

出席 CRYPTO 2001 at UCSB (美國加州大學, Santa Barbara 分校)會議報告

中央警察大學 王旭正

壹、前言

如往年地，在二十一世紀裡的第一次的國際密碼會議於美國加州大學的 Santa Barbara 分校舉行（如圖一），由於 CRYPTO 會議為最早所主辦的國際密碼會議，爾後陸續有 Eurocrypt 與 Asiacrypt 等於歐洲與亞洲地區舉行的國際密碼會議，相較之下，對於 CRYPTO 的舉行，主辦單位自然更為重視其地位與相關籌辦事項。我國在資訊安全與密碼技術研究上在資訊安全學會(CCISA)的多年努力下已逐漸獲得國際資訊密碼學界的肯定，而我們每年亦會積極參加 IACR 所舉行此三大最重要國際密碼會議，CRYPTO，Eurocrypt 與 Asiacrypt。

在本次的出席 CRYPTO 2001 裡，除聆聽最新發表研究論文，收集、交換來自世界各地的新近研究報告、心得之外，亦是延續今年五月份我們學會於出席 Eurocrypt 2001 裡所爭取到 Asiacrypt 2003 的主辦權，並得於此次會議裡召開 Asiacrypt 2001, 2002, 2003 的籌備會議(Asiacrypt Steering Committee, ASC)裡了解各主辦單位的承接經驗，並說明目前進度，未來的發展等議題。

由於 CRYPTO 為各個國際密碼會議裡的最主要會議，因此本次會議裡也是許多研究學者所躍躍欲試、爭取研究受到重視的最佳發表處。基於此，資訊安全學會亦如往例一般的出席此一盛會，希能完成上述幾項重要任務，藉此能更將我國學術研究的發展臻至世界級水準。

貳、出席 ASC Board Meeting

如前言所提，本次除參加 CRYPTO 2001 外，並代表出席 ASC Board meeting，了解這些年 Asiacrypt 的舉行經驗與未來 2001, 2002, 2003 的進度，此次於八月二十日下午五時於 UCSB 校園裡的 Anacapa Formal Lounge 舉行，出席人員有

1. 澳洲的 Prof. Ed Dawson、Prof. Jennifer Seberry，
2. 韓國的 Prof. SangJae Moon、Prof. Pil Joong Lee、Prof. Kwangjo Kim，
3. 日本的 Prof. Hideki Imai、Prof. Tsutomu Masumoto 與
4. 台灣的本人出席。

整個會議進行由 Prof. Dawson 所主持。其流程為：

- 一、Asiacrypt 2000 於日本舉行的經驗分享：由 Prof. Masumoto 說明相關進行方式。
- 二、Asiacrypt 2001 的籌辦情形：由 Prof. Dawson 說明現階段的工作。由於 Asiacrypt 2001 將在今年 12 月於澳洲黃金海岸(Gold Coast, Australia)。此會議為亞洲密碼

的重頭戲，因此在當天 ASC 的重點在於說明此會議的相關工作執行狀況。依據已結束審查工作統計，此次 Asiacrypt 2001 共有 153 篇論文投稿，計錄取 33 篇，錄取率與同年的 Eurocrypt、CRYPTO 的情形大致相同，皆具高水準的學術研究論文。另在全部的五天會議行程上，Prof. Ed Dawson 作了非常詳細、有趣的介紹，並希望諸位 ASC members 能共襄盛舉，鼓勵各國學生、學者專家來參與，亦由於澳洲著名的黃金海岸觀光區舉行，Prof. Dawson 保證會議參與者絕對值回票價。

三、報告 Asiacrypt 2003 於台灣舉行的狀況：此部份亦是筆者此次的重要目的之一，首先筆者在會前已將相關資料(於學會九十年七月十七日第六次理監事聯席會議有關 Asiacrypt 2003 籌備工作做成的討論決議)發送給每位 ASC 參與人員，並一一握手致意，尋求未來舉行的全力支持與經驗協助，亦全部獲得正面回應與鼓勵，令筆者感到欣慰與興奮，相信我們學會必能傾全力辦好 Asiacrypt 2003 的活動。在報告中，筆者將整個工作分組做一說明，並提及將視需求會做擴大的任務編組。對於本次準備工作，ASC 成員站在鼓勵與了解執行狀況來聽取內容，故皆給予肯定，並補充希望一切能依計劃執行，並定期召開籌備會議。另外下次的進度報告將於 Asiacrypt 2001 會議中做報告(將於 0100 PM, Dec. 9, 2001, 召開會議，ASC 希望能有更完整的 proposal)。

