行政院國家科學委員會專題研究計畫 成果報告

量子計算機之系統架構研究與設計(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-002-004-
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：郭斯彥

計畫參與人員：博士班研究生-兼任助理：盧勤庸、王秀安、朱怡霖、周耀新
碩士班研究生-兼任助理：王瀚偉、柯見銘

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 10 月 29 日

行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告
□期中進度報告

量子計算機之系統架構研究與設計

計畫類別：■ 個別型計畫　□ 整合型計畫
計畫編號：NSC－95－2218－E－002－004
執行期間：95 年 8 月 1 日 至 96 年 7 月 31 日

計畫主持人：郭斯彥
共同主持人：
計畫參與人員：盧勤庸、王秀安、王瀚偉、柯見銘、朱怡霖、周耀新

成果報告類型(依經費核定清單規定繳交)：□精簡報告　■完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
■出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立台灣大學 電機工程學系

中　華　民　國　96 年　10 月　23 日

中英文摘要及關鍵詞(keywords)

自從量子電腦的概念於 1980 年代初期被提出後[1-3]，量子資訊科學便成為一門相當新而發展快速的研究領域。此外,量子計算機的發展近年來逐漸受到物理及計算機學者的重視，量子通信以及量子計算演算法紛紛被提出來解決現今存在的問題，甚至開創新的應用。本計劃由量子電路的觀點研究量子計算系統之架構，同時以核磁共振(Nuclear Magnetic Resonance, NMR)之技術實作一個量子計算系統。透過核磁共振(NMR)量子計算機的實作研究，進而研發一套有效率使用量子計算機的程式工具 NMRPPGEN，除可加速實現各種量子演算法外，並可以幫助了解量子計算機之架構。除此之外，本計畫以基於量子物理之特性討論量子安全計算以及模糊傳輸之實作方法，更進一步地研究量子計算的可能應用。

要實作完成一部量子電腦，發展一套有效的量子電路合成方法是有必要的。量子電路的基本元件是量子位元，因為量子位元製作不易，所以合成出來之量子電路需要具有較低成本和較容易實作的特性。當電路的設計過程中,測試量子布林電路功能的正確性是必須的,我們提出一個方法可以有效地測試量子布林電路,這個方法是採用由後向前掃描方式,可以找到最少的測試向量,以證明電路是正確,並且可以標示有問題元件的位置,以利更進一步的除錯。本計劃中，我們使用表格式演算法發展出一個量子布林電路化簡方法，表格法可以透過電腦輔助加快速度,可以對具有 6 變數以上的量子布林邏輯電路進行化簡工作,這種方法尤其適合多變數的情況,對於不同的應用,所使用的電路通常是較複雜的,我們必須儘可能的化簡電路,我們提出一個方法可以有效地化簡一個量子布林電路,方法是使用表格法進行化簡,只使用一個輔助的量子位元,並且保持輸入量子位元的不變。這個方法可以同時地執行 AND 和 XOR 函數化簡，當一個量子布林電路被化簡後，我們還必須驗證化簡後的電路與原來電路有相同的功能。在量子電路的設計及化簡的過程中，驗證兩個量子電路是否具有相同的功能是很重要且必須的。我們提出一個可以有效率地驗證量子布林電路的演算法。這個演算法利用回溯的方法找尋檢查向量來驗證量子布林電路的功能是否正確。再者，我們提出一個稱為 XQDD 的資料結構，且提出如何利用 XQDD 表示一個量子電路，並驗證不同設計的兩個量子電路是否具有相同的功能的演算法。我們也提出能驗證具有不同 qubit 數的可逆電路的方法。使用 XQDD 表示一個量子電路所需的節點數少於其他的表示方法。因此從時間及空間上來看，這個方法都能有效率地驗證量子電路。

此外，本計劃還說明如何使用量子布林電路實作 Grover 搜尋演算法中 oracle 和 invesion-about-average 的功能。我們首先以 SAT 問題為例說明量子電路設計的原則。之後我們提出兩種實際應用的量子電路設計。第一是電話簿搜尋，雖然這是 Grover 演算法的典型例子，我們說明作為一個實際生活的應用是不切實際的。第二，我們給了另一個比較可能的實際應用：破除對稱性密碼系統。雖然這兩個應用看似有不同的搜尋條件，實際上她們都可視為某種單向函數，而我們所提出的設計方法可以應用在所有類似的問題上面。

在有了量子電路合成的工具之後，本計劃選擇使用核磁共振的方式來實作一個量子計算系統。我們利用基於碳的同位素碳 13 之三氯甲烷(chloroform)中的^{1}H和^{13}C ($^{13}CHCl_3$)做為資訊的承載單位，NMR RF 脈衝用來操控其中之量子狀態，以實現一個 2 位元的NMR量子計

算系統雛形。值得注意的是，只要承載資訊的單位(量子位元)可以根據量子力學的方式進行操作，一個量子計算系統獨立於底層的實作技術，並不因其改變而受影響。

而 NMRPPGEN 是一個近似量子電腦編譯器的中階程式工具，我們只要將想要執行的量子運算邏輯閘(例如: Hadamard Gate)作為輸入，即能合成操作 NMR 量子電腦執行該運算的 NMR 脈衝程式 (Pulse Program)。雖然本計劃以 7 位元量子電腦(丁烯酸；Trans-Crotonic Acid)做為例子，但其所使用的分子不限定只能使用丁烯酸，它可以透過各承載單位原子之間的 J-Coupling 參數設定，即可執行各種不同分子的 NMR 脈衝程式合成。這項研究對於量子電腦實驗以及量子電腦程式設計的方便性都有相當大的助益。

量子計算的另一個令人矚目的工程應用是量子密碼學，許多在古典密碼學中難解的問題，可以利用量子物理的特性有效的解決。舉例而言，模糊傳送(Oblivious Transfer)古典上可以用數學的方法 (例如 RSA 演算法)來實現。然而這些數學方法是建構在困難的數學問題上，安全性是屬於有條件性的(Conditional Secure)，而且有一些困難的數學問題可以用量子物理的方法來破解。為了解決這個問題，本計畫希望利用量子物理的非局域(Non-Locality)特性來建立一個無條件安全(Unconditional Secure)的模糊傳送。本計畫的部分即在討論如何利用量子計算中糾纏的特性來建立無條件安全的模糊傳送。

由於索爾演算法的發明,許多植基於離散對數難題與值因數分解的密碼系統將有被破解的危機,也代表著現有許多安全通訊協定將不再安全.我們提出一套新的量子安全通訊機制,它允許欲通訊的兩方可以安全地互傳傳統訊息.不像傳統的安全協定,我們所提出的量子安全通訊機制的安全性將由量子物理的合理性來作保證.

近年來奈米科技的研究大多著重在奈米現象於實體設備階層的應用。在此計畫中，我們說明奈米現象不只可以使用在實體階層，而可以應用在更高層次如網路通訊協定中。我們研究使用量子糾纏態來實現網路認證和加解密的可能應用。本通訊協定的安全性是以奈米物理定律為基礎，而不是傳統演算法中未證明的複雜數學演算法。

另外，網路最大流量問題在工程界有非常多的應用.在此計畫中,我們發展了一個量子演算法在 O(n2.5)的時間複雜度之內解決網路最大流量問題.就我們所知,比起現有的傳統演算法以及量子演算法來說,我們所提出的演算法都是最快的.

關鍵詞：量子計算，量子通信，量子電路，電路合成，電路檢測，核磁共振技術。
量子計算，量子通信，核磁共振技術，脈衝程式合成，非局域性，安全計算，模糊傳輸。

Abstract

The study of quantum information science has expanded rapidly since the theoretical model of quantum computers were introduced in the early 1980's [1-3].Besides, recently, the study of quantum computer and quantum information has become increasingly important in the physics and computer science community. Many physical implementation proposals on how to build a quantum computer have been proposed and some of them have been successfully realized. In this project, we study the architecture of quantum computing systems from the circuit point of view and demonstrate physical implementations using nuclear magnetic resonance (NMR) technology. We studied the implementation of Nuclear Magnetic Resonance (NMR) quantum computer. We developed an efficient utility called NMRPPGEN (NMR Pulse Program GENerator) to automatically generate the NMR pulse program that can be used to implement any quantum algorithm.

To implement a quantum computer, it is necessary to develop an efficient quantum circuit synthesis method. Since the quantum bit (which is the basic component of a quantum circuit) is very expensive, a good quantum circuit has to be designed in a cost-effective way and, at the same time, it must be easy for implementation. During the design process, testing a designed function for a quantum Boolean circuit is necessary. In this project, we present an algorithm that can efficiently test a quantum Boolean circuit by using the back propagation method. The algorithm can find the minimum test vectors to prove the correctness of a circuit and locate the possible positions of failed gates for further debugging. In this project we describe a simplification method of quantum Boolean circuits using a tabulation algorithm. The Tabulation method can he used with a computer to simplify Boolean logic functions with up to 6 or more variables, especially with a large number of variables. For the various applications, their circuits usually are complex and we must simplify the circuit design to the hest ofour ability.

In this project, we present an algorithm that can efficiently simplify a quantum Boolean circuit with an arbitrary number of input variables by using the tabulation method. In terms of the space consumption, we use only one auxiliary qubit as the output qubit, and keep all the input quhits unchanged. This method performs AND and XOR function simplification simultaneously. After a quantum Boolean circuit is simplified, we verify the circuits to confirm its function is correct. Synthesis of quantum circuits is essential for building quantum computers. It is important to verify that the circuits designed perform the correct functions.

In this project, we propose an algorithm which can be used to verify the quantum circuits synthesized by any method. The proposed algorithm is based on BDD (Binary Decision Diagram) and is called X-decomposition Quantum Decision Diagram (XQDD). In this method, quantum operations are modeled using a graphic method and the verification process is based on

comparing these graphic diagrams. We also develop an algorithm to verify reversible circuits even if they have a different number of garbage qubits. In most cases, the number of nodes used in XQDD is less than that in other representations. In general, the proposed method is more efficient in terms of space and time and can be used to verify many quantum circuits in polynomial time.

