改良式ElGamal-like數位簽章於電子商務環境之應用

王連杰
萬能科技大學資訊管理系

陳正鎔
萬能科技大學資訊管理系

孫屏台
萬能科技大學資訊管理系

摘要

由於網路及資訊科技進步，導致企業組織日常運作多已採用資訊系統輔助營運作業。在推動電子商務時，因各企業或消費者位於不同地點，彼此須隨時經由網路溝通，然而經由網路傳輸資訊，容易被入侵者從中擷取或意圖干擾，因此對網路傳遞的訊息需加保護，以免遭受損失，故安全的網路環境是電子商務之基礎。本研究提出一個改良的可偵測原始文件被偽造、冒用、竄改時，具應變能力的ElGamal-like數位簽章協定，引入公正第三者仲裁傳送者與接收者間糾紛，另外本協定具雙重防線抵禦能力，若發現惡意者在入侵第一道防線時，即能適時查覺，並舉證交由公正第三者仲裁糾紛，且本協定執行效率佳，耗費成本低，得以維護電子商務交易資料在網路傳輸上的安全。

關鍵字：資訊安全、數位簽章、電子商務、公平交易協定、離散對數

A Modified ElGamal-like Digital Signature in the Application of Electronic Commerce

Lian-Jie Wang
Department of Information Management,Vanung University

Jonathan Jen-Rong Chen
Department of Information Management,Vanung University

Pin-Tai Sun
Department of Information Management,Vanung University

Abstract

Recent network and information technology developments have enabled numerous enterprises to conduct routine operations using an e-business model. Because remote customers and businesses communicate over a network, they are vulnerable to invaders eavesdropping or forging messages or data. Therefore, internet security is fundamental to electronic commerce. This paper proposes a modified ElGamal-like digital signature scheme to protect original messages from being forged, counterfeited and interpolated. The scheme introduces a trusted third party that arbitrates disputes between the sender and receiver. Using a double-line of defense, the scheme locates the malicious invasion at the first line, collecting evidence which it transfers to the trusted third party arbitrating the dispute. Therefore, this improved digital signature scheme can manage the threat of forge activity and protect the transfer of e-commerce data over networks, and performs more efficiently than others.

Key words: Information Security, Digital Signature, Electronic Commerce, Fair Exchange Protocols, Discrete Logarithm

壹、前言

近年來由於資訊科技蓬勃發展與電信通訊網路技術進步，無論是製造或服務業，為追求降低成本，增進產品品質，提升服務效率，在目前環境下競相採用資訊、通訊等軟硬體設備及技術，大幅度地將此類應用鑲嵌於營運模式中，以期企業內之資源充分整合與利用，並透過網路建構資訊流通管道，整合採購、進貨、庫存、生產、出貨、行銷、人事、會計等作業流程，以有效提昇企業生產力和競爭力，期望降低成本及提昇服務品質，以維持成長動力。

以往電腦科技運用範疇僅限於企業組織內各部門，而今已隨網路通訊的進展擴大到企業之外，需與其他組織聯繫，運用網路無遠弗屆的特性，突破時間與空間的藩籬及限制，使企業以較經濟規模的方式運作，進而創造大量商機，企業之間透過網路以結合產業上、中、下游廠商，達到供應鏈整合。依據此類商業模式，不僅可簡化企業內部資訊流通成本，且使企業與企業之間交易流程更為迅速，並減少成本耗損。根據經濟部「電子商務法制及基礎環境建構計畫」調查顯示，國內B2C線上購物市場規模2006年約新台幣979.5億元，2010年時，市場規模已達2,417億元（許美玲 2006）。雖然2008年受到國際金融海嘯影響，造成消費者信心不足及整體零售業景氣不如預期，資策會產業情報研究所（MIC）已經下修網路購物規模，於2008年8月進行的台灣網友調查，針對網路使用行為以及B2C市場消費行為剖析，在新業者加入及既有業者服務品質提升，為網友帶來更多網路購物選擇，加上網路消費者參與率及消費金額持續增加，2008年台灣B2C市場規模達到1,365億元，C2C市場規模則為1,071億元，較往年成長幅度約為38.5%（詹超宇 2008ab、2009）。

網際網路的出現造就了電子商務交易型態崛起，由於提供及時與多元資訊特色，促使網路使用人口不斷成長，網際網路儼然形成一個新型市場通路，依據「創新資訊應用研究計畫」調查顯示2007年12月底止，我國經常上網人口突破千萬大關，達1,003萬人，網際網路連網應用普及率為44%（葉亭佳 2008）。網路的應用帶來商機，電子商務是建立在網際網路上的一種商業應用，許多經濟行為隨之改變，由於出現網際網路，已使商業競爭從實體市場移轉至虛擬網路空間市場。消費者可輕易地透過網路快速連結，在各個虛擬賣場中自由選購所需產品或服務，其購物行為從傳統實體商店延伸到新型態的虛擬商店，逐漸改變人類生活習慣，也創造新的商業行為及經濟模式（Monsuwe et al. 2004）。

電子商務發展至今，相關商流、金流、資訊流及服務流皆是數位化形式，構成與以往不同的企業營運型態。網路匿名與開放特性，引發虛擬世界無法完全套用實體世界中的經驗，在此環境中竊取訊息、冒名欺騙、複製文件、竄改資料、偽造事實，皆是輕而易舉。因此衍生許多安全議題，隨之也同時產生更多資訊在運用交換傳遞時，必須深入思考的問題。若要利用網路取代傳統通信方式，進行商業交易或傳輸敏感資料，須建置保密安全而又能驗證使用者身份的網路訊息傳輸機制（Corritore et al. 2003）。

無論個人或企業利用電腦透過網路傳輸資料或訊息，如未經預先規劃處理，對有心人士而言，就如明信片般隨手可得而一覽無遺，所造成的後果與損失難以預料。因為企業或個人經由網路進行資料傳輸時，由於雙方所有訊息往來，都以數位格式為之，無法面對面接觸辨識，身份容易偽稱，資料易被仿造，或遭人攔截竄改（Graff 2001）。由於網路消費不確定性較實體購物為高，且易招網路駭客攻擊、暗植間諜軟體、木馬程式入侵、蠕蟲癱瘓威脅，導致資料外洩或系統平台運作失靈，再加上新聞媒體負面報導的推波助瀾影響，使得網路交易安全始終是網路交易時的主要議題（許美玲 2006）。根據E世代公民對話誌（2007）委託政治大學民意與市場調查研究中心最新完成的「台灣網路安全信心調查」，只有34%民眾對網路安全有信心，低於歐美先進國家水準（美國53%、德國43%），其中又以「業者保護個資」最令民眾憂心，表示沒信心比例高達63.1%，其次是「政府保護個資」的45.2%，緊追在後的為「網路交易安全」，沒信心比例為44.7%。

因此，本研究從資訊安全角度為出發點，提出改良的數位簽章協定，以滿足電子商務在交易時需要。全文共分五章，接下的章節中，第二章將對電子商務與一般傳統數位簽章的作法加以回顧與探討，第三章在描述本研究所提出的改良式數位簽章新協定，並在第四章中對本文所提新協定予以安全性與效率分析，第五章為對本文予以總結，並敘述改良式ElGamal數位簽章協定，對有關於資訊安全方面日趨複雜多變的電子商務環境之因應作法，最後在附錄中則將本研究所提數位簽章協定，以例證方式作詳細說明。

貳、文獻探討

隨著通訊與資訊科技蓬勃發展，各產業在例行營運流程中，運用網際網路已成為現今商業活動發展主流趨勢，隨著資訊平台運作日趨成熟，越來越多的企業選擇網路交易模式，電子商務是透過網路快速傳輸能力所建立的一種交易制度，而造成盛行主要原因，即為滿足消費者享受購物不受時間與空間限制，或企業用戶便利的運用資訊系統，以節省實體商店營運成本，具有縮短產品上市週期，降低生產成本，創新銷售機會，減少庫存等效益，更能改善服務品質，不僅帶動全球經濟與社會轉型，也顛覆傳統商業經營模式。

一、電子商務的類型與發展

Turban et al.（2006）定義電子商務為經由電腦網路，特別是網際網路，進行產品、服務或資訊的買賣或交換，說明了利用網路進行商品買賣交易的實際用途。根據Kalakota與Whinston（1997）定義，凡是透過網際網路提供銷售、販賣或服務的商業活動皆可視為電子商務。而Zwass（1996）認為凡使用通訊網路進行商業資訊分享、維持商業關係，以及從事商業交易活動及行為，均可視為電子商務。一般而言電子商務應用範疇廣泛，因經營模式不同而有很多分類方式，大體而言，整個交易型態還是以下列三種商業模式為主：