四、Asiacrypt 2002 報告與 Asiacrypt 2004 的討論：明年(2002)的 Asiacrypt 於紐西蘭舉行，該主辦人(General Chair)為 Prof. Hank Wolfe，亦為 IACR 的理事之一，對於相關準備事項已完成 Call for paper 的定稿，並積極至相關國際資訊安全會議中宣傳文宣，期能收到功倍之效果。另在會期細節上，由於得視投稿/刊稿的情形而定，暫無法說明，其餘大部份皆已就緒，該單位目前將重心擺在全力宣傳上。至於 Asiacrypt 2004 的主辦國，由於此次 ASC 希望能做一章程調整，將亞洲密碼會議的舉辦由 ASC 會員自行討論決定，再將結果提供 IACR 做備查，然此次在多方討論與會議時間已超過預計的二個小時甚多，仍無法有關 Asiacrypt 2004 的主辦國的決定，故移至下次的 ASC 再討論。

五、整個會議時間為 0500~0720 PM，已超過了預算時間。

參、出席 CRYPTO 2001

一年一度的國際密碼盛事 CRYPTO，今年仍在美國加州大學的聖塔芭芭拉分校(The University of California, at Santa Barbara)舉行，也許是常年皆在此地舉行，故所有會議程序、進行、用膳；住宿、參觀、休閒 等節目活動皆是駕輕就熟，尤其在主要論文發表的會場為該校的戲劇電影院，在座席後方還有專人為會場音量、燈光做控調，氣勢仿如一場別開生面的舞台秀。在介紹本次 CRYPTO 的學術論文前，先為整體的統計數據作描述來初步了解整個作業流程。

● 投稿論文：156 篇，接受論文：34 篇，發表論文：33 篇(因一篇臨時抽掉)，
在這些數據中，我們台灣有 7 篇論文投稿。

● 本次會議的註冊參加國家人員前幾名統計：

- 1、美國(USA)：220 人
- 2、南韓(South-Korea)：43 人
- 3、法國(France)：39 人
- 4、日本(Japan)：31 人

其中，韓國在本次 CRYPTO 2001 中，共有 43 人參加，且其有 3 篇論文有這次會議中發表，可見這些年來，韓國政府投注大量人力、經費培植資訊安全與密碼研究已獲得不錯的成績。對於此，筆者亦在次會場中，與一群來自韓國漢城大學數學系的研究群多次交換意見。以此一研究群為例，得知韓國政府可補助學術群體 8 人(其中 1 人為帶隊教授，2 人為博士生，5 人為碩士生)，來參加此一會議，希能有系統培養新一代生力軍。另外韓國的資訊安全與密碼研究，亦於基礎科系之數學系紮根，筆者認為以國內的基礎科系實力並不亞於國際其它國家，若能於重點發展中，將資訊安全與密碼研究納入發展中，相信在密碼技術的培養與發揮，亦能有實質之成效，以利植於我國資訊安全與公開金鑰基礎建設的自行研擬標準與開發。對於歷來參加人數統計方面：此處我們另外有個有趣的數字統計如下：

1997：506 人

1998：529 人

1999：509 人

2000：502 人

2001：497 人

雖然人數皆差異不大，然筆者個人以為是否換個地點舉行可增加新鮮感，人數是否有明顯的增加效果，值得玩味！接下來，我們即為這五天的行程作重點說明與簡介：

第一天(08/19)：傍晚時分，開始報到 or 現場註冊，當然會場內擠滿了來自世界各國的研究學者，亦彷彿置身於聯合國。

第二天(08/20)：為正式論文發表，亦由於是第一天，所以會場內，幾乎坐滿席的參與人員。整天共安排了五場 sessions(其中含一場 為 Invited talk)。分別如下：

- session 1：Foundations
- session 2：Traitor Tracing
- session 3：Invited Talk：“Quantum Information Processing in Semi-conducts：An experimentalist’s view”
- session 4：Multi-Party Computation
- session 5：Two-Party Computation

在第一個 session 中由，由 Bill Aiello 所主持，內部含 2 篇論文，分別探討一些較新的密碼函數發現與定義，由於皆剛定義出來的，故在文章表現上皆先以“Extended Abstract”來 presentation。而第二個 session 即相當有趣，亦有 2 篇文章發表，皆相關於 Tracing Traitors 的研究，其中的一篇“Self Protecting Pirates and Black-Box Traitor Tracing”在實際 Pay-TV 系統的節目內容安全保護上可發揮相當的地功效，可應用實際系統的開發，上述第二個 session 乃由 Erez Petrank 所主持。之後大會為能吸引聽於眾的注意力，在第 3 個 session 安排 Invited talk，由此次 CRYPTO 的 General Chair, Joe Kilian 所主持，其主題為“Quantum information processing in semi-conductors: an experimentalist's view”演講者為 UCSB 內的 Mark Sherwin 教授所主講，Mark 一開場即提到 Quantum Cryptography 在近年來已引起相當注意，也期待能突破此一新領域的研究，然大都集中在理論上之鑽研，所以 Mark 在花了相當的時間在做實際的實驗性半導體設計，期能在硬體的開發上，亦有階段性配合，並將實際開發的過程和與會人員進行分享。該講演引起熱烈的討論，當然意見正反不一，直至主持人中止討論，才結束一場激烈的學術爭論，不過亦由此得知 Quantum Cryptography 的魅力所在。對於任何事似乎愈有魅力，話題 爭論愈是明顯。至於下午的 Session 4、Session 5 分別為 Multi-party 與 Two-party 的安全通訊的計算問題研究，這部份的議題在歷年的 CRYPTO 會議裡亦有頗多著墨與學術發表。