Besides, in this project, we show how quantum Boolean circuits can be used to implement the oracle and the inversion-about-average function in Grover's search algorithm. Before illustrating how this can be done, we present the circuit design principle using the satisfiability (SAT) problem as an example. Then, based on this principle, we show the quantum circuits for two different kinds of applications. The first one is searching a phone book. Although this is a typical example of Grover's algorithm, we show that it is impractical as a real-world application. As the second application, we give the quantum circuits for a more practical application – breaking a symmetric cryptosystem. Although these two applications have quite different types of search criteria, they are both one-way functions and the proposed circuits can actually be generalized to any such problems.

With the capability of performing quantum circuit synthesis, we report an experimental realization of quantum switch using nuclear spins and magnetic resonant pulses in this project. The nuclear spins of ^{1}H and ^{13}C in carbon-13 labeled chloroform are used to carry the information. Then nuclear magnetic resonance pulses are applied to perform quantum operations on a two-qubit quantum computer prototype. Note that, an ideal quantum computation system is independent of the underlying physical implementation, as long as the information carrier (qubit) can be manipulated according to quantum mechanics.

However, NMRPPGEN is a compiler-like utility which can be used to generate NMR pulse program for NMR quantum computers. Its input is a text file which contains a series of quantum logic gates (such as Hadamard Gate) and the output is an NMR Pulse Program. In addition to the pulse program synthesizer, we have also implemented a web-based I/O interface which can be used to configure various parameters. For example, by configuring J-coupling parameters for the target molecule, NMRPPGEN can generate the NMR pulse program for the target molecule.

On the other hand, in this project we also studied a promising engineering application in quantum computing called quantum oblivious transfer (OT). Oblivious transfer, a special communication protocol, is widely used in various variants of security issue or cryptographic application such as contrast signing, secrets exchange, coin flipping, etc. Oblivious transfer allows a party to sent two messages to the receiver who can choose one of them and learn it, remaining ignorant about the other, while the sender who has no ideal about what the receiver choice. Although mathematical method such as RSA scheme can be used to build OT, the protocol is only conditional secure since its security is based on mathematical conjectures. In this project, we have resolved this issue based on quantum physics. As an example, we presented a

contract signing protocol based on our proposal. We also discussed the initialization circuits and various security issues of our protocol.

Due to the discovery of Shor's algorithm, many classical crypto-systems based on the hardness of solving discrete log and factoring problem are theoretically broken using quantum computers. This means that some of the classical secret communication protocols are no longer secure and hence motivate us to find other secure crypto-systems. In this project, we present a new quantum communication protocol which allows two parties, Alice and Bob, to exchange classical messages securely. Eavesdroppers are not able to decrypt the secret message and can be detected if they do exist. Unlike classical crypto-systems, the security of this protocol is not based on the hardness of any unproven mathematic or algorithmic problem. Instead, it is based on the laws of nature.

Recent progress in nanotechnology has focused on applying nanoscale phenomenon in physical layer or device level applications. In this project, we show that nanoscale phenomenon can not only be used in physical layer, but also in high layer application such as communication protocols. We study the possibility of performing authentication and encryption based on quantum entanglement, which is a phenomenon available only at the nanoscale level. Unlike classical authentication and encryption algorithms, the security of this protocol is based on nanoscale physical laws, instead of any unproven mathematic conjecture.

Maximum flow problem has many applications in the engineering community. In this project, we propose a quantum algorithm to solve the maximum flow problem in O(n2.5) time, which, to the best of our knowledge, is faster than all other classical and quantum algorithms.

Keywords: Quantum Computing, Quantum Communications, Quantum Circuits, Circuit Synthesis, Circuit Testing, Nuclear Magnetic Resonance (NMR).Quantum Computing, Quantum Communications, Nuclear Magnetic Resonance, Pulse Program, Non-Locality, Secure Computation, Oblivious Transfer.

目錄

壹、報告內容

一、前言

量子資訊科學是一門相當新的研究領域，自從 1994 年量子演算法被發現可以用來在多項式時間內解出因數分解以及離散對數的問題後，有關量子計算、量子通訊的研究便疾速增加，也開始吸引大量研究經費的投入，目前在美國、歐洲、日本以及中國大陸，已經有許多專為此新領域而成立的研究團隊或研究機構。雖然目前具有幾個量子位元的量子電腦已有初步成果，多量子位元的量子電腦仍在設計與實驗中。也正由於世界各先進國家對量子計算及量子通信之發展尚處於實驗階段，本計劃之執行便也格外顯得前瞻而具有國際競爭性。

此外,實作量子計算機是一門相當有潛力的研究領域,有關各式量子計算機的實作吸引了大量美國、歐洲、日本以及中國大陸研究學者的投入，本計劃成功地實作 NMR 量子計算機之結果也格外具有國際意義。如何加速量子計算機的發展，便成為目前的課題。另外，量子計算在工程上的其他應用也受到極大的重視，尤其是在密碼學上是否能做到無條件式的安全，更是受到廣泛的研究與注目。本計劃研究的模糊傳輸，其在電子商務以及電信通訊上的保密安全，有非常大的助益。故本計劃的研究成果，即有可能對於新世紀的資訊科技及產業，促成極大的貢獻。

二、研究目的

本子計畫擬對量子電路之合成、測試、以及量子系統之實作方式做一深入研究，以期能帶動國內量子資訊科學的研究風氣。其內容與成果包括量子電路合成及測試之理論分析，演算法探討，以及如何使用核磁共振的方式來製作一個量子計算系統的實作過程。

另外,就核磁共振量子計算機之脈衝程式合成、以及量子計算在密碼學上之實際應用方面，其研究內容與目的包括下列各項。

1. 探討實作 NMR 量子計算機編譯工具的可能性。
2. 如何以此編譯工具的概念加速量子計算機的發展。
3. 研究量子計算於其他工程上面之應用，例如其是否可使用於模糊傳送。
4. 如何利用量子糾纏實作一個無條件式安全的量子模糊傳送。

三、文獻探討

量子電腦的概念最先是於 1980 年代初期被提出的 [1]-[3],從那時開始便有許多學者紛紛投入這個領域的研究。在安全金鑰傳遞 [4]、多項式時間分解質因數 [5] 以及快速資料庫搜尋演算法 [6] 等應用紛紛出現後，量子資訊有了很大的進展，這些結果使得量子資

訊科學在最近成為發展最快速的研究領域。另外，其他方面如量子電路的合成以及各種量子計算機的實作技術，包括離子井[8]、光學腔[9]、核磁共振[10]、量子點[11]以矽基解決方案[12]等等，都讓這個領域更加接近實際應用的階段。

第一位提出並實作NMR量子計算機成功的研究團體是N. Gershenfeld及Issac Chuang [1]。當時是以高純度之^{13}C Chloroform完成Deutsch Problem，此後便有許多學者陸續完成其他演算法或是基於其它分子的實作[2-5]。後來雖然有人提出量子計算機系統軟體的概念，但如本計畫般實作一個實際可用的NMR脈衝程式產生器還是屬十分前瞻的研究。

此外，模糊傳送是在 1981 年由Michael O. Rabin所提出的[6]，這個協定的定義是：傳送者送一個資訊給接收者，接收者有 1/2 的機率會收到；1/2 的機率不會收到，而最後傳送者不知道接收者到底收到了沒。1985 年，Shimon Even, Oded Goldreich, 和 Abraham Lempel 提出另一種模糊傳送模式，稱為 1-2 OT，其定義：傳送者送兩段資訊給接收者，接收者只能獲得其一，而傳送者無法知道接收者收到那一個。1-2 OT亦是我們一般所定義的模糊傳送，但又可細分為接收只可以指定所要收到的訊息，及接收者不能指定所要接收的訊息，只能隨機得到。近幾年，模糊傳送引進了量子力學[7-13]，成為了一個新的研究領域---量子模糊傳送。有許多研究利用量子的糾纏性來建立模糊傳送，也有不使用糾纏性，使用例如BB84 協定的方法建立，亦有用間接的方式來達成的。許多方法都還在研究階段，期望能找出最好的方式。

四、研究方法

本研究之整體目的在於對量子電路以及量子系統之實作方式、核磁共振量子計算機之脈衝程式合成，以及對量子計算於密碼學做一深入研究。想要達成實作量子計算系統的目的，必須先就量子電路的合成及測試等子目標著手。所以，本計劃之研究方法包含先分析及解決下述之子目標。子目標一是我們必須設計一個多變數的量子布林電路化簡方法，這個方法要可以化簡多變數的量子布林邏輯函數。當電路化簡之後，我們還需要驗證測試化簡的量子布林電路是否和原來電路有等效的作用，這個方法就是函數驗證。所以，本研究之第二個子目標在於提出一個驗證測試化簡的量子電路的方法。最後，基於以上之研究，我們便可利用對量子電路的瞭解來架構一部核磁共振量子電腦，並利用 RF 脈衝來實作操控它所需要之量子作用。接下來，我們便描述研究這些階段性目標的一些結果。

在 NMR 脈衝程式合成方面，我們先從精準控制脈衝波施打時間點及範圍、分析核心材料對參數設定的影響為子目標著手。為達成精準控制脈衝波，我們必須先計算施打在每種原子上的脈衝波影響時間，然後設計一個二維么正矩陣來動態控制施打脈衝波的目標及時間，矩陣中的行表示時間點、列表示施打脈衝波目標，矩陣中的元素值非 1 即 0，當某元素值為 1 時即表示該時間點須對該目標施打脈衝波。接著必須確認此矩陣是否能夠有效分割脈衝波對核心材料的影響不致重疊。除精準控制脈衝波外，還要提出有效的參數設定模

