行政院國家科學委員會專題研究計畫 成果報告

量子演算法之研究及其在密碼學之應用(3/3)
研究成果報告(完整版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 95-2218-E-002-005-
執 行 期 間 ：95 年 08 月 01 日至 96 年 07 月 31 日
執 行 單 位 ：國立臺灣大學電機工程學系暨研究所

計 畫 主 持 人：雷欽隆

計畫參與人員：博士班研究生-兼任助理：邱允鵬、廖燕華
碩士班研究生-兼任助理：林峻鋒、康照群
講師級-兼任助理：林峻鋒、康照群

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 96 年 11 月 02 日

行政院國家科學委員會專題研究計劃成果報告

量子演算法之研究及其在密碼學之應用
Quantum Algorithms and its Application in Cryptography

計劃編號：NSC 95-2218-E-002-005-
執行期限：95 年 8 月 1 日至 96 年 7 月 31 日
主持人：雷欽隆　台大電機系教授

一、中文摘要

在量子現象被運用來提升計算速度後，量子電腦的概念已逐漸形成，目前數個量子位元(Quantum Bit)的電腦已經實驗成功，而更多量子位元的電腦也正在設計與驗證中。利用量子電腦之強大計算能力，Peter Shor 提出可在多項式時間內解出因數分解的量子演算法。目前密碼學中許多重要的安全磐石，都將面臨被破解的夢魘。不過，已有學者利用量子現象設計出完美安全(Perfect Secure)的密碼技術，這些新發明著實令密碼學家相當振奮。的確，量子電腦的來臨對目前資訊安全造成危機，但也是個轉機，它將為資訊安全與密碼學開創全新的研究領域。世界各國學術機構正展開量子計算的相關研究。

本研究計畫的主要標的是量子自動機理論、量子演算法與量子密碼學。希望藉由基礎理論之研究能對量子計算之特性與能力能有更深一層之了解，進而設計出實用之量子演算法。在量子演算法的設計上，我們將以密碼應用為主。『水能載舟，也能覆舟』，在計畫第一年我們探討有哪些傳統的密碼演算法會因量子計算強大的能力而被破解。另一方面，我們也將探討有哪些量子特性可用來建構傳統計算機系統所無法達成之密碼演算法。

在計畫第二年我們探討量子模糊傳輸及其應用。模糊傳送是一種特殊的通訊協定，被廣泛的應用在許多安全議題及密碼加密上，例如:秘密交換、丟銅板問題或簽合約問題等等。古典模糊傳送可以用數學的方法來實現，例如RSA演算法。然而這些數學方法是建構在困難的數學問題上，安全性是建構在數論難題的基礎上。我們可以用量子的方法來破解之。為了解決這樣子的問題，本計畫希望建立一個能抵擋量子攻擊之模糊傳輸協定,Popescu and Rohriich 提出一個"non-locality machine"簡稱 PR-Box。模糊傳送可以用PR-Box來實現，而PR-Box亦可用量子纏繞的特性來建立，其安全性是無條件的安全。在計畫第三年我們針對量子電腦可破解公開金鑰密碼系統的問題，探討一些利用量子力學特性，所發展出來的演算法，這些演算法是建立在物理的學理上，而非建構在未被證明，假設是困難的數學問題上。

關鍵詞：量子計算、量子演算法、量子密碼學、量子模糊傳輸。

Abstract

Even since the introduction of quantum computation to the computing world, many practical quantum experiments have been successfully carried out. By taking advantage of the tremendous computing power of quantum computers, Peter Shor has shown that factor large numbers can be done in polynomial time. Public key cryptosystems, digital signature schemes as well as many other schemes that depended on this

difficulty of factoring large numbers would become vulnerable. On the other hand, perfect secure cryptographic key distribution scheme based on quantum computing has been developed. Indeed, quantum computing will threaten the security of many classical cryptographic schemes, but it can also make classically infeasible computing tasks become feasible. Quantum computing has attracts the attentions of most leading scholars and research institute in the world.

