一個應用於行動商務環境中以群體為導向－提名式代理簽章機制為基底之數位版權管理架構

羅濟群
交通大學資訊管理研究所

黃俊傑
交通大學資訊管理研究所

摘要

由於資訊科技進步與網路環境等基礎建設的完成，傳統的媒體與文件等相關產品亦隨之數位化。為保護數位內容及保障創作者的智慧結晶，便有數位版權管理系統(Digital Rights Management, DRM)的出現。DRM系統提供一個安全的管理平台，將數位內容轉換成受保護－數位內容，並將解密金鑰置於執照中。消費者在完成付款程序後，方能獲取該受保護－數位內容相對應之執照，以取得數位內容。因此，DRM系統對數位內容提供私密性、完整性與可認證性之保證。

在無線網路環境，行動設備有其限制及具動態的網路環境特性，因此，DRM系統必須調適至該應用環境，稱之為行動式數位版權管理(M-DRM)。在M-DRM中，關於執照合法性的認證便是一個很重要的議題。故本研究針對應用於行動商務環境之M-DRM系統內的執照合法性做研究。本研究提出一個以群體為導向－提名式代理簽章機制(Group-Oriented Nominative Proxy Signature Scheme, GO-NPSS)，在此機制中原始簽章者可將本身的簽章能力轉由一群代理人來完成，且原始簽章者可以指派哪些人具有簽章驗證能力。本研究希望在行動商務環境中，數位內容提供者可以順利的提供消費者完成執照合法性驗證的方法，由數位內容提供者指派一群代理者(n個人)，且只要同時有t 或 t 個人以上，($1 \le t \le n$)，即可完成代理簽章(Proxy Signature)的工作。數位內容提供者可以指定特定一群簽章驗證者(l個人) ，且只要同時有w或w個人以上，($1 \le w \le l$)，即可驗證由代理簽章者所產生的代理簽章之合法性。此外，本研究亦對GO-NPSS機制之安全性進行分析，以證明本研究所提之機制滿足簽章機制安全上的要求。

關鍵字：數位版權管理系統、行動式數位版權管理、執照、行動商務、以群體為導向的提名式代理簽章機制

A Group-Oriented Nominative Proxy Signature Scheme for Digital Rights Management in Mobile Commerce

Chi-Chun Lo
Institute of Information Management, National Chiao Tung University

Chun-Chieh Huang
Institute of Information Management, National Chiao Tung University

Abstract

The increasing availability of information technology and computer networks has made the process of trading digital content through Internet very convenient. However, digital contents are easy to be copied and redistributed in ways that violate the intended use of the product. Digital Rights Management (DRM) is a system used to protect digital assets and control the distribution and usage of those digital assets. DRM systems separate protected content and digital license. A digital license controls the contents to be accessed by consumers. A consumer could download digital license after paying the money. DRM systems provide confidentiality, integrity and authenticity protection for digital contents.

Nowadays, mobile commerce is getting more important as the mobile networks and services expand widely. While mobility presents some special requirements and limitations, it also creates new possibility for DRM. A DRM system must be adapted into a new one, Mobile DRM (M-DRM). One of the major issues raised by M-DRM systems concerns the integrity of this license. In this paper, we propose a group-oriented nominative proxy signature scheme (GO-NPSS) which supports a content provider to delegate his/her signing ability to the partial members of a group of clearinghouses having n members and to designate the partial members of a group of consumers, purchasing the same products, having l members to verify their digital licenses. In the proposed scheme, (t, n) proxy signers sign the specific digital license on behalf of the content provider and (w, l) verifiers verify the proxy signature. The proposed scheme can guarantee that the digital products come from the authorized providers. A formal security analysis demonstrates that our scheme is secure enough to be used in DRM systems.

Key words: Digital Rights Management, Mobile Digital Rights Management, Digital License, Mobile Commerce, Group-Oriented Nominative Proxy Signature Scheme

壹、導論

隨著網際網路(Internet)的盛行、電腦系統效能提昇及網路頻寬的加大，使得大家更容易的在網路上下載相關軟體與影視資訊。相關出版業者也將文件數位化，並將數位內容透過網路方式行銷至消費者手中。然而，大多數的數位內容都被非法放置於網路上，造成了數位內容的提供業者與著作者的傷害。為保護數位內容不易被盜用，於是有了數位版權管理系統(Digital Rights Management, DRM)概念的產生。DRM是一套安全管理系統，它提供一個信賴平台，將數位內容安全的由數位內容提供者(Content Provider)傳送至消費者(Consumer)。因此，DRM系統成為數位內容保護的屏障。

一、研究背景

DRM系統提供一套完整的解決方案，以保證數位內容不易被非法的複製與取用。故DRM系統相關技術的持續研發是非常重要的。現有的DRM系統，大都採用以執照為基礎的運作架構(License-based DRM)(Jeong et al. 2005)，亦即是說，數位內容提供者(Content Provider, CP)將受保護－數位內容(Encrypted Digital Content)和執照分開置放與傳送至消費者的手中。當消費者獲得上述兩項資料後，先從執照中獲取金鑰(Content Key, CK)，再藉由此金鑰解開受保護－數位內容。故整個DRM核心重點在於如何保護數位內容及確保執照的合法性。

在現有網路架構下的DRM系統，提供了所有安全上的保護，這些保護機制用以保障數位內容提供者所提供的數位內容的合法性、資料內容不可被複製及修改等特性。DRM系統之所以能提供上述的服務，其原因在於安全機制的建立，包括：加密系統的使用、數位浮水印(Watermarking)、數位指紋(Fingerprinting)等的應用及可信賴的計算平台之提供等等。然而，在整個DRM系統安全機制中，最重要的還是那把加密鑰匙，及如何保證這把鑰匙的合法性。由於現有網路環境，它是一個有線與無線與各種通訊平台的整合。故以企業為背景的DRM系統中，例如B2C的經營模式，其提供服務及執照管理的伺服務器都可以在線上(on-line)的環境上很容易被實踐出來。尤其是執照管理的伺服務器，因為他們是以在線上的方式提供受保護內容對應其金鑰之執照產生。對消費者而言，在完成所有的消費行為後，可以方便的獲取受保護的數位內容及相對應的執照，進而可以使用該數位商品。

然而，在現今的無線網路環境下，行動商務(Mobile Commerce)結合C2C的商業經營模式越來越普遍。故若我們思考一個純行動商務的環境，在此環境中，沒有有線網路的環境可以提供持續的網路服務，所有的服務提供者及消費者都是以行動設備來接取無線網路。此時，提供執照服務的伺服器，如何對執照進行簽署與順利的分送到消費者手中，便成了一個很重要的議題。因為它有可能因設備計算能力不足、無法提供足夠的電力或是離開了此無線網路環境等等，而使其服務被終止。因此，對於執照的簽署及取得

就無法像現有網路環境來的便利與確定。對消費者而言，就必須冒著完成付費行為，但有可能無法使用該數位商品的風險。因此，在一個純行動商務的環境中，如何確保個人所產出的數位內容不被盜用，數位執照的產生與簽署及如何將現有的DRM系統移植至此行動商務環境，成為很重要的課題。

二、研究動機與目的

無線網路(Wireless Networks)可依其架構分成有基礎網路架構(Infrastructure)與無基礎網路架構(Infrastructureless)兩種。前者藉由無線網路橋接器(Access Point, AP)提供無線網路用戶存取網路之設備；後者於無線網路環境中並沒有提供無線網路橋接器，因此，為讓封包可以順利的由來源端傳送至目的端，任一網路節點它都必須具備兩個角色，一個是主機另一個是路由，例如無基礎行動網路(Wireless Ad Hoc Networks, WANs)便是此種架構。尤其在後者的環境中，由於任一個網路節點都有可能隨時離開，導致拓樸會隨時改變，也增加網路的複雜度。除此之外，由於該節點的離開，將導致它目前正在執行與網路環境應用的程序將被中止，而無法提供服務。

數位化的內容比起傳統的媒體更易被複製與散佈，故更需要藉由DRM系統來保護數位內容。在行動商務環境中，由於行動設備有其特性與限制，例如：行動裝置的電力及其運算能力的限制及網路存取的限制，故使用DRM系統作為數位內容保護時，需考慮它的運行環境。由於任何使用者都有可能會離開網路環境。因此，若是數位內容提供者離開網路環境，如何讓消費者可以順利的獲得受保護－數位內容和執照，以及確保來源的完整性與合法性成為一個很重要的議題。因此，若能導入以群體為概念的方式來完成原先數位內容提供者必須執行的項目。如此，在以純無線網路所構成的行動商務環境中，因為可以保證線上有一群代理人員，結合他們的力量，並在以一個門檻的條件下，這群人協力合作完成執照的簽署工作便顯得更為容易。