式，以表現出不同量子電腦核心材料對脈衝波合成工作的影響。基於以上的研究，我們即能夠設計出一套準確的脈衝程式合成裝置，進而有效利用 RF 脈衝來進行各種量子演算法的實驗。在量子計算之應用方面我們首先將量子糾纏與非區域性做了一徹底的研究。之後再設計了一台虛擬的非區域性機器(Non-Loacl Machine)，該機器能利用量子計算的特性達成古典物理上無法達成的事情。其後，我們再利用非區域性機器的特性來達成量子模糊傳輸。

五、結果與討論

就量子電路之合成及檢測來研究量子計算之系統架構而言，在量子電路合成方面，為了要完成量子電腦，我們必須建立量子布林電路，這些電路是由量子邏輯閘組成的，不像傳統的 AND-OR-NOT 電路，量子布林電路是以 NOT、CN 和 CCN 閘當成基本元件，雖然有一個不同的基本邏輯閘，電路仍然可以使用傳統 AND、XOR 和 NOT 函數進行電路合成。

在本計劃中，我們提出了一個表格式演算法，表格式演算法可以用來簡化布林函數，特別是針對較多的變數的情況，這個演算法的概念有兩個優點，分別說明如下:

1）這個演算法可以程式化，以做為量子布林電路的化簡工具。

2）對於量子布林電路的化簡，這個方法是一個非常有前景的技術。

本表格式演算法是利用列表方式，分別針對 AND 和 XOR 函數進行化簡，在每一個週期，可以找到一個最簡化的項目，這個項目具有最多的 1，並且可以產生一個部份方程式，最後組合這些部份方程式，就可以到化簡結果。假設原來的真值表有 n 個變數，這個演算法的說明如下:

1. 計算 1 的數目，如果超過 2^{n-1}，則更改 1 為 0，0 更改為 1。
2. 對 1 進行分組。
3. 執行 AND 函數產生。
4. 執行 XOR 函數產生。
5. 從上面步驟 3 和 4 中，選擇最簡化的項目，根據所選的項目，可以得這個項目的布林函數，接下來，更改這個項目中的 1 為 0，0 更改為 1。
6. 如果仍然有 1 存在，則跳到步驟 2。
7. 最後，組合所有布林函數。

至於在量子電路檢測方面，我們也提出了電路測試演算法，在這個演算法中，利用由後向前傳遞方式找到一組測試向量。輸入這組向量到電路中，檢查輸出向量是否正確，可以利用測試結果找到有問題的量子位元。假設 n 個位元的量子布林電路有 m 個量子邏輯閘，這個演算法的說明如下:

1. 掃描整個電路，並且記錄每一個目的量子位元的位置。
2. 選一個未標示的量子位元，這個位元是某個邏輯閘的目的量子位元，然後標示這個位元。
3. 利用由後向前傳遞方式，找到測試方程式。
4. 根據測試方程式，可以得到一組測試向量。

5. 如果仍然有未標示的量子位元，則跳到步驟 2。
6. 組合所有測試向量，可以得到一組必要測試向量。
7. 輸入必要測試向量到電路中，並且找到具有不正確值的輸出量子位元。
8. 根據錯誤量子位元的位置，可以找到故障閘的可能位置。

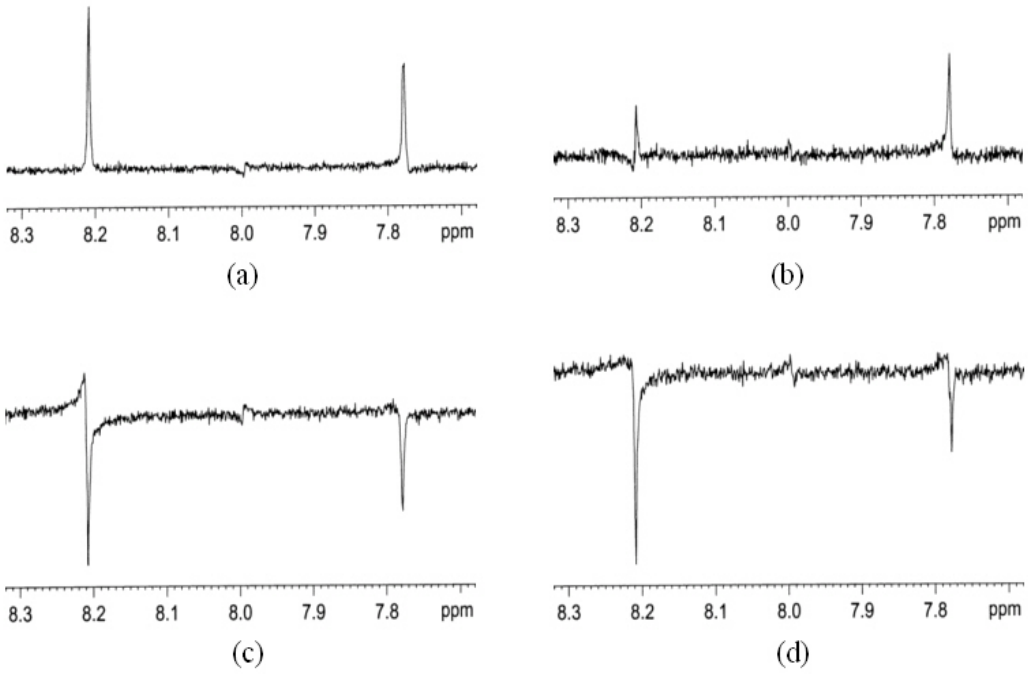
在有足夠的技術能合成及檢驗量子電路之後，便可以開始著手實作量子計算系統。最近幾年來量子實際製作方法的進展十分地迅速，，讓科學家有許多不同方法可以實現量子力學的應用。在這些解決方案中，核磁共振是一項比較成熟的技術，在化學和醫學領域中也已經有了廣泛的應用。在許多報告中也證明了NMR能夠實作量子計算系統，並且解決傳統計算所無法解決的問題。本計劃選擇使用核磁共振的方式來實作量子計算系統，利用基於碳的同位素碳 13 之三氯甲烷(chloroform)中的^{1}H和^{13}C ($^{13}CHCl_3$)做為資訊的承載單位，實現 2 位元的NMR量子計算系統之雛形。值得注意的是，只要承載資訊的狀態可以根據量子力學的方式進行操作，一個量子計算系統其實是不受限於底層的技術。

量子計算機中最重要的動作就是兩個(或多個)量子位元之間的互相作用。兩個量子位元的條件式邏輯可以透過自旋交互作用(spin-spin coupling)的效果來達成，本計劃中，自旋交互作用是^{1}H和^{13}C自旋狀態之間的互動結果，以Hertz (Hz)為單位來量測。由於這個偶合關係，一個量子位元的進動就可以根據其他量子位元的狀態增加或減少。如果在脈衝波順序中加入某些特定的自由演化(free evolution)時間，目標量子位元的狀態就可以依據控制量子位元的狀態條件式的進行相位移轉。這基本上就是一個控制-相位轉移(control-phase-shift)閘，它也可以用來產生其他量子條件式邏輯閘。**CN**閘是兩個量子位元條件式邏輯閘的其中一個範例，**CN**閘可以分解成兩個**H**閘和一個 π 角度的控制-相位轉移閘。

在實驗方面，我們將$^{13}CHCl_3$置於室溫中的d6-Acetone來做為此交換器之平台，利用其中的^{1}H和^{13}C原子來承載資訊。實驗的脈衝波能量在頻道 1 (^{1}H)中設為 3.00 dB，在頻道 2 (^{13}C)中則設為-3.00 dB。對頻道 1 的 90 度脈衝波時間為 9.5μs，頻道 2 則為 12.6μs。因為單一量子位元操作的旋轉角度跟能量和RF脈衝波的時間成正比，所以經過簡單的計算就可以得到 45 度和 180 度脈衝波的時間。在自旋交互作用控制下的自由演化是量子計算中條件式邏輯的來源，^{1}H和^{13}C之間的自旋交互作用量測結果為 215 Hz。因此，計算之後 90 度的自由演化時間為 1.165μs，180 度旋轉則需 2.33μs，剛好是 90 度旋轉的兩倍。這些參數都必須指定到Bruker脈衝波程式中的D、P以及PL陣列。

在 NMR 的實驗中通常需要執行多次相同的掃描，以便改善其雜訊比(signal to noise ratio)，這個掃描的次數稱為 NS (Number of Scans)。在標準的化學實驗中，典型的 NS 值通常介於 1000 到 10000 之間，依據樣本的密度而定。另外，為了讓樣本達到穩定狀態，在實際的脈衝波之前必須先試幾個試驗的脈衝波，這個時候不用收集它的 NMR 訊號。這個參數稱為 DS (Dummy Scans)，DS 值通常介於 4 到 8 之間。因為本實驗使用了濃縮的樣本，所以 NS 與 DS 參數分別設為 8 和 0。其他必要的參數還有時間域(Time Domain size, TD)的大小，它是用來指定時間軸上欲收集資訊的時間點總數；以及 FID Resolution (FIDRES)，用來指定每個點之間的頻率範圍。本實驗的 TD 設為 32k，FIDRES 則設為 0.305176 Hz。結果若以 10000 Hz 的 Spectral Width (SW)做觀察，需要時間大約為 1.63845 秒。

本計劃利用國科會貴儀中心之Bruker Avance DMX-500MHz NMR系統，將$^{13}CHCl_3$置於室溫中的d6-Acetone來做為此交換器之平台，利用其中的^{1}H和^{13}C原子來承載資訊。實驗中我們將頻道 1 設為^{1}H，頻道 2 設為^{13}C，由此觀察連續三個量子位元互動(CN閘)的作用。在收集資料與後續處理(尤其是相位修正)之後，連續三個量子位元互動(CN閘)的作用如圖一所示。圖中顯示了正確的CN閘的動作。由於CN閘是一個基本閘，它與單量子位元旋轉可以組成任何量子操作，故而就理論上而言，我們已經可以達成操控NMR量子電腦的結果了。