（一）企業與消費者進行交易（B2C）

此為最基本且常見交易方式，即企業販賣貨品或服務給消費者，以網路連線、電子傳送技術來促成企業與顧客間交易，顧客可以藉由網路媒介來瞭解商品資訊，利用電子現金及其他安全付費機制來購買商品或服務，一般多指線上購物網站，除此之外如拍賣網站、旅遊網等亦較常見，此類交易不受時空限制，為目前一般人較熟悉的一種類型。

（二）企業與企業進行交易（B2B）

B2B的電子商務是指企業間透過網路及相關資訊科技，將訂單、交易款項，或其他商業資訊與文件直接傳送。例如供應商、製造商、零售商以及物流業，經由策略聯盟形成供應鏈關係，國內最具代表性的如各集團企業所設計建置的電子交易市集，以建構企業採購電子交易環境為目標，針對上游供應商，提供具有垂直整合能力的線上訂單系統，管理訂單及進出貨處理，又對下游客戶建立往來紀錄，解決長久以來繁瑣的傳統人工作業程序，在網路及資訊科技協助下，上下游業者資訊可以即時暢通，透過密切協調配合，使供應鏈中使用者有滿意的產品及服務，企業本身亦可節省時間降低成本，提升利潤及競爭力。

（三）消費者與消費者進行交易（C2C）

另一種常見交易方式為一般個人之間，在網站上消費交易行為，經過網路中間商所建構的網站執行撮合，例如個人拍賣網、購物網站、一般的ICQ討論等，穿越時空限制，讓位於各地的顧客同時上網競標喊價，消費者利用此類網站販賣或購買其他消費者的商品，以滿足消費者享受購物樂趣，脫離時間與空間束縛。然而目前已進入Web2.0時代，社群網站及成千上萬的部落客（Bloggers）紛紛出現，網友也相當踴躍互動參與，針對某些特定主題，深入剖析發表個人意見，不少個人部落格每天都可吸引為數眾多的網友瀏覽、討論，已有專業內容媒體雛型，逐漸形成網路界的意見領袖，具有某種程度影響力，電子商務業者進而借重網路意見領袖的力量，來協助商品行銷。因此對於有意願參與的網友，若推薦其產品或為產品背書，則提供利潤分享之紅利制度，除了商品或服務交易外，更增加知識與經驗的分享，使參與的網友不只是電子商務網站的消費者，還能扮演口碑行銷、人際行銷的角色。

二、電子商務與資訊安全的關係與發展

（一）資訊安全的重要性

一個成功蓬勃發展電子商務環境，首先要能解除使用者對安全性與隱私權的疑慮，例如，個人身份、電子付款交易資料或企業運作專業的知識、方法、技術、訣竅等的隱私及保全更是重要關鍵。一般而言，藉由網路傳輸文件訊息，基於安全需求，應達到下列幾點：（Schneier 1996; Mel & Baker 2001; Udo 2001）

1. 傳輸或儲存的文件資料，經過加解密技術，避免被無關的入侵者獲知，達到保密要求，以符合機密性（Confidentiality）。

2. 文件接收者可確認此文件之傳送者身分，避免被冒名傳送假資料，以達資料來源辨識性（Authentication）。
3. 傳輸的文件應避免被篡改、重送、替代、偽造、遺失以保持原始資料的完整性（Integrity）。
4. 確保文件傳送者不可於傳送訊息之後，狡賴已傳送過該文件資料的不可否認性（Non-repudiation）。

如何利用相關技術與認證機制來保護資料在傳輸過程中完成上述特性，以確保資訊完整正確及公信力，遂成為各企業在溝通交流資訊時尤須考慮的重點。傳統上將文件密封、簽名等方式的作法，對電子形式的數位資料而言，根本無法適用。欲達到上述安全的電子商務環境要求，須仰賴密碼學技術中加解密方法與數位簽章等方式共同達成。一般而言，除了機密性需要加解密技術外，其他功能皆可運用數位簽章方式來實現（Graff 2001; Schmeh 2003），因此本研究提出改良式ElGamal-like數位簽章協定，以因應日趨複雜多變的網路環境。

（二）電子商務糾紛與線上公平交易協定

資訊與網路的運用導致電子商務迅速興起，交易量日趨龐大，以eBay在2007年底為例，平均每秒鐘產生一筆價值2000美元以上的網路交易（Johnson & Cooper 2009），隨之而來發生紛爭勢所難免，eBay於1993年開幕最初二周內即有155件糾紛（Katsh & Rifkin 2001），與eBay結盟的仲裁組織SquareTrade在1999年中期設立，到現在已解決來自一百二十多國超過八十萬筆以上的爭議（Abernethy 2003），肇致糾紛並非壞事，經由紛爭所產生的互動過程，反而能夠激發新的動力或創意，關鍵是糾紛的管理，盼使糾紛不至成為進步的阻礙才是應有態度，發生糾紛後若以傳統訴訟方式，則難免曠日廢時。因此在買賣雙方本持誠信及維持商誼原則下，協商、調解、仲裁或其他爭議解決程序，日漸興盛。

電子商務交易具即時、異地特性，發生糾紛以線上方式解決，廣為一般所採行，由於處在網路環境，易受駭客或未經授權的第三者非法接觸，使人有不安全及隱私被偷窺之感，相關業者遂運用加解密技術，提供線上仲裁過程與資料的保全，但在使用上增加困難造成使用者卻步，同時雙方身份亦難認定，多重問題懸而未決，始終困擾並存在於電子商務業者與消費者之間。

公平交易係指雙方交易結束後，一是雙方都得到了自己想要的商品或服務，或是發生異常則任何一方都得不到有關對方商品或服務，更遑論交易者身分或其他訊息。公平交易協定的觀念最早源起於電子郵件內容交換和保障電子線上交易（Ketchpel 1995; Deng et al. 1996; Zhou & Gollman 1996），主要作法在雙方進行交換或交易時保存證據，作為萬一發生糾紛時的處理依據，交易雙方可能因金額太小，或身分認定困難造成舉證方式不易（Ketchpel & Garcia-Molina 1996）。為解決上述交易困境，逐漸發展出下列數種公平交易運作方式，如漸進式交換協定（Gradual exchange protocols），由於買賣雙方互不相識，交易初期雙方僅透露己方部分資訊，經數回合往來後，彼此建立互信，再將所有資訊與對方交換，以達交易目的，採用此方式雙方須具備一定程度的先決條件，如

雙方須有相當的電腦運算能力才能順利運作，經同時往來數次之後才交易完成，耗用網路頻寬且運算量過大，有違經濟原則，實用價值較低，此協定於B2C或C2C的場合即難以運用，因一般消費者與企業間的電腦運算能力難以相比（Blum 1983; Even et al. 1985; Brickell et al. 1987）。

目前學者探討集中在引入公正第三方的協定，線上公正第三者交換協定（Online trusted third party exchange protocols）是一具客觀公正第三者介入雙方交易，買賣雙方先將己方識別資訊與欲交易的資料，送交公正第三者，再透過此公正第三者將資料交予對方，此期間若任一方因不可抗拒之原因中斷交易，因公正第三者的存在得以確保另一方的權益。公正第三者接獲雙方交易通知後，須先對雙方身份確認，資料驗證等繁複手續，在效率上仍有改進空間（Zhou & Gollmann 1997; Park et al. 2003; Ray et al. 2005）。此外維持公正第三者介入雙方交易，須付出相當代價，協定能否順利進行主要依賴於公正第三者，容易成為交易瓶頸（马昌社 2007）。

為提高交易時執行效率，及有效證明交易雙方的不可否認性，學者相關的研究，遂以公正第三者以離線方式來處理交易糾紛（Asokan et al. 1998; Bao et al. 1999; Markowitch & Kremer 2001），公正第三者在發生交易紛爭時才介入處理，由於公正第三者初期並未涉入交易協定，故僅能於發生糾紛時提供證明，而非原始的證據，可能引發交易公平性問題。此外若公正第三者本身喪失中立性或缺乏誠信，則又衍生更多的問題（Dodis & Reyzin 2003; Shao 2008）。因此處理電子商務交易糾紛，實為當前值得關注與探討的焦點。

