行政院國家科學委員會專題研究計畫　期中進度報告

量子演算法之研究及其在密碼學之應用(1/3)

計畫類別：個別型計畫
計畫編號：NSC93-2218-E-002-103-
執行期間：93 年 08 月 01 日至 94 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：邱允鵬　黃俊穎　陳寬達

報告類型：精簡報告
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 94 年 6 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 93-2218-E-002-103
執行期限：93 年 8 月 1 日至 94 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』，我們將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。

我們將運用量子系統獨特的平行性(Parallelism)與干涉性發展出比目前更為快速的密碼分析法(Cryptanalysis)來破解因數分解(Factorization)、離散對數(Discrete Logarithms)與對稱式密碼系統(Symmetric Cryptosystems)。其次，也將利用量子無法複製(No-Cloning)之特性與測不準原理設計出完美安全的高效率量子金鑰交換(Quantum Key Exchange)協定、低成本之量子錢幣(Quantum Money)與高效能量子秘密分享機制(Quantum Secrecy-Sharing Schemes)。最後，本計畫將研究如何應用量子的其他特性於密碼學中，例如疊加(Superposition)現象、糾纏(Entanglement)現象與量子運算之可逆性(Reversibility)等，以期開發出創新的量子密碼演算法。希望藉
由本計畫的實施，整合相關的研究資源，進而提升國內在量子計算理論與演算法領域的研究水平，迎頭趕上世界水準。

關鍵詞：量子計算、量子演算法、量子自動機理論、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 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, 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.

We will investigate the possibility of adopting quantum parallelism for fast cryptanalysis. We will also study the possibility of adopting the non-cloning feature of quantum objects to design efficient algorithms for quantum money. In addition, we shall study what other quantum phenomena (such as superposition, entanglement, reversibility, etc.) might be useful for quantum algorithm design. Under this project, we expect to integrate the research potential in the nation and collaborate with leading researchers in the world.

Keywords: Quantum Computing, Quantum Algorithm, Quantum Automata, 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)、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靨。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。本計畫量子自動機理論方面的研究方法，將依循前人討論新模型的流程，針對傳統自動機，加入量子計算的觀念，接著檢視其完整構成條件，然後對於這類的量子計算模型加以探討，並且研究這個模型和古典模型之間的關連。

在量子計算理論中，我們討論量子計算模型的基本原則是，將古典計算理論提到的各種計算模型中，所有與狀態變動有關的面向，由原先布林代數「非此即彼」的觀念，全部改成量子計算模型中的狀態疊加的觀念，然後由這樣的觀念出發，藉以探討下列三種計算模型上的變化：

1. 所產生的量子計算模型，其在量測一次或者量測多次的情況下，與古典計算理論的模型相比較，所接受的語言的變化。
2. 所產生的量子計算模型，是否具有可程式性，亦即是否存在有一個該模型的特例，使得我們可以輸入其他相同模型的描述，而使得該特例能夠模擬輸入的模型。
3. 所產生的量子計算模型的一些相關判定性問題是否為可決定。

在計畫的第一年中，我們已針對這些問題做深入的探討與分析，做為繼續研究之方向依據。此外，在這個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

在計畫的第一年中，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
- 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

針對這些結果做深入的探討與分析，將是本計畫後兩年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., 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.
4. 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.
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. 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.
7. Bennett, C. H. and Brassard, G., "Quantum public key distribution reinvented", Sigact News, vol. 18, no. 4, 1987, pp. 51 - 53.
8. Bennett, C. H., "Quantum cryptography: Uncertainty in the service of privacy", Science, vol. 257, 7 August 1992, pp. 752 - 753.
9. 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.
10. 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.
11. Bernett C. H. and Brassard G., “An Update on Quantum Cryptography,” Crypto’84, 1984, pp. 19-22.
12. 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.
13. Brassard G., and Crepeau C., “25 Years of Quantum Cryptography,” ACM SIGACT News, Cryptology Column, 1996, pp. 13-24.
14. 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.
15. 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.
16. Cleve, R., Ekert, A., Macchiavello, C., and Mosca. M., “Quantum algorithms revisited,” Proc. R. Soc. London A, 454:339—354, 1998.
17. Collins, G. P., "Quantum cryptography defies eavesdropping", Physics Today, November 1992, pp. 21 - 23.
18. Deutsch, D., “Quantum theory, the Church-Turing Prniciple and the universal quantum computer,” Proc. R. Soc. London A, 400:97, 1985.
19. Ekert A. K., “Quantum Cryptography based on Bell’s Theorem,” Physical Review Letters, Vol. 67, No. 6, 1991, pp. 661-663
20. Ekert, A. K., "Adventures in quantum cryptoland" (in Japanese), Parity, vol. 7, February 1992, pp. 26 - 29.
21. Ekert, A. K., "Przygoda w kwantowej krainie szyfrow", Wiedza i Zycie, July 1991, pp. 45 - 49.
22. 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.
23. Flam, F., "Quantum cryptography's only certainty: Secrecy", Science, vol. 253, 1991, page 858.
24. Griffiths, R. B. and Niu, C. S., “Semi-classical Fourier transform for quantumcomputation,” Phys. Rev. Lett., 76(17)3228—3231, 1996.
25. Huttner, B. and Ekert, A. K., "Tolerable noise in quantum cryptosystems", Journal of Modern Optics, to appear.
26. 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.
27. Nielsen M. A. and Chuang I. L., Quantum Computation and Quantum Information, Cambridge University Press, 2000.
28. Peterson, I., "Bits of uncertainty: Quantum security", Science News, vol. 137, 2 June 1990, pp. 342 - 343.
29. 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.
30. 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.
31. Shor, P. W., “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comp., 26(5)1484 - 1509, 1997.
32. Townsend, P. D. and Phoenix, S. J. D., "Quantum mechanics will protect area networks", Opto and Laser Europe, July 1993, pp. 17 - 20.
33. 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.
34. Wallich, P., "Quantum cryptography", Scientific American, May 1989, pp. 28 - 30.
35. Wiedemann, D., "Quantum cryptography", Sigact News, vol. 18, no. 2, 1987, pp. 48 - 51; but please read also [48].
36. Wiesner S., “Conjugate Coding,” ACM SIGACT News, Vol. 15, No. 1, 1983, pp. 78-88.