能在 IACR 的活動中取得信任與經驗基礎。

Dec. 06, 2005

至印度第四天，似乎已適應此處的一些生活與語言特質，回復較正常些的睡眠與生活作息並與服務生閒話家常，也習慣了些他們的印度口音。所以文化習性的了解是與不同民族溝通的很重要催化劑。從此處，自己想到，任何事務的熟悉與深入不就是得由最內在的文化開始嗎，如此的生活學習才能根存，不會過往縱逝啊！

今天的活動，似乎一大早撲了個空，原本 0900AM 的演講並未如期舉行。也許我未留意這些臨時的改變，而後經詢問與了解，原來此次二場 Invited Talks 其中的一場 Prof. Andrew C. Yao，人因臨時事件並無法舉行。而僅有 Prof. Bart Preneel 的 Talk 照舊。對此改變，也許有不少與會同我一般，未能清楚狀況，故在 0900 時會場有不少人端坐在那兒，撲了空。但沒關係，即來之，則安之，我就在那兒看看書，端拿著 notebook 整理些資料，也因為臨時性的狀況，故早上所有的行程皆提前 30 鐘進行。0930 開始今天所有發表文章的活動，今天的文章發表主題分別為

「**PROVABLE SECURITY**」與

「**PRIVACY AND ANONYMITY**」

共二大主題。下午大會則安排一個 Day-tour 至 “Mahabalipuram” 進行文化參訪，自由參加！有興趣的人可隨行。其意就如同 Asiacrypt 2003 在 Taiwan 當時我們安排至台北市的故宮博物館一般，每次的國際型研討會，主辦單位皆希望與會者賓至如歸，為該主辦單位與國家留下最好的印象，也算另類的國民外交之一。當然在參訪完後，隨即安排僅有一場的豐盛晚宴，款待所有的與會者，賓客盡歡。大會也趁此機會介紹印度的美食佳餚。

事實上，這些除正式的論文討論/發表/研究外，Tour、Banquet 等皆是 Asiacrypt/ Crypto/ Eurocrypt 的重要特色。在每次的新的舉辦地點討論，似

乎這些都是 Steering committee 的 Profs. of Heavyweights 所關注的焦點之一。在今天我的外交工作上,亦將我們的CCISA的業務推廣介紹 Prof. Tanja Lange 與 Prof. Bart Preneel。這二位為此次會議的 Invited Speakers。在會議中，因相關機會坐在他們的旁邊，藉此交換一些研究經驗，未來的工作與討論一些庶務的看法。最後並將 ACM conference 2006 in Taiwan 的資訊再當面告之，並遞予 Call-for-participation。想當然爾，他們的臉上喜悅，也直接反應此次行程的學術與“外交”工作的豐富收獲！

Dec. 07, 2005

星期三的開始，今早的睡眠，又比前些日子更好，好似我已是在”在印度定居的台灣人”僅為我不會印度話，仍如往昔趕在 0700AM 進餐廳，享受一天的重要 Breakfast，由 Hotel 提供。由於此 Hotel (Taj Coromandel) 在當地頗負盛名，亦是會議的主辦地點，大會安排所有人住宿於此，以利大會的整個行程安排，如同 Asia Crypt 2003，我們安排圓山大飯店，以我們最負具特色的 Hotel 來招待遠方的貴客。事實上，筆者在出發至 India 前 1 日，才在住宿上得以獲得解決。(因為起初聯絡 Accommodation 時，會議地點的 Hotel 早已被預定滿了)我也終於鬆了口氣，不會流落 India 街頭.

接下來回到今天的議程，分別表列如下:

「**BLOCK CIPHERS AND HASH FUNCTIONS**」、

「**STREAM CIPHER CRYPTANALYSIS**」、

「**CRYPTANALYTIC TECHNEQUES** 」、

「**BILINEAR MAPS**」及

特別安排與傳承的「**RUMP SESSION** 」。

今天皆為此會議的發表文章與討論，我一整天下來眼力有些吃力，眼疾的老毛病復發，只剩單眼能正常運作。眼前的事物在「矇矓美」下，只能用聽力發揮最大的想像空間，大過倒是無傷大雅於會議文章討論發表的參與。

今天算是報到/註冊起的第三天，所有事項的安排似乎對於所有與會者而言都已較熟悉。唯一不同的是，隔天就是最後一天了，所以部份人員已在詢問接待單位，如何回程接送搭機的事宜。此次除大會行程外，其它相關旅遊(12/06 下午)與住宿/旅程的接待安排皆委託 Hi-tour, India 全程負責。此舉同於 Asiacrypt 2003 我們亦請公關公司，來負責招待事宜。如此可讓大會議程人員專心於研討會內含的安排/學術性討論。此次由於決定啟程至 India 參與 Asiacrypt 2005 的時間，已是非常接近 12 月上旬，故在短短二星期的準備中，