The main research targets of this project are quantum automata theory, quantum algorithms and quantum cryptography. By studying the theoretical foundations of quantum computing, we hope we can have a better understanding of the power of quantum computing and can design practical and effective quantum algorithms. In particular, in the first year of the project, we shall focus on what classically infeasible cryptographic tasks might become feasible using quantum computers. For example, can we break AES (Advanced Encryption Standard) efficiently using quantum computers? We still do not know. In particular, can we solve any NP-hard problem with polynomial-time quantum computation? (I.e., is NP a subset of QP?) Next, we are also interested in what new quantum objects might be created and adopted to construct secure cryptographic protocols that are impossible using classical computation models.

In the second year of the project, We study quantum oblivious transfer and its applications in the second year. Oblivious transfer, a special communication protocol, is widely used in various variants of security protocols and/or cryptographic applications such as Contrast Signing, Secrets Exchange, Coin Flipping and so on. Oblivious transfer has been developed in many different forms since it was introduced in 1981 by Michael 0. Rabin. The so-called Rabin's oblivious transfer means: sender sends information to receiver with probability 1/2, while the sender is not sure whether the receiver obtain it or not. And the form mentioned above, a more useful one, is called 1-2 oblivious transfer or l-oiit-of-2 oblivious transfer. All of these forms have been used in various cryptographic problems. Nevertheless, the classic implementations are based on the difficulty of number theoretical problems such as RSA scheme, which is vulnerable if quantum computes exist We can use quantum method to defeat these systems and it will not be secure any more. Therefore, we try to resolve this issue by quantum way. Popescu and Rohriich have provided a "non-localiry machine" or "PR machine," which can realize oblivious transfer and we can build PR machine by quantum entanglement.

In the final year of the project, we focus on the problem that traditional public cryptosystems cannot withstand the power of quantum computers. We will develop new algorithms based on the physic characteristics of quantum rather than the unprovr computationally hard problems.

Keywords: Quantum Computing, Quantum Algorithm, Quantum Cryptography, Quantum Oblivious Transfer.

二、緣由與目的

在量子現象被運用來提升計算速度後，量子電腦的概念已逐漸形成，目前數個量子位元(Quantum Bit, Q-bit)的電腦已經實驗成功，而更多量子位元的電腦也正在設計與驗證中。自從1980 年代起，已有許多的量子電路及量子演算法發表於各種不同的國際會議及期刊論文，例如量子電傳(quantum teleportation)、Deutsch’s 演算法、Deutsch-Jozsa 演算法、量子傅立葉轉換和量子搜尋演算法(quantum search algorithm)等。這些演算法皆比傳統的電子計算機演算法具有更高的效能。其中最具震撼性的就是Peter Shor利用量子電腦之強大計算能力所提出可在多項式時間內解出因數分解的量子演算法。其後，量子資訊科學便成為一門極具挑戰性以及潛力的學門。它吸引了無數從物理、數學、電機、以及計算機等領域的學者之注意。尤其是

目前資訊安全中所深深倚賴的公開金鑰系統 (如RSA 密碼系統或橢圓曲線密碼系統等) 大都是基於解離散對數或因數分解等問題的困難度，因此如果量子電腦成功地被實現，基於這些問題之困難度的加密系統、數位簽章、及密碼協定都將變的不安全，無法達到有效的保密效果。因此，目前密碼學中許多重要的安全磐石，都將面臨被破解的夢魘。不過，已有學者利用量子現象設計出完美安全(Perfect Secure)的密碼技術，這些新發明著實令密碼學家相當振奮。的確，量子電腦的來臨對目前資訊安全造成危機，但也是個轉機，它將為資訊安全與密碼學開創全新的研究領域。世界各國學術機構正展開量子計算相關的研究，Stanford、U.C. Berkeley、MIT 以及IBM 等成立了SQUINT 研究團隊，其目標包括合成分子型式之量子電腦、展示量子演算法、研究如何發展大型之量子電腦系統等。此研究團隊有美國國防部之經費補助，預計於近期內能設計並建置一雛形NMR 量子電腦。在另一方面，Caltech、MIT 及USC 等校亦成立QUIC 研究團隊投入於量子計算之研究。此團隊之研究內容除了理論的探討外亦包含了實際層面的研究，最終之目的亦為實現量子電腦之雛形。除了上述之研究團體外，亞洲如中國大陸、日本及新加坡等亦有初步之研究成果，但台灣各大學目前在這方面的研究則顯然落後，值得各單位積極投入人力與資源，以期在最短時間內躋身世界一流大學之列。