（三）相關數位簽章文獻回顧與運作方式

Diffie 與 Hellman（1976）首先發表公開金鑰密碼系統的概念，思考如何讓網路上兩位素昧平生者達到相互金鑰交換（Key exchange），解決傳統密碼系統在傳遞密鑰時的問題，當時並未提出實際作法，但已掀起一股研究與設計公開金鑰密碼系統的思潮，Rivest等人於（1978）年以數論（Number theory）為基礎，研究出植基於計算因數分解難題的第一套公開金鑰密碼系統與數位簽章，此系統產生一對金鑰組，稱為公鑰（Public key）和私鑰（Private key），所有參與者都可以取得每個人的公鑰，而私鑰為個人所擁有，運作時以此兩把不同但具有對應關係的金鑰組，進行加密或解密動作，一個訊息用同一個人的公鑰加密，就必須用私鑰解開，反之，用私鑰加密就必須用公鑰解開，通常若入侵者只知道密碼系統的演算法和加密金鑰，由於在設計時遵循單向暗門函數原則，所以入侵者無法經由分析計算得到解密金鑰。此期間較受矚目的研究方法還有基於解離散對數（Discrete logarithm）難題的公開金鑰密碼系統與數位簽章協定，ElGamal 即屬此類密碼系統的代表。

自公開密碼系統的觀念啟迪世人後，相關學者發表的數位簽章研究如雨後春筍，茲擇要簡述於後，Rivest等人（1978）年提出分解因數難題為依據的數位簽章，Rabin於次年（1979）亦發表類似概念的數位簽章，Ong等人則提出更進一步在計算上較具效率的數位簽章（Ong et al. 1984），但Pollard & Schnorr於（1987）年則指出Ong等人的數位簽章演算法有安全疑慮。而Naccache則將Ong等人的數位簽章演算法予以修正，解決安全上的問題（Naccache 1994）。

植基於離散對數難題的數位簽章則由ElGamal於（1985）年首先發表，之後學者陸續提出各種以解離散對數難題為基礎的變形數位簽章，Horster 等人於（1994）年綜合各學者作法，提出整合式的 Meta-ElGamal signature，將解離散對數難題的數位簽章，歸納為七大類。嗣候，許多國家公布的數位簽章標準多以解離散對數難題為藍本，如美國的DSA（National Institute of Standards and Technology 1992），前蘇聯的 GOST（Michels et al. 1996）及韓國的 KCDSA（Lim & Lee 1998）。

McCurley 在（1988）年設計出第一個安全性基於解離散對數和因數分解雙重難題的金鑰分配系統，啟引學者藉由解雙重難題的複雜度以建構數位簽章，Harn於（1994）年以個別使用者均有其專屬模數（modulus）建置雙重假設複雜度之策略，其方法與原始ElGamal立論之旨趣不同，以建構數位簽章，唯Lee與Hwang（1996）年指出Harn的數位簽章，在解離散對數部分有安全上的疑慮，並提出改進的演算法。同一時期He 與 Kiesler（1994）年也發表以解雙重難題的數位簽章，將離散對數指數上之密碼予以平方，企圖迫使攻擊者須同時破解雙重假設之複雜度，才有可能挑戰其系統，而Lee與Hwang（1995）年指出此種數位簽章僅建構於解離散對數難題而已。Laih與Kuo（1997）年更指出He與Kiesler的數位簽章並非建構於解雙重難題而能將其破解。同樣的Shao（1998）年也嘗試以類似He與 Kiesler之方法創設另一雙重複雜度之簽章策略，卻被Lee分析出Shao的研究僅具因數分解難題而已（Lee 1999），隨後許多學者陸續發表攻防論述的相關研究，礙於篇幅所限，僅能於此擇要概述。

一般而言RSA數位簽章的簽署方式可視為固定式，即同一份文件每次簽章均相同，ElGamal數位簽章對同一明文所簽署的簽章，每次均可由參數選擇不同，而產生變化，屬於機率式數位簽章，進而增加有心人士破解難度（Diffie 1988; Stinson 2005; Stallings 2004）。

數位簽章協定一般架構與運作，如圖1所示，目前業界採用數位簽章方式，就像是在電子形式文件上親筆簽名一樣，亦即將欲傳送的電子文件，經過公開金鑰加密法中傳送者的私鑰予以運算，它能證明傳送者製作或至少同意了附有其數位簽章的電子文件，足以辨識訊息是由該特定人士所發出。同時，傳送與接收雙方透過適當證據，可以輕易驗證整份文件的完整性，即使局部增刪修改也難以遁形。接收者收到此數位簽章文件後，可藉傳送者的公鑰以比對鑑定發訊者身分，無法逃避曾經撰寫過此文件的事實，具有不可否認的特性，進而確認文件內容在簽章後，是否遭受惡意竄改，因此接收者對於文件來源及其完整性更能掌握且有信心（Stinson 2005; Schmeh 2003; Viswanathan 2006）。

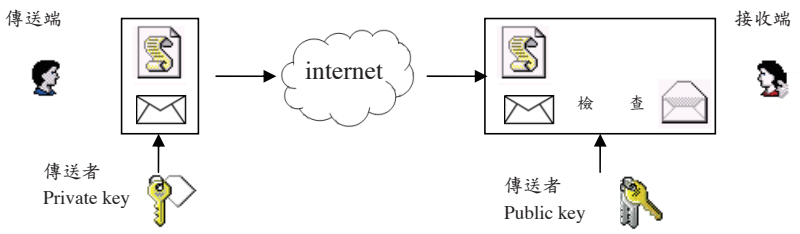

圖1：數位簽章協定架構圖

ElGamal數位簽章協定基本運作方式如下：

1. 前置作業階段

由傳送者首先選一大質數p，及p之原根g，設定其私鑰x進行下列的算式以得出公鑰y，並公開參數p, g

$$y \equiv g^{x} \pmod{p}$$

其中$1 < x < p-1$

2. 簽署階段

傳送者任選一與$p-1$互質之數k，即$\gcd(k, p-1)=1$，計算下列算式

$$r \equiv g^{k} \pmod{p}$$

傳送者將欲簽署的明文m經下列算式運算得到簽章s

$$m \equiv xr + ks \pmod{p-1} \quad (1)$$
$$s \equiv k^{-1}(m - xr) \pmod{p-1}$$

將$\{m, s, r\}$傳給接收者。

3. 驗證階段

接收者接獲$\{m, s, r\}$，與之前的公鑰y，驗證算式

$$g^{m} \equiv y^{r} r^{s} \pmod{p}$$

若上列算式成立，明文m的正確簽章即為$\{s, r\}$無誤，否則即表示$\{s, r\}$有偽造之嫌（ElGamal 1985; Wu 2000; Hwang & Lee 2004）。

參、改良式ElGamal-like數位簽章協定運作介紹

本文基於探討主體聚焦起見，針對數位簽章協定運作基本核心，精進ElGamal數位簽章協定，導入公正第三者（Trusted third party）仲裁糾紛。假設在電子商務網路交易環境中，有一公正第三者之認證機構，在交易雙方發生糾紛時擔任仲裁角色，整個運作概分為下列各階段：

一、前置作業階段

基於在網路上傳輸資料安全考量之下，首先選取質數p須符合下列條件$p=4n+1$,$n=p_1 \times q_1$，且p_1, q_1二數為互質大質數（Harn 1994; He 2001; Shao 2002），再預先選出二個特定數，其中g_1為任一模p（modulo）之原根的四次方後，取其模p之餘數，並且其序（order）為n；另一數 g 是模 p 而其序為p_1，此外隨機任選$\{x_a, k\} \in Z_p$，其中x_a當作私鑰與參數 p_1, q_1, g_1 皆需妥慎保管，而p，n，g三個參數則可公開，k係使數位簽章每次均產生變化而選不同的值，亦須比照私鑰妥適保管。首先由傳送者運算下列算式

$$y_a \equiv g^{x_a} \pmod{p} \quad (2)$$
$$r \equiv g^{k} \pmod{p} \quad (3)$$

傳送者的公鑰與私鑰分別為y_a、x_a。另以之前所選的g_1，計算下列算式

$$w \equiv g_1^{x_a} \pmod{p} \quad (4)$$

將算式（4）算出之w與g_1經由安全通道，送交公正第三者，作為往後如發生爭議，作為解決糾紛的驗證憑據，亦為傳送者偵知簽章是否被入侵者偽造、冒用、竄改的線索。此外位於另一端的接收者任選一數$x_b \in Z_p$計算下列算式

$$y_b \equiv g^{x_b} \pmod{p} \quad (5)$$

上列算式中的y_b、x_b分別為接收者的公鑰及私鑰，並將y_b告知傳送者。

二、交易階段

假設雙方進行電子商務交易，欲傳送的明文為m，需符合下列算式（Harn & Xu 1994）經傳送者運算得到數位簽章s_1

$$m \equiv s_1 x_a + kr \pmod{n} \quad (6)$$
$$s_1 \equiv x_a^{-1}(m - kr) \pmod{n}$$