圖一、NMR 量子計算機連續執行 CN 閘後的結果

接下來將研究如何利用 NMR 量子計算系統來實現量子演算法，其目標如下：

1. 量子演算法之理論與設計
2. 量子演算法於 NMR 量子計算系統之實作
3. NMR 量子計算機之脈衝程式編譯器
4. 多位元 NMR 量子計算系統之實作

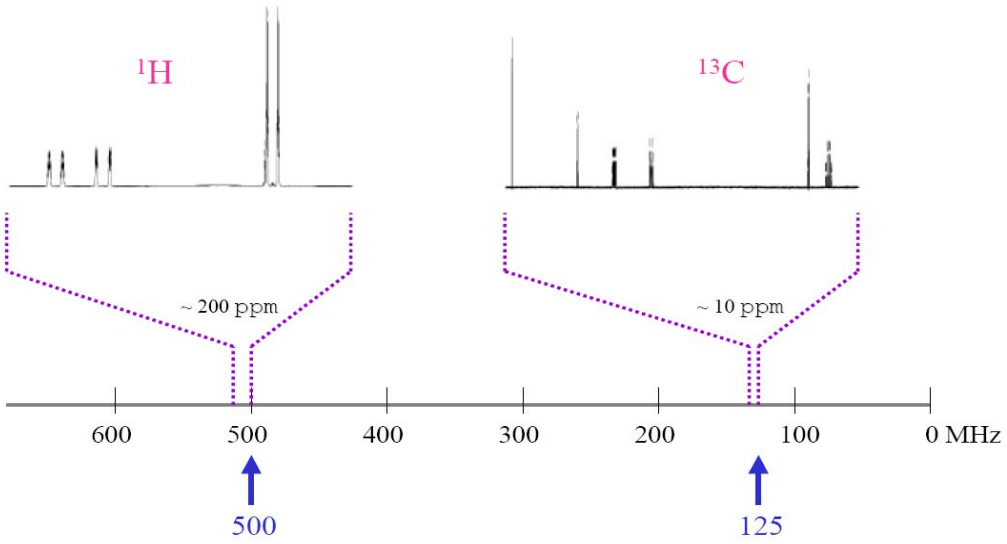
在NMR脈衝程式合成方面，我們先由核磁共振量子計算機之脈衝程式合成來研究量子計算之系統架構。基於NMR量子計算機技術上的成熟以及我們先前實作的成果，我們仍使用NMR做為核心技術。而計算機之核心分子則使用將C改為^{13}C的丁烯酸(化學結構簡式為$CH_3-CH=CH-COOH$)。其中C之同位素與H做為資訊承載單位共計有 7 顆記為：C_1、C_2、C_3、C_4、H_1、H_2、H_3。本計畫即以這樣一個多位元的量子計算機模型為基礎，發展一套脈衝程式合成工具 “NMRPPGEN”。由先前的研究我們已經得到了各基本量子閘的脈衝序

(pulse sequence)雛形，明確地說我們已經能夠產生出單一 90°以及 180°的脈衝程式，如表(一)。

Gate	Pulse Sequence
NOT	$X(\pi)$
H	$h \Rightarrow Y(\frac{\pi}{2})$ ， $h^{-1} \Rightarrow \bar{Y}(\frac{\pi}{2})$
CN	$Y_b(\frac{\pi}{2})Z_b(\frac{\pi}{2})\ \tau\ Z_a(\frac{\pi}{2})Y_z(\frac{\pi}{2})$

表一、各量子電路對應的脈衝序

然而面對多位元的計算系統，首要的挑戰就是如何能夠精準的控制施打脈衝波的時間點及位置。從圖(一)可以看出，因為此分子中有 4 個碳原子及 3 個氫原子，故各個碳原子及各個氫原子上施打脈衝波的頻率都很相近。



圖一、丁烯酸的頻譜分布

在本計畫中，我們採用選擇型脈衝波(selective pulse)來改變量子的相位，其特色就是在於當該脈衝波的波形平緩，同時施打的時間較長，但是在頻譜上卻有較窄的影響範圍。我們採用的選擇型脈衝波參數如表(二)，其中的能量一欄指的是衰減的程度。

Type	Width	Angle	Duration	Power
^{13}C	1000Hz	90°	2122us	33.89db
^{13}C	1000Hz	180°	734us	18.64db
H	200Hz	90°	10610us	56.72db
H	200Hz	180°	3670us	41.50db

表二、Selective Pulse 各項設定值

硬體儀器設備方面，本計劃利用國科會貴儀器中心之 Bruker Avance DMX-500MHz 系統，對量子計算機核心同一時間僅能針對兩種不同的原子施打脈衝波，因此我們將條件設置為單一時間僅能施打一次脈衝波，並且考慮選擇型脈衝的影響時間要為下次的脈衝時間預留時間差。為了達成智慧化脈衝程式合成，我們利用一個 8x8 的正交矩陣使其列與列之間兩兩正交，當作是反向脈衝的施打依據。將該矩陣轉化成方波圖，在量子物理的觀點上，如此兩兩反向與正向的時間相等將能夠達成抵銷量子間自旋交互作用(Decoupling)。經過部分的相位平移以及修改，我們找出適用於合成 CN 閘之中自由演化(Free Evolution)部分的波形，然後以程式自動計算對不同量子進行該波形的脈衝時間點。我們即可將剩餘的單一脈衝插至自由演化波形的前後端，並且用程式偵測可相互抵銷的部份(例如:對同一顆量子執行兩次 N 閘)，接著對脈衝程式執行合成的動作，讓多區塊的獨立脈衝程式結合成一個連續動作的完整脈衝程式。經過以上研究出來的參數設定值以及控制脈衝的方法，我們便能夠利用 NMRPPGEN 來精準控制脈衝波並完成脈衝程式合成。

更進一步地，我們研究使用不同核心對於脈衝程式合成的影響，設計了一個網頁介面提供參數設定的功能。研究者在使用相同硬體的 NMR 量子計算機環境下可以根據不同的核心分子來改變參數的設定。輸入的參數內容包含有：核心分子的位元數、使用哪種原子承載資訊、哪種原子作為觀測基準，以及各原子之間的交互影響頻率常數。參數輸入的網頁介面如圖(二)所示。

Basic Configuration:

Number of qubits: 7

Nucleus Types: ☑ H ☑ C ☐ F ☐ N

Observed Nucleus: C

Coupling Constant Setting: (in Hz)

Qubit Index		1 (C)	2 (C)	3 (C)	4 (C)	5 (C)	6 (C)	7 (C)
1	C	-2327.0	41.6	1.6	7.1	3.8.0	6.2	127.5
2	C	41.6	-18599.2	69.7	1.4	156.0	-0.7	-7.1
3	C	1.6	69.7	-15412.8	72.4	-1.8	162.9	6.6
4	C	7.1	1.4	72.4	-21685.1	6.5	3.3	-0.9
5	C	3.8	156.0	-1.8	6.5	-3560.3	15.5	6.9
6	C	6.2	-0.7	162.9	3.3	15.5	-2938.2	-1.7
7	C	127.5	-7.1	6.6	-0.9	6.9	-1.7	-969.4

PreLoad Value

圖二、NMRPPGEN 參數設定介面

運算核心在 7 位元以下的執行環境，NMRPPGEN 皆能夠產生出適當的脈衝程式。使用的方式如下所述：

1. 使用預設值完成參數設定或是自訂參數值。
2. 輸入想要執行的量子電路內容：N、H、CN 等，註解則在列首加入“;”符號。
3. 程式確認並檢查輸入是否有誤，接著執行 NMRPPGEN 產出脈衝程式。

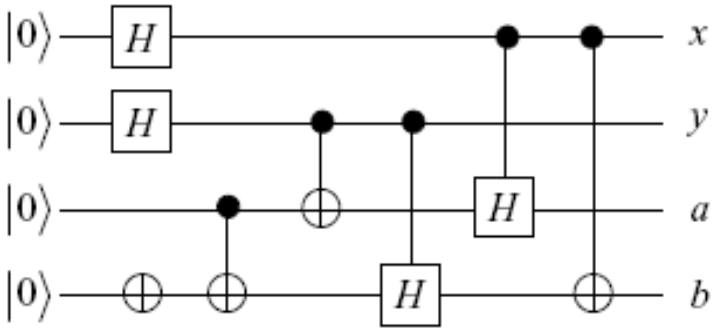
以上的研究使得我們能夠以自動化的方式達成脈衝程式合成，在高位元的量子計算機系統下可避免複雜的脈衝程式發生人為的錯誤，並且藉由 NMRPPGEN 的強化更有機會達到最佳化脈衝程式合成的目的。

至於在量子計算於其他方面之應用，我們也展示出量子計算不但能應用在實體層或在裝置上，亦可以有更高階的應用，例如量子密碼學。在本計畫中，我們也研究了量子糾纏的一些特性，並給了一個實際的例子來說明如何應用量子糾纏的現象及其他量子的特性來達成安全的計算。安全計算在比對機密或敏感的資料時，有極大的用處，可以不洩漏非必要的資料，並安全的得到計算後的結果。例如解決著名的約會問題或是富翁問題。除此之外，安全計算還可能可以簡單的對應到一個密碼學的基本類別－模糊傳輸。

模糊傳輸在簽訂電子合約，認證電子信，同時秘密交換與遠距丟銅板等問題上，提供了解決方案。同時，不像古典的密碼學大都是有條件式的安全，我們所提出的量子模糊傳輸，其安全性是基植於奈米尺度下物質的自然特性，是經由實驗所能證實的物理特性，而非僅只是依賴數學上的猜想。

根據我們的研究結果，量子模糊傳輸可以藉由分享如圖(三)所示之量子狀態而達成。其原理基本上是先利用該量子狀態實作一個非區域性機器，此非區域性機器可以用來實作安全計算(Secure Computation)[7]以及模糊傳輸。其大致步驟如下。

1. 當 Alice 及 Bob 分享此量子狀態後，各人可以測量量子位元 x 及 y 的狀態。
2. 如果測量結果與自己之輸入相符合，則 Alice 測量量子位元 a、Bob 測量量子位元 b，否則回到步驟 1.
3. Alice 及 Bob 兩人各公佈其結果，並做 XOR 後即可得到非區域性機器的結果。
4. 根據 S. Wolf 及 J. Wullschleger 的通信協定，可以實作一個量子模糊傳輸。



圖三、OT 初始狀態量子電路圖

在理論上我們可以畫出各式各樣的量子電路圖,但在日後實際設計與製造各種量子設備時我們仍需要可靠的量子裝置,並檢驗所產生的量子電路是否可以正常地執行工作,所以量子電路的檢測是很重要的.