三、結果與討論

本計畫的目標是希望藉由基礎理論之研究能對量子計算之特性與能力能有更深一層之了解，進而設計出實用之量子演算法。在量子演算法的設計上，我們將以密碼應用為主，因此我們有必要先研究相關的文獻，以了解一般研究量子計算模型的基本方式。

量子計算及量子資訊的數學模式是使用希爾柏空間(Hilbert space)來描述量子計算的基本單元，其基本單元稱為量子位元(quantum bit)，簡稱qubit，這個觀念與古典計算理論中的資訊基本單位—位元(bit)具有完全迥異的性質；也因為這個迥異的性質，使得量子計算模型經常和所對應的古典計算模型具有相當不同的特性。
希爾柏空間是一個多線性空間，其主要運算是矩陣的張量乘積、直和、與間跳排列。量子位元是以疊加的方式作為結合的效應，而其數學表示法即為量子位元的張量乘積。如同電子計算機的位元一般，一個qubit 有兩個基本量子態(quantum state)，|0>和 |1>，量子態以機率分佈的方式來描述。在現成的數學模式中，qubit 的基本狀態可用長度為二的向量基底(vector bases)來表示。一個qubit 的狀態可由其線性組合形成另一個狀態。因此，一個疊加的量子位元可用向量來表示。多個量子位元(multiple quantum bits)也可用疊加的方法結合在一起。量子位元的疊加現象可用兩個量子位元的張量乘積來表示，兩個量子位元的係數平方和也必須等於1。

我們可以想見，對於一個n 個量子位元的計算系統而言，所有可能狀態的維度會高達2^n維。乍看之下，這種計算模型的潛力異常地豐富，因為可能這種計算模型真的具有同時處理2^n維計算的能力；是否這種模型真的具有這麼強大的能力呢？這就是在討論量子計算模型時要討論的重要課題之一。

一般研究量子計算模型的基本方法，主要是在於將古典計算模型中的位元的觀念，以量子位元的觀念加以代換，接著將古典模型中已知的定理加以修改，成為量子計算模型中的假說，接著加以探討所提出的假說是否成立，以及如果不成立必須如何修改。

本計畫在第一年探討量子金鑰交換協定，在計畫第二年我們探討量子模糊傳輸及其應用。模糊傳送是一種特殊的通訊協定，被廣泛的應用在許多安全議題及密碼加密上，例如:秘密交換、丟銅板問題或簽合約問題等等。模糊傳送的定義是『傳送者可以送兩段資訊給接收者，接收者可以

從兩個之中選一個，接收到這個資訊的內容;而另一個資訊則無法得知其內容。』對於傳送者來說，他並不知道接收者到底收到那一個資訊。也就是說，這個通訊協定可以傳送若干資訊，但又無法精確得知所傳送的資訊，故稱模糊傳送。古典模糊傳送可以用數學的方法來實現，例如RSA演算法。然而其安全性是建構在數論難題的基礎上。我們可以用量子的方法來破解之。為了解決這樣的問題，利用Popescu and Rohriich 所提出"non-locality machine"(簡稱PR-Box)，本計畫建立一個能抵擋量子攻擊之模糊傳輸協定。我們說明模糊傳輸如何用PR-Box來實現，而PR-Box亦可用量子纏繞的特性來建立，其安全性是無條件的安全。