傳送者再任選一與$\{x_a, k\}$不同之一數h與之前收到的接收者之公鑰y_b計算下列算式

$$f \equiv g^h \pmod{p} \quad (7)$$
$$z \equiv s_1 y_b^h \pmod{p} \quad (8)$$

將$\{m, y_a, r, f, z\}$傳給接收者。

三、驗證階段

接收者收到$\{m, y_a, r, f, z\}$資料後，則以下列算式還原s_1

$$s_1 \equiv z f^{-x_b} \pmod{p} \quad (9)$$

之後再執行算式（10）

$$g^m \equiv y_a^{s_1} \times r^r \pmod{p} \quad (10)$$

若算式（10）成立，則認為傳送訊息m無誤，否則拒絕接受。

四、協商爭議階段

如傳送者與接收者交易發生糾紛時，可隨機每次任選一個與n互質的整數t計算算式（11）

$$T \equiv g_1^t \pmod{p} \quad (11)$$

傳送者設定$s_2 = s_1$後，計算下列算式

$$s_2 \equiv T_{X_a} + tv \pmod{n} \quad (12)$$

由傳送者將$\{s_2, T, v\}$送交公正第三者，再由公正第三者取出前置作業階段，傳送者預先存證的w與g_1，執行運算

$$g_1^{s_2} \equiv w^T T^v \pmod{p} \quad (13)$$

若算式（13）驗證不成立，則傳送與接收雙方即知原來透過網路所傳訊息已有被惡意者入侵現象，因此公正第三者經由算式（13）驗證成立與否，作為排解爭議、糾紛之依據。綜觀本研究所提的改良式ElGamal-like數位簽章協定，主要特點為有二道驗證步驟，即算式（10）和算式（13），為與原ElGamal簽章協定最大不同之處。所強調的第二道驗證防線，係由算式（11～13）構成，由於參數t可由傳送者每次隨機任選一個與n互質的整數，故算式（13）在運作時能達到重複使用的效果，以增進本研究的數位簽章強固性。整個改良式ElGamal-like數位簽章協定運作架構，如圖2所示，詳細運算過程於附錄一、二舉例說明。本文基於探討主體聚焦起見，置重點於改良ElGamal數位簽章協定的運作，增加其安全強度與執行時效率，同時導入公正第三者仲裁糾紛。由於原ElGamal數位簽章協定並未對雜湊函數（Hash function）著墨（ElGamal 1985），基於簡明為出發點，故並未將雜湊函數、隨機亂數的生成、時戳等納入討論。

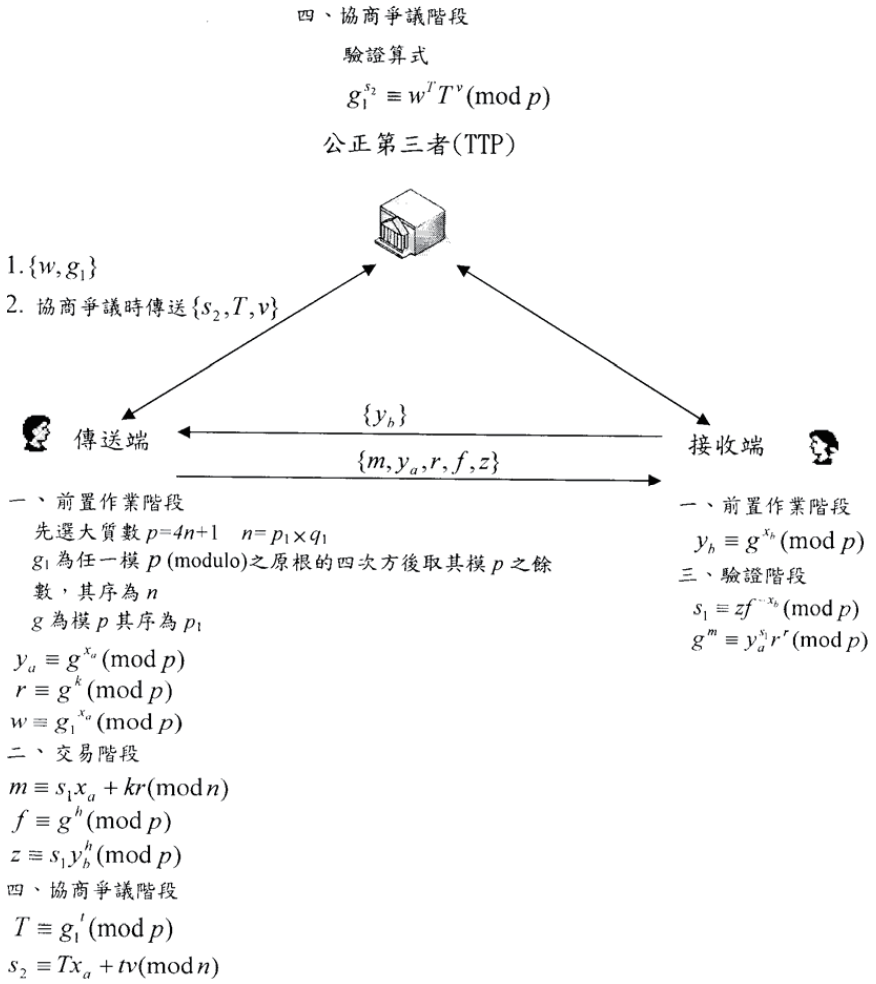

圖2：改良式ElGamal-like數位簽章協定運作方式圖

肆、安全分析及討論

一、安全性分析與效率比較

（一）改良式ElGamal-like數位簽章協定的安全性

改良式ElGamal-like數位簽章協定，在前置作業階段對參數設定，基於布局考量，有不同於原ElGamal簽章協定的方式與作法，在傳送者發送訊息之前，將算式（4）算出的w與g_1值經安全通道送交公正第三者，作為伏筆以為事後發生糾紛，解決爭議的憑據，同時傳送者亦能經由w與g_1值並輔以$\{s_2,T,v\}$值經由算式（13）運算是否產生異常結果來判斷與偵測改良式數位簽章協定被駭客入侵的證據。

原ElGamal簽章協定中，傳送者經由算式（1），可順利得出s，而對入侵者來說算式（1）係一個方程式，卻有二個未知數$\{x,k\}$，欲求其解在計算上是不可能的，足可抵擋入侵者攻擊（ElGamal 1985）。本研究所提出的改良式簽章中的算式（6）對傳送者來說，亦僅有s_1為未知數，但是對入侵者而言卻有二個未知數$\{x_a,k\}$，其困難程度的效果與原ElGamal簽章協定相同，所以算式（6）在安全上是無虞的，同理算式（12）的安全性亦同。此外算式（6）及（12）與算式（1）結構相似，以演算法對時間複雜度之估計精神而言，所耗費的時間成本與ElGamal簽章概略相當。

在驗證階段中傳送者與接收者於驗證簽章的過程，係依模指數與對數的運算性質，經由算式（6）推導

$$g^m \equiv g^{s_1 x_a + kr} \pmod p \tag{14}$$

$$g^m \equiv g^{s_1 x_a} \times g^{kr} \pmod p \tag{15}$$

$$g^m \equiv (g^{x_a})^{s_1} \times (g^k)^r \pmod p \tag{16}$$

由算式（2～3）與算式（16），可得算式（10）成立，同理可證算式（13）亦成立。因此本研究的ElGamal-like數位簽章協定之驗證能力與原始ElGamal數位簽章協定相同。