基於上述想法，本研究針對執照合法性的驗證，提出一個以群體為導向的提名式代理簽章機制(Group-Oriented Nominative Proxy Signature Scheme, GO-NPSS)，在此機制中原始簽章者可將本身的簽章能力轉由一群代理人來完成，且原始簽章者可以指派哪些人具有簽章驗證的能力。本研究所提的GO-NPSS機制，希望在行動商務的環境中，數位內容提供者可以順利的提供消費者完成執照合法性驗證。換句話說，由數位內容提供者指派一群代理者(n個人)，且只要同時有t 或 t 個人以上，($1 \le t \le n$)，即可完成代理簽章(Proxy Signature Scheme)的工作；此外，數位內容提供者可以指定特定一群簽章驗證者(l個人) ，且只要同時有w或w個人以上，($1 \le w \le l$)，即可完成代理簽章者所產生出來的簽章的合法性驗證。在此協定下可以很清楚的發現，即使數位內容提供者暫時離開現有的無線網線環境，仍可讓消費者驗證執照是來自於他，沒有人可以竄改或偽冒。故消費者可以由執照內之金鑰解開受保護－數位內容。如此，將數位版權管理應用於行動商務環境內，對於執照之簽章與驗證部份即可獲得解決。

本研究之架構包括：第貳章為文獻探討，探討現有數位版權管理、代理簽章及提名

式代理簽章等等；第參章為本研究所提之以群體為導向－提名式代理簽章機制之內容做具體描述；第肆章為安全性分析，以保證本研究所提之機制滿足數位簽章及代理簽章機制於安全性上的要求；第伍章為效能分析；第陸章為結論及未來研究方向。

貳、文獻探討

於此章節中將針對數位版權管理、代理簽章及提名式代理簽章，作文獻探討。藉由上述的探討了解各自的特性為何。

一、數位版權管理

數位內容產業的產值隨著資訊科技與網路的發展將大大提升，例如：近來越來越多的出版業者將文件數位化，透過電子書的方式，方便消費者閱讀。然而，如何保護該數位內容而不遭受非法複製與盜用，即是一個重要的課題。DRM系統提供一個值得信賴的安全管理平台，使得數位內容不易遭受非法複製與盜用。於此系統中要達到的安全目標，主要包括：資料內容的私密性(Confidentiality)、完整性(Integrity)與可認證性(Authenticity) ，簡稱CIA。其中，私密性藉由加密與解密演算法(Encryption/ Decryption Algorithms)可達成，以防止未授權的消費者讀取數位內容；完整性是為確保資料於傳遞過程未遭受任何的修改，可藉由雜湊函數(Hash Function)與數位簽章(Digital Signature)機制達成，以防止數位內容被修改或篡改；於可認證性部份，包括資料內容認證(Content Authentication)、使用者認證(User Authentication)與硬體設備認證(Device Authentication)，以上可藉由數位浮水印(Watermarking)、生物辨識系統(Biometrics)或使用軟體機制如標簽(Ticket)或權杖(Token)方式及由可信任計算平台聯盟(Trusted Computing Platform Alliance, TCPA)/ (Trusted Computing Group, TCG)所提出的可信任的平台模組(Trusted Platform Module, TPM)等機制與技術達成，以保證資料來源、消費者及硬體設備是合法。經由上述機制的設計，即可確保數位內容提供者有足夠的保證，可將數位內容安全的送至消費者的手中。

依據Liu 等人所提的DRM系統(Liu et al. 2003)，其基本運作架構包括以下四個部份：數位內容提供者、數位內容散佈者(Content Distributor)、使用執照供應商(Clearinghouse)或稱之執照伺服器(License Server)及消費者，如下圖1及圖2所示。其中數位內容提供者將數位內容進行加密成受保護的數位內容，再將它送至數位內容散佈者。另外，並與使用執照供應商進行該數位內容的相關規範(Usage Rule)及協商產生該執照的金鑰；數位內容散佈者主要是提供受保護的數位內容讓消費者可購買或下載的環境；使用執照供應商將產生相對該數位內容的執照，並將協商的金鑰、消費者資訊、權限及憑證等相關資訊放入該執照，最後，對該執照進行簽章；消費者須提供DRM管理平台，並完成身份認證與付款後，消費者會從數位內容散佈者獲得受保護的數位內容，並從使用執照供應商獲得執照，再以執照內的金鑰以獲得數位內容。

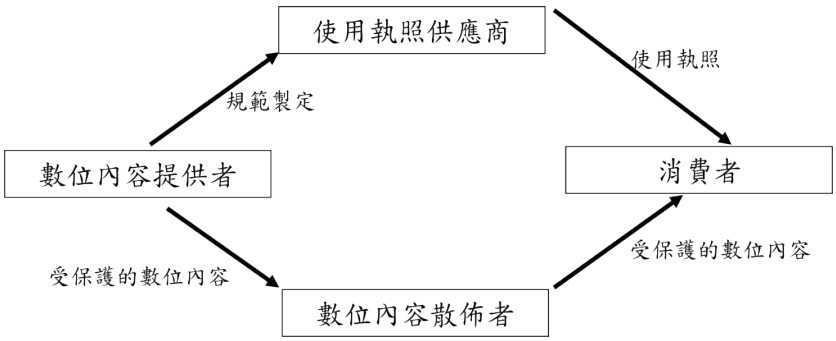

圖1：DRM系統基本架構(Liu er al. 2003)

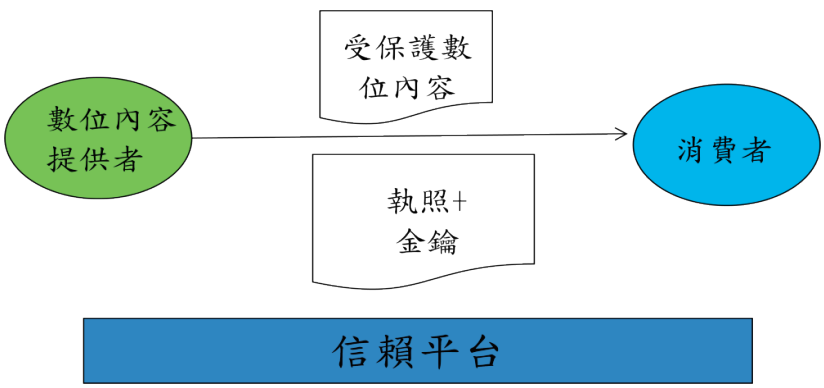

圖2：DRM系統運作模式

微軟公司亦提供數位版權管理平台(Microsoft Website)，包括office IRM (Information Rights Management)及Windows RMS(Rights Management Services)，並將其應用於手持視訊及音樂播放器上。而其金鑰及執照管理架構如下圖 3。在此架構中包括數位內容提供者、使用執照供應商及消費者三個角色。首先，藉由seed與key ID以產生受保護數位內容之加密金鑰；同理，使用執照供應商亦會使用同樣的方式產生該加密金鑰。未來此金鑰會被寫入於執照內。當消費者進行購買數位商品時，它必須完成兩個程序才能使用該數位商品。首先，它必須於數位內容提供者處下載受保護的數位內容。之後，位於消費者端的數位版權管理平台會先檢驗是否有符合該數位商品對應之執照。若不存在，必須從使用執照供應商中下載該執照。當使用者獲得執照後，必須確認該執照的合法性，以避免使用到偽冒之執照。待所有程序完成後，消費者即可使用該執照將受保護的數位內容解開，進而使用該商品。

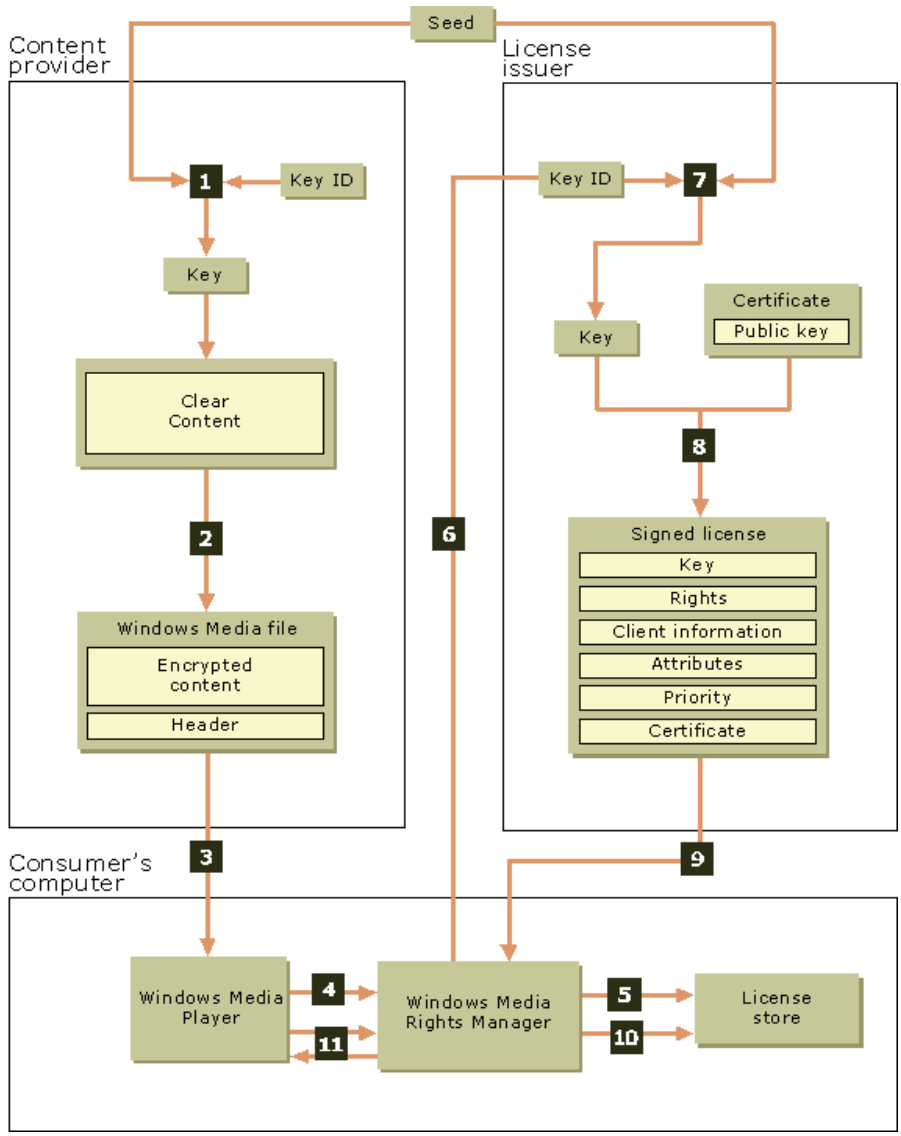

圖3：微軟金鑰及執照管理架構 (Microsoft Website)

