行政院國家科學委員會專題研究計畫 成果報告

無仲裁機構的多方公平交換協定之設計
研究成果報告(精簡版)

計畫類別：個別型
計畫編號：NSC 100-2410-H-029-007-
執行期間：100年08月01日至101年07月31日
執行單位：東海大學資訊管理學系

計畫主持人：陳澤雄
共同主持人：鐘玉芳
計畫參與人員：碩士班研究生-兼任助理人員：林姿菁
碩士班研究生-兼任助理人員：林峰祺
博士班研究生-兼任助理人員：蕭宗志

報告附件：出席國際會議研究心得報告及發表論文

公開資訊：本計畫涉及專利或其他智慧財產權，2年後可公開查詢

中 華 民 國 101年08月23日

中文摘要：透過網路平台所發展的電子商務應用商機與技術，在日漸趨於成熟的同時，也帶動新一波的行銷方式；然而，如何確保交易之際的公平性，仍是相關應用中亟待克服的難題。針對公平性的技術發展，本計畫擬就電子商務應用中的各類公平交換協定進行設計與分析。在許多資訊安全機制的實際應用中，安全性與公平性的實施，往往必須透過所謂可信任的第三方(Trusted Third Party)，也就是通訊的傳送方與接收端在傳遞資料的過程中，必須經由某第三方機制的輔助，才能進行，但第三方的設計在實際運作上仍存在許多爭議；因此，本計劃提出無仲裁機構的交換協定，並且針對公平交換協定實際應用上常遭遇的共謀攻擊問題，包括來自內部惡意成員的合謀、或內部成員與外部第三者的共謀等，進行研究；並且應用密碼技術與新的交換方法，制定常數回合的多方公平交換協定，解決現行的多方交換協定中效率不彰的問題。本計畫達到理性參與者之間的納許均衡(Nash Equilibrium) ，採用賽局理論對公平交換協定進行設計與分析，提高協定之效率與安全性。

中文關鍵詞：公平交換協定、安全多方計算、賽局理論、共謀攻擊

英文摘要：While the development of e-commerce over the Internet has come to mature in its application to business opportunities and technologies, assuring fairness in trade and exchange remains a major problem in practice. Directed towards the development of this fairness aspect of the technology, this project aims to design and analyze various fair exchange protocols applied in e-commerce. In most applied information security mechanisms, the attainment of security and fairness is derived only through a trusted third party, i.e. the exchange of information between the sender and the receiver must be processed through the help of a third party. However, when put into practice, there exist many controversies in the designing of this third party. Therefore, this project proposes for an exchange protocol that requires no intermediaries. To solve the present inefficiency in multi-party exchange protocols, research is carried out on collusion attack problems that fair exchange protocols face when put into practice, such as internal conspiracy, conspiracy by external third parties, or conspiracy between selected internal members with an outside third party, with the establishment of round constant multi-party fair exchange protocol using cryptography and new exchange methods. Aiming to raise protocol efficiency and security by maintaining the Nash equilibrium in rational participants, this project adopts Game Theory in the design and analysis of fair exchange protocol.

英文關鍵詞： Fair exchange protocol； Secure multi-party computation； Game Theory； Collusion attack

無仲裁機構的多方公平交換協定之設計

The Design of TTP-free Multi-party Fair Exchange Protocol

計畫編號：NSC 100-2410-H-029-007

執行期限：九十九年八月一日至一百年七月三十一日

主持人：陳澤雄 教授 東海大學資訊管理學系

共同主持人：鍾玉芳 教授 東海大學電機工程學系

計畫參與人員：蕭宗志 中興大學資工系博士班

林姿菁 東海大學資訊管理研究所

林峰祺 東海大學資訊管理研究所

摘要

透過網路平台所發展的電子商務應用商機與技術，在日漸趨於成熟的同時，也帶動新一波的行銷方式；然而，如何確保交易之際的公平性，仍是相關應用中亟待克服的難題。針對公平性的技術發展，本計畫擬就電子商務應用中的各類公平交換協定進行設計與分析。在許多資訊安全機制的實際應用中，安全性與公平性的實施，往往必須透過所謂可信任的第三方(Trusted Third Party)，也就是通訊的傳送方與接收端在傳遞資料的過程中，必須經由某第三方機制的輔助，才能進行，但第三方的設計在實際運作上仍存在許多爭議；因此，本計劃提出無仲裁機構的交換協定，並且針對公平交換協定實際應用上常遭遇的共謀攻擊問題，包括來自內部惡意成員的合謀、或內部成員與外部第三者的共謀等，進行研究；並且應用密碼技術與新的交換方法，制定常數回合的多方公平交換協定，解決現行的多方交換協定中效率不彰的問題。本計畫達到理性參與者之間的納許均衡(Nash Equilibrium) ，採用賽局理論對公平交換協定進行設計與分析，提高協定之效率與安全性。

關鍵字：公平交換協定、安全多方計算、賽局理論、共謀攻擊。

Abstract

While the development of e-commerce over the Internet has come to mature in its application to business opportunities and technologies, assuring fairness in trade and exchange remains a major problem in practice. Directed towards the development of this fairness aspect of the technology, this project aims to design and analyze various fair exchange protocols applied in e-commerce. In most applied information security mechanisms, the attainment of security and fairness is derived only through a trusted third party, i.e. the exchange of information between the sender and the receiver must be processed through the help of a third party. However, when put into practice, there exist many controversies in the designing of this third party. Therefore, this project proposes for an exchange protocol that requires no intermediaries. To solve the present inefficiency in multi-party exchange protocols, research is carried out on collusion attack problems that fair exchange protocols face when put into practice, such as internal conspiracy, conspiracy by external third parties, or conspiracy between selected internal members with an outside third party, with the establishment of round constant multi-party fair exchange protocol using cryptography and new exchange methods. Aiming to raise protocol efficiency and security by maintaining the Nash equilibrium in rational participants, this project adopts Game Theory in the design and analysis of fair exchange protocol.

Keywords: Fair exchange protocol; Secure multi-party computation; Game Theory; Collusion attack

壹、 研究背景與目的

網路技術的快速發展，帶動網路商務活動略顯頻繁，也使得電子交易成為電子商務活動中的基本要素；因此，確保電子交易的公平性為資訊安全領域的新挑戰。公平性的目標在於保護顧客與商家的權益，確保雙方在進行交易時，無法進行欺騙行為，也保護互不信任的合作夥伴之間，得以在互不侵犯且公平的狀態下，完成雙方的交易。

在面交的交易行為中，買家與賣家雙方可以透過「銀貨兩訖」的方式確保交易的公平性；然而，在電子交易中，買賣方之間的資料傳輸都是經由網際網路完成，目前網路環境包括 Internet 皆以非同步的方式進行，無法以一手交錢一手交貨的方式完成交易，由此可見，電子交易的公平性實為電子商務發展的關鍵點。

21 世紀，許多人都有在網路進行購物、比價、拍賣的經驗，類似的電子行銷方式，帶給網購族群相當大的便利。但享受便利的同時，電子商務相關的安全性問題也逐漸浮現，主要的原因是網路本身的特性，例如：參與者身份的隱藏性、參與者地域分佈的廣泛性等，因而造成網路詐欺案例層出不窮，欺詐手法的更讓人防不勝防；為了確保個人利益不受侵犯所採取的各種防護措施，例如：使用第三方支付平台等，不但使交易變得更為不便，往往也只是徒增執行成本的額外負擔，還是無法徹底防範詐欺行為的發生，因此對於電子商務的發展造成極大的阻礙。因此，研究設計出一個安全且效能高的公平交換協定，可以廣泛應用在各類電子商務活動中，對於電子交易的安全性而言，具備重要發展的意義。

貳、 相關研究與現況

根據Kremer等人的研究[1]發現網路行銷相關的電子商務協定及交易公平性的機制，包括以下所列：

(1) 電子購物 (Electronic Purchase of Goods)：以電子貨幣交換商品的機制。

(2) 電子易貨 (Barter)：以價值相等的電子資料交換資訊的機制。

(3) 數位合約簽署 (Digital Contract Signing)：對電子檔案進行數位簽署並互換資料的機制。

(4) 不可否認性協定 (Non-repudiation Protocols)：交換電子資料時，同時檢查資料發送者與接收者雙方的不可否認證明的機制。

(5) 確認電子郵件 (Certified E-mail)：將電子訊息與該訊息接收回條進行交換的機制。

以上所描述的皆是在本質上針對同樣的問題提出解決方案，因此可歸類為公平交換協定。然而，為了提供效能更高的解決方法，發展出許多協定，以下為公平交換協定相關研究的發展過程之說明。

一、 公平交換協定之發展及其現狀

公平交換問題的提出可以追溯自八十年代。早期的解決方式是以秘密的逐步交換方式、或者以機率論的公平性，提出解決方案；之後，才逐漸發展出基於可信任第三方 (Trusted Third Party，TTP) 的公平交換協定；發展之初，每一次的交換活動都必須透過TTP的參與才得以完成，之後的相關研究發展，逐漸降低對TTP的依賴度，因而有所謂樂觀公平交換協定的提出。建置TTP所附加的計算及成本費用相當高，現實應用環境中的使用者，對於TTP的信任度也存有疑慮，因此相關研究傾向可免除TTP的公平交換協定，其中實用性較高者以針對數位簽章交換問題提出的合併簽章協定較受肯定。

(一) 早期的公平交換協定

秘密交換式公平交換協定[2]的運作方式，主要是透過一次一個位元將雙方的金鑰完成交換的方式，一來一回，使雙方擁有相近的金鑰知識。若交換過程中，交換程序被以非正常的方式中止，則剩餘未知的交換位元可以使用暴力搜尋計算予以破解，雙方還是可以各自完成計算金鑰的任務。其後，Tedrick 等學者[3]提出雙方逐步交換二進位數字取代單一位元的交換方式，但因為每一次交換的資訊量較大，可能衍生交換雙方擁有的金鑰知識不平衡的問題，所以其中一方必須先判斷對方是否有企圖進行欺騙，再進行交換。文獻[2, 3]則提出基於平方根問題的判斷方法，Even 等[4]則主張以不經意傳輸判斷方式解決平方根問題的方法。

上述的方法雙方都必須擁有近似的計算能力，才能以相同的時間與成本完成交換計算。這種方法顯示出在網路上非同步交換的特性，往往需要較高的通訊成本，嚴格來講，還是存在「一位元的不公平性」問題。此外，由於無法得知另一方是否願意利用暴力搜尋完成被中斷的交換程序，若有其中一方完成計算、而另一方卻未完成該程序，這種交換結果本身就是不公平的交換。然而，在應用上，相對於個人的使用者，大型公司通常擁有較好的硬體裝備，甚至電腦群組，在交換過程中明顯佔有較大的優勢，因此不適用於電子交易應用。

在 2000 年 Boneh 與 Naor[5]提出一個方法，用以降低協定對於雙方計算能力的依賴度，避免計算能力較強的一方獲得形勢上的絕對優勢，但還是必須耗費大量的交換回合完成，實用性仍有改善的空間。建立在機率概念上的公平交換協定[6-7]可以視為隨機化的協定，用意在降低某方欺騙的機率，進而增加訊息量，使該方獲得更多資訊或另一方未獲任何資訊的機率降至 1/n，其中 n 為一個安全參數，近似通訊回合數。基本上，這種方式意味不公平的機率可以任意地縮小。然而，為了達到此一公平性，隨機化協定必須依賴被交