第三天(08/21)：已進入第三天，今天白天的安排僅以上午的議程為主，分別為

- Session 6：Elliptic Curves
- Session 7：OAEP(Optimal Asymmetric Encryption Padding)

其中 Elliptic 部份由 T. Okamoto 所主持，並共有 3 篇論文發表，分別著重在 LSB 的預測性，加/解密效率的提昇與應用於 Identity-Based 上的機制。至於另一主題‘OAEP’是在 RSA 的保護機制上所提出的較新理念的加強與改良機制。事實上透過 OAEP 能夠有效地阻擋在公開金鑰系統中的 adaptive chosen ciphertext attack，因此在 OAEP 的延伸研究上吸引近年來密碼學者的注意。到了晚上，則為在 CRYPTO 系列(CRYPTPO、Eurocrypt、Asiacrypt)裡的盛宴：Rump session 的公開演講，每名登記者皆可有 3-8 分鐘的時間去暢談研究的最新狀況，今年的登記比起往年更是踴躍，共有 37 篇文章要上台發表，該 Rump Session 的主持人 Stuart Haber 相當地辛苦，需要在短時間即得要求每位講演者結束，而 Rump Session 所發表的文章，皆由 speaker 自行事前登記即可上台發表文章，因此筆者鼓勵國內學者能多參與此一盛會，並事先將研究成果或可能趨勢在 Rump session 中作登錄即可發表。

以下列出 37 篇今年 CRYPTO 裡 Rump session 的文章標題以為參考：

1. Weaknesses in the key-scheduling algorithm of RC4
2. Using the Fluhrer, Martin, and Shamir attack to break WEP
3. A verifiable secret shuffle and its application to e-voting
4. No more panic in Florida: Reality or dream?

5. Cryptanalysis of the revised NSS signature scheme
6. Cryptanalysis of a pseudorandom generator based on the braid group, or The decisional Ko-Lee assumption is false
7. The compression side channel
8. Umbral optimal normal bases
9. Financial Cryptography '02
10. Announcements from NIST
11. HDCP—as spec'd
12. CryptoBroker
13. A new class of invertible mappings
14. A working implementation of the time-memory trade-off of Hellman, and how many 40-bit keys can we break with a simple computer during a short rump-session
15. Deterministic and bountiful generation of block substitution tables with maximal nonlinearity
16. New covering radius of Reed-Muller codes for t -resilient functions
17. A trivial attack against CBC-PAD: Breaking SSL, IPSEC, WTLS, ...and Alert on nonlinearity: Linearities in Rijndael, Kasumi
18. Securely combining public-key cryptosystems
19. A provably secure IND-CCA public-key encryption scheme as efficient as El-Gamal
20. Bidirectional security
21. Generating long shared keys in the storage-bounded model
22. On the composition of authenticated Byzantine agreement
23. On the model of distinguishers in computational zero knowledge
24. Reusable time-lines and applications
25. Non-malleable commitments based on factoring
26. How many 40-bit keys can we break...during a short rump-session talk?
27. Short signatures from the Weil pairing
28. A short DSS-based signature
29. Composition and efficiency tradeoffs for forward-secure digital signatures
30. Secure digital signatures with McEliece and new records in short signatures
31. Security notions of unconditionally secure signature schemes
32. Quantum coin flipping with arbitrary small bias is impossible
33. A quantum information-theoretical model for quantum secret-sharing schemes
34. A dual watermarking and fingerprinting system
35. State-varying hybrid stream cipher
36. Tree decision Diffie-Hellman problem

37. Introduction GammaPi

其中較令悚動的為” How many 40-bit keys can we break...during a short rump-session talk? ”, speaker 為 J.-J Quisquater, 該學者利用一台 Notebook 當場嚐試要破解, 據稱沒有問題, 然 J.-J 當天運氣不佳, 沒能在時效內破解 40-bit 之 key, 殊為可惜。