開放式行動聯盟(Open Mobile Alliance, OMA)針對行動商務環境提出DRM管理架構，包括於2002年起草並於2004年被制定的OMA DRM 1.0及2004年起草並於2006年被制定的OMA DRM 2.0。其中OMA DRM 1.0包括：向前鎖定(Forward-Lock)、組合傳遞(Combined Delivery)與分開遞送(Separate Delivery)等三種架構(OMA DRM Website)。這三種架構之消費者端可以藉由mms協定(Multimedia Messaging Service)將數位內容或受保護的數位內容下載至行動平台。向前鎖定限制數位內容無法由消費者轉傳至其他位置；後兩者的差異在於受保護的數位內容與執照是否分開存放，若合在一起則為組合傳遞模式，若是分

開則為分開遞送模式，在此模式中執照可藉由WAP Push協定傳送至該消費者手中。OMA DRM 2.0是延伸OMA DRM 1.0之分開遞送模式而來。在此架構下增加了公開金鑰基礎建設(Public Key Infrastructure, PKI)的憑證管理架構，用公開金鑰將執照進行加密，以提升整個系統的安全性。目前大多數應用於行動商務的DRM系統是採用分開遞送模式。目前大多數應用於行動商務的DRM系統是採用分開遞送模式。

二、 代理簽章機制

代理簽章機制是數位簽章的一個變形，已經陸續被應用在分散式的計算環境(Lee et al. 2001; Kim et al. 2001; Kesselman et al. 1998)。例如：Lee等人所提的強代理簽章機制(Strong Proxy Signature Scheme)、Kim等人所提的單次代理簽章機制(One-time Proxy Signature Scheme)等。數位簽章具有完整性、可認證性、可驗證性(Verifiability)、不可偽造性(Unforgeability)與不可否認性(Non-repudiability)等特性。其中完整性與可認證性已於數位版權管理描述；可驗證性指的是驗證者可以驗證此簽章之合法性；不可偽造性指的是任何一個人都無法偽造原始簽章者的身份產生數位簽章；不可否認性的目的是為確保原始簽章者不能否認他所簽署的文件。而代理簽章指的是原始簽章者可以將其簽章能力委派給一個代理人來負責。於1996年Mambo, Usuda與Okamoto最早提出代理簽章機制(Mambo et al. 1996)，之後陸續有學者提出新的代理簽章機制，例如：門檻式代理簽章(Threshold Proxy Signature)(Sun 1999; Sun et al. 1999; Zhang 1997)與多重代理簽章(Multi-Proxy Signature)(Hwang & Shi 2000)等等。

代理簽章機制可依照原始簽章者授權方式區分成：完全授權(Full Delegation)、部份授權(Partial Delegation)、授權憑證(Warrant)與結合授權憑證之部份授權(Delegation by Warrant)等四種模式。

1. 完全授權模式：原始簽章者將簽章所需的私密金鑰交給代理簽章者，此時代理簽章者具有等同於原始簽章者的能力。此種授權方式非常危險，因為代理簽章者擁有它的私密金鑰，所以它可以隨意簽署任何文件，且驗證者無法從所簽署之文件辨別是由原始簽章者所簽署或是由代理簽章者所簽署。
2. 部份授權模式：原始簽章者將個人的私密金鑰經過一系列的計算產生代理金鑰(Proxy Key)，然後送給代理簽章者。因此，代理簽章者可利用此金鑰產生代理簽章。由於原始簽章者所持的金鑰與代理簽章者所持代理金鑰不一樣，因此，驗證者可以區別此簽署文件是由何者簽署。而在此授權模式下，又可區分未受保護(Proxy-Unprotected)與受保護(Proxy-Protected)兩種狀況：前者，代理簽章者直接使用代理金鑰對文件作簽署，此種方式雖可區別原始簽章與代理簽章之不同，但對代理簽章者而言並不公平，因為假若原始簽章者利用此代理金鑰對文件簽署，對驗證者而言，它無法辨認是由何者所簽署；後者，代理簽章者收到代理金鑰後，並非直接使用它，而是將它與自己的私密金鑰經過一系列的計算，以產生新的代理金鑰，當有文件需要簽署時，使用新的代理金鑰加以簽署，它解決了公平

性問題，亦即是說，原始簽章者由於沒有代理簽章者之代理金鑰，故無法假冒代理簽章者對文件作簽署。

3. 授權憑證：由原始簽章者之私密金鑰簽署後產生一個授權憑證給代理簽章者，此憑證內容需包括代理權限與期限及可簽署文件的類型等等。代理簽章者拿到此憑證之後，利用自己的私密金鑰簽署所需代簽之文件，並將憑證一起送給接收者。而驗證者它除了需驗證此簽署文件的正確性外，還需檢查此憑證之合法性，以確保是否由原始簽章者授權給此代理簽章者簽署之文件。
4. 結合授權憑證之部份授權：此授權模式結合授權憑證與部份授權之特性。換句話說，代理簽章者除了獲得原始簽章者的授權憑證外，它還會獲得原始簽章者的代理金鑰。對代理簽章者而言，它可以採未受保護或受保護模式進行簽章之產生。

代理簽章除了須符合數位簽章之完整性、可認證性、可驗證性、不可偽造性與不可否認性外，它還必須具備可區別性(Distinguishability)、識別性(Identifiability)與不可轉移性(Non-Transferability)。可區別性指的是由代理簽章者所產生的代理簽章與原始簽章者所產生的簽章是可被辨別的；識別性指的是從代理簽章之內容，原始簽章者可以知道代理簽章者的身份；不可轉移性指的是代理簽章者不可將原始簽章者所授予的代理簽章能力轉移至他人手中。

三、提名式代理簽章機制

最早提出提名式簽章機制(Nominative Signature Scheme)是由Kim等學者在1995提出(Kim et al. 1995; Kim et al. 1996)，之後Park等學者(Park & Lee 2001)將其觀念與代理簽章結合在一起，稱之為提名式代理簽章(Nominative Proxy Signature Scheme)。在此之後，後續有學者Tan等人(Tan & Liu 2004)，在此機制下做部份修改。它與代理簽章最不同的地方，在於它必須透過第三者，亦即被提名者(Nominee)的幫忙來驗證簽章的有效性。因此，它比代理簽章機制更適合用在行動商務的環境。由於提名式代理簽章只能由被提名者來驗證，因此原始簽章者及代理者的身份都可以被保密。除了保密性的優點外，由於一般的行動裝置本身的計算能力及電力都較為缺乏，透過提名式代理簽章的方式，原始簽章者就可以把簽章原本要執行的大量計算，交付給代理簽章者來做，以節省電力。

依據驗證者被提名的方式可分成：原始簽章者提名式代理簽章(Original-nominative proxy signature) 與由代理簽章者來提名驗證者的提名式代理簽章(Proxy-nominative proxy signature)。其中原始簽章者提名式代理簽章機制較適合訊息接收者是由原始簽章者決定的無線通訊環境，這是因為原始簽章者有權決定驗證者的身份；而proxy-nominative proxy signature則較適合用於電子商務環境，這是因為原始簽章者如同製造商的角色，而代理簽章者如同銷售商的角色，故由銷售商決定驗證者(消費者)的角色較為恰當。另外，提名式代理簽章機制必須滿足下述特性：

1. 必須滿足所有數位簽章與代理簽章的特性。
2. 只有原始簽章者(或代理簽章者)，可以提名驗證者。

3. 原始簽章者與代理簽章者不可否認他們所產生的簽章。
4. 只有被提名者可以直接驗證代理簽章是否有效。
5. 如果有必要，只有被提名者可以向第三者證明簽章的有效性。