在量子電路檢測方面，除了之前我們提出的電路測試演算法外，我們還對於量子布林電路的測試性進行深入的分析與研究，最後我們證明出對任意的量子布林電路都具有壹可測性.證明的步驟與得出的定理性質如下:

1. 任何古典方法下的電路都可以被轉換成量子布林電路
2. 任何古典電路都可以用最小的空間輸入轉換成量子布林電路
3. 任何的量子布林電路可以包含通用多重受控非閘
4. 任何通用多重受控非閘都是一對一映成
5. 任何量子布林電路都是一對一映成
6. 任何可逆的布林電路都是一對一映成
7. 任何由一對一映成細胞組成的反覆邏輯陣列都是一對一映成
8. 任何由一對一映成細胞組成的反覆邏輯陣列都具有常數可測性
9. 任何可逆的反覆邏輯陣列都具有常數可測性
10. 任何量子的反覆邏輯陣列都具有常數可測性與最小可測性
11. 任何量子的反覆邏輯陣列都具有壹可測性
12. 任何量子布林電路都具有壹可測性

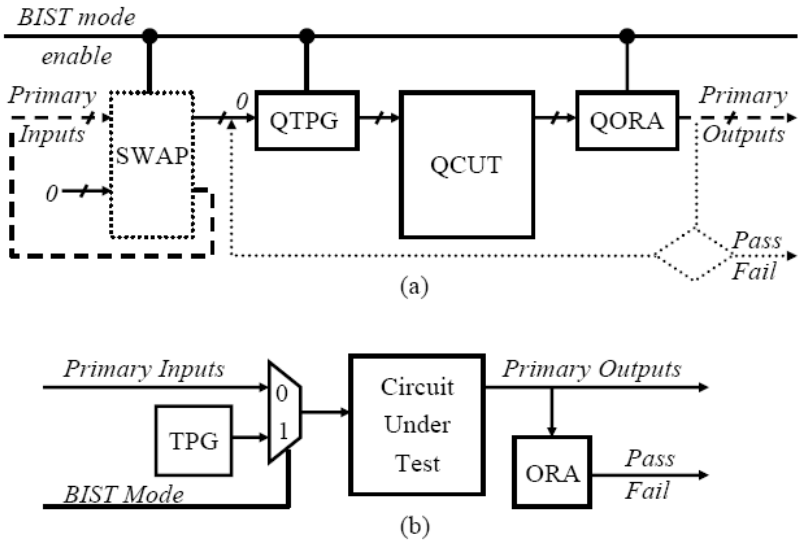
接下來我們可以利用哈達馬閘與多重受控非閘來使得量子反覆邏輯陣列都具有壹可測性。也就是說，對於任意的量子布林電路，測試樣本的數目與陣列的大小無關且同時與輸入的長度無關。這樣優良的性質可以用來應用於量子的內建自我測試系統上，並使得任意的量子反覆邏輯陣列與量子布林電路都同時具有壹可測性。

本技術可供有興趣之廠商將之進一步開發為量子布林電路的內建自我測試系統，適合前瞻之資訊，電子等製造業。傳統的測試系統都需花費太煩雜的程序及時間，不僅需要輸入大量的資訊來探測，同時也需要很長久的等待時間，而在傳統測試方法下的結果有時無法明確指出錯誤。本技術不但可以節省大量的輸入及輸出，同時也節省寶貴的測試等待時間，並且可以在很少的測試次數之內,檢測出電路是否有錯誤。

本技術推廣及運用的整體價值甚高，在傳統測試方法下，需要依據不同電路的特性量身打造不同的內建自我測試系統。本技術提出的方法具有通用性，可適用於任意的量子布

林電路，同時具有較低的額外成本。

圖四為量子與傳統內建自我測試系統架構之比較圖。其中(a)為量子內建自我測試之系統架構，(b)為傳統內建自我測試之架構。



圖四、量子與傳統內建自我測試系統架構比較圖
(a).量子內建自我測試架構 (b).傳統內建自我測試架構

至目前討論的結果為止完成之工作項目包含下列各項：

1. 量子電路合成之理論與演算法
2. 量子電路測試之理論與演算法
3. 以核磁共振的方式來實作 2 位元之量子計算系統
4. NMR 量子計算機之脈衝程式編譯器之實作
5. 網頁式 NMRPPGEN 設定與執行介面
6. 量子糾纏與非區域性之研究。
7. 利用量子特性實做一非區域性機器。
8. 利用非區域性機器實作量子模糊傳輸。
9. 證明對任意的量子布林電路都具有壹可測性。
10. 利用量子布林電路具有壹可測的性質來設計量子內建自我測試系統。

接下來預計將包括其他量子計算機實作方法之研究，特別是在擴充性(Scalibility)方面的研究，因為此領域是目前量子計算裡面一個亟待研究的課題。如果上述目標能順利達成，預計可帶動國內量子計算領域之研究，使得量子計算與通信之相關產業更易於早日到來。

貳、參考文獻

[1] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines,” J. Stat. Phys., vol. 22, no. 5, pp. 563–591, 1980.

[2] R. Feynman, “Simulating physics with computers,” Int. J. Theor.Phys., vol. 21, pp. 467–488, 1982.

[3] D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” in Proc. R. Soc. Lond. A, vol. 400, 1985, pp.97–117.

[4] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Computers Systems and Signal Processing, 1984, pp. 175–179.

[5] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in Proc. 35th Annu. IEEE Symp. Foundations of Computer Science, 1994, pp. 124–134.

[6] L. Grover, “A fast quantum mechanical algorithm for database search,” in Proc. 28th Annu. ACM Symp. Theory of Computing, 1996, pp.212–219.

[7] I. M. Tsai and S. Y. Kuo, “Quantum boolean circuit construction and layout under locality constraint,” in Proc. 1st IEEE Conf. Nanotechnology, 2001, pp. 111–116.

[8] J. Cirac and P. Zoller, “Quantum computation with cold trapped ions,” Phys. Rev. Lett., vol. 74, pp. 4091–4094, 1995.

[9] Q. Turchette, C. Hood, W. Lange, H. Mabuchi, and H. Kimble, “Measurement of conditional phase shifts for quantum logic,” Phys. Rev. Lett., vol. 75, pp. 4710–4713, 1995.

[10] N. Gershenfeld and I. Chuang, “Bulk spin resonance quantum computation,” Science, vol. 275, pp. 350–356, 1997.

[11] D. Loss and D. DiVincenzo, “Quantum computation with quantum dots,” Phys. Rev. A, vol. 57, pp. 120–126, 1998.

[12] B. Kane, “A silicon-based nuclear spin quantum computer,” Nature, vol.393, pp. 133–137, 1998.

[13] N. Gershenfeld and I. Chuang, "Bulk spin resonance quantum computation," Science, vol. 275, pp. 350-356, 1997.

[14] I. Chuang, N. Gershenfeld and M. Kubinec, "Experimental Implementation of Fast Quantum Searching," Phys. Rev. Lett., vol. 80, no. 15, pp. 3408-3411, 1998.

[15] I. Chuang, L. Vandersypen, X. Zhou, D. Leung and S. Lloyd, "Experimental realization of a quantum algorithm," Nature, vol. 393, pp. 143-146, 1998.

[16] J. Jones, M. Mosca and R. Hansen, "Implementation of a quantum search algorithm on a quantum computer," Nature, vol. 393, pp. 344-346, 1998.

[17] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, M. Sherwood and I. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic

resonance," Nature, vol. 414, pp. 883-887, 2001.
[18] M. Rabin, How to exchange secrets by oblivious transfer, Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
[19] A. Yao, Protocols for secure computations, in Proceedings of IEEEFOCS82, pages 160-164, Chicago, 1982.
[20] S. Popescu, D. Rohrlich, in Proceedings of Causality and Locality in Modern Physics and Astronomy: Open Questions and Possible Solutions: A Symposium to Honor Jean-Pierre Vigier, Toronto, Canada, 25-29 August 1997.
[21] J.S. Bell, Physics (Long Island City, NY) 1 (1964) 195.
[22] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Phys. Rev. Lett. 23 (1969) 880.
[23] Mayers, D.; Salvail, L. Quantum oblivious transfer is secure against all individual measurements in Physics and Computation, 1994. PhysComp'94, Proceedings., Workshop on 17-20 Nov. 1994 Page(s):69-77.
[24] Gertner, Y.; Kannan, S.; Malkin, T.; Reingold, O.; Viswanathan, M.; The relationship between public key encryption and oblivious transfer Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on 12-14 Nov. 2000 Page(s):325-335.
[25] Wolf, S.; Wullschleger, J.; Oblivious transfer and quantum non-locality, Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on 4-9 Sept. 2005 Page(s):1745-1748.
[26] T. Toffoli (ed. J. W. de Bakker and J. van Leeuwen), Automata, languages and programming, pp.632. New York: Springer. 1980.
[27] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation", Phys. Rev. A, 52(5): 3457–3467, 1995.
[28] D. P. DiVincenzo, "Quantum gates and circuits", Proc. Roy. Soc. Lond. A, 454, 261–276, 1998.
[29] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[30] I.-M. Tsai and S.-Y. Kuo, "An algorithm for quantum boolean circuit construction", in Proc. 2001, IEEE Conf. Nanotechnol., pp. 111–116, July 2001.
[31] I.-M. Tsai and S.-Y. Kuo, "An algorithm for minimum space quantum boolean circuits construction", Journal of Circuits, Systems, and Computers, 15(5): 719–738, October 2006.
[32] R. Landauer, "Irreversibility and heat generation in the computing process", IBM Journal of Research and Development, 5(3): 183–191, 1961.
[33] W. H. Kautz, "Testing for faults in combinational cellular logic arrays", in Proc. 8th Annu. Symp.Switching Automata Theory, pp. 161–174, 1967.
[34] P. R. Menon and A.D. Friedman, "Fault detection in iterative arrays", IEEE Trans. on Computers, vol. C-20, pp. 524–535, May 1971.
[35] A. D. Friedman, "Easily testable iterative systems", IEEE Trans. on Computers, vol. C-22, pp. 1061–1064, Dec. 1973.