第四天(08/22) : 今天共安排 5 場 sessions, 其中包含一場 Invited talk, 各分別如下 :

- session 8 : Encryption and Authentication
- session 9 : Signature Schemes
- session 10 : Invited talk with “ Privacy, Authentication & Identity : A recent history of cryptographic straggles for freedom ”
- session 11 : protocols
- session 12 : cryptanalysis

亦同往年一般: 數位簽章的研究持續不斷, 其中的一篇文章”The order of encryption and authentication for protecting communications(or: How secure is SSL)”提出在安全通訊中常用的 SSL 屬於 authenticate-then-encrypt method, 這種方式不夠安全, 作者另行提出更安全的 MAC method 以 encrypt-then-authenticate 處理, 這部份的觀點, 筆者覺得十分特殊, 值得深入再開發研究。另外, 在密碼分析上的文章, 其中的一篇”Crytanalysis of RSA signatures with fixed-pattern padding,” 本篇論文改進了先前的研究; 討論在 RSA 的簽章處理裡, 所夾帶的額外 fixed-pattern 必須至少於模組數的 2/3 長度才足夠安全, 此部份的分析, speaker 非常仔細地說明其來龍去脈, 筆者覺得此部份可作為我們在 RSA 簽章應用上的考量而避免於被破密攻擊的危險。在今天的 sessions 中, 大會亦安排了第二場的 Invited Talk, 演講者為來自業界的 Daniel J. Weitzner 此題目由於不涉及技術, 純粹以隱私權、身份鑑定等議題的社會定位與發展趨勢做說明, 在座者的出席與 08/20 的第一場的 Invited Talk 人數相較之下稍少了些, 在創新性上較沒有特殊性。今天最後的一個節目是 IACR General Meeting, 由 IACR 主席 Kevin McCurley 主持, 所有 IACR 理事大都出席。會中說明此次 CRYPTO 主辦的相關過程與論文收集、審查, 接受的所有庶務, 本篇報告的相關的論文投稿, 各國參加狀況, 皆由此會議得知。節目最後並為未來的幾場重要密碼會議, 諸如 Asiacryp2001, 2002, Eurocrypt 2002, 2003, CRYPTO 2002, 2003 做宣傳, 筆者認為我們主辦的 Asiacrypt 將得在未來 2 年的任何國際會議中做多次的宣傳, 歡迎鼓勵, 世界各國學者來參與投稿。

第五天(08/23): 最後一天的議程, 安排至中午, 共有 3 場 sessions 分別為 :

- session13 : Applications of Groups and codes
- session14 : Broadcast and Secret sharing
- session15 : Soundness and Zero-knowledge

在這 3 場的 session 中的第一個 session, 我們要留意的是韓國在密碼研究的發展, 在今

天的發表中，囊括了 3 篇文章分別為

”Nonlinear Vector Resilient Functions”、

”New Public Key Cryptosystem using Finite Non Abelian Groups”、

”Pseudorandomness from Braid Group” ,

在數學基礎的紮根上，韓國的學者的確投諸相當心力，這也是筆者於前述中所提，國內亦可在基礎數學系所中鼓勵朝密碼研究，亦定能有非凡的成績表現。另外二場的 sessions 內容:Broadcast and Secret sharing 與 Soundness and Zero-knowledge 亦為每年 CRYPTO 會議所編列的重要主題，國內在研究上其實也有不少作品符合這些主題，可在學理基礎再加強與論證，當可很快在國際密碼佔有一席之地。

肆、會議心得與攜回資料

- A、密碼與安全技術是 Internet 時代的趨勢，東亞國家在這方面早已投注心力，我們得再加緊腳步，想必 Asiacrypt 2003 在台灣主辦，是一個契機，希望學會能整體規劃集合一些研究結果，在密碼安全研究上能推出幾群研究的重要與最新成果。
- B、承續九十年七月十七日第六次理監事會議通過鼓勵優秀學者，學生出國參與國際密碼會議，藉由參與國際會議帶回最寶貴的資料與經驗。亦希真正能促請政府部門(如 NII推動小組)能撥經費於補助教授 學生群參與類似 IACR所舉辦 CRYPTO, Eurpcrypt, Asiacrypt 系列的會議，我們的密碼安全研究才得以有紮根的培養。
- C、攜回資料：
 - I. CRYPTO 2001 論文集一冊。
 - II. 註冊參加名單一份。
 - III. 多張 call for paper(含 Asiacrypt 2001, Asiacrypt 2002, ICISC 2001, IWAP 2001, 2002 IEEE International Symposium on Information Theory, PKC 2003, Fast Software Encryption Workshop 2002 ... 等等)



圖一：會議地點，UCSB