參、以群體為導向的提名式代理簽章機制

一、研究架構

本研究將設計一個符合在行動商務的環境中，就DRM系統中執照之簽章產生與驗證，提出一個稱之為以群體為導向的提名式代理簽章機制(GO-NPSS)。在行動商務環境中，每一個主機都需考量本身電力的耗費與計算能力的可行性以及有可能因為無線網路環境暫時無法提供鏈結等，所造成執行中的程序被強迫中止的問題。因此，必須思考某些執行緒不是本身可以負荷或是某些應用於網路環境的服務可能會被中止。為此，本研究針對在行動商務環境中，若由單一數位內容提供者及消費者執行執照之簽章產生與驗證，可能會面臨上述問題，提出一個可行的解決方案。

由於現今無線網路環境蓬勃發展，例如：802.11n標準的提出再加上3G與4G環境慢慢建置完成，行動商務已經成為可行的方案。越來越多的人願意將自己的創意包裝成數位商品，並置放於網路銷售。針對這種越來越成熟的C2C線上商業經營模式，創意者的數位商品應該要加以保護，以防止被非法的複製與盜用。因此，將DRM系統應用於行動商務的環境有其必要性，在此稱為行動式數位版權管理(Mobile DRM, M-DRM)。在C2C經營模式下的M-DRM並不需要數位內容散佈者的角色，消費者可以直接在數位內容提供者處下載受保護－數位內容，故M-DRM架構如下圖 4所示。M-DRM系統主要的工作是保護數位內容及確保執照的合法性。如同文獻探討所描述，因無線網路環境之限制，不能直接將現有DRM系統應用於行動商務環境。故本研究就M-DRM系統中執照之簽章產生與驗證，提出GO-NPSS之簽章產生與驗證機制，以符合行動商務環境的要求。

於GO-NPSS機制中，對執照之簽章產生與驗證之概念設計如下：數位內容提供者扮演原始簽章者的角色，一群使用執照供應商扮演代理簽章者的角色，對同一種產品之消費者扮演簽章驗證者的角色。在GO-NPSS機制中數位內容提供者可將本身的簽章能力轉由一群使用執照供應商來完成，且數位內容提供者可以指派哪些人具有簽章驗證的能力。換句話說，由數位內容提供者指派一群使用執照供應商(n個人)，且只要同時有t 或 t 個人以上，($1 \le t \le n$)，即可完成代理簽章的工作；此外，數位內容提供者可以指定特定一群消費者者(l個人)，且只要同時有 w 或 w 個人以上，($1 \le w \le l$)，即可完成驗證由使用執照供應商所產生出來的代理簽章的合法性。除此之外，本研究所提的GO-NPSS機制需滿足數位簽章、代理簽章與提名式代理簽章之安全性要求。故在本研究機制下即使數位內容提供者或使用執照供應商暫時無法提供服務或消費者無法單獨完成執照簽章驗證工作的條件下，仍可順利進行執照簽章的產生與驗證。

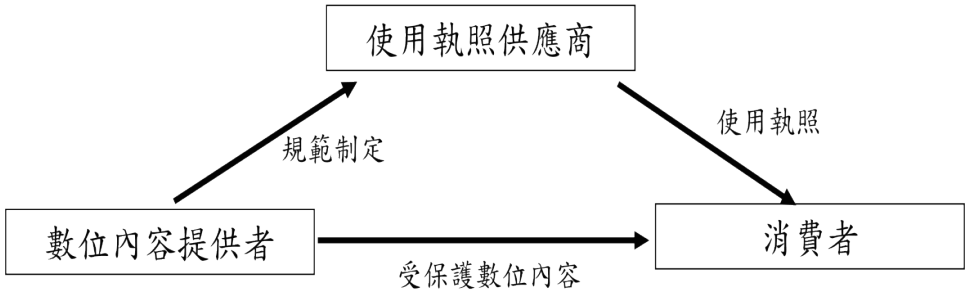

圖4：M-DRM系統基本架構

二、GO-NPSS機制參數描述

由於GO-NPSS機制是基於數論(Number Theory)的基礎下完成安全性的設計，故本小節將針對GO-NPSS機制之所需參數進行描述。相關參數之描述如下表 1所示。

表1：GO-NPSS機制參數描述

Items	Descriptions
p	a large prime
q	a large prime and a factor of p-1
g	a generator in GF(p) with order q , such that mod $g^q \equiv 1 \ mod \ p$
CP	Content provider, the role of original signer
CHG	A group of clearinghouses, the role of proxy signers
CVG	A group of consumers, the role of signature verifiers
x_i	i's private key
y_i	i's public key, such that $y_i \equiv g^{x_i} mod \ p$
PV_{CHG}	CHG's private key
PPV_{CHGi}	Partial proxy group private key generated by $CHGi$
y_{CHG}	CHG's public key, such that $y_{CHG} \equiv g^{pv} mod \ p$
PV_{CVG}	CVG's private key
PPV_{CVGj}	Partial verifier group private key generated by CVG_j
y_{CVG}	CVG's public key, such that $y_{CHG} \equiv g^{pvCVG} mod \ p$
M_w	A warrant which records the identities of CP, CHG, and CVG, license, t, n, w, l, and expiration time
T	Time stamp which against replay attack
k_1, k_2	Shared by CHG members
h (·)	One-way Hash Function, this function operates on an arbitrary length input message M and returns with fixed length
‖	Concatenation, the operation of joining two character strings

三、GO-NPSS機制之設計

GO-NPSS機制之設計是以群體為導向的提名式代理簽章機制，其內涵為：群體導向表示具門檻式秘密分享(Threshold-Based Secret Sharing)，而提名式代理簽章機制表示某一個受保護－數位內容對應之執照的簽章產生與驗證方式，如下圖 5。另外，GO-NPSS採用原始簽章者提名式代理簽章及結合授權憑證之部份授權模式而成。GO-NPSS之安全性乃基於解因數分解(Factorization Problem, FP)與離散對數(Discrete Logarithm Problem, DLP)之困難度上完成，相關的安全性分析將於下章節做詳盡說明。

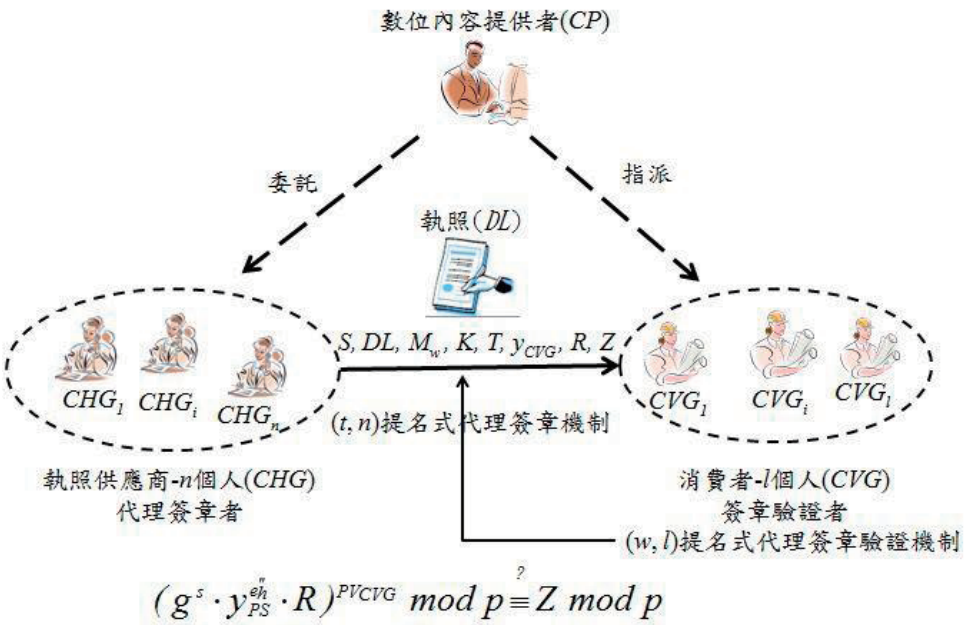

圖5：GO-NPSS機制

GO-NPSS機制共分成五個階段完成，包括：初始階段(Initialization Phase)、委派階段(Delegation Phase)、代理金鑰產生階段(Proxy Key Generation Phase)、提名式代理簽章產生階段(Nominative Proxy Signature Generation Phase)與原始簽章者提名式代理簽章驗證階段(Original-Nominative Proxy Signature Verification Phase)。以下將就各階段內容做說明：

1. 初始階段

於初始階段主要工作是讓 *CHG* 成員與 *CVG* 成員產生他們各的自私密金鑰分享，即是 s_{CHGi} 與 s_{CVGj}。這兩個私密金鑰均由各自的群組成員採秘密分享的機制產生。用此方式產生的群體私密金鑰，更具有公平性。這是因為群體中的成員共同參與私密金鑰的產生。

首先，*CP* 需先決定參與的成員，其中：*CHG* 成員為 $\{CHG_1, CHG_2, \ldots, CHG_n\}$ ，*CVG*

成員為$\{CVG_1, CVG_2, \ldots, CVG_l\}$，並完成所有成員的身份認證，成為合法的群組成員。此身份認證可採以無線公開金鑰基礎建設(Wireless Public Key Infrastructure, WPKI)之數位憑證完成。WPKI是應用於無線網路環境PKI機制，其功能包括：身分認證、存取控管、使用授權、傳輸保密、資料完整性與不可否認性等。WPKI運作機制包括PKI註冊及安全交易。當任一使用者向PKI Portal申請憑證時，WPKI Portal傳送憑證的URL位置，且憑證機構也會將該憑證傳給憑證資料庫。未來使用者可使用自身的憑證完成身份認證之程序。