此外本研究之算式（6）與（10），實為ElGamal數位簽章系統之變形（Harn & Xu 1994; Horster et al. 1994），唯算式（11～13）係依ElGamal數位簽章系統延伸，為本研究所設計的新方法，萬一交易發生異常時，以解決電子商務環境中所發生的糾紛。而在前置作業階段選定n為兩大質數p_1,q_1的乘積，且$p=4n+1$並以p進行模運算，其目的在建構系統安全強度，即本研究之數位簽章協定架構底蘊，具備同時解因數分解與離散對數複雜度之難度（Harn 1994; He 2001; Shao 2002）。

此外本研究的改良數位簽章協定中接收者將其公鑰y_b告知傳送者後，傳送者以算式（7～8）得出f,z，再將f,z傳給接收者，以隱匿原始簽章，避免s_1於公開網路傳送，因入侵者無法接觸到s_1，使入侵者毫無破解原始簽章的線索，而入侵者破解算式（9）的前提是須知悉接收者的私鑰x_b，對入侵者而言將遭遇解離散對數之難題，而增加破解的複雜度，進而提高改良數位簽章協定的安全性，維護傳送者的清白。

（二）改良式ElGamal-like數位簽章協定的特色與被攻擊時的因應作法

假設改良式數位簽章協定被入侵者破解，而遭人偽造或構陷時，由傳送者將$\{s_2,T,v\}$交由公正第三者，公正第三者再取出傳送者於前置作業階段事先存證的w與g_1值，作為排解糾紛之依據，為利了解本研究改良式ElGamal-like數位簽章協定運作過程，請參閱附錄一的舉例說明。

首先如果接收者懷疑所收經由傳送者私鑰運算後的訊息，即懷疑算式（6）被惡意入侵者破解，且經由算式（10）驗證相符，如附錄一實例中算式（23）與（25）所顯示的情形，由於所得結果和算式（17）與（20）相同，此時傳送者可將相關資料交由公正第三者驗證比對，公正第三者因事先已有w與g_1值並輔以$\{s_2,T,v\}$值，作為佐證資料，經算式（13）驗算後，能夠做出公正判斷，其運算情況如算式（21～22）與（26～27）所示，故具備解決此項紛爭的能力。

若發現改良式數位簽章協定被入侵者所擷取後加以偽造，公正第三者可經由算式（13）予以驗證真偽解決爭議，並證實相關參數是偽造的。因為本改良式數位簽章協定在前置作業階段的布局，於選擇參數時預先規劃未雨綢繆，事先選定具特定條件的二個數g與g_1，入侵者雖破解算式（6），但私鑰x_a值並非唯一，對入侵者來說，需再進行第二輪的破解動作，還要再對算式（12）進行破解分析，此時傳送者經由算式（13）運算後得知不同，進而發現簽章被人偽造，所以改良式ElGamal-like數位簽章協定具有二道安全防線即算式（10）與（13），共同建構一個安全的電子商務交易環境。由算式（11～13）所構成的第二道驗證防線，係以參數s_2與第一道防線產生勾稽連繫的關鍵，究其原因乃於交易階段算式（6）的s_1值其所在的有限體為$GF(p_1)$，協商爭議階段算式（12）的s_2值其所在的有限體為$GF(n)$，而s_1與s_2出現的頻率具某種契合性，係因本數位簽章協定於前置作業階段設定$n=p_1\times q_1$之故（Stinson 2005; Silverman 2004）。同時算式（11）中的參數t可由傳送者每次隨機任選一個與n互質的整數進行運算，故算式（13）在運作時能不受侷限達到重複使用的效果，此種特色為ElGamal數位簽章又被稱作機率式數位簽章的緣由，詳細運作說明請參閱附錄二。

經由算式（4）所得之w與g_1值並輔以$\{s_2,T,v\}$值，為構成本系統之第二道防線關鍵，而算式（4）中g_1為p之原根的四次方後，取其模p之餘數，且其序（order）為n，所以經mod p運算後得知w出現的周期長度應為n，如駭客以窮舉方式的暴力法（Brute-force search）而言，被分析的機率為$n/2$，由本系統前置作業階段的設定$p=4n+1,n=p_1\times q_1$，且p_1,q_1二數為互質的大質數，故駭客能得逞的機會甚低。以演算法對時間之估計原則而言，即在現有計算能力範圍 ，不可能在多項式時間以不可忽略的機率，分析出此一大質數。同理，參數s_1與s_2被惡意攻擊者分析出的機率，可由算式（6）與（12）的模n運算得知其機率亦為$n/2$，所以本協定的架構應無安全虞慮。

其實，由於本研究所提出的雙重防禦能力數位簽章協定，在前置作業階段布局時，援引失敗即停（Fail stop）概念（Pfitzmann & Waidner 1991; Susilo et al. 2000），此特色蘊含於算式（6）的數位簽章s_1中，可參閱本文附錄一中所述，在正常狀況時交易階段之s_1，與遭惡意入侵時交易階段之s_1運算結果明顯有異，詳見算式（19）與（24）。因此傳

送者發現異常徵候警覺私鑰x_a有被偽造的可能時，立即採取應變措施，此刻雙方即可停止數位簽章協定運作，達到維護交易安全的目標，確保傳送者的清白。

（三）相關公平交易協定效率比較

目前使用以RSA為基礎的數位簽章協定，運用日漸成熟普遍，參酌马昌社（2007）的研究中比較協定運算效率的方式，對比本研究之ElGamal-like協定，由算式（6～10）得知指數運算次數為7次，協商爭議時由算式（11）與（13）可知指數運算次數為4次。另外，马昌社研究中假設RSA模長為1024bits，故本研究之p值如比照為同樣長度，則在驗證時公正第三者除w值外，仍須參考$\{s_2,T,v\}$值故可驗證數位簽章長度為1024×4（bits），在運算過程的中間暫存值可能較大，但最後經模p運算處理，故實際於網路傳輸的數位簽章長度為1024bits，本研究與其他學者的協定比較請參閱表1，由表內顯示可知本研究所提之ElGamal-like數位簽章協定，無論在正常或爭議時的指數運算次數均優於其他學者的方案，運作時成本耗費較低，且數位簽章長度適中，有利於實際電子商務環境的運用。

表1：本研究與相關協定的效率比較

協定名稱 / 運算比較	本研究 ElGamal-like 協定	马昌社協定（2007）	周永彬等協定（2004）	Ateniese's Protocol（2004）	Bao et al.'s Protocol（1998）	Chen's Protocol（1998）
協定中指數運算次數	7	9	10	16	>20	>26
協商爭議時指數運算次數	4	6	3	11	5	11
可驗證的數位簽章長度單位（bits）	4096	8192	2^{137}	8192	4096	3072
運算方法	ElGamal	RSA	RSA	RSA	RSA	RSA

二、未來研究方向

本文所討論之改良式ElGamal-like數位簽章協定在傳輸時，係對明文m為討論標的，因此在傳輸及保密上須對較長的訊息予以分解為字串以便處理。因此可再引入將明文加密時，提升執行效率作為研究方向（Hwang et al. 2002），以使敏感性資料在傳輸上獲得安全的保障。基於避免本研究所提之數位簽章協定架構討論重點失焦，對於雜湊函數、隨機亂數、時戳等議題並未討論，為使數位簽章協定架構更為完備，亦可將此等議題加入數位簽章協定內。

一般而言，傳送者、接收者若為一般普羅大眾，所具備的資訊設備資源與能力相對薄弱，直接面對擁有無限計算能力的入侵者，實所不宜。當懷疑異常警覺遭人入侵時，緝捕現行犯的行為，宜由司法警政等執法單位扮演。至於與執法單位通報聯繫配合等問題，亦可成立另一研究主題。此外可將本改良式ElGamal-like數位簽章協定予以實作，開發應用系統，達成產、學界合作的目標。

伍、結論

隨著電子商務日趨興盛，網路交易已成全球性議題，為達此目標資訊系統在現今的企業環境下，廣泛地被運用以支撐企業的運作。當企業越來越依賴資訊系統，資訊科技不僅帶來效益與機會，也帶來更多的風險。當企業藉由e化過程提高競爭力時，也需一併考量隨之而來資訊安全的風險控管，針對數位資料，必須要有完整機制，以解決安全上的需求，資訊安全現今已成為企業組織中一個策略性議題。因此在電子商務的網路環境中，必須對資訊安全基礎建設投入大量資源與努力。

在資訊化社會中，各項業務溝通、資料往來、訊息傳遞等，都與網路密切結合，各類型企業組織，從政府單位、金融機構、學術團體到民間企業，都受到密度極高的網路攻擊（Bojanc & Borka 2008; Kumar et al. 2008）。安全的網路環境是電子商務發展的基礎，若無安全則使用者對資訊系統失去信心，網路安全是影響電子商務成功與否的關鍵因素之一（Ranganathan & Ganapathy 2002）。