在計畫第三年我們針對量子電腦可破解公開金鑰密碼系統的問題，探討一些利用量子力學特性，所發展出來的演算法，這些演算法是建立在物理的學理上，而非建構在未被證明，假設是困難的數學問題上。我們發現儘管BB84 是一個理論上安全的演算法，仍然有許多新的方法被發明來改進它的缺點，近年來大多是利用Entanglement Swapping (ES)來達成。同樣是利用ES 原理，卻各有各的優缺點，其中難能可貴的有通信過程中不必傳送量子的特性，或是最後一個演算法完整且提供認證的功能。可惜仍沒有一個比較完美的方式來實做QKD，其中大部分的方法都不像BB84 迅速傳送完量子迅速測量能夠避開量子狀態保存不易的問題，這應該是目前實做上的一大困難點。此外，不需搭配事前share 動作的方法也相對的比較複雜。目前除了舊有的BB84 之外，其他方法都只是理論上可行罷了。因此在技術進步之前，還有很大的空間讓我們發揮。

四、計劃成果自評

在本計畫中，我們已完成下列預設目標:

- 蒐集與研讀量子自動機理論與模型相關文獻
- 蒐集與研讀模糊傳輸相關文獻
- 熟悉量子之特性與行為
- 整理與比較相關之量子自動機模型
- 研究並分析quantum finite automata 之特性
- 研究並分析quantum pushdown automata 之特性
- 研究並分析quantum Turing machines 之特性
- 探討量子模糊傳輸之可行性
- 利用non-locality machine來實現模糊傳輸
- 用量子纏繞的特性來建立PR-Box
- 建立一個能抵擋量子攻擊之模糊傳輸協定

針對這些結果做深入的探討與分析，將是未來相關量子密碼研究方向之重要依據。

五、參考文獻

1. Barnett, S. M. and Phoenix, S. J. D., "Bell's inequality and rejected-data protocols for quantum cryptography", Journal of Modern Optics, vol. 40, no. 8, August 1993, pp.1443 - 1448.
2. Barnett, S. M. and Phoenix, S. J. D., "Information-theoretic limits to quantum cryptography", Physical Review A, vol. 48, no. 1, 1993, pp. R5 - R8.
3. Barnett, S. M., Huttner, B. and Phoenix, S. J. D., "Eavesdropping strategies and rejected-data protocols in quantum cryptography", Journal of Modern Optics, vol. 40, no. 12, December 1993, pp. 2501 - 2513.
4. Bellare, M. and Micali, S., "Non-interactive oblivious transfer and applications", 547-559, Springer-Verlag, lecture Notes in Computer Science No. 435, 1990.
5. Bennett, C. H. and Brassard, G., "An update on quantum cryptography", Advances in Cryptology: Proceedings of Crypto 84, August 1984, Springer - Verlag, pp. 475 - 480.