[36] S. K. Lu, J. C. Wang and C. W. Wu, “C-Testable Design Techniques for Iterative Logic Arrays”, IEEE Trans. on VLSI, vol. 3, no. 1, pp. 146–152, March 1995.

[37] M. A. Breuer, “Fault detection in a linear cascade of identical machines”, in Proc. 9th Annu. Symp.26 Switching Automata Theory, pp. 235–243, 1968.

[38] C.-H. Sung, “Testable sequential cellular arrays”, IEEE Trans. on Computers, vol. C-25, no. 1, pp.11–18, Jan. 1976.

[39] C.Y. Su and C.W. Wu, “Testing Iterative Logic Arrays for Sequential Faults with a Constant Number of Patterns”, IEEE Trans. on Computers, vol. 43, no. 4 pp. 495–501, April 1994.

[40] H. Fujiwara and S. Toida, “The complexity of fault detection problems for combinatioinal logic circuits”, IEEE Trans. on Computers, vol. C-31, pp. 555–560, June 1982.

[41] C. W. Wu and P. R. Cappello, “Easily testable iterative logic arrays”, IEEE Trans. on Computers, 39(5): 640–652, May 1990.

[42] X. Ma, J. Huang, C. Metra, F. Lombardi, “Testing Reversible 1D Arrays for Molecular QCA”, in Proceedings of IEEE Symposium on Defect and Fault Tolerance in VLSI Systems (DFT‘06), pp. 71–79, Oct. 2006.

[43] A. Chakraborty, “Synthesis of Reversible Circuits for Testing with Universal Test Set and CTestability of Reversible Iterative Logic Arrays”, in Proc. 18th Int. Conf. VLSI Design (VLSID‘05), pp. 249–254, 2005.

[44] K. Patel, J. Hayes and I. Markov, “Fault testing for reversible circuits”, IEEE Trans. on Computer-Aided Design, vol. 23, no. 8, pp. 1220–1230, 2004.

[45] V. Shende, A. Prasad, I. Markov and J. Hayes, “Synthesis of reversible logic circuits”, IEEE Trans. on Computer-Aided Design, 22(6): 710–722, 2003.

[46] P. Gupta, A. Agrawal, N. K. Jha, “An Algorithm for Synthesis of Reversible Logic Circuits” IEEE Trans. on Computer-Aided Design, 25(11): pp. 2317–2330, Nov. 2006.

[47] I.-M. Tsai and S.-Y. Kuo, “Digital switching in the quantum domain”, IEEE Trans. Nanotechnol., vol. 1, pp. 154–164, Sep. 2002.

[48] L. T. Wang, C. W. Wu and X. Wen, Design for Testability: VLSI Test Principles and Architectures, Elsevier (Morgan Kaufmann), San Francisco, 2006.

參、計畫成果自評

本計畫研究量子電路之合成及檢測的理論，並以實作的方式達成實作 NMR 量子計算系統之雛形，為國內之首例，深具指標意義。本技術不但可用於量子計算系統，亦可用於量子網路上交換系統(量子交換機)之實現，可謂國內一項創舉。另外，本計畫在研究 NMR 量子計算機脈衝程式之合成方面，以實作輸出入介面及合成引擎的方式達成 NMR 量子計算機編譯系統之雛形，為國內之首例，實為難得。本技術不但可用於 NMR 量子計算系統，其概念亦可用於其他架構之量子計算機編譯系統，可謂一項創舉。除此之外，本計畫在量子糾纏及其非區域性，除可以解決一般安全計算上的問題，並可實作上層之另一基本密碼學上的重要元件－模糊傳輸。利用模糊傳輸，吾人更可以做多一些目前電子化社會中常見的應用，例如掛號認證的電子信函、遠距電子合約簽署、同步機密訊息交換等應用，且無需假手他人或透過第三方公正機構，如應用量子密碼學，即可達成此單純兩造間的安全計算，且不會有洩漏多於資訊的疑慮。

目前在本計劃內完成且已被接受之研究論文共計 22 篇，條列如後，成果可謂相當豐碩。

(1) I. M. Tsai, S. Y. Kuo, S. L. Huang, Y. C. Lin, and T. T. Chen, "Experimental Realization of an NMR Quantum Switch," Proceedings of the 2004 ERATO conference on Quantum Information Science(EQIS'04), Sept. 2004, Tokyo, Japan.
(2) I. M. Tsai, C. M. Yu, W. T. Tu, and S. Y. Kuo, "A Secure Quantum Communication Protocol using Insecure Public Channels," Proceedings of the 20th International Information Security Conference (SEC'05), May 2005, Chiba, Japan.
(3) I-Ming Tsai and Sy-Yen Kuo, “Performing Authenticated Encryption with Nanoscale Phenomenon”, to appear in IEEE-NANO-2005
(4) Han-Wei Wang, I-Ming Tsai and Sy-Yen Kuo, “Protocol and Applications for Sharing Quantum Private Keys”, to appear in IEEE-Carnahan-2005
(5) Han-Wei Wang, I-Ming Tsai, Chih-Neng Chung and Sy-Yen Kuo, “A scheme to enhance the error-checking capability of encoded quantum information”, to appear in European conference on Circuit theory and design (ECCTD-2005)
(6) C. Y. Lu, S. A. Wang, I. M. Tsai, and S. Y. Kuo, "An Efficient Testing Method for Quantum Boolean Circuits," Proceedings of the 2004 ERATO conference on Quantum Information Science (EQIS'04), Sept. 2004, Tokyo, Japan.
(7) H. W. Wang, I. M. Tsai, and S. Y. Kuo, "A Circuit Approach for Implementing Quantum Memory," Proceedings of the 2004 IEEE Conference on Nanotechnology (IEEE-NANO 2004), August 2004, Munich, Germany.
(8) S. A. Wang, C. Y. Lu, and S. Y. Kuo, "An Efficient Functional Verification Method for Quantum Boolean Circuits," Proceedings of the 2004 IEEE Conference on Nanotechnology (IEEE-NANO 2004), August 2004, Munich, Germany
(9) C. Y. Lu, S. A. Wang, and S. Y. Kuo, "Quantum Boolean Circuits Construction Using Tabulation Method," Proceedings of the 2004 IEEE Conference on Nanotechnology

(IEEE-NANO 2004), August 2004, Munich, Germany

(10) Yi-Lin Ju, I-Ming Tsai, and Sy-Yen Kuo, "Performing authenticated encryption with nanoscale phenomenon," Proceedings of the 2005 IEEE Conference on Nanotechnology (IEEE-NANO 2005) , vol. 2, Page(s):537 - 540.

(11) H. W. Wang, T. S. Lin, I. M. Tsai, and S. Y. Kuo," Protocol and Applications for Sharing Quantum Private keys," Proc. of the 39th IEEE International Carnahan Conference on Security Technology, pp. 204-207. 2005.

(12) I-Ming Tsai, Chia-Mu Yu, Wei-Ting Tu, and Sy-Yen Kuo, ``A Secure Quantum Communication Protocol Using Insecure Public Channels,'' Proceeding of 20-th IFIP Information Security Conference (SEC 2005), Pages: 113-126, May 2005, Makuhari-Messe, Chiba, Japan.

(13) Yao-Hsin Chou, I-Ming Tsai and Sy-Yen Kuo, 2006 July, "Enhancing Dependability through Quantum Entanglement in a Real-Time Distributed System", in Proceedings of IEEE-NANO 2006, volume 2, pages 859-862

(14) T. S. Lin, I. M. Tsai, H. W. Wang, and S. Y. Kuo," Quantum Authentication and Secure Communication Protocols," to appear in Proc. of the 6th IEEE Conference on Nanotechnology 2006, volume 2, pages 863-866.

(15) Yao-Hsin Chou, I-Ming Tsai and Sy-Yen Kuo, 2006 July, "Quantum Entanglement and Its Applications on Secure Computation", in Proceedings of IEEE-NANO 2006, volume 2, pages 878-881.

(16) I-Ming Tsai and Sy-Yen Kuo, "An Algorithm for Minimum Space Quantum Boolean Circuits Construction", in World Scientific "Journal of Circuits, Systems, and Computers", 15(5): 719–738, October 2006.

(17) Yao-Hsin Chou, I-Ming Tsai, Chien-Ming Ko and Sy-Yen Kuo,2006 December, "Quantum Oblivious Transfer and Fair Digital Transactions", in Proceedings of IEEE-PRDC 2006, Page(s):121 – 128, Riverside, USA, Dec. 2006.

(18) Yao-Hsin Chou, I-Ming Tsai, and Sy-Yen Kuo, 2007 January, "Quantum Entanglement, Non-Locality and Secure Computation", in Proceedings of IEEE-ICQNM 2007, Page(s):15 –20, Jan. 2007, Gosier, Guadeloupe.

(19) Chia-Mu Yu, I-Ming Tsai, Yao-Hsin Chou, Sy-Yen Kuo,``Improving the Network Flow Problem using Quantum Search,'' to appear in Proceeding of 7-th IEEE Conference on Nanotechnology (IEEE-NANO 2007), August, 2007, Hong Kong, PRC.

(20) Yao-Hsin Chou, I-Ming Tsai, Sy-Yen Kuo, ``Quantum Boolean Circuit is 1-Testable,'' to appear in Proceeding of 7-th IEEE Conference on Nanotechnology (IEEE-NANO 2007), August, 2007, Hong Kong, PRC.