另外，*CP* 公開p、q 與 g 等系統參數給所有成員。以下就 *CHG* 私密金鑰與 *CVG* 私密金鑰產生與分享作描述：

1.1 *CHG* 私密金鑰分享產生，如下圖 6：

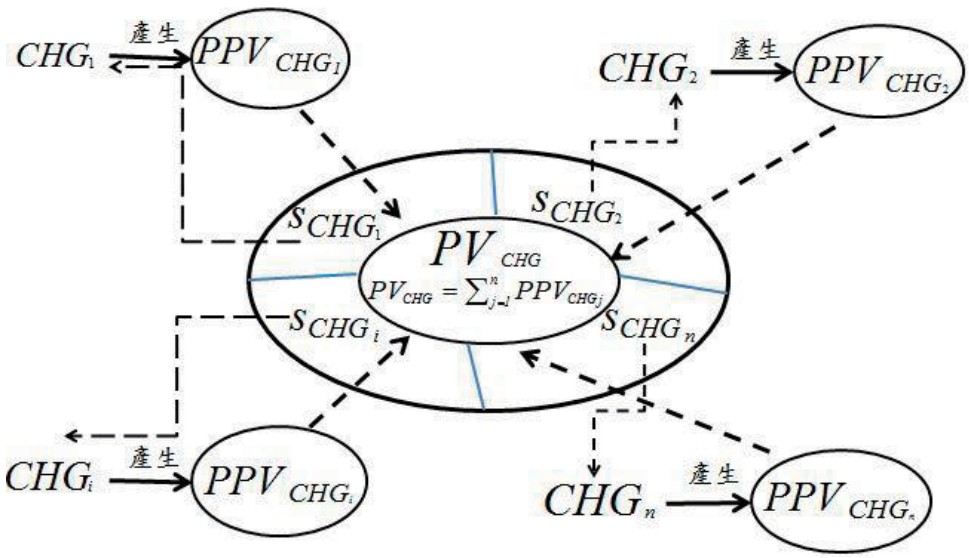

圖6：*CHG*私密金鑰分享產生

*CHG*內的成員 *CHGi* 依下列五個步驟產生PV_{CHG}之分享 $S_{CHG\,i}$。

- 步驟1：*CHG* 部份私密金鑰產生

於此步驟，每位*CHG*成員*CHGi*藉由亂數產生器隨機產生兩個參數$a_{CHG_i}, PPV_{CHG_i} \in_R Z_q^*$，並完成下列式子的計算及簽章$sign(h(PPV_{CHG_i}), r_{CHG_i}, c_{CHG_i})$的產生：

$$r_{CHG_i} \equiv g^{a_{CHG_i}} mod\ p \quad (1)$$

$$PPV_{CHG_i} \equiv x_{CHG_i} \cdot r_{CHG_i} + a_{CHG_i} \cdot c_{CHG_i}\ mod\ q \quad (2)$$

$$y'_{CHG_i} \equiv g^{PPV_{CHG_i}} \equiv y_{CHG_i}{}^{r_{CHG_i}} \cdot r_{CHG_i}{}^{c_{CHG_i}}\ mod\ p \quad (3)$$

於式(2)中，PPV_{CHG_i} 為成員*CHGi* 所貢獻之部份私密金鑰。當所有 PPV_{CHG_i} 被產生後，*CHG* 之私密金鑰，PV_{CHG}，即可被計算出來。PPV_{CHG_i} 並不會直接被廣播至*CHG*中，取而代之的，它將被轉換成y'_{CHG_i}，產生方式如式(3)所示。此外，由於要算出

PPV_{CHG_i}是一個DLP的問題，故除了*CHGi*本身外，沒有人可以推出此部份私密金鑰。

● 步驟2：PPV_{CHG_i}秘密分享

於此步驟，*CHGi*藉由秘密分享機制將PPV_{CHG_i}分享給*CHG*成員。首先，*CHGi*產生一個維度(Degree)為$t-1$的多項式$f_i(\beta)$，如式(4)所示。未來每位*CHGj*可獲得*CHGi*的祕密分享$f_i(j)$。當有t個或t個以上的*CHGi*成員合作時，藉由Lagrange多項式內插法(Lagrange Interpolation)可重建PPV_{CHG_i}。

$$f_i(\beta) = PPV_{CHG_i} + e_{i,1}\beta + e_{i,2}\beta^2 + \cdots + e_{i,t-1}\beta^{t-1} \bmod q \quad (4)$$

$$f_i(j),\ \forall j = 1, \ldots, n; j \neq i \quad (5)$$

● 步驟3：PPV_{CHG_i}秘密分享

於此步驟，*CHGi*安全的將$f_i(j)$送至*CHGj*，並廣播$g^{PPV_{CHG_i}}$, $g^{e_{i,1}}$, …, $g^{e_{i,t-1}}$。

● 步驟4：PPV_{CHG_i}秘密分享驗證

於此步驟，*CHGi*驗證所有*CHGj*之$f_j(i)$的有效性。其驗證方式如下：

$$g^{f_j(i)} \equiv g^{PPV_{CHG_j}} \cdot (g^{e_{j,1}})^i \cdot (g^{e_{j,2}})^{i^2} \cdots (g^{e_{j,t-1}})^{i^{t-1}} \bmod p \equiv g^{PPV_{CHG_j}} \cdot A_{j,1}^{i} \cdot A_{j,2}^{i^2} \cdots A_{j,t-1}^{i^{t-1}}, \text{ where } A_{j,k} = g^{e_{j,k}},\ \forall k = 1, \ldots, t-1. \quad (6)$$

● 步驟5：PV_{CHG}秘密分享

若*CHGi*完成所有驗證，並確認所獲得的分享都是合法後，計算$s_{CHG_i} = \sum_{j=1}^{n} f_j(i) \bmod q$。此外，$s_{CHGi}$就是$PV_{CHG}$的分享。這是因為在不失一般性(Without Loss of Generality, W.L.O.G)的情況下，令

$$f(\beta) = PV_{CHG} + e_1\beta + e_2\beta^2 + \cdots + e_{t-1}\beta^{t-1} \bmod q = \sum_{j=1}^{n} f_j(\beta) \bmod q, \text{ where } PV_{CHG} = \sum_{j=1}^{n} PPV_{CHG_j} \quad (7)$$

$$s_{CHG_i} = f(i) = \sum_{j=1}^{n} f_j(i) \bmod q \quad (8)$$

式(7)是用來產生PV_{CHG}秘密分享的多項式。由式(8)得知，s_{CHGi}就是*CHGi*在PV_{CHG}中所獲取的分享$f(i)$。此外，*CHG*的公開金鑰，y_{CHG}，可由式(9)產生。

$$y_{CHG} \equiv g^{PV_{CHG}} \bmod p \quad (9)$$

由於PV_{CHG}於式(9)之安全性乃基於解DLP的困難度，即使有攻擊者獲取y_{CvG}和g，仍無法解出PV_{CHG}。換句話說，只有任*CHG*中成員個數達到t個或以上合作，才能重建多項式而獲得PV_{CHG}。

1.2 *CVG*私密金鑰分享產生，如下圖7：

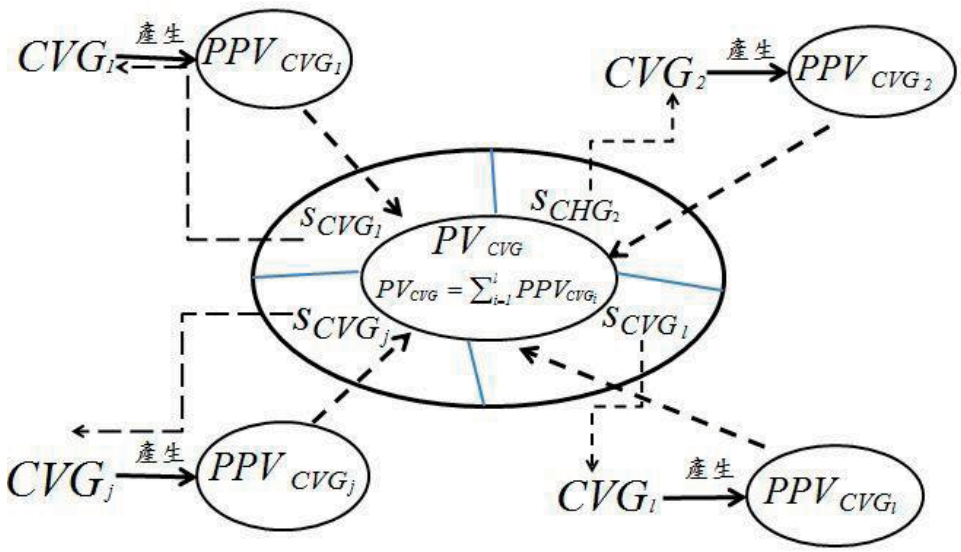

圖7：*CVG*私密金鑰分享產生

*CVG*內的成員CVG_j依下列五個步驟產生PV_{CVG}之分享S_{CVGj}。

● 步驟1：*CVG*部份私密金鑰產生

於此步驟，每位*CVG*成員CVG_j藉由亂數產生器隨機產生兩個參數$a'_{CVG_j}, PPV_{CVG_j} \in_R Z_q^*$，並完成下列式子的計算及簽章$sign(PPV_{CVG_j}), r'_{CVG_j}, c'_{CVG_j})$的產生：

$$r'_{CVG_j} \equiv g^{a'_{CVG_j}} mod\ p \quad (10)$$

$$PPV_{CVG_j} \equiv x_{CVG_j} \cdot r'_{CVG_j} + a'_{CVG_j} \cdot c'_{CVG_j}\ mod\ q \quad (11)$$

$$y'_{CVG_j} \equiv g^{PPV_{CVG_j}} \equiv y_{CVG_j}{}^{r'_{CVG_j}} \cdot r'_{CVG_j}{}^{c'_{CVG_j}}\ mod\ p \quad (12)$$