6. Bennett, C. H., "Quantum cryptography: Uncertainty in the service of privacy", Science, vol. 257, 7 August 1992, pp. 752 - 753.
7. Bennett, C. H., Brassard, G. and Mermin, N. D., "Quantum cryptography without Bell's theorem", Physical Review Letters, vol. 68, no. 5, 3 February 1992, pp. 557 - 559.
8. Bernett C. H. and Brassard G., “An Update on Quantum Cryptography,” Crypto’84, 1984, pp. 19-22.
9. Brassard G., and Crepeau C., “25 Years of Quantum Cryptography,” ACM SIGACT News, Cryptology Column, 1996, pp. 13-24.
10. Brassard, G. and Crépeau, C., "Quantum bit commitment and coin tossing protocols", Advances in Cryptology, Crypto '90 Proceedings, August 1990, Springer - Verlag, pp. 49 - 61.
11. Brassard, G., Crépeau, C., Jozsa, R. and Langlois, D., "A quantum bit commitment scheme provably unbreakable by both parties", Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, 1993, pp. 362 – 371.
12. Cleve, R., Ekert, A., Macchiavello, C., and Mosca. M., “Quantum algorithms revisited,” Proc. R. Soc. London A, 454:339—354, 1998.
13. Ci'epeau, C., "Equivalence between two flavors of oblivious transfers", in CRYPTO 87, LNCS 293, 1988.
14. Collins, G. P., "Quantum cryptography defies eavesdropping", Physics Today, November 1992, pp. 21 - 23.
15. Deutsch, D., “Quantum theory, the Church-Turing Prniciple and the universal quantum computer,” Proc. R. Soc. London A, 400:97, 1985.
16. Ekert A. K., “Quantum Cryptography based on Bell’s Theorem,” Physical Review Letters, Vol. 67, No. 6, 1991, pp. 661-663
17. Ekert, A. K., "Adventures in quantum cryptoland" (in Japanese), Parity, vol. 7, February 1992, pp. 26 - 29.
18. Ekert, A. K., "Przygoda w kwantowej krainie szyfrow", Wiedza i Zycie, July 1991, pp. 45 - 49.
19. Ekert, A. K., Rarity, J. G., Tapster, P. R. and Palma, G. M., "Practical quantum cryptography based on two-photon interferometry", Physical Review Letters, vol. 69, no. 9, 1992, pp. 1293 - 1295.
20. Flam, F., "Quantum cryptography's only certainty: Secrecy", Science, vol. 253, 1991, page 858.
21. Goldreich, 0., Micali, S., and Wigderson, A., "How to play any mental game", in Proceedings of the nineteenth annual ACM conference on Theory of computing, 218-229,1987.
22. Griffiths, R. B. and Niu, C. S., “Semi-classical Fourier transform for quantumcomputation,” Phys. Rev. Lett., 76(17)3228—3231, 1996.
23. Huttner, B. and Ekert, A. K., "Tolerable noise in quantum cryptosystems", Journal of Modern Optics, to appear.
24. Mayei's, D. and Salvail, L., "Quantum oblivious transfer is secure against all individual measurements", Proceedings of Workshop on Physics and Computation, 69-77, 1994.
25. Muller, A., Breguet, J. and Gisin, N., "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km" Europhysics Letters, vol. 23, no. 6, 20 August 1993, pp. 383 - 388.
26. Nielsen M. A. and Chuang I. L., Quantum Computation and Quantum Information, Cambridge University Press, 2000.
27. Peterson, I., "Bits of uncertainty: Quantum security", Science News, vol. 137, 2 June 1990, pp. 342 - 343.
28. Phoenix, S. J. D. and Townsend, P. D., "Quantum cryptography and secure optical communication", British Telecom Technology Journal, vol. 11, no. 2, April 1993, pp. 65 - 75.
29. Popescu, S. and Rolirlich, D., "Open questions and possible solutions", in Proceedings of Causality and Locality in Modern Physics and Astronomy, A Symposium to Honor Jean-Pierre Vigier,

Toronto, Canada, 1997.
30. Rabin, M., "How to exchange secrets by oblivious transfer". Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
31. Rarity, J. G., Owens, P. C. M. and Tapster, P. R., "Quantum random number generation and key sharing", Journal of Modern Optics, vol. 41, no. 12, December 1994, pp. 2435 - 2444.
32. Shor, P. W., “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comp., 26(5)1484 - 1509, 1997.
33. Townsend, P. D. and Phoenix, S. J. D., "Quantum mechanics will protect area networks", Opto and Laser Europe, July 1993, pp. 17 - 20.
34. Townsend, P. D., Rarity, J. G. and Tapster, P. R., "Single photon interference in a 10km long optical fibre interferometer", Electronics Letters, vol. 29, no. 7, April 1993, pp. 634 - 635.
35. Wallich, P., "Quantum cryptography", Scientific American, May 1989, pp. 28 - 30.
36. Wiedemann, D., "Quantum cryptography", Sigact News, vol. 18, no. 2, 1987, pp. 48 - 51; but please read also [48].
37. Wiesner S., “Conjugate Coding,” ACM SIGACT News, Vol. 15, No. 1, 1983, pp. 78-88.
38. Wolf, S., "Reducing oblivious string transfer to universal oblivious transfer", in Proceedings of International Symposium on Information Theory, 465. SntTfnrn Tralv, 2000.