換事件的特殊特性、或非一般性的系統假設，舉例而言：前者如具有特殊格式的合約[6]，後者如通訊通道的延遲具有限制[7]等，因此，整體而言實用性不高。

依據某些不可否認性協定[8]相關研究中，同時也提到公平交換協定的應用。所謂不可否認性的特性，包括發送的不可否認性與接收的不可否認性，意指參與者可以透過證據的收集與提供，使對方無法否認某事件的發生。

不可否認性在某種含義上可以藉由公平交換完成，將交換的某一項目作為另一項目的回條。相較於公平交換協定[9]，不可否認性協定的交換項目之間具有相依關係，如同確認電子郵件，回條必須包含一個與原始訊息相關的資訊，例如：原始訊息的雜湊值。目前，大多數公平交換協定都具有不可否認性[9]，使雙方之間的每個交換都具有不可否認性，藉此實現公平交換。然而，使用不可否認性協定所建立的公平交換協定無法達到強公平性的需求，只有當爭議發生時，透過不可否認性的證據，達到弱公平性的需求。

(二) 基於 TTP 的公平交換協定

實用的公平交換協定主要為分散式運算的公平交換協定，雖然實用，但必須透過一個仲裁者 TTP 參與運作，稱之為可信任的第三方。根據參與協定的程度，TTP 大致可以概分為以下四種[10]。

(1)線內式 TTP (Inline TTP)

協定執行的過程中，每一次的訊息傳遞都必須透過 TTP，稱之為線內式 TTP。線內式 TTP 的模式最早是在確認電子郵件協定時[11-13]所提出的概念，訊息發送者先將訊息發送給 TTP，以 TTP 作為可信任的仲裁者，負責傳遞及產生證明。線內式 TTP 承擔許多通訊、計算及儲存上的負荷，因此普遍存在以下問題：

1) TTP 單方面集中管理許多敏感資訊，例如：將待轉發的訊息予以暫存、

記錄通訊過程以產生證據；類似的作法，不但會使效能大幅降低，也相對提高資料的風險性。

2) 透過 TTP 負責轉發所有資訊，無形中增加通訊量，而導致效能降低。

3) 一旦 TTP 停擺，協定也無法運作。因此，線內式 TTP 公平交換協定只適用於小規模的應用環境，而不適用於開放式網路中大規模電子商務。

(2) 線上式 TTP (Online TTP)

仲裁者參與協定的每個會議但卻不參與傳遞訊息的模式，稱之為線上式 TTP,其作用在於減少線內式 TTP 的工作量，以解決 TTP 效率不高的問題。以具備發送人不可否認性的電子郵件訂貨協定[12]為例，當訂貨人 A 發送訊息給出貨人 B 時，必須先將訊息加密之後，再將加密過的訊息郵件寄給 B，並且將加密金鑰傳送給 TTP； B 收到郵件之後，必須先處理發貨的程序，再將貨物送達的證據傳送給 TTP，才能從 TTP 取得 A 的解密金鑰，對郵件訊息進行解密。線上式的 TTP 毋須再擔任轉發訊息的角色，但還是必須產生協定會議的通訊證據，本質上並未能夠有效地解決 TTP 的效率問題。

(3) 離線式 TTP (Offline TTP)

只有在不可信任的參與者做出不正確的行為，或發生網路錯誤時，才需要 TTP 參與運作的模式,稱之為離線式 TTP;離線式 TTP 公平交換協定的提出，主要是在於解決線上式 TTP 效率不佳的問題，又稱之為樂觀公平交換協定 (Optimistic Fair Exchange Protocol)。

在樂觀公平交換協定中,參與雙方會嘗試自行完成交換,只有發生錯誤時,參與者才會請求 TTP 介入，協助參與者公平地完成或終止協定；所謂發生錯誤的情況，通常包括參與者惡意的行為或網路錯誤。樂觀公平交換協定假設在大多數情況下，參與者都能夠誠實地完成交換，且網路發生錯誤的機率極微小，因此稱之為「樂觀」協定。

協定分為兩個部分，其一為主協定，負責在正常且無 TTP 參與的情況下

完成雙方的交換程序；其二為爭端處理子協定，負責在爭端發生時，尋求 TTP 參與程序，確保協定的公平性，是目前應用尚較常見的 TTP 式的公平交換協定；其公平性，必須依賴交換項目的可生成性與可刪除性加以判定，若被交換的項目不具備上述特性，則只能達到弱公平性。

針對公平交換協定的研究，Asokan 等學者提出樂觀公平交換的概念[14]，而 Zhou 等提出樂觀的不可否認性協定[15]，但上述二者的運作都必須透過同步通道進行，將會造成時間性的危害，因此，無法保證協定可以在明確的時間內結束。為了改善此一問題，Asokan 等提出新的樂觀協定[16]，將協定的運作建立在非同步的通道上。此外，Kremer 等也提出具備不可否認性的樂觀資訊交換協定[17]。

(4) 隱形式 TTP (Transparent TTP)

當一個離線式 TTP 所產生的證據，與 A 和 B 在未發生網路問題或錯誤交換事件的情況下所交換的證據，一樣且不可區分，則稱為之隱形式 TTP。

隱形式 TTP 最初是使用在 Micali 提出的確認電子郵件協定[18]中。其後，Asokan[19]隨即提出使用隱形式 TTP 的數位簽章協定，當爭議發生時，藉由 TTP 直接為某方還原原始資訊，而不僅只是提出某方正確執行協定的證明，該方法使用可驗證的加密方式，但效率不高。Ateniese 等所提出的隱形式 TTP 協定[20]，則利用另一種可驗證的加密方法，相較於 Asokan 提出的協定，效率更高。之後，Markowitch 等提出效率更高的協定[21]。直到 2004 年，周永彬等提出一個根據 RSA 簽章設計的隱形式 TTP 公平交換協定[22]。2005 年時，Nenadic 等提出驗證加密式的電子貨品傳遞協定[23]。

除了上述分類項目，某些協定則以對 TTP 的信任度為考量，例如：Franklin 等提出半可信的 TTP 方法[24]，就是在不相同且不誠實的參與者共謀的情況下，TTP 無法得到任何關於交換訊息的資訊。

(三) 無 TTP 的公平交換協定及合併簽章協定

離線式 TTP 交換協定雖可達到較高的效率，但還是存在 TTP 的設置、信任度、以及建置 TTP 的附加成本等問題[25]，都會影響使用 TTP 式公平交換協定的意願。

早期雖然並未使用 TTP，但因實用性不高，卻還是不斷的提出新的設計方法，並發展出無 TTP 的公平交換協定。

進入無 TTP 式公平交換協定的介紹之前，必須針對不可能性結論提出說明。1980 年，Even 與 Yakobi [26]提出以數位簽章協定為基礎的不可能性結論證明，也就是指在 TTP 不干涉的情況下，不存在一個解決數位合約簽署問題的確定性協定。1999 年，Pagnina 與 Gartner 提出在不使用 TTP 的情況下，不可能存在一個公平交換協定的證明[27]，並且說明一個可以應用公平交換協定設計的演算法，用以解決分佈一致性問題，這代表公平交換協定的困難度至少與解一致性問題的困難度相當。如果將不可能性結論應用在公平交換協定上，事實上，在公平交換協定中，參與者彼此之間採取互不信任的態度，惡意參與者用一個最簡單的攻擊都會導致協定的停止，因此，雙方都必須維持 1-crash-tolerant 的警覺狀態。

由於無 TTP 式公平交換協定的設計，不在於提供意義上的公平性，而是以允許存在些微的優勢差距，提出解決方法。有關於無 TTP 式公平交換協定相關技術的發展，首先在數位簽章方面有所突破，2004 年，Chen 等首度提出合併簽章(Concurrent Signature) 的概念[28]，以解決公平合約簽署(Contract Signing) 問題。首先，交換簽章的雙方必須先交換一個具備正確性、可驗證性，以及簽章匿名性的「模糊簽章」(Ambiguous Signature)。之後，其中一方須公佈「關鍵參數」(Keystone)；藉此，驗證者可以如真正的簽章者一般，將兩個不確定簽章者的簽章予以「合併」。透過合併簽章協定，可以實現無 TTP 的公平交換協定，同時也避免頻繁而大量的訊息交換，進而提高公平合約交

換的效率。

Susilo 等[29] 指出，在 Chen 的方法中，若雙方都是誠實的參與者，則在公開關鍵參數之前，任何第三者都可以確定參與雙方簽署訊息的行為；因此，Susilo 等提出完美合併簽章 (Perfect Concurrent Signature)，在關鍵參數被公開之前，即使雙方都是值得信賴的參與者，仍然保有合併簽章簽署者身份的模糊性 (Full Ambiguity)；作法有二，其中之一是以 Schnorr 提出的環簽章為基礎，另一個則是根據雙線性配對理論發展的機制。

隨後，Susilo 等又提出應用雙線性配對所設計的三方合併簽章協定[30]，Chow 等提出兩個基於身份的完美合併簽章方法[31]，Nguyen 等以 Schnorr 的簽章機制為依據，提出非對稱式的合併簽章方法[32]，Tonien 等利用環簽章及雙線性配對方法提出一個多方的合併簽章協定[33]。

然而，在 2007 年，Huang 等指出相關研究[34]中的方法缺乏公平性。具體而言，透過選取某些通訊參數，初始簽章者 A 可以成功地欺騙對應簽章者 B，並且以文獻[29]的方法為基礎，進行修改，提出安全性證明。然而，此一改進方法還是存在不公平性以及安全性的問題[35]，包括：產生合併簽章後，參與雙方都有針對新訊息偽造一個可被驗證為合法簽章的能力，用以欺騙對方，這是協定的不公平性問題，此其一；又或者是參與的雙方都有獨自偽造可被驗證為合法雙方合併簽章的能力，此其二，這是安全性上的問題。

此外，上述合併簽章協定中，一方為初始簽章者，負責選定關鍵參數以及發送個人的模糊簽章；另一方為對應簽章者，配合初始簽章者及傳送個人的模糊簽章，參與的雙方處於不對稱的運作模式，這種模式往往會衍生不公平性的問題。因此， Han 等[36]建立一個對稱式的完美合併簽章方法，以完全對稱的模式，設計參與者的運作方式，並且提出使模糊簽章沒有發送先後次序差異性的方法。

(四)多方公平交換協定

上述協定都是單方面角度對單方面角度進行的研究成果，但實際運作上，以多方公平交換協定的實用性較高。相對於前者，多方公平交換協定設計的困難度更為複雜，目前主要都是以雙方交換協定為基礎，透過多個交換拓撲架構的建置而完成。

舉例而言，Franklin 等以交換式的拓撲架構為基礎，提出多方公平交換協定的分類機制[37]。Bao 等學者[38]以及 Franklin 等學者[37]則提出環形拓撲架構的多方公平交換協定；其中，每一個參與者 e_i $(0 \leq i \leq \mathrm{n}-1)$從 e_i-1 獲得期望訊息，並且向 e_i+1 提供個人的訊息。Franklin 提出的環形拓撲架構是多方協定設計方法中最簡單的一種，但 Gonzalez 等[39]卻指出該方法的不公平問題，因此提出利用矩陣拓撲架構的多方協定；其中，每一個參與者從參與者子集合中得到期望訊息，並向參與者子集合提供個人的訊息。Asokan 等[40]則在同步網路的背景環境下設計一個利用矩陣拓撲交換架構協定。Kremer 等提出線上式 TTP 及離線式 TTP 的多方不可否認性協定[41-43]，只需使用 n 次的兩方協定，效能明顯提升。Onieva 等則針對 Kremer 提出的線上 TTP 多方不可否認性協定[44]，加以改善，使發送方可以對一個接收方發送不同的訊息。