於式(11)中，PPV_{CVG_i}為成員CVG_j所貢獻之部份私密金鑰。當所有PPV_{CVG_i}被產生後，*CVG*之私密金鑰，PV_{CVG}，即可被計算出來。PPV_{CVG_i}並不會直接被廣播至*CVG*中，取而代之的，它將被轉換成y'_{CVG_j}，產生方式如式(12)所示。此外，由於要算出PPV_{CVG_i}是一個DLP的問題，故除了CVG_j本身外，沒有人可以推出此部份私密金鑰。

● 步驟2：PPV_{CVG_i}秘密分享

於此步驟，CVG_j藉由秘密分享機制將PPV_{CVG_i}分享給*CVG*成員。首先，CVG_j產生一個維度為 *w - 1* 的多項式$\psi_j(\beta)$，如式(13)所示。未來每位 CVG_j可獲得 CVG_j的祕密分享 $\psi_j(i)$。當有 *w* 個或 *w* 個以上的 CVG_j成員合作時，藉由Lagrange多項式內插法可重建 PPV_{CVG_i}。

$$\psi_j(\beta) = PPV_{CVG_j} + e_{j,1}\beta + e_{j,2}\beta^2 + \cdots + e_{j,w-1}\beta^{w-1}\ mod\ q \quad (13)$$

$$\psi_j(i),\ \forall i = 1, \ldots, l; i \neq j \quad (14)$$

● 步驟3： PPV_{CVG_i}秘密分享傳遞

於此步驟， CVG_j 安全的將 $\psi_j(i)$ 送至 CVG_j，並廣播$g^{PPV_{CVG_j}}$, $g^{e_{j,1}}$, …, $g^{e_{j,w-1}}$。

● 步驟4： PPV_{CVG_i} 秘密分享驗證

於此步驟，CVG_j 驗證所有CVG_j 之 $\psi_i(j)$ 的有效性。其驗證方式如下：

$$g^{\psi_i(j)} \equiv g^{PPV_{CVG_i}} \cdot (g^{e_{i,1}})^{j} \cdot (g^{e_{i,2}})^{j^2} \cdots \cdot (g^{e_{i,w-1}})^{j^{w-1}} \bmod p \equiv g^{b'v_j} \cdot B_{i,1}^{j} \cdot B_{i,2}^{j^2} \cdots \cdot B_{i,w-1}^{j^{w-1}}; \text{ where } B_{i,k} = g^{e_{i,k}},\ \forall k = 1, \ldots, w-1. \quad (15)$$

● 步驟5：PPV_{CVG_i} 分享產生

若CVG_j 完成所有驗證，並確認所獲得的分享都是合法後，計算 $s_{CVG_j} = \sum_{i=1}^{l} \psi_i(j) \bmod q$ 此外，S_{CVGj} 就是 PV_{CVG} 的分享。這是因為在W.L.O.G的情況下，令

$$\psi(\beta) = PV_{CVG} + e_1\beta + e_2\beta^2 + \cdots + e_{w-1}\beta^{w-1} \bmod q = \sum_{i=1}^{l} \psi_i(\beta); \text{ where } PV_{CVG} = \sum_{i=1}^{l} PPV_{CVG_i} \quad (16)$$

$$s_{CVG_j} = \psi(j) = \sum_{i=1}^{l} \psi_i(j) \bmod q \quad (17)$$

式(16)是用來產生 PV_{CVG} 秘密分享的多項式。由式(17)得知，s_{CVG_j} 就是CVG_j 在 PV_{CVG} 中所獲取的分享$\psi(j)$。此外，CVG 的公開金鑰， y_{CVG}，可由式(18)產生。

$$y_{CVG} \equiv g^{PV_{CVG}} \bmod p \quad (18)$$

由於 PV_{CVG} 於式(18)之安全性乃基於解DLP的困難度，即使有攻擊者獲取 Y_{CVG} 和 g，仍無法解出 PV_{CVG} 。換句話說，只有任CVG 中成員個數達到 w 個或 w 個以上合作，才能重建多項式而獲得 PV_{CVG} 。

2.委派階段

於委派階段主要工作是 CP 將產生代理分享(Proxy Shares)給 CHG 之成員。本階段共包含下列四個步驟：

● 步驟1： CP 之代理金鑰產生

於此步驟，CP 依受保護－數位內容對應之執照產生一個授權憑證 Mw，並藉由亂數產生器隨機選取一個參數$k \in_R Z_q^*$，並計算：

$$K \equiv g^k \bmod p \quad (19)$$

$$e_h = h(M_w||T||K||y_{CVG}) \quad (20)$$

$$\sigma \equiv x_{CP} \cdot e_h + k \bmod q \quad (21)$$

於式(21)中，σ 即是 CP 所產生的代理金鑰，此代理金鑰隱含著 CP 與 CVG 的資訊、Mw 資訊及時間戳記等資訊。其中執照資訊雖隱含於 Mw 中，但由於解開受保護－數位

內容所需金鑰是被加密，故未來只有那群被 *CP* 指定為 *CVG* 之消費者方能獲得該金鑰。*CP* 藉由秘密分享機制將σ分享給 *CHG* 之成員 CHG_i ，未來只要有 *t* 個或 *t* 個以上成員之合作，即可重建 CHG_i。

● 步驟2： σ 秘密分享

於此步驟， *CP* 藉由秘密分享機制將 σ 分享給 *CHG* 之成員 CHG_i，如式(22)所示。

$$f'(\beta) = \sigma + d_1\beta + d_2\beta^2 + \cdots + d_{t-1}\beta^{t-1} \tag{22}$$

$$\sigma_{CHG_i} \equiv f'(i); \forall i = 1, \ldots, n \tag{23}$$

於式(23)中， σ_{CHG_i} 即是 CHG_i 所獲得的 σ 之部份分享。只有在 *t* 個或 *t* 個以上 *CHG* 成員之合作下，方可重建 σ 。

● 步驟3： σ_{CHG_i} 傳遞

於此步驟， *CP* 安全的將 σ_{CHG_i} 傳遞給 CHG_i，並將; $D_j \equiv g^{d_j} mod\ p;\ \forall j = 1, \ldots, n$ 及廣播 $(M_w||T||K||y_{CVG})$ 。

● 步驟4： σ_{CHG_i} 驗證

於此步驟，CHG_i 藉由 $e_h{}^*$計算，如式(24)所示，與式(25)之驗證。若驗證後滿足則接受此 σ_{CHG_i} ，否則拒絕 σ_{CHG_i} 。

$$e_h{}^* = h(M_w||T||K||y_{CVG}) \tag{24}$$

$$g^{\sigma_{CHG_i}} \equiv y_{CP}{}^{e_h{}^*} \cdot K \cdot \prod_{j=1}^{t-1} D_j{}^{i^j}\ mod\ p \tag{25}$$

式(25)之證明如下：

Pf:

$$\because g^{\sigma_{CHG_i}} mod\ p = g^{f'(i)} mod\ p$$

$$\Rightarrow g^{\sigma_{CHG_i}} mod\ p = \left(g^{\sigma + d_1 i + d_2 i^2 + \cdots + d_{t-1} i^{t-1}}\right) mod\ p$$

$$= \left(g^{x_{CP} \cdot e_h + k} \cdot \prod_{j=1}^{t-1} D_j{}^{i^j}\right) mod\ p$$

$$= \left(y_{CP}{}^{e_h{}^*} \cdot K \cdot \prod_{j=1}^{t-1} D_j{}^{i^j}\right) mod\ p$$

Q.E.D

3.代理金鑰產生階段

由於本研究採受保護提名式代理簽章機制，故CHG_i 並不會直接使用 σ_{CHG_i}。於本階段，CHG_i 會將 σ_{CHG_i} 轉換成$\sigma_{CHG_i}{}'$，如式(26)所示。在W.L.O.G的情況下，假設有 *t* 個 *CHG* 成員 $\{CHG_1, CHG_2, \ldots, CHG_t\}$，他們各自計算自己的 $\sigma_{CHG_i}{}'$：

$$\sigma_{CHG_i}{}' \equiv \sigma_{CHG_i} + s_{CHG_i} \cdot e_h\ mod\ q \tag{26}$$