(21) Shiou-An Wang, Chin-Yung Lu, I-Ming Tsai and Sy-Yen Kuo, "An XQDD-Based Verification Method for Quantum Circuits," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (accepted for publication).

(22) Yi-Ling Ju, I-Ming Tsai, and Sy-Yen Kuo, "Quantum Circuit Design and Analysis for Database Search," IEEE Trans. Circuits Syst. I (accepted for publication).

肆、可供推廣研發成果資料表

可供推廣之研發成果資料表

□ 可申請專利　■ 可技術移轉　日期：94 年 5 月 23 日

國科會補助計畫	計畫名稱：量子計算機之系統架構研究與設計 計畫主持人：郭斯彥 計畫編號：　NSC 93-2218-E-002-098　　學門領域：資訊二
技術/創作名稱	以核磁共振技術實作量子交換機之方法
發明人/創作人	蔡一鳴，郭斯彥
技術說明	中文：目前量子通信網路尚大多由「點對點」之連結所形成。量子通信網路之所以尚未形成真正的「網路」的原因是因為缺乏量子網路上有如傳統交換機或路由器之交換設備。本量子交換技術可使得量子通信網路具有真正的交換功能，大幅化簡目前點對點傳輸之複雜度。 英文：Currently the topology of quantum communication networks is dominated exclusively by the so-called *point-to-point* configuration. The reason why a true *network* is still not popular is that there is no switching or routing capability in the current quantum networks. However, the technology of quantum switching provides a possibility to extend the current quantum *point-to-point* configuration into a true quantum *network*.
可利用之產業及可開發之產品	本技術可供有興趣之廠商將之進一步開發為量子網路上之交換設備(量子交換機)，適合前瞻之資訊，通信等製造業。
技術特點	傳統交換機可傳送古典位元之信號，但無法傳送量子位元之信號。本交換技術可以在達成交換功能之外，並保持原有輸入資訊之量子狀態。此為量子通信網路所必備，但傳統交換設備所無法做到之處。
推廣及運用的價值	本技術推廣及運用的整體價值甚高，因為推廣本技術除可以使廠商在量子通信產業取得領先之優勢外，並可以帶動國內在量子資訊領域之研發及製造風氣，使台灣繼續保持電子資訊製造業大國之地位。

※　1. 每項研發成果請填寫一式二份，一份隨成果報告送繳本會，一份送　貴單位研發成果推廣單位（如技術移轉中心）。

※　**2. 本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。**

※　3. 本表若不敷使用，請自行影印使用。

可供推廣之研發成果資料表

□ 可申請專利　■ 可技術移轉　日期：95 年 5 月 23 日

國科會補助計畫	計畫名稱：量子計算機之系統架構研究與設計 計畫主持人：郭斯彥 計畫編號：　NSC 94-2218-E-002-037　　學門領域：資訊二
技術/創作名稱	核磁共振量子計算機之脈衝程式編譯器
發明人/創作人	蔡一鳴；鍾俊人；朱瑋中；郭斯彥
技術說明	中文：核磁共振量子計算機之脈衝程式編譯器是一個近似量子電腦編譯器的中階程式工具，我們只要將想要執行的量子運算邏輯閘作為輸入，即能合成操作 NMR 量子電腦執行該運算的 NMR 脈衝程式 (Pulse Program)。 英文：　NMRPPGEN is a compiler-like utility which can be used to generate NMR pulse program for NMR quantum computers. Its input is a text file which contains a series of quantum logic gates and the output is an NMR Pulse Program.
可利用之產業及可開發之產品	本技術可供有興趣之廠商將之進一步開發為核磁共振量子計算機上之編譯器，適合前瞻之資訊，通信等製造業。
技術特點	1. 以類似編譯器的理念設計，能加速 NMR 量子計算機之發展 2. 輸出的產生程式化，容易對 Pulse Program 做最佳化 3. 輸出入介面與合成引擎採分離式設計，設計較有彈性
推廣及運用的價值	本技術推廣及運用的整體價值甚高，尤其對量子計算機有前瞻性研發的廠商有相當的助益。

※　1. 每項研發成果請填寫一式二份，一份隨成果報告送繳本會，一份送　貴單位研發成果推廣單位（如技術移轉中心）。

※　**2. 本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。**

※　3. 本表若不敷使用，請自行影印使用。

可供推廣之研發成果資料表

□ 可申請專利　■ 可技術移轉　　日期：96 年 6 月 28 日

國科會補助計畫	計畫名稱：量子計算機之系統架構研究與設計 計畫主持人：郭斯彥 計畫編號：　NSC 95-2218-E-002-004　　學門領域：資訊二
技術/創作名稱	量子布林電路內建自我測試系統
發明人/創作人	周耀新，郭斯彥
技術說明	中文：　我們利用哈達馬閘與多重受控非閘來使得量子反覆邏輯陣列都具有壹可測性。也就是說，對於任意的量子布林電路，測試樣本的數目與陣列的大小無關且同時與輸入的長度無關。這樣優良的性質可以用來應用於量子的內建自我測試系統上，並使得任意的量子反覆邏輯陣列與量子布林電路都同時具有壹可測性。
	英文：　Hadamard and general CCN gates are used to make QILA and 1-testable. That is, for any quantum boolean circuit, the number of test patterns is independent of both the size of the array and the length of the inputs. This property can be applied to perform the quantum built-in self-test (QBIST), which makes any Boolean circuit 1-testable.
可利用之產業 及 可開發之產品	本技術可供有興趣之廠商將之進一步開發為量子布林電路的內建自我測試系統，適合前瞻之資訊，電子等製造業。
技術特點	傳統的測試系統都需花費太煩雜的程序及時間，不僅需要輸入大量的資訊來探測，同時也需要很長久的等待時間，而在傳統測試方法下的結果有時無法明確指出錯誤。本技術不但可以節省大量的輸入及輸出，同時也節省寶貴的測試等待時間，並且可以在很少的測試次數之內，檢測出電路是否有錯誤。
推廣及運用的價值	本技術推廣及運用的整體價值甚高，在傳統測試方法下，需要依據不同電路的特性量身打造不同的內建自我測試系統。本技術提出的方法具有通用性，可適用於任意的量子布林電路，同時具有較低的額外成本。

※　1. 每項研發成果請填寫一式二份，一份隨成果報告送繳本會，一份送　貴單位研發成果推廣單位（如技術移轉中心）。

※　2. **本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。**

※　3. 本表若不敷使用，請自行影印使用。

參加 2007 年國際高可靠度系統與網路會議報告

郭斯彥

一、出國目的

此次出國主要是參加 2007 年國際高可靠度系統及網路會議 (2007 International Conference on Dependable Systems and Networks) 及訪問英國里丁大學信息科學研究中心主任劉科成教授(Prof. Kecheng Liu)。國際高可靠度系統及網路會議是國際上容錯計算與網路領域的最重要會議，我們有一篇與計畫相關的論文再此會議發表。劉科成教授在里丁大學主持 Informatics Research Center 同時也是 School of Systems Engineering 的教授。目前我在學界科專負責的部份與他的 Lab 有相關的技術研究，因此他希望能互相合作。

二、考察、訪問過程

2007 年國際高可靠度系統及網路會議 (2005 International Conference on Dependable Systems and Networks) 於 2007 年 6 月 25 日至 6 月 28 日於英國蘇格蘭首府的愛丁堡市舉行。由於這個會議較特別的是它有兩個 Symposium 同時舉行，一個是 Dependable Computing and Communication，另一個是 Performance and Dependability Evaluation，因此參與的人不少，整個會場顯得相當的熱鬧。

DSN2005 今年約有超過 350 人參加，它是國際上容錯計算與網路領域的最重要會議，且論文接受率相當低，只有約 20% 左右，因此水準頗高。我們的論文題目為 ”Randomized Distributed Algorithm for Peer-to-Peer Data Replication in Wireless Ad Hoc Networks。論文在會議的第一天下午發表，愛丁堡是蘇格蘭的首府，一個非常具有歷史傳統的城市，主辦單位的安排亦相當好，晚宴安排至附近的古堡用餐，並欣賞夜景，令人印象深刻。6 月 29 日到達倫敦，住進飯店。30 日一早坐火車至里丁大學，隨即至實驗室參觀。這個 Lab 主要在做資訊處理及無線網路之應用，經費來源皆從校外，例如政府計畫、技術轉移、諮詢顧問等。他們並且做了幾個 Demo，相當不錯，感覺上他們的研究相當重視實務及應用，與我們的學界科專計畫頗為相像。

三、考察、訪問心得

這次訪問收獲良好，除了建立與他們的關係外，也充分了解到他們實驗室的專長並吸取他們的經驗，尤其是在實作上，可以供我們執行學界科專參考。另外他們工作的 Infrastructure 感覺上也比台灣好，校園環境之美化，實驗室設備管理，均有值得借鏡之處。

四、建議意見

英國大學其研究所水準已達國際水準，英語為其教授母語，溝通上相當容易，值得多與他們交流。

Randomized Distributed Algorithm for Peer-to-Peer Data Replication in Wireless Ad Hoc Networks

Hong-Zu Chou, Szu-Chi Wang, and Sy-Yen Kuo
Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan
sykuo@cc.ee.ntu.edu.tw

Abstract

In this paper, a randomized distributed algorithm is proposed to enhance data accessibility in wireless ad hoc networks. Furthermore, in order to analyze the behavior of our algorithm, a probabilistic approach is presented to derive the upper bound of convergence by a novel technique called path coupling, which gives more insight into factors determining system performance.

1. Introduction

Recently, peer-to-peer (P2P) systems have been extensively investigated [1]. Under the paradigm of P2P communications, data accessibility is crucial for overall system performance. In order to increase data accessibility for P2P applications, various data replication schemes have been proposed. However, these research results may not suitable for wireless ad hoc networks due to the vast differences in network characteristic.