由於多方數位簽章協定的其中一方，必須向所有其他方發送合約簽署，同時也必須接收所有其他方所發送的合約簽署，所以是一個完全圖形的拓撲架構。Asokan 等設計在同步網路下[45]與非同步網路下的多方合約簽章協定[47-48]。Mukhamedov 等提出的多方合約簽章協定[49-50]，更進一步利用私有合約簽署，使發送的訊息量大為降低。

多方公平交換協定大多採取數次兩方交換協定的模式，協定的效能明顯與參與者數量多寡及交換訊息數量有密切的關聯度，因此不適用於大群組間的多方交換。

二、 公平交換協定之安全性分析

首先，針對公平性定義加以說明；其次，就公平交換協定應滿足的安全特性，進行介紹；最後，說明公平交換協定的安全性分析方法。

(一)公平性

公平性的定義一開始是利用計算能力表達的。Even 等針對合約簽署架構提出一個公平性定義[4]，稱為「合併性」 (Concurrency)，就是若其中一方 A 正確地執行協定，則另一方 B 若不提供個人對於合約的簽署，也無法獲得 A 對合約的簽署。Even 等並未對此定義所衍生的問題提出解決方案，但針對交換問題的解決，則提出一個較弱的定義，稱為「近似合併性」(Approximate Concurrency) ，也就是若其中一方 A 正確地執行協定，則 A 可以在協定執行的各個階段中，以相當高的機率，計算出另一方 B 對此合約的簽署，A 在此過程中所花費的計算量，與 B 計算 A 對合約的簽署相當。因此，這個公平性的定義主要是透過計算能力而制定。

而後，在解決合約簽署問題上，Ben 等提出使用機率論定義公平性[7]，方式如下：當其中一方 A 有能力使用另一方 B 認為合約已經為雙方所合併，則 A 佔有優勢。若 A 正確地執行協定，則該合約簽署協定對 A 而言為公平的狀態。

有些學者嘗試找出一個通用的公平性定義，在普遍受認可的非形式化公平性定義中，交換協定公平性的描述為：完成交換協定執行之後，所有相關者均可獲得個人所期望之訊息，或沒有任何人可以獲得任何訊息。因此，上述定義方式僅適用於特定的公平交換協定。

在數位合約簽章下，Asokan 等學者利用賽局理論 (Game Theory) 定義公平性[19]，也就是假設惡意的參與者可以利用一個非法的簽章交換到合法的簽章，則稱該合約簽章交換協定為不公平。Garay 等[51]則提出一個樂觀合約簽署協定的公平性，包含下列：

(1)在其他參與者沒有接收到合約簽署的情況下，一個不誠實的參與者想要接收到一個合法的合約簽署是不可能的。

(2)一個合法的參與者從 TTP 接收到一個取消的資訊後，其他的參與者要接收到一個合法的合約簽署是不可能的。

Franklin 等[24]指出，在公平交換結束時，下列條件必須為真：

(1)若 A、B 與 TTP 皆為誠實的狀況，則 A 可以接收到 B 的資訊，B 也能接收到 A 的資訊。

(2)若 A 與 TTP 為誠實、且 B 為不誠實的狀況，則 B 無法接收到 A 的任何資訊，除非 A 已接收 B 的資訊。

(3)若 B 與 TTP 為誠實、且 A 為不誠實的狀況，則 A 無法接收到 B 的任何資訊，除非 B 已接收 A 的資訊。

(4)若 A 與 B 為誠實的、且 TTP 為不誠實的狀況，則 TTP 無法接收到 A 與 B 的任何資訊。

第四點與 TTP 的機密性有關，只有在金鑰交換時才會用到，但與公平性無關。針對不可否認性協定的公平性，Zhou 等提出定義[15]結束訊息交換程序後，協定可以為訊息來源端與接收方提供對方不可否認的訊息證據 (發送、接收)；執行協定時，不可使其中任一方取得比另一方更多的優勢 (資訊或證據)。

Asokan 在文獻[9]中提出弱公平性的概念，說明某些特定環境下，公平性協定是可以被打破的。在符合弱公平性的協定中，行為良好卻被危害的一方可以透過 TPP 的協助，向外部的仲裁者提出無辜的聲明與證明。若其中一方 A 沒有得到個人期望的訊息，可以向外部仲裁者提出對方 B 確實接收 A 所發送訊息之回條的證明。若執行錯誤行為的一方拒絕合作，TTP 將開立一份證明給 A，取代 A 所丟失的資訊。透過弱公平性，因而得以在公平性與不可否認性協定之間建立一個連結，雖不保證參與者能得到期待的訊息，但至少可以取得另一方也加入交換協定運作的不可否認證據。

除了上述適用於一般公平交換問題的公平性定義，部份安全特性則是針對特定問題所提出，茲列舉如下：

(1)不可否認性：一旦參與協定，任何參與者都無從否認其參與行為。

(2)不可濫用性[51]：無論在任何時間點，參與者都無法向外部任一方證明個人具有終止或成功完成協定的能力，這是 Garay 等學者於 1999 年提出的概念。

(3)以作者的選擇性回條確認電子郵件的問題：這是 Kremer 等提出的概念，稱之為作者的選擇性回條 (Author-based Selective Receipt)；一旦發送者的身份被接收者得知，則後者無法阻止協定自動發送回條給前者的設計。

Kremer[1]不但將交換協定安全性中的一般性定義與模組化定義[10]加以整合，並且主張若有一個安全的交換協定存在，則該協定須滿足以下強制的特性：

(1) 可行性 (Viability)：在通訊通道品質為可靠的情況下，當所有參與者都是誠實的時候，交換一定會成功。

(2) 公平性 (Fairness)：在通訊通道品質為可靠的情況下，完成交換協定後，所有的參與者都可以獲得期待的訊息。

(3) 時間性 (Timeliness)：在通訊通道品質為可靠的情況下，參與者都備在有限的時間內正確執行協定的能力，且具備中止協定、以保持公平性的能力。

(二)公平交換協定之安全性分析

公平交換協定與認證協定的攻擊模式與通訊模式皆不同。以攻擊模式而言，認證協定皆假設遵守 Dolev-Yao 攻擊者模型，協定的誠實參與者總是採取合作的模式完成協定，並且阻止外部攻擊，達到資料的原始認證、身份認證或

金鑰的一致性；因此，參與者的目的在於協助成功地完成協定。公平交換協定則採取參與者彼此互不信任的不合作觀點，阻止對方欺騙自己，且允許參與者中途退出協定。

利用 Z 語言，卿斯漢等學者建立一個用以分析公平交換協定的形式化模型[52]，並且制定出交換項目的形式化定義，此一模型的公平性具有對目標的可追蹤性，因此得以更完整地反映公平交換協定的需求。為了提高協定的效率，對協定詳加檢測、證明與設計，因此提出可適用於公平交換協定的新安全特性—不可濫用性、擬定可適用於可信賴第三方的定義，以及設計安全且效能高的公平交換協定之準則。此外，針對多方環境下的公平交換協定進行分析、並且設計問題進行研究，透過分析協定的訊息來源與交易雙方之間的通道組成、事件及事件間的各種關係，提出一個簡單、精確的一般公平交換協定層次化模型[53]，規範可以反映公平交換協定內在要求的多種安全需求，並藉此針對多方公平交換協定，進行分析、檢測與設計。

參、 研究方法

研究內容主要是探討公平交換協定及其問題延伸，其中包括降低多方公平交換協定的交換回合複雜度問題，設計無 TTP 的公平交換協定、以解決使用 TTP 所造成的低效率與系統負荷增加的問題，及公平交換協定的可證明安全性問題。

一、代表性的公平交換協定

以下列舉三個具有代表性的公平交換協定，分別為雙方的樂觀公平交換協定 (Optimistic Protocol for Fair Exchange)、多方合約簽署協定 (Multi-party Contract Signing Protocol)，以及完美合併簽章協定 (Perfect Concurrent

Signature Protocol)。

(一)樂觀的公平交換協定

以 Asokan 等提出的樂觀公平交換協定[14, 19, 40]為例,參與的雙方首先會嘗試不經由 TTP、而以一己之力完成交換,只有當發生錯誤時,才會要求 TTP 介入，協助完成或終止協定。這種交換雖然還是必須加入 TTP 的輔助，但可以將使用 TTP 所造成的低效率問題，降至最低，實用性較高。

(二)多方合約簽署協定

以 Mukhamedov 等提出的多方合約簽署協定[49-50]為例,牽涉多方的公平交換協定的架構設計，十分複雜，基本上，不外乎利用雙方交換協定，再經由不同的交換拓撲架構設計而成，Mukhamedov 等提出的方法是其中效率最高的一種，同樣屬於樂觀的多方公平交換協定，運作過程必須透過一個公平的第三者完成，且須執行$(n(n-1)\lceil n/2 \rceil+1)$個訊息的傳遞次數後，才能完成最後的交換。這種架構的交換次數顯然與參與者數量有直接的關聯度，實用性較低。

Mukhamedov 等同時還提出私密合約簽章承諾方法(Private Contract Signature Promises，PCS Promises)，其內容如下列所述。

私密合約簽章,是指參與者 P_i 在 m 與 P_j 之間存在一個可信任的第三者 T,其關係表示式為 $\text{PCS}_{P_i}(m, P_j, T)$，以下為其特性：

(1)$\text{PCS}_{P_i}(m, P_j, T)$；其中，$P_i$ 可以被建立、也可以被偽造。

(2)每一個 P_i、P_j 以及 T 都無法區別建立的 P_i 與偽造的 P_i 之間的差異性。

(3)$\text{PCS}_{P_i}(m, P_j, T)$可以被轉換為一個由 P_i 與 T 所組成的可驗證簽章

私密合約簽章承諾方法包含三大組成部份，依序為參與者程序，可信任的第三者中止程序，以及可信任的第三者恢復程序。以下為參與者 P_i 所執行的

程序：

回合 1：

步驟 1：對於所有 $j < i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, 1), P_i, T)$，若其中任何一項未能及時接收，則 P_i 退出。

步驟 2：對於所有 $j > i$，P_i 將 $\mathrm{PCS}_{Pi}((m, 1), P_j, T)$傳送給 P_j。

步驟 3：對於所有 $j > i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, 1), P_i, T)$；若其中任何一項未能及時接收，則 P_i 發出請求中止要求。

步驟 4：對於所有 $j < i$，P_i 將 $\mathrm{PCS}_{Pi}((m, 1), P_j, T)$傳送給 P_j。

回合 r = 2- [n/2] ：

步驟 5：對於所有 $j < i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, r), P_i, T)$；若其中任何一項未能及時接收，則 P_i 發出請求協助要求。

步驟 6：對於所有 $j > i$，P_i 將 $\mathrm{PCS}_{Pi}((m, r), P_j, T)$傳送給 P_j。

步驟 7：對於所有 $j > i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, r), P_i, T)$；若其中任何一項未能及時接收，則 P_i 發出請求協助的要求。

步驟 8：對於所有 $j < i$，P_i 將 $\mathrm{PCS}_{Pi}((m, r), P_j, T)$傳送給 P_j。

回合[n/2] + 1：

步驟 9：對於所有 $j < i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, +1), P_i, T)$及其簽章 $\mathrm{S}_{Pj}(m)$；若其中任何一項未能及時接收，則 P_i 發出請求協助的要求。

步驟 10：對於所有 $j \neq i$，P_i 將 $\mathrm{PCS}_{Pi}((m, \lceil n/2 \rceil + 1), P_j, T)$及其簽章 $\mathrm{S}_{Pi}(m)$傳送給 P_j。