法諺有云「舉證之所在，敗訴之所在」，說明舉證於訴訟中之關鍵性，舉證之不易，隨著社會活動及交易的多元化，難度日益提高，負有舉證責任的一方，常因舉證不足而遭敗訴命運，主張有利於己之事實者，就其事實有舉證責任[1]，因此舉證責任攸關勝訴與否。改良式ElGamal數位簽章協定擴展原數位簽章架構，考慮仲裁或訴訟時關鍵的舉證問題，在目前社會誠信觀念日趨淡薄，道德價值淪喪，固有的恪守誠信、童叟無欺等傳統美德業已蕩然無存的社會中，有其重要涵義及應用價值。

在目前嚴峻挑戰的環境下，本研究的改良ElGamal-like數位簽章協定，具下列特點：

一、精進原數位簽章協定執行效率，無論在正常或爭議時的指數運算次數均優於其他學者的方案，運作時耗費執行成本較低，且數位簽章長度適中，以利實際推廣應用。

二、擴展原數位簽章協定架構，事先將相關參數存證，以應法律上對舉證責任的需求，預作未雨綢繆，因兩造對簿公堂於進行仲裁或訴訟時，舉證乃勝訴的關鍵。

三、引入公正第三者作為發生爭議解決糾紛的依據，尤其目前社會功利主義與自我意識高漲，誠信氛圍淡薄，硬拗巧詐風氣瀰漫，如遇任何一方存心毀約故意狡賴，或入侵者蓄意干擾訛詐，若無公正第三者介入仲裁，予以公正評判，所造成之損失與後果將難以評估。

四、若遭入侵者破解第一道防線時，入侵者仍需針對本研究提出的改良ElGamal-like數位簽章協定的第二道防線進行分析破解，除再增加入侵者破解成本外，更能確保本簽章協定的安全性。

五、傳送者有能力偵知簽章是否被偽造，並能提出有效佐證，停用此數位簽章適時重新協定新的簽章，保障電子商務交易環境安全。

[1] 民事訴訟法第277條

由於誠信是商業行為的核心，安全是所有商業交易的基礎，對缺乏真實人際互動的電子商務而言，建立信任與安全交易環境，始終是電子商務的核心與關鍵問題（Graff 2001; Srinivasan 2004）。此外資訊系統已成為企業營運骨幹，若發生遲滯、怠速、反應遲鈍導致運轉失靈或停機，可能癱瘓整個企業正常經營，將使企業商譽毀於一旦，在目前以降低成本為導向，追求效率為目標，服務顧客為圭臬的驅使之下，資安防護能力漸成企業營運指標的表徵之一，資訊安全是一股不可違逆的潮流，對組織或企業來說，必須衡量自身承受安全的風險與成本之平衡，訂定一套符合本身需求的資訊安全政策，才能維持企業競爭力於不墜。

致謝

感謝諸位匿名審查委員惠賜寶貴意見並悉心指正，特此致謝。

參考文獻

1. E世代公民對話誌（ALS），2007，『台灣網路安全信心調查』。（available online at http://www.als.org.tw/article/new_paper_sg.asp?id=168）
2. 周永彬、張振峰、卿斯漢，2004，『基于RSA签名的优化公平交换协议』，软件学报，第15卷．第7期：1049～1055頁。
3. 马昌社，2007，『简单快速的优化公平交换协议』，计算机工程，第33卷．第15期：13～15頁。
4. 許美玲，2006，『電子商務信賴機制締造B2C雙效雙贏』，經濟部商業司。
5. 葉亭佳，2008，『創新資訊應用研究計畫—我國網際網路用戶數調查』，經濟部技術處。
6. 詹超宇，2008a，『2008年台灣網友C2C消費發展趨勢』，資策會產業情報研究所。
7. 詹超宇，2008b，『2008年台灣網友行為與B2C消費發展趨勢』，資策會產業情報研究所。
8. 詹超宇，2009，『2008年台灣電子商店發展現況與趨勢』，資策會產業情報研究所。
9. Abernethy, S.“Building Large-Scale Online Dispute Resolution & Trustmark Systems,”*Proceedings of the UNECE Forum on ODR*, 2003.
10. Asokan, N.,Shoup, V. and Waidner, M.“Asynchronous protocols for optimistic fair exchange,”*IEEE Symposium on Research in Security and Privacy*, Oakland, CA, 1998, pp.86-99.
11. Ateniese, G.“Verifiable Encryption of Digital Signatures and Applications,”*ACM Transactions on Information and System Security* (7:1), 2004, pp.1-20.

12. Bao, F.,Deng, R. and Mao, W. "Efficient and Practical Fair Exchange Protocols with Off-line TTP," *Proceedings of IEEE Symposium on Security and Privacy*, 1998, pp.77-85.
13. Bao, F.,Deng, R.,Nguyen, K. Q. and Varadharajan, V. "Multi-party fair exchange with an off-line trusted neutral party," *Proceedings of the 10th International Workshop on Database and Expert Systems Applications*, Berlin, Germany,1999, pp. 858-863.
14. Blum, M. "How to Exchange (Secret) Keys," *ACM Transactions on Computer Systems* (1:2),1983, pp.175-193.
15. Bojanc, R. and Borka, J. B. "An economic modelling approach to information security risk management," *International Journal of Information Management* (28:5), 2008, pp.413-422.
16. Brickell, E. F.,Chaum, D.,Damgard, I. B. and Graaf, J. v. d. "Gradual and verifiable release of a secret," *Advances in Cryptology- CRYPTO 1987* pp.156-166.
17. Chen, L. "Efficient Fair Exchange with Verifiable Confirmation of Signatures," *Proc. of Advances in Cryptology (ASIACRYPT' 98)*, 1998 pp. 286-299.
18. Corritore, L. C.,Kracher, B. and Wiedenbeck, S. "On-line trust: concepts, evolving themes, a model," *International Journal of Human-Computer Studies* (58:6), 2003, pp.737-758.
19. Deng, R. H.,Gong, L.,Lazar, A. A. and Wang, W. "Practical protocols for certified electronic mail," *Journal of Network and System Management* (4:3), 1996, pp.279-300.
20. Diffie, W. "The first ten years of public-key cryptography," *Proceedings of the IEEE* (76:5), 1988, pp.560-577.
21. Diffie, W. and Hellman, M. "New Directions in Cryptography," *IEEE Transactions on Information Theory* (22:6), 1976, pp.644-654.
22. Dodis, Y. and Reyzin, L. "Breaking and repairing optimistic fair exchange from PODC2003," *ACM Workshop on Digital Right Management*, 2003, pp.47-54.
23. ElGamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans.Information Theory* (31:4), 1985, pp.469-472.
24. Even, S.,Goldreich, O. and Lempel, A. "A Randomized Protocol for Signing Contracts," *Communications of the ACM* (28:6), 1985, pp.637-647.
25. Graff, J. C. *Cryptography and E-Commerce*, John Wiley & sons. 2001
26. Harn, L. "Public-key cryptosystem design based on factoring and discrete logarithms," *Computers and Digital Techniques, IEE Proceedings* (141:3),1994 pp.193-195.
27. Harn, L. and Xu, Y. "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electronics Letters* (30:24),1994, pp.2025-2026.
28. He, J. and Kiesler, T. "Enhancing the Security of ElGamal's Signature Scheme," *IEE Proc.-E,* (141:4), 1994, pp.249-252.
29. He, W. H. "Digital signature scheme based on factoring and discrete logarithms," *Electronics Letters* (37:4), 2001, pp.220-222.