的確相當緊湊地處理所有事項，其中在住宿的聯絡即透過 Internet 與 Hi-tour 近二星期的協調/溝通，終於順利覓得棲身之地。在會期中我亦特別留意此次大會所安排的 Internet Facilities 。我認為這是會議主辦單位得用心的重點之一，因為 Internet 可使得所有人透過 Internet 做跨越空間的通連。然美中不足(亦或筆者淺見)，大會的電腦僅安排 6 台，似乎稍嫌少(或很少)，在面對近 200 人(或更多)的與會者，電腦的使用應至少有 1/10 以上的比例(筆者觀點)，讓與會者能享受除會議內容外，亦能自在地對外通聯。另外由於此次 Internet 的界接是以 Wireless 為通連環境，在會期中的經常性"No Signal" 亦造成不少困擾，事情做到一半就 "掛了" 時有所聞。例如 RSA 的作者之一 Prof. Shamir， 此次亦參加了議程，筆者亦代表我們學會 CCISA 對 Prof. Shamir 表達問候之意(Asiacrypt 2003 in Taiwan, Prof. Shamir 為我們 CCISA 邀請的重量級貴賓)。在會期中總是看他穿梭於 Internet Facilities 與議場中，嘴裡最常念念有詞的是 "No signal now" or "Is it working now?"這些皆是舉辦國際大型會議應特別留意之處啊。 最後在今天的重頭戲之一，晚上的「**RUMP SESSION**」。從發表論述的資料名單來看似乎不怎麼踴躍，在開始前，我仍遐想或許會有「奇蹟」出現。一則是期待也許會臨時多些發表場次，因為往往會前幾天名單只是暫列，在當天會場裡，看到的才是最真實的。另一則期待，則是期待 Crypto 2004 的類似「Hash-MD5 Breaking」故事能在此處上演。是否亦能親身感受一種學術研究在瓶頸點突破那一剎那的臨場「感動」?這些願望可惜並未在此次的「**RUMP SESSION** 」上演！所有劇碼是依照原始之名單依序演出，不過在節目裡一些新鮮想法倒是有趣。然是否「感動」，則還未至此地步！其中值得一提的是有關「**Skype Cryptosystem Overview**」，Skype 是近年的新興密碼通訊產品，對於密碼界的確是一項值得注意的密碼應用工具。這是由老牌學者 Tom Berson「演出」的戲碼。這位仁兄似乎是 IACR 活動的常客，相當活躍於會場中，在參加 IACR 國際活動時，筆者經常看到他穿梭其中。猶記得筆者與會 Crypto 2001 時(Venue at the University of California , Santa Barbara, CA)，亦在 Steering Committee 中，與

他一起討論台灣舉辦 Asiacrypt 2003 的議題。這位仁兄說話還蠻有趣的(筆者認為那是因為他熟稔 IACR 的人、事、物，故怡然自得)。

最後要提的是，在「**RUMP SESSION** 」中，有提供相關未來重要研討會的 Announcements。例如此次中有下列的國際會議作廣告(Call-for-papers):

- 4th International Conference on Applied cryptography and Network Security (ACNS'06), June 6-9, 2006, Singapore
- Asiacrypt 2006, Dec. 3-7, 2006, Shanghai, China
- ACISP 2006 MELBOURNE AUSTRALIA

此次的 Asiacrypt 2005 行程我亦將我們 CCISA 舉辦 **ACM Symposium on InformAtion, Computer and Communications Security, Taipei, Taiwan, March 21-24, 2006** 的訊息在會場裡四處見人就邀約與製作許多備份(Hard-copy)於註冊處，供不應求，所以此行任務之一亦算圓滿達成。

我想未來我們 CCISA 參與 IACR 活動時，可充分規劃並事先在整個會期開始前依程序做 Call-for-paper(或其他目的/宣傳)登記，如此即可在「**RUMP SESSION** 」中準備資料作 1 至 2 分鐘 Short-time Talk for Prominent Conference Call-for-papers in Taiwan，至少可為台灣的國際形象打知名度！我特別注意明年 Asia crypt 2006 將在 Mainland China 的上海舉行。屆時我們的代表如何出席，倒是有趣的遐想。

Dec. 08, 2005

12 月 8 日星期四，進入最後一天了。議程 12 月 4 日~12 月 8 日，共 5 天的行程(含第一天的 Tutorial Talk)。今天較不同的地方，在於大會的報告地點改至另一個場地，不在同一個地點。經了解，也許是在場地上與另一個舉辦大型活動的場地在時間上有所衝突。故協調下，換至 2 Km 外的另一地點，當然這路程有提供交通車接駁。不過雖如此，在方便性上，終究略遜原先的地點。這些當然反應在當天與會人員的低出席率上(少了一些或僅前幾天出席率的 6 成左右，不過我想原因或多或少與已是會議最後一天有關，有些與會者今早已趕搭飛機離去)，可見會議地點的重要性。

今天的議題表列如下：

「KEY AGREEMENT」、

「MULTIPARTY COMPUTATION」、

「ZERO KNOWLEDGE AND SECRET SHARING」

整場會議在下午 3 點結束，大夥並道再見。大會主席 Prof. Bimal Roy 並說明這附近有 Shopping Mall，各與會者可去輕鬆一下，了解 India 的觀光、產品、文化等特色，也對地點的改變做進一步的說明。最後提及 INDOCRYPT (International Conference on Cryptology in India) 將於下星期 Dec. 10-12 舉行。若可能的話，請繼續支持 India 在密碼/安全系統上的研究，並能再度與會。

所有行程至此告一段落，所有密碼/安全的學者、專家相約明年，2006 年 Mainland China, 上海見！(Dec. 03-07, 2006) ！