出席 2007 IEEE 安全與隱私國際會議心得報告

雷欽隆

國立臺灣大學電機工程學系教授

會議名稱：2007 IEEE Symposium on Security and Privacy

會議地點：The Claremont Resort, Oakland, California, USA

會議日期：2007/5/20 – 2007/5/23

一、 參加會議經過

IEEE Symposium on Security and Privacy 會議今年依往例在美國加洲 **Oakland** 的 **Claremont Resort** 舉辦。**IEEE Symposium on Security and Privacy** 從 1980 年開始年年舉辦，此會議至今已是第二十八屆。今年 **IEEE Security and Privacy** 會議共有 249 篇論文投稿，Technical Program Committee 成員有 37 位，皆爲一時之選。經過審稿過程，最後選出 29 篇論文。這些論文分別在三天（5/21 ~ 5/23）八個 sessions 發表，會議議程如下：

Monday, May 21, 2007

7:30-9:00	Continental breakfast
9:00-9:15	Opening Remarks (Deborah Shands, Birgit Pfitzmann)
9:15-10:15	Keynote Talk *Reflections on the Future of Security and Privacy* Peter G. Neumann
10:15-10:45	Break
10:45-12:15	Session: Network Security Session Chair: Birgit Pfitzmann

	Accurate Real-time Identification of IP Prefix Hijacking Xin Hu and Z. Morley Mao (30 minutes) *DSSS-Based Flow Marking Technique for Invisible Traceback* Wei Yu, Xinwen Fu, Steve Graham, Dong Xuan and Wei Zhao (30 minutes) *On the Safety and Efficiency of Firewall Policy Deployment* Charles C. Zhang, Marianne Winslett and Carl A. Gunter (30 minutes)
12:15-13:45	Lunch
13:45-15:30	**Session: Authentication** Session Chair: Tuomas Aura *The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies* Stuart Schechter, Rachna Dhamija, Andy Ozment and Ian Fischer (30 minutes) *Cryptanalysis of a Cognitive Authentication Scheme* Philippe Golle and David Wagner (15 minutes) *A Systematic Approach to Uncover Security Flaws in GUI Logic* Shuo Chen, José Meseguer, Ralf Sasse, Helen J. Wang and Yi-Min Wang (30 minutes) *Forward-Secure Sequential Aggregate Authentication* Di Ma and Gene Tsudik (15 minutes) *Extended abstract: Provable-Security Analysis of Authenticated Encryption in Kerberos* Alexandra Boldyreva and Virendra Kumar (15 minutes)
15:30-16:00	Break
16:00-17:30	**Session: 5-minute Work-in-Progress Talks**

	Session Chair: Yoshi Kohno
18:00-20:00	**Reception**

Tuesday, May 22, 2007

7:30-9:00	Continental breakfast
9:00-10:30	**Session: Privacy** Session Chair: Ninghui Li *Endorsed E-Cash* Jan Camenisch, Anna Lysyanskaya and Mira Meyerovich (30 minutes) *Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems* Xinyuan Wang, Shiping Chen and Sushil Jajodia (30 minutes) *Improving the Robustness of Private Information Retrieval* Ian Goldberg (30 minutes)
10:30-11:00	Break
11:00-12:15	**Session: Access Control and Audit** Session Chair: Dan Wallach *Beyond Stack Inspection: A Unified Access-Control and Information-Flow Security Model* Marco Pistoia, Anindya Banerjee and David A. Naumann (30 minutes) *Usable Mandatory Integrity Protection for Operating Systems* Ninghui Li, Ziqing Mao and Hong Chen (30 minutes) *Enforcing Semantic Integrity on Untrusted Clients in Networked Virtual Environments (Extended abstract)* Somesh Jha, Stefan Katzenbeisser, Christian Schallhart, Helmut Veith and

	Stephen Chenney (15 minutes)
12:15-13:45	Lunch
13:45-15:15	**Session: Information Flow** Session Chair: Anupam Datta *Information Flow in the Peer-Reviewing Process (Extended Abstract)* Michael Backes, Markus Duermuth and Dominique Unruh (15 minutes) *A Cryptographic Decentralized Label Model* Jeffrey A. Vaughan and Steve Zdancewic (30 minutes) *Gradual Release: Unifying Declassification, Encryption and Key Release Policies* Aslan Askarov and Andrei Sabelfeld (30 minutes) *Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control* Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, Angela Schuett Reninger (15 minutes)
15:15-15:45	Break
15:45-17:30	**Session: Host Security** Session Chair: Crispin Cowen *Exploring Multiple Execution Paths for Malware Analysis* Andreas Moser, Christopher Kruegel and Engin Kirda (30 minutes) *Lurking in the Shadows: Identifying Systemic Threats to Kernel Data* Arati Baliga, Pandurang Kamat and Liviu Iftode (15 minutes) *ShieldGen: Automatic Data Patch Generation for Unknown Vulnerabilities with Informed Probing*