由於 $\sigma_{CHG_i}{}'$ 隱含著 CHG_i 的身份資訊，未來 CHG_i 不能否認它曾經協助 CP 完成代理簽章的工作。

4.提名式代理簽章產生階段

於提名式代理簽章產生階段，CHG 成員 $\{CHG_1, CHG_2, \ldots, CHG_t\}$ 主要工作是對執照 (DL)進行簽署。本研究所提之提名式代理簽章，於簽署過程並不會揭露他們的代理金鑰 $\sigma_{CHG_i}{}'$。本階段共包含下列三個步驟：

- 步驟1：ξ_{CHG_i} 產生

於此步驟，k_1 與 k_2 這個參數是被CHG_i成員所分享，其分享之產生與重建與初始階段之秘密分享作法一致。每個 CHG_i 產生 ξ_{CHG_i}，其計算方式如式(27)所示。其中 $(k_2)_{CHG_i}$ 為 CHG_i 對 k_2 之分享，而 $e_h{}'$ 之內容如式(28)所示。

$$\xi_{CHG_i} \equiv (k_2)_{CHG_i} - \sigma_{CHG_i}{}' \cdot e_h{}' \bmod q \tag{27}$$

$$e_h{}' = h(DL||M_w||T||K||y_{CVG}) \tag{28}$$

- 步驟2： ξ_{CHG_i} 傳遞與驗證

於此步驟，CHG_i 安全的將 ξ_{CHG_i} 傳遞給$\{CHG_1, CHG_2, \ldots, CHG_t\}$。當 CHG_i 接收到來自 CHG_{ij} 的 ξ_{CHG_j} 後，它會採下式(29)方式完成驗證之程序。

$$g^{\xi_{CHG_j}} \bmod p \stackrel{?}{\equiv} (y_{(k_2)_{CHG_j}} \cdot \prod_{i=1}^{t-1} {Q_i}^{j^i}) \cdot [{y_{CP}}^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} {D_j}^{i^j} \cdot (y_{CHG} \cdot \prod_{i=1}^{t-1} {A_i}^{j^i})^{e_h}]^{-e_h{}'} \bmod p \tag{29}$$

於式(29)中 $y_{(k_2)_{CHG_j}}$ 即是 $(k_2)_{CHG_j}$ 以 g 為原根之模 p 運算，亦即是說，$y_{(k_2)_{CHG_j}} \equiv g^{(k_2)_{p_j}} \bmod p$。而； $Q_i \equiv g^{q_i} \bmod p;\ \forall i = 1, \ldots, t-1$。

Pf:

$$\because g^{\xi_{p_j}} \bmod p = g^{(k_2)_{CHG_j} - \sigma_{CHG_j}{}' \cdot e_h{}'} \bmod p$$

$$\Rightarrow g^{\xi_{p_j}} \bmod p = \left(g^{(k_2)_{CHG_j} + q_1 \cdot j + q_2 \cdot j^2 + \cdots + q_{t-1} \cdot j^{t-1}}\right) \cdot (g^{\sigma_{CHG_j}{}'})^{-e_h{}'} \bmod p$$

$$= \left(\left(y_{k_2}\right)_{p_j} \cdot \prod_{i=1}^{t-1} {Q_i}^{j^i}\right) \cdot \left(g^{\sigma_{CHG_j} + s_{CHG_j} \cdot e_h}\right)^{-e_h{}'} \bmod p$$

$$= (y_{(k_2)_{CHG_j}} \cdot \prod_{i=1}^{t-1} {Q_i}^{j^i}) \cdot [{y_{CP}}^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} {D_j}^{i^j} \cdot (y_{CHG} \cdot \prod_{i=1}^{t-1} {A_i}^{j^i})^{e_h}]^{-e_h{}'} \bmod p \quad \text{Q.E.D}$$

若上述驗證無誤，CHG_i將計算出 k_1 和 k_2 , $R \equiv g^{k_1 - k_2} \bmod p$與$Z \equiv {y_{CVG}}^{k_1} \bmod p$。

- 步驟3：代理簽章產生

於此步驟，CHG_i 對 DL 進行簽署，以產生簽章 S，其產生方式如式(30) ，其中 $f'''(0) = k_2$，$\sigma' \equiv \sigma + PV_{CHG} \cdot e_h \bmod q$。然後，$CHG_i$將$S, DL, M_w, K, T, y_{CVG}, R, Z$送至$CVG$。

$$S \equiv k_2 - \sigma' \cdot {e_h}'' \bmod q = f'''(0) - (f'(0) + f(0) \cdot e_h) \cdot {e_h}'' \bmod q \quad (30)$$

$${e_h}'' = h(DL||M_w||K||T||y_{CVG}||R||Z) \quad (31)$$

5.原始簽章者提名式代理簽章驗證階段

於原始簽章者提名式代理簽章驗證階段，任意 CVG 成員w 個或 w 個以上合作即可進行簽章驗證工作。在W.L.O.G的情況下，假設有$\{CVG_1, CVG_2, \dots, CVG_w\}$個成員參與簽章驗證，他們主要工作是對 DL 之簽章 S 進行驗證。首先，$\{CVG_1, CVG_2, \dots, CVG_w\}$合作以重建多項式，並算出$CVG$ 之私密金鑰 PV_{CVG}。再以式(32)完成簽章的驗證。其中，$y_{PS} = g^{f'(0)+f(0)\cdot e_h} \bmod p$ 。

$$\left(g^S \cdot y_{PS}^{{e_h}''} \cdot R\right)^{PV_{CVG}} \bmod p \stackrel{?}{\equiv} Z \bmod p \quad (32)$$

Pf:

1. $\because y_{PS} = g^{f'(0)+f(0)\cdot e_h} \bmod p$

$= g^{\sigma} \cdot (y_{CHG})^{e_h} \bmod p$

$= (g^{x_{CP}\cdot e_h + k}) \cdot (y_{CHG})^{e_h} \bmod p$

$= {y_{CP}}^{e_h} \cdot K \cdot (y_{CHG})^{e_h} \bmod p$

$= K \cdot (y_{CP} \cdot y_{CHG})^{e_h} \bmod p$

2. $\therefore \left(g^S \cdot y_{PS}^{{e_h}''} \cdot R\right)^{PV_{CVG}} \bmod p$

$= \left(g^{k_2 - \sigma'\cdot {e_h}''} \cdot (K \cdot (y_{CP} \cdot y_{CHG})^{e_h})^{{e_h}''} \cdot g^{k_1 - k_2}\right)^{PV_{CVG}} \bmod p$

$= \left(g^{k_1 - (\sigma + PV_{CHG}\cdot e_h)\cdot {e_h}''} \cdot (K \cdot (y_{CP} \cdot y_{CHG})^{e_h})^{{e_h}''}\right)^{PV_{CVG}} \bmod p$

$= \left(g^{k_1 - (x_{CP}\cdot e_h + k + PV_{CHG}\cdot e_h)\cdot {e_h}''} \cdot (g^k \cdot (g^{x_{CP}} \cdot g^{PV_{CHG}})^{e_h})^{{e_h}''}\right)^{PV_{CVG}} \bmod p$

$= \left(g^{k_1 - (x_{CP}\cdot e_h + k + PV_{CHG}\cdot e_h)\cdot {e_h}''} \cdot (g^{k + x_{CP}\cdot e_h + PV_{CHG}\cdot e_h})^{{e_h}''}\right)^{PV_{CVG}} \bmod p$

$= (g^{k_1})^{PV_{CVG}} \bmod p \equiv {y_{CVG}}^{k_1} \bmod p \equiv Z$ Q.E.D

本研究機制藉由上述五階段的操作後，數位內容提供者可於行動商務的環境提供消費者完成執照合法性驗證。因此，不管是任何角色的使用者即使暫時無法提供或是使用服務，都不會造成執照無法簽署與驗證。故GO-NPSS機制適用於以執照為基礎的數位版權管理的行動商務環境中。此機制的設計讓以C2C為經營模式的數位內容提供者得以提供數位內容給消費者，而相關的執照簽章之產生與驗證可由一群人基於公平的基礎下協力完成，不需擔心網路環境及本身的計算能力與電力供應的問題。

肆、安全性分析

本章節將就GO-NPSS機制作安全性分析，以確保本研究所提的機制滿足安全上的要求。由於本研究所提的機制是代理簽章的變形，故須滿足代理簽章上安全的要求，包括：完整性、可認證性、可驗證性、不可偽造性、不可否認性、可區別性、識別性、不可轉移性。另外，還就代理簽章者的偏差(Proxy Signers Deviation)與私密金鑰的依存性(Secret Key's Dependence)作討論。

