行政院國家科學委員會專題研究計畫　成果報告

量子密碼協定之研究與設計

計畫類別：個別型計畫
計畫編號：NSC92-2218-E-002-054-
執行期間：92 年 12 月 01 日至 93 年 10 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：吳宏仁、廖燕華、李俊頡、陳寬達

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 4 月 1 日

行政院國家科學委員會專題研究計劃成果報告

量子密碼協定之研究與設計
Study and Design of Quantum Cryptographic Protocols

計劃編號：NSC 92-2218-E-002-054
執行期限：92 年 12 月 1 日至 93 年 10 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研究現有之 量子密碼協定並了解其設計原理與技巧。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密碼協定。

關鍵詞：量子計算、量子演算法、量子密碼學。

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 goal of this research is to study existing quantum cryptographic protocol and understand how it works and its theoretical foundations. 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 cryptographic protocols.

Keywords: Quantum Computing, Quantum Algorithm, Quantum Cryptography.

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) [14]、Deutsch's 演算法 [38]、Deutsch-Jozsa 演算法 [37]、量子傅立葉轉換[31, 52]和量子搜尋演算法(quantum search algorithm) [53]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 [63]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

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。

此外，在這個先導研究中我們發現量子密碼面臨的主要挑戰如下：

1. 量子理論仍在起步階段，要掌握各種量子模型之能力是極具挑戰性的作。
2. 若沒有實驗平台，在設計量子密碼協定時，必須完全用理論來推導驗證，所以必須要確實掌握量子之特性與行為。
3. 在量子密碼協定中必須發展更精密的錯誤更正碼及檢驗技術。建立量子通道是研發量子密碼系統最重要的一個步驟。目前主要是以光纖傳輸為主，實驗平台不易建立。
4. 目前尚未有實際可行的量子簽章技術，因此很多安全需求如不可否認性等不太容易在量子模型中完成。

四、計劃成果自評

在這個先導研究中深入探討BB84 QKD演算法並與三種最新利用Entanglement Swapping的方法比較。這些採用Entanglement Swapping技巧的protocol除了比前者新之外，更改進了BB84的一些缺點。此外，在本研究中我們整理出量子密碼面臨的主要挑戰，這些結果都有助於後續量子密碼系統之研發。

五、參考文獻

1. Ardehali, M., "Efficient quantum cryptography", manuscript, 1992.
2. 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.
3. 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.
4. Barnett, S. M., Ekert, A. K. and Phoenix, S. J. D., "Optical key to quantum cryptography", SERC Nonlinear Optics Update, United Kingdom Science and Engineering Research Council, vol. 5, Summer 1993, pp. 3 - 7.
5. 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.
6. 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.
7. Bennett, C. H. and Brassard, G., "Quantum cryptography: Public-key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179.
8. Bennett, C. H. and Brassard, G., "Quantum public key distribution reinvented", Sigact News, vol. 18, no. 4, 1987, pp. 51 - 53.
9. Bennett, C. H., "Quantum cryptography: Uncertainty in the service of privacy", Science, vol. 257, 7 August 1992, pp. 752 - 753.
10. Bennett, C. H., Brassard, G.., Crépeau, C., and Jozsa, R., “A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels,” Phys. Rev. Lett., 70:1895—1899, 1993.
11. 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.
12. Bernett C. H. and Brassard G., “An Update on Quantum Cryptography,” Crypto’84, 1984, pp. 19-22.
13. Bernett C. H. and Brassard G., “Quantum Cryptography: Public Key Distribution and Coin Tossing,” International Conference on Computers, systems and Signal Processing, 1992, pp. 3-28.
14. Brassard G., and Crepeau C., “25 Years of Quantum Cryptography,” ACM SIGACT News, Cryptology Column, 1996, pp. 13-24.
15. 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.
16. 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.
17. Cleve, R., Ekert, A., Macchiavello, C., and Mosca. M., “Quantum algorithms revisited,” Proc. R. Soc. London A, 454:339—354, 1998.
18. Collins, G. P., "Quantum cryptography defies eavesdropping", Physics Today, November 1992, pp. 21 - 23.
19. Deutsch, D., “Quantum theory, the

Church-Turing Prniciple and the universal quantum computer," Proc. R. Soc. London A, 400:97, 1985.
20. Ekert A. K., "Quantum Cryptography based on Bell's Theorem," Physical Review Letters, Vol. 67, No. 6, 1991, pp. 661-663
21. Ekert, A. K., "Adventures in quantum cryptoland" (in Japanese), Parity, vol. 7, February 1992, pp. 26 - 29.
22. Ekert, A. K., "Przygoda w kwantowej krainie szyfrow", Wiedza i Zycie, July 1991, pp. 45 - 49.
23. 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.
24. Flam, F., "Quantum cryptography's only certainty: Secrecy", Science, vol. 253, 1991, page 858.
25. Gottlieb, A., "Conjugal secrets - The untappable quantum telephone", The Economist, vol. 311, 22 April 1989, page 81.
26. Griffiths, R. B. and Niu, C. S., "Semi-classical Fourier transform for quantumcomputation," Phys. Rev. Lett., 76(17)3228—3231, 1996.
27. Huttner, B. and Ekert, A. K., "Tolerable noise in quantum cryptosystems", Journal of Modern Optics, to appear.
28. Muller, A., Breguet, J. and Gisin, N., "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km" urophysics Letters, vol. 23, no. 6, 20 August 1993, pp. 383 - 388.
29. Nielsen M. A. and Chuang I. L., Quantum Computation and Quantum Information, Cambridge University Press, 2000.
30. Peterson, I., "Bits of uncertainty: Quantum security", Science News, vol. 137, 2 June 1990, pp. 342 - 343.
31. 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.
32. 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.
33. Shor, P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comp., 26(5)1484 - 1509, 1997.
34. Stewart, I., "Schrodinger's catflap", Nature, vol. 353, 3 October 1991, pp. 384 - 385.
35. Townsend, P. D. and Phoenix, S. J. D., "Quantum mechanics will protect area networks", Opto and Laser Europe, July 1993, pp. 17 - 20.
36. 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.
37. Wallich, P., "Quantum cryptography", Scientific American, May 1989, pp. 28 - 30.
38. Werner, M. J. and Milburn, G. J., "Eavesdropping using quantum-nondemolition
39. measurements", Physical Review A, vol. 47, no. 1, January 1993, pp. 639 - 641.
40. Wiedemann, D., "Quantum cryptography", Sigact News, vol. 18, no. 2, 1987, pp. 48 - 51; but please read also [48].
41. Wiesner S., "Conjugate Coding," ACM SIGACT News, Vol. 15, No. 1, 1983, pp. 78-88.
42. Zimmer, C., "Perfect Gibberish", Discover, September 1992, pp. 92 - 99.