	Weidong Cui, Marcus Peinado, Helen J. Wang and Michael Locasto (30 minutes) *Minimal TCB Code Execution* Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter and Arvind Seshadri (15 minutes) *Using Rescue Points to Navigate Software Recovery (Short Paper)* Stelios Sidiroglou, Oren Laadan, Angelos Keromytis and Jason Nieh (15 minutes)
17:30-17:45	Break
17:45-18:30	Business Meeting

Wednesday, May 23, 2007

7:30-9:00	Continental breakfast
9:00-10:30	Session: Hardware and Replication Session Chair: Wenke Lee *Moats and Drawbridges: An Isolation Primitive for Reconfigurable Hardware Based Systems* Ted Huffmire, Brett Brotherton, Gang Wang, Tim Sherwood, Ryan Kastner, Timothy Levin, Thuy Nguyen and Cynthia Irvine (30 minutes) *Trojan Detection using IC Fingerprinting* Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi and Berk Sunar (30 minutes) *On the Optimal Communication Complexity of Multiphase Protocols for Perfect Communication* Kannan Srinathan, N. R. Prasad and C. Pandu Rangan (30 minutes)
10:30-11:00	Break

11:00-12:30	**Session: Encryption** Session Chair: Patrick McDaniel *Ciphertext-Policy Attribute-Based Encryption* John Bethencourt, Amit Sahai and Brent Waters (30 minutes) *Attacking the IPsec Standards in Encryption-only Configurations* Jean Paul Degabriele and Kenneth Graham Paterson (30 minutes) *Multi-Dimensional Range Query over Encrypted Data* Elaine Shi, John Bethencourt, T.-H. Hubert Chan, Dawn Song and Adrian Perrig (30 minutes)
12:30-12:45	**Closing Remarks** (Patrick McDaniel, Avi Rubin, and Yong Guan)
11:00-13:00	Boxed lunch

從議程的安排可以看出目前安全與隱私研究趨勢的主流在 Network Security、Authentication、Private Information Retrieval、Access Control and Audit、Information Flow、Host Security、Hardware Protection 及 Encryption 等。特別值得一提的是本次的 keynote speech 特別邀請 Prof. Peter G. Neumann 演講，講題是 *Reflections on the Future of Security and Privacy*，Prof. Neumann 細說安全與隱私過去 28 年之發展過程及各階段之重要成果及里程碑，同時也探討安全（系統、實務）與隱私（理論、密碼）兩派學者間之競合，十分精采，同時大會也特別配合，將過去在本會議發表的所有論文整理並製作成光碟。

本人於 5 月 20 日下塌 **The Claremont Resort**，直到 5 月 23 日都待在此地；並與參加會議的各國學者交換研究心得，特別是和 UC Berkeley Doug Tygar 等教授商討合作事宜。

二、 <u>與會心得</u>

此次遠赴美國參加會議，有數點心得：

1) 有不小比例的論文，都是自己定出一個新的題目，而不只是拿舊的題目繼續改進而已。一旦定出新的題目，對於該領域還是很有貢獻——因爲它延伸了這個研究領域的範圍。因此，日後除了專研原有的題目外，也應該多花一些時間來做「延伸思考」。

2) 好的研究通常會持續地延伸下去，不論在廣度或深度。它們不一樣的地方就是在「別人已經喊停的地方」堅持下去，這時就很可能出現很多不一樣的觀點或成果。

三、 建議

我覺得此次參加國際會議獲益良多，建議有志於學術研究的學者們多多爭取參加國際頂尖學術會議的機會。尤其整個會議是採用 Single session 方式進行，每篇論文都是精華，不論在研究，或是視野都有十分的助益。

四、 攜回資料名稱及內容

- 會議論文集一本
- 1980 ~ 2007 會議論文光碟片