步驟 11：對於所有 $j > i$，P_i 等待來自 P_j 的私密合約簽章承諾 $\mathrm{PCS}_{Pj}((m, +1), P_i, T)$及其簽章 $\mathrm{S}_{Pj}(m)$；若其中任何一項未能及時接收，則 P_i 發出請求協助的要求。

(三)完美的合併簽章協定

樂觀公平交換協定的提出，雖然可以將使用 TTP 所造成的低效率問題降至最低，但 TTP 在實際應用中仍存在諸多待解決的問題。因此，Susilo 等學者嘗試提出可免除仲裁單位的公平交換協定之設計方法，並且率先於公平合約簽章的背景下，獲得突破性的進展，提出完美的合併簽章協定[30-31,33-34]，其關鍵技術在於將 Schnorr 提出的環簽章架構—ASIGN 納入協定內容的設計中。以下為合併簽章協定，介紹如下：

1. 合併簽章演算法

(1) SET UP：

步驟 1：選取兩個大質數 p 與 q，以及一個生成數 $g \in Z_p^*$，其階度為 q。

步驟 2：產生一個密碼雜湊函數 H1: {0, 1}*→ Z_q^*。

步驟 3：設定 $M = K = Z_p^*$，且 $F = Z_q^*$。

步驟 4：參與者 A 選取其私鑰 $xA \in Z_q^*$，並且計算對應公鑰 $y_A = g^{x_A}$ 。

步驟 5：參與者 B 選取其私鑰 xB，並且計算對應公鑰 $y_B = g^{x_B}$ 。

(2) ASIGN：

步驟 1：取得 $\hat{s} \in F$ 與 $m \in M$。

步驟 2：選擇一個任意數 $\alpha \in Z_q^*$。

步驟 3：計算 $c = H1(m \| g^{\alpha} y_j^{\hat{s}})$。

步驟 4：計算 $\tilde{s} = (\alpha - c) x_i^{-1} (\bmod q)$ 。

步驟 5：輸出 $\sigma = (c, \hat{s}, \tilde{s})$ 。

Averify 演算法為(σ, y_i, y_j, m)，其中 可用以驗證 $c = H_1 (m \| g^c y_i^{\tilde{s}} y_j^{\hat{s}})$的正確性；若等式成立，則輸出 accept；否則，輸出 reject。

verify 演算法為(k, S)，其中，$k \in$K 為關鍵參數、$S = (m, \sigma, y_i, y_j)$且 $\sigma = (c, \hat{s}, \tilde{s})$ 。

verify 演算法的作用，在於檢查 k 執行關鍵參數驗證演算法(Keystone Verification Algorithm)的有效性；若驗證值為 reject，則輸出 reject；否則，執行 Averify (S)。此外，verify 的輸出值等同 Averify。

2. 合併簽章協定

(1) A 執行參與合併簽章程序如下：

步驟 1：選取訊息 m_A∈M。

步驟 2：隨機挑選一個關鍵參數(keystone) k∈K，並且設定 $s_2 = H_1(k)$。

步驟 3：執行 $\sigma_A \leftarrow ASIGN(y_A, y_B, x_A, s_2, m_A)$，得到 $\sigma_A = (c, s_1, s_2)$。

步驟 4：選擇一個任意數 $t \in Z_q^*$，並且計算 。

步驟 5：公開 $(m_A, \sigma_A, \hat{t})$，且傳送給 B。

(2) B 執行參與合併簽章程序如下：

步驟 1：測試 Averify $(\sigma_A, y_A, y_B, m_A)$ 是否為 accept，用以驗證 σ_A 的有效性；否則，中止 B 的執行程序。

步驟 2：選取訊息 m_B∈M。

步驟 3：計算 $r \leftarrow \hat{t}^{x_B}$ ，並且設定 $s_2' \leftarrow s_2 + r \pmod q$。

步驟 4：執行 $\sigma_B \leftarrow ASIGN(y_B, y_A, x_B, s_2', m_B)$，得到 $\sigma_B = (c', s_1', s_2')$。

步驟 5：公開 (m_B, σ_B)，且傳送給 A。

(3) A 執行合併之簽章程序如下：

步驟 1：測試 Averify $(\sigma_B, y_B, y_A, m_B)$的輸出值是否為 accept；否則，中止協議。

步驟 2：計算 $r = s_2' - s_2 \pmod q$。

步驟 3：驗證 $r = y_b^{tx_A}$ 是否成立；若等式不成立，則中止協議。

步驟 4：對資訊 $\Gamma \leftarrow SEQDL\,\{\gamma : r = y_B^{t\gamma} \wedge \hat{t} = g^{t\gamma} \wedge y_A = g^{\gamma}\}\,(k)$進行簽署。

步驟 5：公開關鍵參數 (keystone) $\kappa = (k, r, t, \Gamma)$。

二、 公平交換協定研究

本計畫提出公平交換協定的說明，透過通訊時間複雜度的分析、不透過一個公正的第三方運作機制的設計方法，以及運用賽局理論為基礎所建構的安全性分析模式。針對可免除仲裁單位的公平交換協定之設計、高效率的多方公平交換協定之研究、公平交換協定的安全性分析，進行介紹如下:

(一)可免除仲裁單位的公平交換協定之設計

若採取無仲裁單位的交換協定,則只能達到弱公平性,並不具備強公平性。客觀而言，目前的電子交易應用大多數屬於商務領域，不涉及高度敏感的資料，並不需要採納嚴謹程度較高的強公平性，也就是在交換資料的過程中，受損害的一方可以提供對方不誠實行為的證據給予裁決方，使個人權益得以在事後獲得補償、不致於受損，並使對方得到懲罰，也就是所謂弱公平性的安全性定義，實際應用上的商務活動大抵也採取類似的運作法則。

目前，多數公平交換協定大多是透過 TTP 的運作模式。在理論研究的理想狀態下，一般均假設 TTP 確實可以以公正客觀的立場存在；然而，在實際應用中，TTP 及其聲譽的建立，誠非易事。其一，在完全分散式的網路應用中，不會只存在一個 TTP；其二，即使只有一個 TTP，也還是由某一實體機構所擔任，也就是或多或少會存在人為運作的風險，因而使其可信度大打折扣；其三，維護及雇用 TTP 協助運作的成本，都必須支用時間與成本費用的額外負擔，舉例而言，Asokan 等提出的樂觀公平交換協定，在交換運算時，必須使用 TTP 的相關參數，這些都是額外的計算成本。

現行的公平交換協定大都以樂觀公平交換的概念為基礎,並且無可免俗的採取 TTP 的運作模式。只有針對特定需求的公平合約簽署問題，才提出不透過 TTP 運作的合併簽章協定,主要是因為這一類協定交換的內容是數位簽章、而非特定資訊之故；合併簽章協定的設計主要透過環簽章而得以實現。透過

具備簽章匿名性與合併解除機制的設計，進而激發不透過 TTP 運作的公平合約簽署的設計概念。

公平交換協定的設計，必須考慮到交換資料的普及性，因此，必須以新的資訊安全技術實現無 TTP 的公平交換協定。本計畫針對合適的資安技術進行研究，設計可免除仲裁單位的各種公平交換協定，實現弱公平性。

(二)高效率的多方公平交換協定之研究

不論是環形拓撲的交換架構、矩陣拓撲的交換架構、或是完全拓撲的圖形交換架構，多方公平交換協定的基本原理，都是透過一系列的雙方交換，完成多方交換的過程；交換回合的複雜度與參與者個數成正相關，例如，上述章節中提到的 Mukhamedov 多方合約簽署協定，不但必須使用 $n(n-1)\lceil n/2 \rceil + 1$ 個訊息的傳遞完成交換過程，而且訊息的交換具有先後順序，無法同時處理，正因如此，實用性往往受到相當大的質疑。因此，運用特定的公平交換協定，研究多方交換的機制，避免採取兩兩交換的方式，以減少交換的回合數，達到常數回合的交換複雜度，提出實用且高效能的多方公平交換協定。

(三)公平交換協定的安全性分析

公平交換協定的分析方法，包括隨機預言模型(Random Oracle Model)、標準模型下通過相關規定的證明方法、Z 語言邏輯方法、串空間分析方法等。雖然協定的安全性可從各種不同的角度切入，加以證明，但上述方法無法辨別參與者是否按照協定的規則執行參與的程序，因此並未能確實反應公平交換的特性。

在電子商務應用中，理性的參與者採取的行為，一定是使個人利益達最大化的決策。因此，可以將賽局理論的觀點導入公平交換協定的分析與設計上。賽局理論可以符合公平交換的特性，賽局參與者為通訊雙方，並且假定雙方均為理性的參與者，則公平交換的過程本身即為一個以達各方最大利益為目

標的多方賽局。此一過程可切合非合作賽局的條件，非合作賽局論主張納許均衡原理；該原理強調個人追求最大收益、最小損害的邏輯策略。假設賽局中有 n 個參與者，則存在一個稱之為納許均衡的合作點，意指賽局的每一個參與者都認為在獲取其他參與者策略的情況下，個人會選擇最佳化的策略，以回應對手的策略，也就是所有人都採取最大限度地達到個人的最大利益。因此，在將賽局理論的觀點導入公平交換協定的設計與分析時，首先必需解出協定參與者之間的納許均衡點，再以此均衡點規範參與者的行為，使其惟有嚴謹地按照協定規則執行，方能獲得最大的利益。此外，共謀攻擊也是公平交換協定安全性分析中常見的一大問題；事實上，只要協定存在多個參與者，即無可豁免於共謀攻擊的問題。因此，本計畫針對不同的共謀攻擊方式進行研究，包括惡意的參與者、不公正的 TTP 共謀攻擊，以及惡意參與者的子集合共謀攻擊問題等，提出可以防止共謀攻擊的公平交換協定。

肆、 結論

本計畫經由整合後設計出一套實用性高的多方公平交換協定，並且提出安全性證明。在設計無 TTP 公平交換協定的同時，必須先解決合併簽章協定中的公平交換問題，方能實現可交換任意項目的無 TTP 公平交換協定。提高效能部份，設計出符合常數回合交換的多方公平交換協定。安全性分析部份，採用賽局理論對公平交換協定進行分析，並且提出共謀攻擊問題的解決方法，設計防止共謀攻擊的公平交換協定。

首先說明無 TTP 公平交換協定，適當的資訊安全技術將是設計無 TTP 公平交換協定的關鍵。而後合併簽章協定的主要研究，在於使用環簽章解決合約簽署中的公平交換問題，並將簽署者與簽署者的訊息予以合併。因此，本計畫將安全多方計算、共享秘密、同態加密、模糊傳送等密碼架構導入公平交換協定，藉由其特性實現無 TTP 公平交換協定的設計。

其次本計畫設計出新的多方公平交換協定，避免使用兩兩交換訊息的模式，以提高執行效能。而後安全多方計算的技術發展方面，已經可以透過加法與乘法的組合運算計算任意函數。

最後則是分析並解決共謀攻擊問題，在公平交換協定的運作過程中，多個參與者所擁有的資訊比單一參與者所擁有的更多。合謀者可能在協定執行過程中利用所能掌握的資訊計算出公正參與者的交換方法，因而導致不公平問題的發生。然而，共謀攻擊可能的防範方式有以下兩種，第一種方式是限制惡意參與者的數量，換言之，即確保協定包含一定數量的公正參與者，但這種方法適合應用在不公開的共用方法交換協定上，不公開的共用方法則可以透過安全多方計算實現，若惡意的參與者數量少於門檻值，則無法採取攻擊；第二種方式是採取追蹤的方式，也就是賦予參與者的每一個行為可追蹤性，一旦發生惡意的攻擊行為，就可以憑藉可追蹤性追蹤惡意的共謀攻擊者；這種方法屬於被動防禦的一種，使用範圍較廣泛，但會拖累協定的效能。

參考文獻

[1] S. Kremer, O. Markowitch and J. Zhou, “An Intensive Survey of Fair Non-Repudiation Protocols,” *Computer Communications*, Vol. 25, No. 17, pp. 1606-1621, 2002.