30. Horster, P.,Michels, M. and Petersen, H. *Meta-ElGamal Signature Schemes Using a Composite Module*. Technical Report TR-94-16-E University of Technology Chemnitz-Zwickau. 1994
31. Hwang, M. S.,Cheng, C. C. and Hwang, K. F.”An ElGamal-Like Cryptosystem for Enciphering Large Messages,”*IEEE Trans. on Knowledge and Engineering* (14:2), 2002, pp.445-446.
32. Hwang, S. J. and Lee, Y. H.“Repairing ElGamal-Like Multi-signature Schemes Using Self-certified Public Keys,”*Applied Mathematics and Computation* (156:1), 2004, pp.73-83.
33. Johnson, N. A. and Cooper, R. B.“Media, affect, concession, and agreement in negotiation: IM versus telephone,”*Decision Support Systems* (46:3), 2009, pp.673-684.
34. Kalakota, R. and Whinston, A. B. *Electronic Commerce: A Manager's Guide*, MA Addison-Wesley. 1997
35. Katsh, E. and Rifkin, J. *Online Dispute Resolution-Resolving Conflicts in Cyberspace*, Jossey-Bass. 2001
36. Ketchpel, S.“Transaction protection for information buyers and sellers,”*Proceedings of the Dartmouth Institute for Advanced Graduate Studies' 95*, Superhighway, Electronic Publishing and the Information, 1995.
37. Ketchpel, S. and Garcia-Molina, H.“Making trust explicit in distributed commerce transactions,”*Proceedings of the 16th International Conference on Distributed Computing Systems*, 1996, pp. 270-281.
38. Kumar, N.,K., M. and Holowczak, R.“Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls,”*Decision Support Systems* (46:1), 2008, pp.254-264.
39. Laih, C. S. and Kuo, W. C.“New Signature Schemes Based on Factoring and Discrete Logarithms,”*IEICE Trans. Fundamentals* (E80A:1), 1997, pp.46-53.
40. Lee, N. Y.“Security of Shao's Signature Schemes Based on Factoring and Discrete Logarithms,”*IEE Proc.* (146:2), 1999, pp.119-121.
41. Lee, N. Y. and Hwang, T.“The Security of He and Kiesler's Signature Schemes,”*IEE Proc.-E* (142:5), 1995, pp.370-372.
42. Lee, N. Y. and Hwang, T.“Modified Harn signature scheme based on factoring and discrete logarithms,”*IEE Proc. Computers And Digital Techniques* (143:3), 1996, pp.196-198.
43. Lim, C. H. and Lee, P. J. *A study on the proposed Korean digital signature algorithm*. Advances in Cryptology-Asiacrypt’ 98, Springer Verlag, 1998 pp.175-186.
44. Markowitch, O. and Kremer, S.“An optimistic non-repudiation protocol with transparent trusted third party,”*International Security Conference 2001 Lecture Notes in Computer Science*, Malaga, Spain, 2001, pp.363-378.

45. McCurley, K. C. "A key distribution system equivalent to factoring," *Journal of Cryptology* (1:2),1988, pp.95-106.
46. Mel, H. X. and Baker, D. M. *Cryptography Decrypted*, Addison Wesley. 2001
47. Michels, M.,Naccache, D. and Petersen, H. "GOST 34.10-A brief overview of Russia's DSA," *Computers and Security* (15:8), 1996, pp.725-732.
48. Monsuwe, T. P.,Dellaert, B. G. C. and Ruyter, K. D. "What Drives Consumers to Shop Online? A Literature Review," *Journal of Service Industry Management* (15:1), 2004, pp.102-121.
49. Naccache, D. "Can O.S.S. be Repaired? Proposal for a New Practical Signature Scheme," *Advances in Cryptology: Proceedings of Eurocrypt '93 New York*, Springer-Verlag, 1994, pp.233-239.
50. National Institute of Standards and Technology, U. S. "The Digital Signature Standard Proposed by NIST," *Communication of ACM* (35:7), 1992, pp.36-40.
51. Ong, H.,Schnorr, C.and Shamir, A. "An Efficient Signature Scheme Based On Quadratic Equations," *Proceedings of the 16th Symposium on the Theory of Computing*, Washington, 1984, pp. 208-216.
52. Park, J.,Chong, E. and Siegel, H. "Constructing fair exchange protocols for e-commerce via distributed computation of RSA signatures," *Proc. of the 22nd Annual ACM Symposium on Principles of Distributed Computing*, 2003, pp.172-181.
53. Pfitzmann, B., and Waidner, M. "Fail-stop Signatures and Their Application," *Securicom. '91*, 1991, pp. 145-160.
54. Pollard, J. and Schnorr, C. "An Efficient Solution of the Congruence $x^2 + ky^2 = m \bmod n$," *IEEE Trans. on Information Theory* (IT-33:5), 1987, pp.17-28.
55. Rabin, M. O. *Digitalized Signature and Public-Key Functions as Intractable as Factorization*. MIT/LCS/TR-212 MIT Lab. for Computer Scince, Combridge Mass. 1979
56. Ranganathan, C. and Ganapathy, S. "Key Dimensions of Bussiness-to-consumer Web Sites," *Information & Management* (39:6), 2002, pp.457-465.
57. Ray, I., Ray, I. and Natarajan, N. "An anonymous and failure resilient fair-exchange e-commerce protocol," *Decision Support Systems* (39:3), 2005, pp.267-292.
58. Rivest, R. L.,Shamir, A. and Adleman, L. "A Method for Obtaining Signatures and Public-Key Cryptosystems," *Comm. of the ACM* (21:2), 1978, pp.120-126.
59. Schmeh, K. *Cryptography and Public Key Infrastructure on the Internet*. New York, John Wiley & Sons. 2003
60. Schneier, B. *Applied Cryptography*. New York, John Wiley & Sons. 1996
61. Shao, Z. "Signature schemes based on factoring and discrete logarithms," *Computers and Digital Techniques, IEE Proceedings* (145:1), 1998, pp.33-36.
62. Shao, Z. "Digital signature schemes based on factoring and discrete logarithms," *Electronics Letters* (38:24), 2002, pp.1518-1519.

63. Shao, Z.“Fair exchange protocol of signatures based on aggregate signatures,”*Computer Communications* (31:10), 2008, pp.1961-1969.
64. Silverman, J. H. *A Friendly Introduction to Number Theory 2e*, Pearson, 2004
65. Srinivasan, S.“Role of Trust in E-Business Success,”*Information Management & Computer Security* (12:1), 2004, pp.66-72.
66. Stallings, W. *Cryptography and Network Security Principle and Practices*, Prentice Hall. 2004
67. Stinson, D. R. *Cryptography Theory and Practice*, CRC press. 2005
68. Susilo, W., Safavi, N.R., Gysin, M., and Seberry, J.“A New and Efficient Fail-stop Signature Scheme,”*The computer journal* (43:5) , 2000, pp 430-437.
69. Turban, E.,King, D.,Lee, J. K. and Viehland, D. *Electronic Commerce 2006: A Managerial Perspective*. New Jersey, Prentice Hall. 2006
70. Udo, J. G.“Privacy and Security Concerns as Major Barriers for E-Commerce: a Survey Study,”*Information Management & Computer Security* (9:4), 2001, pp.165-174.
71. Viswanathan, K.“Secure E-Commerce: Understanding the Public Key Cryptography Jigsaw Puzzle,”*Information Systems Security* (14:6), 2006, pp.44-52.
72. Wu, T. C.“ElGamal-Like Digital Signature and Multisignature Schemes Using Self-certified Public Keys,”*The Journal of systems and software* (50:2), 2000, pp.99-105.
73. Zhou, J. and Gollman, D.“A fair non-repudiation protocol,”*Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA,1996, pp.55-61.
74. Zhou, J. and Gollmann, D.“An efficient non-repudiation protocol,”*10th Computer Security Foundations Workshop, IEEE Computer Society Press*, 1997, pp.126-132.
75. Zwass, V.“Electronic Commerce: Structures and Issues,”*International Journal of Electronic Commerce* (1:1), 1996, pp.3-23.