- 完整性：為確保訊息傳遞過程不被竄改，故須提供完整性的確認。GO-NPSS機制以e_h、e_h'、e_h''來滿足此要求。這是因為它們都由單向雜湊(One-way Hash Function)運算完成。而單向雜湊函數具有一個很大的特色，就是不同的輸入可以產生不同的輸出。因此，若訊息於傳遞過程中被修改，就會被偵測出來，故可以提供完整性的保護。
- 可認證性：本研究機制於初始階段就必須完成身份認證。另外關於代理簽章本身的可認證性乃藉由隨機參數與時間戳記完成，另外此方式可以保證訊息沒有被重送，以防止重送攻擊(Replay Attack)。
- 可驗證性：由於每組代理簽章都對應到不同的參數，未來可以驗證某一個數位簽章是由哪一群代理簽章者所產生，故滿足可驗證性之要求。
- 不可偽造性：任何一個人都無法偽造原始簽章者(CP)或代理簽章者(CHG)的身份來產生數位簽章。此攻擊無法成功，這是因為任一攻擊者要產生$\dot{\sigma} \equiv x_{CP} \cdot \dot{e_h} + \dot{k} \bmod q$，使其滿足的前題是必須獲得 $\dot{\sigma}$ 的私密金鑰。然而，這是一個DLP的問題。故本研究滿足不可偽造性的要求。
- 不可否認性：由於本研究於代理簽章過程已將 CP、 CHG 與 CVG 所有參與成員之私密金鑰資訊轉換成相對的代理金鑰與驗證金鑰，且 Mw 也提供相關紀錄，故不僅可以達到來源端的不可否認亦可達到接收端的不可否認。
- 可區別性：當一個數位簽章被產生時，要能區別是由 CP 或是 CHG 所產生，是一件很重要的安全性分析。因為若簽章無法被辨別是由哪裡產生，將導致簽章被盜用情況。因為GO-NPSS機制採受保護模式的提名式代理簽章機制，亦即是說，代理金鑰以$\sigma' \equiv \sigma + PV_{CHG} \cdot e_h \bmod q$型式展現。故本研究之機制具有可區別性。
- 識別性： CP 是否可以辨別每一個代理簽章由哪一個 CHG 所產生，即是識別性問題。本研究所提GO-NPSS機制滿足此項要求，這是因為 CP 所產生的 σ 與 e_n 的配對，就包含參與者的身份。未來可藉由此配對資訊來辨識每一個簽章。故本研究之機制具有可識別性的效果。
- 不可轉移性： CHG 不能將代理簽章之權利轉移至他人手中。在本研究中，因為在 σ 與 e_n 的配對中，就包含參與者的身份，故已經事先決定好代理簽章者，不能更替。故本研究之機制具有不可轉移性。

- 代理簽章者的偏差：此安全性分析是為避免代理簽章者誤用代理金鑰，而去產生一個合法且有效的代理簽章。假設 CHG 握有σ 、K 以及 CP 的公開金鑰 y_{CP} 等資訊。因此，只要代理簽章者能夠藉由上述資訊計算 x_{CP} 或是k，即可製造出代理簽章者偏差的效果；或是代理簽章者產生出一個新的且有效的(σ,K)並滿足$\dot{\sigma} \equiv x_{CP} \cdot \dot{e_h} + \dot{k}\ mod\ q$或是$\dot{K} \equiv g^k mod\ p$，均可達此效果。但由於獲得 x_{CP} 與 $\dot{k}$是解DLP的問題。故本研究之機制可防止代理簽章者的偏差。
- 私密金鑰依存性：由於σ是由 CP 的 x_{CP} 計算出來。因此，若沒有CP 的私密金鑰，攻擊者是無法產生出σ。

藉由上述之安全性分析，證明本研究所提GO-NPSS機制符合代理簽章機制之安全性要求。

伍、效能分析

本研究所提之GO-NPSS機制，其安全性是基於解因數分解問題及離散對數問題上。此章節就此機制之步驟作效能分析。此外，每一個參與群組的成員除了參數的不同外，其計算方式是一致的，故群組成員的大小及每次參與代理簽章及驗證的成員多寡與整體計算量是成線性關係。但若參與代理簽章及驗證的成員高過門檻之要求時，其系統的可用性是提升的。

本研究所提之GO-NPSS機制，主要運算包括乘法運算、模加法與模指數的運算，於計算成本上最主要的是做模指數的運算。雖然於計算上會增加成本，但因以群體合作及基於兩個解因數分解及離散對數問題的困難度上，故足以保護該執照之安全性及確保執照可被順利簽署及被消費者驗證與使用。此外，未來也可以藉由硬體的實現，將此運算機制置放於行動設備上，就可解決效能上的缺陷。

陸、結論與未來研究方向

因應行動商務的到來與數位內容須受保護的請求，現有的DRM系統必須被調適至行動商務環境。OMA已經制定M-DRM相關的規範，並有三種模式可供使用。目前大多數應用於行動商務的M-DRM系統是採用分開遞送模式。在此模式中執照的合法性是必須被確認的。但由於行動網路環境，先天上有其限制，例如：具動態的網路拓樸與傳輸距離的受限；再加上行動裝置計算能力不足。故於執照簽章的產生與驗證可能無法由單一主機完成。故本研究提出一個以群體為導向的提名式代理簽章機制，滿足在行動商務的環境中，數位內容提供者可以順利的提供消費者完成執照合法性的驗證。換句話說，由數位內容提供者指派一群代理者(n個人)，且只要同時有 t 或 t 個人以上，($1 \le t \le n$)，即

可完成代理簽章的工作。數位內容提供者可以指定特定一群簽章驗證者(l個人) ，且只要同時有 w 或 w 個人以上，($1 \leq w \leq l$)，即可驗證由代理簽章者所產生的代理簽章之合法性。本研究共分成五個階段進行，包括：初始階段、委派階段、代理金鑰產生階段、提名式代理簽章產生階段與原始簽章者提名式代理簽章驗證階段。藉由這五階段的完成，消費者可以確認由相對應於受保護－數位內容產生的執照之合法性。此外，藉由安全性的分析，證明本研究所提之機制滿足簽章機制安全上的要求。故藉由此機制的設計，數位內容提供者可以順利的提供消費者完成執照合法性的驗證。

未來將持續針對應用於行動商務環境下的M-DRM系統做整體性的探討，例如：應用於可轉移權力下簽章驗證的探討與更具彈性的認證機制設計等等。除此之外，因本研究在考慮所有被選定為代理簽章的群組成員時，經身份驗證後，假設它們是值得被信賴的一群。未來將思考若這些成員的信譽度降低而成為不可信賴的個體時，數位內容提供者是否可以找出該成員，並以其他成員替換之。

致謝

感謝論文審查委員對本研究所提的諸多建議，使本研究之GO-NPSS機制與內容更為完善。

參考文獻

1. Hwang, S.J. and Shi, C.H.“A Simple Multi-proxy Signature Scheme,”*Proceedings of the tenth National Conference on Information Security*, 2000, pp.134-138.
2. Jeong, Y., Yoon, J. and Ryou, J.“A Trusted Key Management Scheme for Digital Rights Management,”*ETRI Journal*, (27:1), 2005, pp.114-117.
3. Kesselman, F.C., Tsudisk, G. and Tuecke, S.”A Security Architecture for Computational Grids,” *The 5th ACM Conference on Computer and Communication Security,* 1998, pp.83-92.
4. Kim, H., Baek, J., Lee, B. and Kim, K.“Secret Computation with Secrets for Mobile Agent Using One-time Proxy Signature,” *The 2001 Symposium on Cryptography and Information Security (SCIS 2001)*, 2001, pp.845-850.
5. Kim, S.J., Park, S.J., and Won, D.H.“Nominative Signatures,”*Proceedings of International Conference on Electronics, Informations and Communications (ICEIC'95)*, 1995, pp.68-71.
6. Kim, S.J., Park, S.J. and Won, D.H.“Zero-knowledge Nominative Signature,” *Proceedings of Pragocrypt'96, International Conference on the Theory and Applications of Cryptology*, 1996, pp.380-392.

7. Lee, B., Kim, H. and Kim, K. "Strong Proxy Signature and Its Applications," *The 2001 Symposium on Cryptography and Information Security (SCIS 2001)*, 2001, pp.603-608.
8. Liu, Q., Reihaneh S.-N. and Nicholas P.S. "Digital Rights Management for Content Distribution," *Proceedings of the Australasian Information Security Workshop conference on ACSW frontiers 2003*, (21), 2003, pp.49-58.
9. Mambo, M., Usuda, K. and Okamoto, E. "Proxy Signatures for Delegating Signing Operation," In *Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS)*, 1996, pp. 48-57.
10. Microsoft DRM(available online at http://www.microsoft.com/windows/windowsmedia/forpros/drm).
11. OMA DRM(available online at http://www.openmobilealliance.org).
12. ark, H.-U. and Lee, I.-Y. "A Digital Nominative Proxy Signature Scheme for Mobile Communication," In *Information and Communications Security (ICICS 2001)*, Springer-Verlag, Lecture Notes in Computer Science 2229, 2001, pp.451-455.
13. Sun, H.M. "An Efficient Nonrepudiable Threshold Proxy Signatures with Known Signers," *Computer Communications*, (22:8), 1999, pp.717-722.
14. Sun, H.M., Lee, N.Y. and Hwang, T. "Threshold Proxy Signatures," *IEE Proc. Computers and Digital Techniques*, (146:5), 1999, pp.259-263.
15. Tan, Z.-W. and Liu, Z.-J. "Nominative Proxy Signature Schemes," *Cryptology ePrint Archive: Report*, No. 298, 2004, pp.1-12 (available online at http://eprint.iacr.org/2004/298).
16. Zhang, K. "Threshold Proxy Signature Schemes," *Proceedings of Information Security Workshop (ISW'97)*, 1997, pp.282-290.