[2] M. Blum, “How to Exchange Secret Keys,” *ACM Transactions on Computer Systems*, Vol. 1, No. 2, pp. 175-193, 1983.

[3] T. Tedrick, “Fair Exchange of Secrets,” *Lecture Notes in Computer Science*, Vol. 196, pp. 434-438, 1985.

[4] S. Even, O. Goldreich and A. Lempel, “A Randomized Protocol for Signing Contracts,” *Communications of the ACM*, Vol. 28, No. 6, pp. 637-647, June 1985.

[5] D. Boneh and M. Naor, “Timed Commitments,” *Lecture Notes in Computer Science,* Vol. 1880, pp. 236-254, 2000.

[6] M. O. Rabin, “Transaction Protection by Beacons,” *Computer and System Sciences,* Vol. 27, No. 2, pp. 256-267, 1983.

[7] M. Ben-Or, O. Goldrich, S. Micali and R. Rivest, “A Fair Protocol for Signing Contracts”, *IEEE Transactions on Information Theory* , Vol. 36, No. 1, pp. 40-46, 1990.

[8] J. Zhou, “Non-Repudiation,” [PhD thesis], University of London, 1997.

[9] N. Asokan, “Fairness in Electronic Commerce,” [PhD thesis], University of Waterloo, Canada, 1998.

[10] S. Kremer, “Formal Analysis of Optimistic Fair Exchange Protocols,” [PhD thesis], Universite Libre de Bruxelles, 2003.

[11] A. Bahreman and J. D. Tygar, “Certified Electronic Mail,” *In Proceedings of the Network and Distributed Systems Security Conference (NDSS 1994),* pp. 3-19, 1994.

[12] J. Zhou and D. Gollmann, “Certified Electronic Mail,” *Lecture Notes in Computer Science,* Vol. 1146, pp. 160-171, 1996.

[13] T. Coffey and P. Saidha, “Non-repudiation with Mandatory Proof of Receipt,” *ACM Computer Communication Review,* Vol. 26, No. 1, pp. 6-17, 1996.

[14] N. Asokan, M. Schunter, and M. Waidner, “Optimistic Protocols for Fair Exchange,” *4th ACM Conference on Computer and Communications Security,* Zurich, Switzerland, pp. 8-17, April 1997.

[15] J. Zhou and D. Gollmann, “An Efficient Non-repudiation Protocol,” *10th IEEE Computer Security Foundations Workshop,* pp. 126-132, June 1997.

[16] N. Asokan, V. Shoup, and M. Waidner, “Asynchronous Protocols for Optimistic Fair Exchange,” *IEEE Symposium on Research in Security and*

Privacy, pp. 86-99, 1998.

[17] S. Kremer and O. Markowitch, "Optimistic Non-Repudiable Information Exchange," *21st Symposium on Information Theory in the Benelux*, pp. 139-146, 2000.

[18] S. Micali, "Certified E-mail with Invisible Post Offices," *An invited presentation at the RSA 1997 Conference*.

[19] N. Asokan, V. Shoup, and M. Waidner, "Optimistic Fair Exchange of Digital Signatures," *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 4, pp. 593-610, 2000.

[20] G. Ateniese, "Efficient Verifiable Encryption and Fair Exchange of Digital Signatures," *6th ACM Conference on Computer and Communications Security*, pp. 138-146, November 1999.

[21] O. Markowitch and S. Saeednia, "Optimistic Fair-exchange with Transparent Signature Recovery," *5th International Conference on Financial Cryptography*, Vol. 2339, pp. 339-350, 2002.

[22] 周永彬、張振峰、卿斯漢、季慶光，《基於 RSA 簽名的優化公平交換協議》，軟體學報, Vol. 15, No. 7, pp. 1049-1055, 2004.

[23] A. Nenadic, N. Zhang, B. M. G. Cheetham and C. A. Goble, "RSA-based Certified Delivery of E-goods Using Verifiable and Recoverable Signature Encryption," *Journal of Universal Computer Science*, Vol. 11, No. 1, pp. 175-192, 2005.

[24] M. K. Franklin and M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Party," *4th ACM Conference on Computer and Communications Security*, pp. 1-5, 1997.

[25] 卿斯漢，《電子商務協定中的可信第三方角色》，軟體學報, Vol. 14, No. 11, pp.1936-1943, 2003.

[26] S. Even and Y. Yacobi, "Relations among Public Key Signature Systems," Technical Report 175, Technion, Haifa, Israel, March 1980.

[27] H. Pagnia and F. C. Gartner, "On the Impossibility of Fair Exchange without a Trusted Third Party," Technical Report TUD-BS-1999-02, Darmstadt University of Technology, Department of Computer Science, Darmstadt, Germany, March 1999.

[28] L. Chen, C. Kudla and K. G. Paterson, "Concurrent Signatures," *Advances in cryptology*, Vol. 3027, pp. 287-305, 2004.

[29] W. Susilo, Y. Mu and F. Zhang, "Perfect Concurrent Signature Schemes," *Information and Communications Security Conference*, Vol. 3269, pp. 14-26, 2004.

[30] W. Susilo and Y. Mu, "Tripartite Concurrent Signatures," *Security and privacy in the age of ubiquitous computing*, Vol. 181, pp. 428-441, 2005.

[31] S. S. M. Chow and W. Susilo, "Generic Construction of Identity-based Perfect Concurrent Signatures," *Information and Communications Security*, Vol. 3783, pp. 194-206, 2005.

[32] K. Nguyen, "Asymmetric Concurrent Signatures Khanh Nguyen," *Information and Communications Security*, Vol. 3783, pp. 181-193, 2005.

[33] D. Tonien, W. Susilo and R. Safavi-Naini, "Multi-Party Concurrent Signatures," *Information Security Conference*, Vol. 4176, pp. 131-145, 2006.

[34] Z. Huang, R. Huang and X. Lin, "Perfect Concurrent Signature Protocol," *International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Vol. 1, pp. 467-472, 2007.

[35] 蔣瀚、徐秋亮、張忠，《一個完美併發簽名協議的分析與改進》，*北郵學報*，2009, Vol.32, No. 2, pp. 115-118, 2009.

[36] J. Han, X. Qiuliang and Z. Bo, "Perfect Concurrent Signature Protocol for

Symmetric Participants," *International Conference on Computational Intelligence and Security Workshops,* Vol. 2, pp. 273-277, December 2008.

[37] M. Franklin and G. Tsudik, "Secure Group Barter: Multi-party Fair Exchange with Semi-trusted Neutral Parties," *Proceedings of Financial Cryptography Conference,* Vol. 1465, pp. 90-102,1998.

[38] F. Bao, R. Deng, K. Q. Nguyen and V. Varadharajan, "Multiparty Fair Exchange with an Off-line Trusted Neutral Party," *Workshop on Electronic Commerce and Security,* Florence, Italy, pp. 858-862, 1999.

[39] N. Gonzalez-Deleito and O. Markowitch, "Exclusion-freeness in Multi-party Exchange Protocols," *5th Information Security Conference,* Vol. 2433, pp. 200-209, 2002.

[40] N. Asokan, M. Schunter and M. Waidner, "Optimistic Protocols for Multiparty Fair Exchange," IBM Research Report RZ 2892, IBM Zurich Reaserch Laboratory Zurich, December 1996.

[41] S. Kremer and O. Markowitch, "A Multi-party Non-repudiation Protocol," *15th International Conference on Information Security,* Beijing, China, pp. 271-280, August 2000.

[42] S. Kremer and O. Markowitch, "Fair Multi-party Non-repudiation," *International Journal on Information Security,* Vol. 1, No. 4, pp. 223-235, July 2003.

[43] O. Markowitch and S. Kremer, "A Multi-Party Optimistic Non-Repudiation Protocol," *International Conference on Information Security and Cryptology,* Vol. 2015, pp. 109-122, December 2000.

[44] J. Onieva, J. Zhou, M. Carbonell and J. Lopez, "A Multi-party Non-repudiation Protocol for Exchange of Different Messages," *Proceedings of the 18th IFIP International Information Security Conference,* Greece, May

2003.

[45] N. Asokan, B. Baum-Waidner, M. Schunter and M. Waidner, “Optimistic Synchronous Multi-party Contract Signing,” Research Report RZ 3089, IBM Research Division, December 1998.

[46] J. A. Garay and P. MacKenzie, “Abuse-free Multi-party Contract Signing,” *International Symposium on Distributed Computing*, Vol. 1693, pp. 151-166, 1999.

[47] B. Baum-Waidner and M. Waidner, “Round-optimal and Abuse-free Optimistic Multi-party Contract Signing,” *Automata, Languages and Programming*, Vol. 1853, pp. 524-535, July 2000.

[48] A. Nenadic, N. Zhang, B. M. G. Cheetham and C. A. Goble, “RSA-based Certified Delivery of E-goods Using Verifiable and Recoverable Signature Encryption,” *Journal of Universal Computer Science*, Vol. 11, No. 1, pp. 175-192, 2005.

[49] A. Mukhamedov and M. D. Ryan, “Improved Multi-party Contract Signing,” *Financial Cryptography and Data Security*, Vol. 4889, pp. 179-191, 2007.

[50] A. Mukhamedov and M. D. Ryan, “Fair Multi-party Contract Signing using Private Contract Signatures,” *Information and Computation*, Vol. 206, No. 2-4, pp. 272-290, 2008.

[51] J. A. Garay, M. Jakobsson and P. MacKenzie, “Abuse-free Optimistic Contract Signing,” *Advances in Cryptology-Crypto 1999*, Vol. 1666, pp. 449-466, 1999.

[52] 卿斯漢、李改成，《公平交換協定的一個形式化模型》，*中國科學 E 輯*,Vol. 35, No. 2, pp. 161-172, 2005.

[53] 卿斯漢、李改成，《多方公平交換協定的形式化分析和設計》，*中國科學 E 輯*, Vol. 36, No. 6, pp. 598-616, 2006.