Many cooperative caching schemes tailored for applications over mobile ad hoc networks have been presented. To cope with the situation in which a fixed access point is not available, Sailhan and Issarny [2] introduced a cache management strategy which can minimize the energy cost, especially for the Web caching problem. In [3], Yin and Cao proposed a hybrid cache scheme, unlike traditional ones that only replicate the contents of objects, the adopted path-caching strategy redirects possible future requests to a nearby node instead of the remote data center. In [4], Hara proposed many replica allocation and data update mechanisms to improve data availability for a partitioned network.

In this paper, we propose a randomized distributed algorithm for data replication. Moreover, we adopted a novel technique called path coupling to derive the upper bound of convergence time of the algorithm. We believe the concepts and the techniques presented here can provide a pragmatic building block for P2P applications over ad hoc networks.

2. System Model

Assume there are n nodes and m objects in a wireless ad hoc network and for simplicity, m is set as $O(n)$.. Each node u has equal transmission radius r and memory capacity $\Phi(u)=c < m$. The number of objects allocated in node u is denoted as m_u. Let $d(u, v)$ denote the hop-distance between node u and node v, the set $N^h(u)=\{v \in V : d(u, v) \le h\}$ is called the h-hop neighborhood of u. In this paper, the system is assumed as a *relaxed asynchronous model*, i.e., the upper bounds on process execution speed, message transmission delays, and clock draft rates are known. Thus we assume that a successful one-to-all *local-broadcast* operation can be accomplished within a constant period t_{lb}.

Albeit perfect synchronization is impossible, rational synchronization can be achieved via extra facilities, such as GPS signals. Therefore, we assume that all nodes are synchronized in rounds which consist of a number of time-slots.

Consider a P2P system, each node u has its *innate objects* (denoted as $INNATE(u)$) and some *replicated objects* (denoted as $REP(u)$). If node u is interested in object o, it issues a query $q(u, o) \in Q$ to search for o. A query $q(u, o)$ is called *resolved* if there exists a query resolution r that indicates the path information to node v, and $o \in INNATE(v) \cup REP(v)$. For all query $q(u, o) \in Q$, if there exits a resolution set R such that $d(u, v) \leq k$, we call Q k-coverable and R a k-covering resolution set for Q.

3.2. Randomized Distributed Algorithm

The main objective of our algorithm is to assure that all query sets become k-coverable. Since a wireless ad hoc network can be constructed without any pre-existing infrastructure, it typically provides a great degree of flexibility. On the other hand, data replication strategies in a centralized or hierarchical fashion are not desirable as the system size becomes large. Moreover, nodes in the same region are apt to require similar object(s). If a deterministic algorithm retrieves the most preferred object, it may cause unnecessary resource drain on the network because too many duplicates are allocated in the vicinity. Therefore, we propose a randomized distributed algorithm that aims to higher scalability and efficiency in a resource-limited network. The pseudo-code of the proposed algorithm is presented in Figure 1, where each node u executes the same procedure to make object allocation decisions.

Randomized Algorithm for Data Replication in node u

```
01.  information_exchange(k);
02.  if (cost_u(o_i) ≤ k)
03.  /* k-coverable: ∀q(u,o_i), 1 ≤ i ≤ m, ∃r ⇒ q(u,o_i), cost_u(o_i) ≤ k */
04.       do nothing;
05.  else{
06.       with probability α, do nothing;
07.       with probability (1 − α) {
08.            choose object o_r from the set R, R = {o_i : cost_u(o_i) > k} u.a.r;
09.            choose object o_d from the set D, D = {o_j : cost_u(o_j) = 0} u.a.r;
10.            if(m_u < c)
11.                 replicate o_r into local memory;
12.            else
13.                 drop o_d from local memory;
14.  }
```

Figure 2. Pseudo-code description of our data replication algorithm.

In line 1, the procedure is a data collector which periodically collects data from node u's 1-hop neighborhood. Each node u contains a distance vector $cost_u$ with size m; in which each element $cost_u(o_i)$ records the hop-distance of object o_i. During the period of t_{lb}, each node local-broadcasts the distance vector to its 1-hop neighbors. Whenever node u collects all the distance information from nodes $v \in N^1(u)$, for each object o_i, if $cost_v(o_i)+1 \leq cost_u(o_i)$, the value of $cost_u(o_i)$ will be updated to $cost_v(o_i)+1$. After executing such operations for k times, if the value of each $cost_u(o_i)$ is smaller or equal to k, it indicates that the query set of all objects is k-coverable, otherwise, there are some queries that cannot be resolved by $N^k(u)$. In order to avoid unnecessary redundancy by replicating objects in cooperation with its neighbors, node u do nothing with probability α, and chooses the candidate object for replicating/dropping with probability $(1-\alpha)$. In lines 6 – 12, the candidates o_r and o_d are chosen uniformly and randomly (u.a.r) from the sets $R = \{o_i: cost_u(o_i) > k\}$ and $D = \{o_j: cost_u(o_j) = 0\}$, respectively. If the local memory is full, object o_d will be dropped; otherwise node u will issue a request for replicating object o_r.

As described above, the steps of information exchange and object replicating/dropping are all repeated in a distributed manner. Note that since the dropping candidate is selected without considering neighbors' states, a node that has reached its stable state may be invoked to execute the algorithm again if a shared object is dropped by some neighbor. However, it is shown in the following sections that all query sets will eventually become k-coverable and the system enters a stable state with high probability (w.h.p.).

4. Stochastic Analysis

Consider our data replication algorithm in which the decisions made by each node only depend on its current state, it is clear that the algorithm satisfies the *memoryless* property and can be treated as a Markov chain with state space Ω (i.e., the set of all configurations). For a randomized algorithm which is operated as a Markov chain, one of the prime objectives is to derive the mixing time of the algorithm. In other words, it refers to how long the algorithm will take to reach one of the legitimate configurations with high probability. Therefore, we now use a powerful

technique called *path coupling* [5] to examine the behavior of the proposed randomized algorithm, more specifically, we show the upper bound of the time before entering one of the legitimate configuration set L. Based on our problem formulation, L consists of all configurations that the query sets are k-coverable. It is not hard to verify that the configurations in L are strongly connected. Moreover, L denotes the states with non-zero probability in the stationary distribution of the corresponding Markov chain. For brevity, the upper bound of memory capacity c is assumed to be large enough to replicate object(s) in the k-hop neighborhood. Furthermore, the self-loop probability α is set to 1/2 for ensuring the aperiodicity of Markov chain.

The state of each node i is expressed as a set $s_i = \{o_1, o_2, \ldots, o_m\}$, where $o_j \in \{0, 1\}$, $1 \le i \le n$, $1 \le j \le m$. The case $o_j = 1$ indicates that object j is in node i's memory. Likewise, $o_j = 0$ indicates that node i does not have the replica of object j. Obviously, the number of 1's appearing in s_i is no more than the memory size c, thus there are C possible states for a node, where $C = \left(\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{c}\right) < 2^m$. If we encode s_i as an integer, the state space Ω of our algorithm can be described by all combinations of s_i. Each possible configuration in Ω is expressed as (s_1, s_2, …, s_n), where $s_i \in \{0,1,\ldots, C\}$. Note that (i) the size of Ω is C^n; (ii) the replicating/dropping decisions made by the participating nodes may cause some movement from one configuration in Ω to another.

A Markov chain is *rapid-mixing* if the (ε-approximate) mixing time is bounded by a polynomial in $\ln(\varepsilon^{-1})$ and the size of each configuration in the state space. Due to the lack of space, we only show that the process of randomized distributed algorithm is rapid-mixing (i.e., converging in a time-efficient manner) and skip details of the mechanical proofs[1].

Proposition 1: For the proposed algorithm, there exist a subset S of $\Omega \times \Omega$, an integer-valued metric δ on $\Omega \times \Omega$ taking the values in $\{0, 2, 4, \ldots, 2cn\}$, and a coupling defined on S, such that for all $(X_t, Y_t) \in S$, $E[\delta(X_{t+1}, Y_{t+1})] \le \beta \cdot \delta(X_t, Y_t)$, where $\beta = 1 - ((m+c)/2mc)$.

Proposition 2. The mixing time of our algorithm is upper bounded by $\frac{2mc}{m+c}\ln(2cn\varepsilon^{-1})$ w.h.p.

6. Conclusions and Future Works

In this paper we concentrate on augmenting data accessibility for peer-to-peer data communications over wireless ad hoc networks. In addition to proposing the randomized algorithm, a path-coupling based method was used to verify the rapid-mixing property of state transition dynamics, together with a (loose) upper bound of the convergence time. In the future, we would like to conduct performance evaluation through much more extensive experiments, including the considerations of data updating, radio signal interference, and node mobility. Furthermore, since wireless communication may suffer from the traditional layered architecture, we hope to achieve further improvement by incorporating cross-layer adaptation.

References

[1] S. Androutsellis-Theotokis and D. Spinellis, ″A survey of peer-to-peer content distribution technologies, ″ *ACM Computing Surveys*, 36(4):335-371, 2004.

[2] F. Sailhan and V. Issarny, ″Cooperative Caching in Ad Hoc Networks, ″ *Proc. Int. conf. on MDM*, pp. 13-28, 2003.

[3] L. Yin and G. Cao, ″Supporting Cooperative Caching in Ad Hoc Networks,″ *IEEE Trans. Mobile Comput*, 5(1): 77-89, 2006.

[4] T. Hara and S. K. Madria, ″Data Replication for Improving Data Accessibility in Ad Hoc Networks,″ *IEEE Trans. Mobile Comput*, 5(11): 1515-1532, 2006.

[5] R. Bubley and M. Dyer, ″Path-coupling: a technique for proving rapid mixing in Markov chains, ″ *Proc. of IEEE FOCS*, pp. 223-231, 1997.

[6] V. Guruswami, ″Rapidly mixing markov chains: A comparison of techniques,″ May 2000. (available at http://cs.washington.edu/homes/venkat/pubs/papers.html)

[7] D. Randall, ″ Mixing, ″ *Proc. of IEEE FOCS*, 2003.

[1] Similar proof techniques can be found in [6][7]