附錄一

為探討本研究所提出的改良式ElGamal-like數位簽章協定運作方式，茲以實例說明如下：

一、正常狀況時：

（一）前置作業階段

選定二個大質數[2] $p_1=53$、$q_1=5$

$n=p_1\times q_1=53$ x $5=265$

$p=4n+1=4$ x $265+1=1061$

[2] 在實際環境中p_1、q_1應為大質數，為利說明起見，以較小的質數摹擬代替

g_1為任一模p（modulo）之原根的四次方後取其模p之餘數，故選p之原根33，四次方後為1185921取其模p之餘數，故$g_1=784$

g是模p而其序（order）為p_1故選$g=37$

1. 傳送者：

選$x_a=11$依算式（2）計算

$y_a \equiv g^{x_a} \pmod p \Leftrightarrow y_a = 37^{11} \bmod 1061 = 931$ （17）

選$k=7$依算式（3）計算$r \equiv g^k \pmod p \Leftrightarrow r = 37^7 \bmod 1061 = 268$

依算式（4）計算$w \equiv g_1^{x_a} \pmod p \Leftrightarrow w = 784^{11} \bmod 1061 = 625$ （18）

2. 接收者：

選$x_b=31$依算式（5）計算$y_b \equiv g^{x_b} \pmod p \Leftrightarrow y_b = 37^{31} \bmod 1061 = 349$

（二）交易階段

欲傳送的資料假設為$m=13$

依算式（6）$m \equiv s_1 x_a + kr \pmod n$

$s_1 \equiv x_a^{-1}(m - kr) \pmod n$

得$s_1 = 11^{-1}$（13-7x268）mod265＝192 （19）

傳送者選一個與x_a, k不相同之數$h=43$

依算式（7）$f \equiv g^h \pmod p \Leftrightarrow f = 37^{43} \bmod 1061 = 873$

依算式（8）$z \equiv s_1 y_b^h \pmod p \Leftrightarrow z = 192\text{x}349^{43} \bmod 1061 = 438$

（三）驗證階段

依算式（9）$s_1 \equiv zf^{-x_b} \pmod p \Leftrightarrow s_1 = 438\text{x}873^{-31} \bmod 1061 = 192$

依算式（10）$g^m \equiv y_a^{s_1} \times r^r \pmod p$

$g^m \pmod p \Leftrightarrow 37^{13} \bmod 1061 = 278$

$y_a^{s_1} \times r^r \pmod p \Leftrightarrow 931^{192}\text{x}268^{268} \bmod 1061 = 278$ （20）

因算式左右兩邊相等，故接收者可確認所收明文m無誤。

（四）協商爭議階段

隨機任選與n互質的一數$t=3$ 依算式（11）計算

$T \equiv g_1^t \pmod p \Leftrightarrow T = 784^3 \bmod 1061 = 19$

設$s_2 = s_1$，即$s_2 = 192$

依算式（12）$s_2 \equiv T_{x_a} + tv \pmod n$

$v \equiv t^{-1}(s_2 - T_{x_a}) \pmod n$

得$v \equiv 3^{-1}$（192-19x11）mod265＝171

依算式（13）$g_1^{s_2} \equiv w^T T^v \pmod p$

$g_1^{s_2} \pmod p \Leftrightarrow 784^{192} \bmod 1061 = 96$ （21）

$w^T T^v \pmod p \Leftrightarrow 625^{19}\text{x}19^{171} \bmod 1061 = 96$ （22）

因算式左右兩邊相等，故公正第三者（TTP）可據以仲裁此明文m是否為真確。

二、遭惡意入侵時：

為使本例證敘述簡明順暢，假設入侵者分析出私鑰與數位簽章，俾便數位簽章協定中數個連續階段依序執行。

（一）前置作業階段

假設在傳輸過程中被惡意者入侵，分析出傳送者的私鑰[3]其值x_a＝382，依算式（2）計算

$$y_a = g^{x_a} \pmod p \Leftrightarrow y_a = 37^{382} \bmod 1061 = 931 \quad (23)$$

與算式（17）所得之值相同。

（二）交易階段

此處假設惡意入侵者依算式（6）算出數位簽章[4]

$$m \equiv s_1 x_a + kr \pmod n$$

$$s_1 = 382^{-1}(13\text{-}7\text{x}268) \bmod 265 = 86 \quad (24)$$

所算出的s_1值與算式（19）所得之s_1＝192不同，傳送者即能警覺，進而發現私鑰已被x_a偽造，此時即可停止數位簽章協定運作，為使本例證敘述順暢起見，暫以s_1＝86進行下一階段。

（三）驗證階段

依算式（10）$g^m \equiv y_a^{s_1} \times r^r \pmod p$

$$g^m \pmod p \Leftrightarrow 37^{13} \bmod 1061 = 278$$

$$y_a^{s_1} \times r^r \pmod p \Leftrightarrow 931^{86}\text{x}268^{268} \bmod 1061 = 278 \quad (25)$$

與算式（20）所算之值相同，即原私鑰x_a＝11如算式（17）所示，而入侵者分析出的私鑰值x_a＝382，接收者如果疏於查證，亦即本簽章協議的第一道防線被破解，即有可能被惡意入侵者得逞的機會。

（四）協商爭議階段

依算式（13）$g_1^{s_2} \equiv w^T T^v \pmod p$ 設$s_2 = s_1$，即s_2＝86

$$g_1^{s_2} \pmod p \Leftrightarrow 784^{86} \bmod 1061 = 282 \quad (26)$$

$$w^T T^v \pmod p \Leftrightarrow 625^{19}\text{x}19^{171} \bmod 1061 = 96 \quad (27)$$

1. 算式（26～27）所得結果並不相同，無法通過算式（13）的驗證，故公正第三者可依據事先存證的w與g_1值並輔以$\{s_2,T,v\}$值，介入仲裁論斷何為正確簽章，達到解決爭議目的。

---

[3] 本階段假設惡意入侵者分析出私鑰x_a，事實上對入侵者而言，須面對解離散對數難題之複雜度，亦即在有限資源的條件下，惡意入侵者無法在多項式時間內解決此一問題。

[4] 算式（6）對惡意入侵者而言，在一個方程式中卻有二個未知數$\{x_a,k\}$，欲解得算式（6）中數位簽章的s_1值，在計算上是不可行的。實際上本研究的數位簽章協定架構中，另將s_1隱匿於算式（7～9），並未於網路上公開傳輸，入侵者無從獲得破解s_1之線索，如欲得到s_1需分析算式（9），入侵者無接收者的私鑰x_b，將遭遇解離散對數難題之複雜度。

2. 算式（13）為本簽章協定提供傳送與接收雙方第二道安全防線，原傳送者亦可經由運算異常結果，而發覺被惡意者所入侵，採取應變措施，以維電子商務交易環境安全。
3. 傳送者的原始簽章即算式（6）中的s_1與傳送者的私鑰x_a兩者密切相關，s_1隨x_a之不同而變，互為表裡關係，s_1僅是私鑰x_a衍伸出的表象，故確保傳送者的私鑰x_a，則本研究之數位簽章協定能夠保障傳送者的清白。
4. 本協定於設計之初，選定g_1為p之原根的四次方後，取其模p之餘數，且其序（order）為n，所以經mod p運算後得知w出現的次數應為n，如駭客以窮舉方式的暴力法（Brute-force search）而言，其猜中w的機率為$n/2$，因p是大質數，故駭客能得逞的機會甚低。

附錄二

以實例探討說明，在爭議協商階段本研究所提出的改良式ElGamal-like數位簽章協定第二道防線運作情形。在附錄一爭議協商階段中，原算式（11）的t值，係隨機任選一個與n互質的整數$t=3$，其運算過程不再贅述。現於算式（2～10）所使用的各參數值均不變的情形下，算式（11）的t值隨機任選一個與n互質的整數，假設$t=14$。

一、正常狀況時：

依算式（11）計算

$T \equiv g_1^{\,t} \pmod p \Leftrightarrow T = 784^{14} \bmod 1061 = 204$

依算式（12）$s_2 \equiv T_{x_a} + tv \pmod n$

$v \equiv t^{-1} \ (s_2 - T_{x_a}) \pmod n$

得$v = 14^{-1} (192\text{-}204\text{x}11) \bmod 265 = 232$

依算式（13）$g_1^{s_2} \equiv w^T T^v \pmod p$

將算式（19）所得之$s_1=192$代入s_2

$g_1^{s_2} \pmod p \Leftrightarrow 784^{192} \bmod 1061 = 96$ （28）

$w^T T^v \pmod p \Leftrightarrow 625^{204}\text{x}204^{232} \bmod 1061 = 96$ （29）

算式（13）運算後左右兩邊相等。

二、遭惡意入侵時：

依算式（13）$g_1^{s_2} \equiv w^T T^v \pmod p$

將算式（24）所得之$s_1=86$代入s_2

$g_1^{s_2} \pmod p \Leftrightarrow 784^{86} \bmod 1061 = 282$ （30）

$w^T T^v \pmod p \Leftrightarrow 625^{204}\text{x}204^{232} \bmod 1061 = 96$ （31）

算式（13）運算後左右兩邊不相等。

由算式（28～29）與（30～31）的結果觀察得知，本研究所提出的第二道防線即算

式（13），隨t值的不同，在運作時能不受侷限達到重複使用的效果，故本研究所建構的二道防線具強固性與實用價值。