近三年已發表之相關期刊及研討會論文

(A) 期刊論文

[1] Y. F. Chung, T. L. Chen, **T. S. Chen,** and C. S Chen, A Study on Efficient Group-Oriented Signature Schemes for Realistic Application Environment, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 4, pp. 2713-2728, April 2012. (SCI, EI, IF:1.664)

[2] Y. F. Chung, T. L. Chen, C. S. Chen, and **T. S. Chen**, The Study on General Secure Multi-Party Computation, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 1, pp. 1-10, Jan. 2012. (SCI, EI, IF: 1.664)

[3] C. H. Liu, Y. F. Chung, T. W. Chiang, **T. S. Chen**, and S. D. Wang, A Mobile Agent Approach for Secure Integrated Medical Information Systems, accepted by the *Journal of Medical Systems*, 2011. (SCI, IF：1.064)

[4] C. H. Liu, Y. F. Chung, **T. S. Chen**, and S. D. Wang, Mobile Agent Application and Integration in Electronic Anamnesis System, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1009-1020, 2011. (SCI, IF: 1.064)

[5] Z. Y. Wu, Y. F. Chung, F. Lai, and **T. S. Chen**, A Password-Based User Authentication Scheme for the Integrated EPR Information System, *Journal of Medical Systems*, Vol. 36, No. 2, pp. 631-638, April, 2012. (SCI, IF: 1.064)

[6] C. H. Liu, Y. F. Chung, **T. S. Chen**, and S. D. Wang, The Enhancement of Security in Healthcare Information Systems, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1673-1688, June, 2012. (SCI, IF：1.064)

[7] T. L Chen, Y. L. Yu, Y. F. Chung, and **T. S. Chen**, Grey-Hierarchy Selection System for Businesses Introducing Electronic Commerce, *African Journal of Business Management,* Vol. 6, No. 22, pp. 6339-6346, May, 2012. (SSCI, IF:1.105)

[8] C. H. Liu, Y. F. Chung, **T. S. Chen**, and S. D. Wang, The Design of ID-Based Access Control System with Time-Sensitive Key for Mobile Agent's Migration, *International Journal of Innovative Computing, Information and*

Control, Vol. 7, No. 12, pp. 7077-7090, Dec 2011. (SCI, EI, IF：1.664)

[9] Z. Y. Wu, Y. F. Chung, F. Lai, **T. S. Chen**, and H. C. Lee, An Enhanced Password-based User Authentication Scheme for Grid Computing, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 7, pp. 3751-3760, July 2011. (SCI, EI, IF: 1.664)

[10] Y. F. Chung, Y. T. Chen, T. L. Chen, and **T. S. Chen**, An Agent-Based English Auction Protocol Using Elliptic Curve Cryptosystem for Mobile Commerce, *Expert Systems with Applications*, Vol. 38, pp. 9900-9907, August, 2011. (SCI, EI, IF: 1.924)

[11] C. H. Liu, Y. F. Chung, **T. S. Chen**, and S. D. Wang, An ID-Based Access Control in a Hierarchical Key Management for Mobile Agent, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 3, pp. 1443-1456, March 2011. (SCI, EI, IF: 1.664)

[12] Victor R. L. Shen, Y. F. Chung, **T. S. Chen**, and Y. A. Lin, A Blind Signature Based on Discrete Logarithm Problem, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 9, pp. 5403-5416, Sep 2011. (SCI, EI, IF: 1.664)

[13] J. Y. Huang, Y. F. Chung, **T. S. Chen**, and I. E. Liao, A Secure Time-Bound Hierarchical Key Management Scheme based on ECC for Mobile Agents, *International Journal of Innovative Computing, Information and Control*, Vol. 6, No. 5, pp. 2159-2170, May 2010. (SCI, EI, IF：1.664)

[14] Victor R. L. Shen, Y. F. Chung, and **T. S. Chen**, A Novel Application of Grey Data Generating Techniques to Information Security, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.2, pp. 501-508, Feb. 2010. (SCI, EI, IF: 1.664)

[15] F. G. Jeng, T. L. Chen, and **T. S. Chen**, An ECC-Based Blind Signature Scheme, *Journal of Networks*,Vol. 5, No. 8, pp. 921-928. November, 2010. (EI)

(B) 研討會論文

1. Z. Y. Wu, D. L. Chiang, T. C. Lin, Y. F. Chung and **T. S. Chen**, A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network, *26th International Conference on Advanced Information Networking and Applications* (*AINA 2012*), pp. 25-28, Fukuoka, Japan, March, 2012.

2. Y. F. Chung, M. H. Kao, T. L. Chen, and **T. S. Chen**, Efficient date-constraint access control and key management scheme for mobile agents, *IMECS 2010*, pp. 252-257 , Hong Kong, China, March 17-19, 2010. (EI)

3. C. H. Liu, Y. F. Chung, J. D. Jhuo, **T. S. Chen**, and S. D. Wang, A Novel Time-bound Hierarchical Key Assignment Scheme for Mobile Agent, *IMECS 2010*, pp. 258-263 , HongKong, China, March 17-19, 2010. (EI)

出席國際會議報告

2012 年 03 月 26~29 日

報告人姓名	陳澤雄	職稱	資管系教授
會議期間	2012.03.26 至 2012.03.29		
會議地點	日本九州福岡工業大學		
會議名稱	2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2012)		
發表論文題目	Secure Authentication Scheme for Supporting Healthcare in Wireless Sensor Networks		

與會心得

今年(2012)參與第26屆International Conference on Advanced Information Networking and Applications Workshops (WAINA 2012），係於2012年3月26-29日在日本九州福岡工業大學舉行。研討會的焦點是針對先進網路技術和應用為主題，提供國際各界的研究專家學者們共同聚會發表新知及交換想法。本次吸引超過100多位專家學者參加亦 是來自20多個國家- 如台灣、日本、韓國、香港、美國、新加坡…等國家的學者專家共計100多篇論文。

我發表論文的時段是當地時間2012年03月26日下午14點00分至15點30分，場次為W-HWISE-S2，發表主題是有關於Sensor and Ad-Hoc Applications，由Keio University, Japan教授Hiroshi Shigeno擔任主持人，該場次總共安排4篇paper發表，我發表論文順序為第二位，報告時間約20分鐘，論文發表完畢後，會中主持人、與會學者提出許多問題討論，會場之討論氣氛相當的熱烈，大家也彼此交換研究心得，增廣見聞並獲取新知。

在此次的研討會議中，邀請到國際知名專家學者與會並發表專題演講，分享最先進的研究成果，除了參加自己的W-HWISE-S2那一場發表會外，亦選擇參加幾場其他主要議題，分享學者們的研究成果，如Cryptography, Authentication and Security、Mesh Networks、Video Streaming and Life Streaming等相關領域。此次研討會讓我受益良多，使個人得到很多新的教學方法與技巧之啟發，相信這些寶貴之技法將可做為今後推動所內教學改善及方法精進與參考，除此之外，透過學術交流的國際會議，在研究的方向上也有很大助益，藉由認識各方領域的研究同好，不但開拓了新的視野也能瞭解未來研究的方向，更有助於引導我國與世界接軌。

Secure Authentication Scheme for Supporting Healthcare in Wireless Sensor Networks

[1]Tsung-Chih Hsiao, [2]Yu-Ting Liao, [3]Jen-Yan Huang, [3]Tzer-Shyong Chen, [1]Gwo-Boa Horng
[1]Department of Computer Science and Engineering, National Chung Hsing University, Taichung, Taiwan
[2]Department of Management, Southampton University, United Kingdom
[3]Department of Information Management, Tunghai University, Taichung, Taiwan
E-mail: arden@thu.edu.tw

***Abstract*—In recent years, the average life expectancy of people is extended and total fertility rate is dropped, bring our country into an aged society. Due to this phenomenon, how to provide the aged people and the patients with chronic diseases a suitable environment of health care has become a critical issue currently. Therefore, we propose a new scheme that applies health care within wireless sensor networks in which sensor nodes can measure the vital signs of the aged people and the patients. The vital signs for blood pressure, pulsation, and body temperature measured by sensor nodes would be transmitted to mobile devices of medical staff and system administrator. Sensor node readings enable the medical staff to understand the conditions of the patients in real time which improves the quality of health care for the patients. According to the personal data protection act, the vital signs of the patients can only be accessed by the authorized medical staff. In order to protect the privacy of patients, the administrator will verify the identity of medical staff through the mobile device with smart card and password. Accordingly, only the verified medical staff can obtain the vital signs such as blood pressure, pulsation, and body temperature of the patients. Besides, the scheme includes a characteristic of time-bounded, and then the medical staffs can obtain the vital signs without re-authenticating and re-login into the system in a period of time. Consequently, the time-bounded property increases the work efficiency of the system administrator and user.**

Keywords-Wireless Sensor Networks; Sensor Node; User Authentication; Smart Card;

I. INTRODUCTION

Our research will use the wireless sensor network to construct a medical environment with security system. First of all, we will use the sensor nodes to collect the patient's physiological information. When the doctor needs that information, he can access to the system to get the data through the PDA or other devices which support wireless network. In the process of data transmission, we propose a high-security method to protect the information from hacking. In this paper, we want to achieve the following purposes:

(1) Enhance the Medical Quality: Doctor can save more time when he gets the patients' physiological information directly through PDA.

(2) Data Accuracy: Because sensor nodes will collect data and transmit it to the data collector, there is no typo going to happen.

(3) Keep Monitoring: Doctor can keep monitoring the patients' physiological information through wireless sensor nodes. Therefore, doctor will be notified quickly if a patient feels not so well.

(4) Protect the Privacy: In our research, we have to make sure only legal user can receive patients' physiological information.

(5) Limited Time: We limit a period of time, and the legal user can't get the information if the time is passed.

The organization of this paper is as follows: Section 2 will introduce encryption and authentication technology background, and then compare other papers based on user authentication. Section 3 will explain the method proposed in this paper. First, we propose a medical environment using a wireless sensor network, and how this method works when a user wants to get the patients' physiological information. Section 4 will conduct the analyses of safety, performance and power. Section 5 is the conclusion of this paper.

II. RELATED WORKS

A. *Encryption System*

Cryptography is a special way to let illegal user be unable to read the message. Therefore, we can through encryption to transfer the original message to the ciphertext to protect some important messages. Similarly, we can decrypt the ciphertext to read the message. Besides, cryptography has these three properties–confidentiality, integrity and non-repudiation. We can use these properties to compose different types of network services.

In cryptography system, it can be divided into symmetric encryption system and asymmetric encryption system according to the number of keys.

In addition to the above described cryptography system, there are some encryption technologies without the key, such as one-way hash function. It is consisted of one-way and hash function [1]. According to one-way function, it is quite difficult to calculate $F(X)$ to get X but is quite easy on the contrary. And hash function means transferring the original message to a fixed-length string, called the message digest. Although we can easily calculate a message digest by one-way hash function encryption technology, we can not get the original message based on this message digest. A good one-way hash function must have the characteristic of Collision Resistance, which means there will not appear the same message digest if the original message is different. One-way hash function is often used in signature.

B. User Authentication

With the development of mobile communications networks, more and more users can through mobile devices to connect the Internet. And User Authentication is used to identify whether the user is legal or not to prevent hackers. Generally speaking, User Authentication can be divided into three parts, as shown below.

(1) Biological Verification: Biological Verification is through the physiological differences to conduct the authentication. Such as: Finger Print, Veins, Retina, Iris, Palm Shape, Voice and Handwriting.

(2) Password Authentication: Password Authentication is through user ID and password to do the verification. It is usually combine IC Card to increase the security.

(3) Document Verification: Document Verification is through user's document to verify the legality. Bar Code, Magnetic Card, IC Card, Smart Card and RFID technology are common way to verify.

In the above three user authentication, Password Authentication is the most widely used, such as [2–7]. We can divide Password Verification into two categories, namely system needs to store the password table and system does not need to store passwords. The first system includes direct-storage password method, one-way function, password encryption, password salt, challenge response and time stamp. The second system contains authentication and encryption method.

Among them, Time Stamp method is that user's ID, password and the login time will be encrypted together. When receiving the ciphertext, the system will decrypt it and get the login time. Then the system will compare the time with the legal time. If the time is correct, the system will go further to verify the user's ID and password. Due to the time is very important in medical field, we record physiological information, such as blood pressure or heart rate, with time to prevent forgery and tampering. In our approach, time stamp method will be used.

C. Authentication Procedure

User Authentication can be divided into three steps, as shown in followings:

(1) Registration Phase: When a user wants to use a system, he has to apply an account. After the manager approve, the user will be gave for authentication information, such as smart cards or password. Then the user has the permission to access the system.

(2) Verification Phase: During this phase, managers will verify the user's information, such as accounts, passwords or smart cards. Only legal user can access to this system.

(3) Login Phase: When a user wants to login to system, he is required to give manager the information used to verify identity.

In wireless network, It is quite important to control the data access. In order to let only the legal user accesses to get the data, we use User Authentication to protect our system. Followings are some papers about User Authentication in wireless sensor network:

C.1. Dynamic User Authentication Scheme for Wireless Sensor Networks

In 2006, Wong et al [8] proposed a dynamic user authentication method for wireless sensor network. It uses the password authentication technology, such as one-way hash function and exclusive OR (Exclusive-OR), and through IEEE 802.15.4 wireless network transmission standard to protect the security of transmission. User can use handheld mobile devices to access data from sensor nodes. Before accessing, the user has to register and gets ID and password. Then the user can login to Sensor Login-Node to access data with authenticated user's identity information. In a limited time, user can login the system several times. However, when the time expires, user needs to register again.

C.2. Improved Dynamic User Authentication scheme for Wireless Sensor Networks

In 2007, Tseng et al [9] proposed a method to improve security based on [8]. They think [8] is easily subjected to Replay Attack and Impersonation Attack. Hence, Tseng et al improve the safety to resist those attacks. In addition, the method also allows the user to change the password. Through one-way hash function, the user's password can be encrypted and well protected.

C.3. Two-Factor User Authentication in Wireless Sensor Networks

In [8] and [9], the system needs to provide additional space to store the user's ID and password after registration. Because [8] and [9] both includes the password table, these two methods are likely to get Stolen Verifier Attack. Therefore, in 2009 Das [10] proposed a two-factor user authentication method to provide a more secure authentication. This method combines smart card with password.

The system does not need to save the password table. It just needs to give a smart card which has the relevant authentication information to the user. In this way, the user and the sensor nodes only use one-way hash function to encrypt and decrypt. Through a hash function, sensor nodes can save more computing time and power consumption, making this method efficiency.

C.4. Improved Two-Factor User Authentication in Wireless Sensor Networks

In 2010, Khan et al [11] proposed an improved authentication based on [10]. They think [11] can not resist Insider Attack and is incapable of changing password. In the same year, Vaidya et al [10] proposed a further improvement of two-factor user authentication. This authentication also combines smart card with password to improve the security. Besides, this method will bring up alternative solutions according to various attacks, such as smart cards stolen.

D. Smart Card

Smart card is an IC chip embedded in a plastic card. It is capable of memo ring, recognizing, encryption/decryption and transmission. Currently, the smart card can be divided into two categories, namely IC memory card and CPU card. The former one only has the function of storing data, such as public telephone cards. The latter one is able to execute data processing, operate and has anti-theft system, such as IC telephone card, IC card, Easy Card and so on.

Smart card has the characteristics as following:

(1) Data Access and Authentication: Each smart card has different PIN(Personal Identity Number). Only the right PIN can access data from smart card.

(2) High Security: Because the smart card is capable of encryption and decryption.

(3) Low Cost: Smart card can work offline. Therefore, the cost will be decreased by connecting less.

(4) Controllable: The smart card contains a small microprocessor and operating system.

(5) Portable: Smart card is small and easy to carry.

III. METHODOLOGY

In this section, we will explain the system environment structure and its application first and then introduce the user authentication method proposed in this paper deeply.

A. System Environment Structure

First, we place wireless sensor nodes on different floors and different wards in the hospital. These wireless sensor nodes (S_n) are managed centrally, and thus each floor can be regarded as a different cluster region.

Figure 1 shows the sensors in each ward can transmit all the collected information to the data collector wirelessly. Then this information is given to the manager through wired transmission for centralized management.

All medical personnel who wish to access the data collected through the nodes must register with the management first. Upon registration, management dispenses a personalized smart card through a secured channel to the applicant. Thereafter, the user can use this smart card together with wireless mobile devices such as PDAs and Notebooks to log into the system. While the user is logging in into the system, data search and access can be conducted with all the sensor nodes in the hospital premises within a limited time. Figure 2 demonstrates how through the integration of the smart card with a PDA, doctors can examine patients' physiological data, . This data includes patients' temperature, heart rate, blood pressure, etc. Likewise, ward information such as room temperature and lighting can also be accessed.

B. System Environment Structure

The proposed method is divided into four phases: registration, login, authentication, and data acquisition. Table 1 shows the definitions of the symbols used.

TABLE I. NOTATION DEFINED

Notation	Explanation
U_i	i-th user
ID_i	i-th user's account
PW_i	i-th user's password
TID_i	i-th user's account used during t time
$h(.)$	One-way hash function SHA
K_{bs}	Management's symmetric encryption key
$\oplus$	XOR
$\|\|$	bit concatenation operator
T	time parameter
S_n	n-th sensor node
a, b	secret parameter to be used as authentication parameter
$F_i(X)$	i-th user's polynomial time

B.1. Registration Phase

When U_i wishes to access resources of sensor node S_n of the hospital, U_i must first register with the management. To do so, U_i sends his account name ID_i and password PW_i through a secure secret channel to the management. When the management receives the registration request, he calculates K_i using his own key K_{bs} and gives it to U_i, including $K_i = h(ID_i \| PW_i) \oplus h(K_{bs})$. Next, a personalized smart card is given to U_i. Parameters in the smart card include < $h(.)$, ID_i, K_i, $h(PW_i)$, a >. a is a secret parameter generated by the management and is stored in S_n at the time when the sensor nodes are layered. S_n is responsible for exchanging the data with U_i. As the secret parameter a is stored in the smart card, users cannot directly nor indirectly access the value of a. Ultimately, the management sends the smart card to U_i through a secure secret channel.

B.2. Log in Phase

When U_i during making rounds wishes to access data of the patient in the ward, he has to log in using his account ID_i and password PW_i.

Step1: U_i inserts his smart card into the mobile device and inputs his account and password. Next, the smart card itself authenticates the entered account and password to check if they match with the account and password stored in the card. If correct, the next step follows; otherwise, the operation is terminated immediately.

Step2: The smart card possessed by user U_i computes a time-stamped signature TID_i and C_i, $TID_i = h(ID_i \| PW_i) \oplus h(a \| T_1)$ and $C_i = h(K_i \| a \| T_1)$, among which T is the current time of U_i.

Step3: < TID_i, C_i, T_1> is given to manager.

B.3. Authentication Phase

When the management receives the log in request from U_i, he authenticates to see if U_i is a legal user.

Step1: Verify T_1. If $(T_1^* - T_1) \leqq \Delta T$, the next step follows; otherwise, the operation is terminated. ΔT represents expected time delay during network transmission.

Step2: The management computes $h(ID_i \| PW_i)^* = TID_i \oplus h(a \| T_1)$ and $C_i^* = h(h(ID_i \| PW_i)^* \oplus h(K_{bs})) \| a \| T_1)$

Step3: The management verifies the C_i sent by $U_{i.}$ If the log in request is permitted, the next step follows; otherwise the message is discarded.

Step4: Upon receiving a log-in request, the management computes the following parameters:

$A_i = h(TID_i \,||\, S_n \,||\, a \,||\, T_2)$

$$F_i = \prod_{j=0}^{m}\left[X - t_j\right] + h\left(b \,||\, TID_i\right)$$

$D_i = F_i\,(X) \oplus h(ID_i \,||\, PW_i) \oplus h(K_{bs})$,

where T_2 is the management system’s time-stamp. All the sensor nodes, and the management share a common secret parameter a; b is a random value.

Step5: Finally, the management sends $< D_i >$ through a secret channel to U_i. Also at the same time, message $< TID_i, A_i, T_2, b >$ is sent to all the sensor nodes near U_i, informing them that U_i is a legal user, and that they should actively reply U_i. Therefore, $< TID_i, A_i, T_2, b >$ can be used by the sensor nodes to verify users’ identity.

Step6: When sensor node (S_n) receives $< TID_i, A_i, T_2, b >$, it first verifies T_2, in the same way as step1. If the $(T_2^* - T_2) \leqq \Delta T$ condition is met, the operation carries on; otherwise, it is terminated. ΔT represents expected network transmission delay. S_n computes $A_i^* = h(TID_i \,||\, S_n \,||\, a \,||\, T_2)$ to verify if it matches with the A_i sent by the management. If it does, S_n sends the searched data to U_i, else no reply is given and the operation is ended.

B.4. Data Acquisition Phase

While the authentication phase is being carried out, the management gives U_i an access certificate. With this, U_i can carry out data access and use multiple times within a limited time. The steps are as follows:

Step1: First, U_i must insert the smart card into a mobile device and input an account and password. Next, the smart card verifies the entered account and password to see if it matches with the account and password in the smart card. If correct, the next step follows; otherwise the operation is terminated immediately.

Step2: If user U_i wishes to access the data of S_n, it need not log-in to the management’s system again, but can use the D_i given by the management for further computations. By substituting the current time T_3 with polynomial $F_i\,(X) = D_i \oplus K_i$, $h(b \,||\, TID_i)$ is obtained. Finally, $E_i = h(b \,||\, TID_i) \oplus h(a \,||\, T_3)$ is computed, after which the access certificate$< E_i, T_3, TID_i >$ is sent to S_n , with T_3 being the time-stamp of U_i.

Step3: When   receives $< E_i, T_3, TID_i >$ at any point of the time, it first verifies T_3. If $(T_3^* - T_3) \leqq \Delta T$ does not hold, the operation is terminated and the message discarded. If it holds, S_n proceeds to calculate $E_i^* = h(b \,||\, TID_i) \oplus h(a \,||\, T_3)$ to verify whether it matches with the E_i that U_i sent. If they match, the data requested by U_i is sent; otherwise, no response is given, and the operation is terminated immediately.

IV. SECURITY ANALYSIS

The following security analysis is done with the hypothesis that with current technology, it is relatively difficult to duplicate or acquire parameters from smart cards. Even if attacker manages to acquire some parameters from smart cards through side channel attacks, the cost of acquiring them would far exceed the value of the parameters. In addition, there are already smart cards devised to withstand side channel attacks and reverse engineering hacks. Next, to enable sensor nodes to withstand node capturing threats that may result into easy access of internal data, we also assume that the sensor nodes use tamper-resistant components for storing confidential data. Though tamper-resistant components are more expensive and that their function is not required in most environments, they are nonetheless necessary in special environments such as healthcare, border security etc., to prevent intentional and unintentional leaks during data transmission. In our case, the sensor nodes are installed in an open environment where attackers can literally capture the nodes. However, through tamper-resistant components, it can be assured that the attackers will not be able to acquire the data in the sensor nodes. According the above hypotheses, our protocol can does withstand the following attacks:

A. Replay Attack

When a user sends a log-in request $< TID_i, C_i, T_1 >$ to the management, he can be assured the request will not be intercepted and used to register with the management. This is because when the management receives a log-in request, it will first verify whether the time-stamp lies within the reasonable delay time. If it doesn’*t*, the management will terminate the log-in request. Moreover, resent intercepted messages will fail because of $(T_1^* - T_1) \leqq \Delta T$.

B. Impersonation Attack

Assume the attacker manages to have TID_i after a successful interception of a log-in request$< TID_i, C_i, T_1 >$. To resend the request, it uses a new time-stamp to recalculate TID_i in order to prevent repeat attacks. However, this is not impossible, as. When the attacker computes TID_i, it will not be possible to derive from the intercepted message because of the one-way hash function protection. Hence, the attacker cannot impersonate as a legal user. Furthermore, attackers cannot duplicate a legal user’s log-in request if he does not have data from his smart card. In addition, it is relatively difficult to derive   from TID_i and smart cards. Attackers also cannot derive $h(K_{bs})$ to forge a legal user’s registration data because $h(K_{bs})$ is stored in K_i, while K_i is stored in the smart card. Thus, impersonation attacks cannot succeed in our method.

C. Stolen-Verifier Attack

In our method, no user’s password or verification data is stored in the system. This prevents stolen-verifier attacks. As neither the management, nor the sensor nodes retain passwords or verification data to authenticate log-in requests, therefore, no passwords can be derived from the internal network. Although users at the registration phase sends a PW_i, however, once the registration phase has been completed, the management deletes the PW_i record immediately. Thus, in our method, stolen-verifier attack is prevented.

D. Guessing Attack

In our method, we do not require password/authentication tables. On the contrary, we make digests for password transmissions and other confidential components. Even if an attacker acquires TID_i, which includes user's PW_i and secret parameter a, when faced with the characteristics of one-way hash function, he will not be able to guess the user's PW_i and secret parameter a separately.

E. Denial-of-Service Attack

For all systems where messages are communicated through public channels, denial-of-service attacks are intrinsic potential threats that can be exploited as when the service provider services a competitor or attacker, a value-added user is denied service. Such attacks can be detected with intrusion detection systems. We do not provide protection for such attacks in our protocol because in one-way protocols, the management only needs to send messages to wireless sensor nodes without having to expect any reply. If the attacker intercepts the message from reaching the node, neither the management, nor the wireless sensor nodes will know.

F. Node Compromise Attack

As most of the sensor nodes are installed in physical open environments, attackers can potentially capture a node and access data or tamper with the internal settings. At the moment, this is rather difficult to prevent. However, there are two methods that can lower the loss in the event of compromised sensor nodes. The first method is through the use of one-time sensor nodes, but which due to cost considerations is often not a viable method. The second method is the use of an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). Thus, in our method, an IDS is installed on the management's end to monitor the sensor nodes and possible attacks periodically. Through the use of IDS or IPS in the environment, effective prevention, detection, and filtration of suspicious message packets can be used to assure the sensor nodes' desired status.

In addition to the attacks mentioned above, our method is also prevented from the use of shared accounts, i.e. sharing one account and password with multiple users, which results into system's burden and account management problems. In most password authentication systems, in order to verify users' identity, the system retains a verification table to manage user authentication. In our method, we do not retain any verification tables with the management, and thus are not faced with related threats. Furthermore, to log-in to the system, a legal user is required to have $< ID_i, PW_i >$and the corresponding smart card. In our proposed method, all parameters related to the log-in phase are calculated with the smart card. Once the card is removed from the system, the system terminates the content accessed by the user from the sensor nodes. Thus, all legal users are required to have a card, which therefore prevents multiple-user login attack.

V. CONCLUSIONS

In this paper, we propose a method to protect the patients' physiological information. We use the User Authentication to identify those medical workers who access to get the patients' physiological information. Through combining the smart card and password authentication, we can control the access and make sure only the legal user can get the data. In addition, legal user can access to get the data several times in a limited time without authenticating. It can enhance the efficiency of data receiving. Last but not least, according to our security, performance and power analysis, it is clear to see that our method can resist attacks such as Replay Attacks, Impersonation Attack and so on. Therefore, what we propose in this paper is quite efficient and meanwhile is capable of resisting attacks.

ACKNOWLEDGMENT

This work was supported partially by National Science Council of Republic of China under Grants NSC 100-2410-H-029-007.

REFERENCES

[1] G. J. Simmons, Contemporary Cryptology: The Science of Information Integrity, IEEE Press Piscataway, NJ, USA, 1992.

[2] C. C. Chang and T. C. Wu, "Remote Password Authentication with Smart Cards," *IEEE Computers and Digital Techniques*, Vol. 138, No. 3, pp. 165–168, 1991.

[3] T. Falas and H. Kashani, "Two-Dimensional Bar-Code Decoding with Camera-Equipped Mobile Phones," *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 597–600, 2007.

[4] M. S. Hwang, "A Remote Login Authentication Scheme Based on the Digital Signature Method," *International Journal of Computer Mathematics*, Vol. 70, No. 4, pp. 657–666, 1999.

[5] M. S. Hwang, "Cryptanalysis of a Remote Login Authentication Scheme," *Computer Communications*, Vol. 22, No. 8, pp. 742–744, 1999.

[6] T. L. Hwang, Y. W. Chen, and C. S. Laih, "Non-interactive Password Authentications without Password Tables," *IEEE Region 10 Conference on Computer and Communication System*, pp. 429–431, 1990.

[7] M. S. Hwang and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28–30, 2000.

[8] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," *IEEE International Conference on Sensor Network Ubiquitous, and Trustworthy Computing*, Vol. 1, pp. 318–327, 2006.

[9] H. R. Tseng, R. H. Jan, and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," *IEEE on Global Telecommunications Conference*, pp. 986–990, 2007.

[10] M. L. Das, "Two-Factor User Authentication in Wireless Sensor Networks," IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1086–1090, 2009.

[11] M. K. Khan, and K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'," *Sensors*, Vol. 10, No. 3, pp. 2450–2459, 2010.

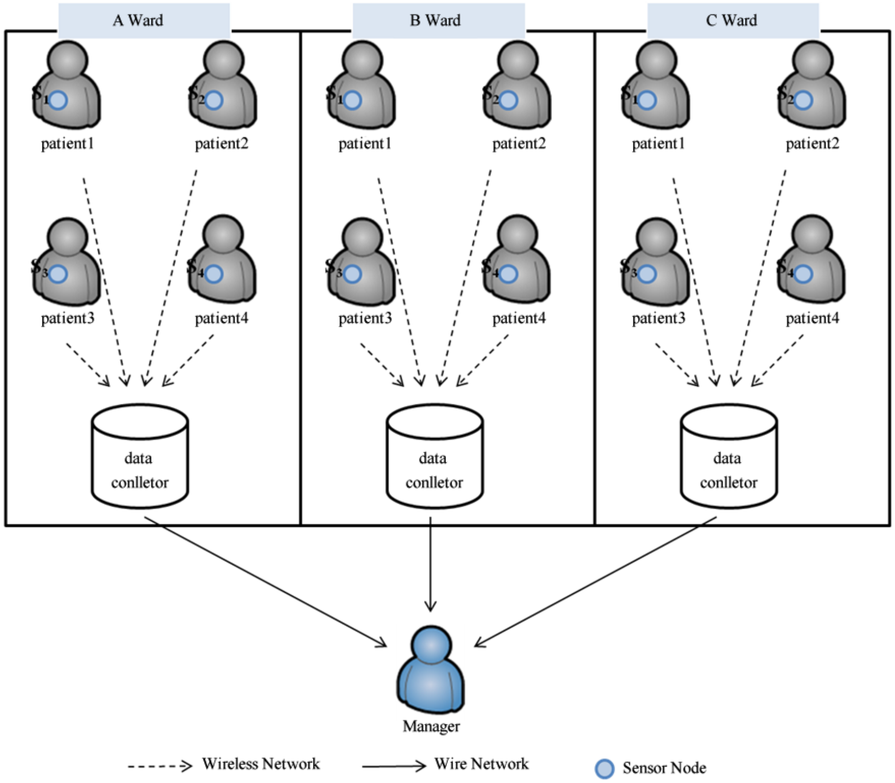

Figure 1. System Environment Structure.

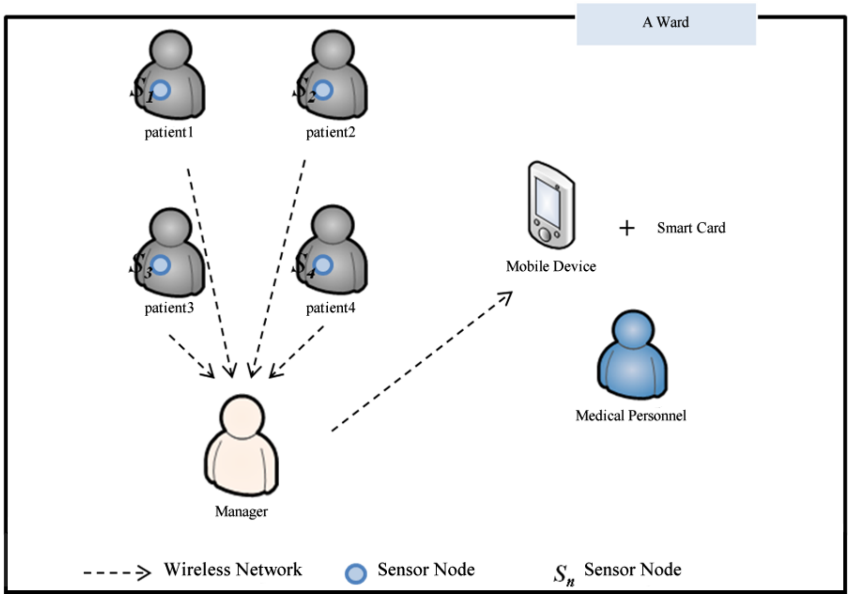

Figure 2. Examine patients' physiological data.

國科會補助計畫衍生研發成果推廣資料表

日期:2012/08/22

國科會補助計畫	計畫名稱: 無仲裁機構的多方公平交換協定之設計
	計畫主持人: 陳澤雄
	計畫編號: 100-2410-H-029-007- 學門領域: 資訊管理
無研發成果推廣資料	

100年度專題研究計畫研究成果彙整表

計畫主持人：陳澤雄	計畫編號：100-2410-H-029-007-
計畫名稱：無仲裁機構的多方公平交換協定之設計	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	2	2	100%	人次	
		博士生	1	1	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	2	2	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	1	1	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	1. 2011 年瑞士日內瓦國際發明展得金牌：指導電機系蔡孟洋同學參加瑞士日內瓦國際發明展。其設計的「床邊照護視訊系統」獲得此次金牌獎。此項作品是利用創意改造而成為醫院床邊實用視訊系統，使資訊傳達、監視記錄、醫療服務等功能更完善、貼心，可滿足使用者全面性需求，並兼顧使用簡易與隱私安全，而獲得評審青睞。 2. 2011 年瑞士日內瓦國際發明展得金牌及特別獎：指導東大附中捷安特巨大董事長劉金標的雙胞胎孫女劉韋彤、劉韋均參加 2011 年瑞士日內瓦國際發明展得金牌及特別獎，其設計的「發音練習矯正系統」獲得此次金牌獎及特別獎。利用光學干涉原理，將攝影鏡頭藏於鏡子後面，運用錄影幫助弱勢小朋友練習及矯正英文發音。

🟥	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：（以 100 字為限）

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

1. 2011 年瑞士日內瓦國際發明展得金牌：指導電機系蔡孟洋同學參加瑞士日內瓦國際發明展。其設計的「床邊照護視訊系統」獲得此次金牌獎。此項作品是利用創意改造而成為醫院床邊實用視訊系統，使資訊傳達、監視記錄、醫療服務等功能更完善、貼心，可滿足使用者全面性需求，並兼顧使用簡易與隱私安全，而獲得評審青睞。

2. 2011 年瑞士日內瓦國際發明展得金牌及特別獎：指導東大附中捷安特巨大董事長劉金標的雙胞胎孫女劉韋彤、劉韋均參加 2011 年瑞士日內瓦國際發明展得金牌及特別獎，其設計的「發音練習矯正系統」獲得此次金牌獎及特別獎。利用光學干涉原理，將攝影鏡頭藏於鏡子後面，運用錄影幫助弱勢小朋友練習及矯正英文發音。