數位權利管理中檔案秘密分享之研究
－對稱式網路會議金鑰之應用

曾綜源	齊若驊	陳正鎔	翁智賢	林主雲
華梵大學資管系主任	華梵大學資管系資安組研究生	萬能技術學院資訊管理系助理教授	國防大學國防管理學院資管系暨國防資訊研究所研究生	國防大學國防管理學院資管系暨國防資訊研究所研究生

m9445216@cat.hfu.edu.tw

■ **摘要**

會議金鑰的建置，在無線隨意網路（MANET,Moblie Wireless Ad Hoc Network）、一對多安全群播（Secure Multicase）等等領域被提出，以達到通訊與資料傳輸時的資訊安全需求。但而技術環境的限制卻使群播並不普及。

為了解決以往主從式 Client-Server 架構在頻寬與效能上的不足，對稱式（Peer to Peer）網路檔案分享機制，在數位權利管理（DRM, Digital Rights Management）、智慧財產權的法律爭議都是十分熱門的議題。其肇因於對稱式網路傳輸雖可以解決頻寬不足的問題，然卻缺乏目前數位權利管理上對認證、保密等等的安全性需求。因此本文嘗試將安全群播環境中常被討論的會議金鑰，修改建置於對稱式網路中，期能在兼顧傳輸效能的前提下，滿足檔案傳輸時，數位權利管理上認證保密等檔案秘密分享應用需求。

關鍵字：對稱式網路、會議金鑰、秘密分享、數位權利管理

■ 1. 緒論

1.1 研究背景

Internet 的興起與人類生活的結合，是無法抵擋的時代潮流，對人類在資訊傳遞、文化演進上均產生重大的影響。回顧以往，資料記載於紙張、照片、書籍等傳統媒體的方式，使資料或資訊的保管存放、傳輸流通、分享交易都有十分大的限制；然而隨著資料數位化、網路興起等等可稱之為新一世代工業革命的帶動下，資料、資訊、情報等數位資訊的存管傳遞都變的更加便利與快速，網際網路促使人類時代、文化巨輪的轉動更加快速。

探討目前數位化資訊的傳輸模式，為了達到識別、認證的電子商務所需安全上的目的，在其架構上不脫所謂主從式 Client-Server 的架構，但當一個十分熱門的數位資訊或權利推出時，伺服端效能與傳輸頻寬往往成為瓶頸。舉例而言；每到年關將近，各種大眾運輸工具的網路售票系統在開放的時間點，大量顧客的訂票詢問（request）透過網路湧入時，往往發生伺服端效能或對外網路頻寬不足，產生無法即時回應的問題；過多的使用者存取造成的服務阻斷（DOS, Denial Of Service）情形，對使用者信心或企業商譽都會造成負面影響，進而影響營收。因此我們不難想見，爾後隨著如線上音樂商店、隨選視訊（MOD, Media On Demand）、隨選書刊（BOD, Book On Demand）等網路化交易行為日趨蓬勃，如何在硬體設備有限處理效能及網路頻寬下，提供使用者龐大的存取需求，是爾後數位內容服務供應商不得不面對的難題。

而資訊傳遞的技術中，群播是種節省網路頻寬及伺服端效能的解決方案，但是其環境建置上有其技術門檻；且在群播的過程中，必須每一個使用者都同時在線上以接收資料，在數位內容供應的商業模式中顯然會影響使用者意願。故因此以群播技術應用於傳送資訊等等議題，多半停留在學術性的探討上，鮮少在商務領域上的應用實例，脫離了使用者意願或習慣的應用技術，即使在學理上有再多的優點，其商務模式都是難以形成的。

分析使用者在存取網際網路時，通常都是使用較多的下載頻寬，上傳頻寬較少利用，而伺服端的情形則正好相反。在這樣的情形下，固然群播技術搭配會議金鑰建置可以使資料傳輸時，節省伺服端的頻寬傳輸與處理效能需求，亦滿足了數位權利管理中機密性、安全性之需求；然而在目前電子商務

販售數位資料，大多都屬於文化娛樂性質，一個 MP3 音樂檔、一段影片、一份電子書；不同使用者對同一份資料的需求時間點，一定會隨著個人生活作息而有很大的不同；因此以現今群播技術而言，是沒有辦法滿足這樣的需求。

1.2 研究動機

一份由創市際市場研究顧問公司於 2003 年 11 月 18 日，公佈於資策會電子商務研究所的『台灣網路「檔案交換」市場現狀』調查報告顯示[5]，該年 9 月份期間，台灣約有 335 萬人曾造訪如 Kuro 官方網站飛行網（music.com.tw）、或 ezpeer 網站等「檔案交換」網站，而該月下載 Kuro 程式的人數計有 80.7 萬；下載 ezpeer 程式的人數則為 38 萬。此外，該報告亦指出在 15 歲到 22 歲的高中生與大學生之中，有 50.2%造訪過「檔案交換」網站。由此我們可以觀察出，近年來對稱式（Peer to Peer）網路進行檔案傳輸大行其道，有別於群播技術上，使用者必須同時接收資料的限制；它滿足了使用者在不同時間、地點存取數位內容的需求。採用對稱式網路進行檔案分享與交換，除了減輕分擔原始資料伺服端的負載外，更使提升其他使用者下載速率；提升使用者使用數位內容服務的意願及滿意度。

目前對稱式檔案傳輸在檔案分享或交換的電子商務應用，如國外的先驅 Napster、Gnutella、及國內的 ezpeer，其對智財權的侵犯及適法性與否所引起的爭議，是非常受到關注的議題。探究其原因除了以對稱式網路檔案檔案傳輸進行數位內容販售的模式，與傳統通路獲利結構牴觸外；亦與對稱式網路上缺乏會議金鑰所能提供的識別認證機制有很大的關係。

另一個可能的狀況是，當一個社群因為有保護智慧財產權、或其他機密性需求顧慮的情形，而需要透過網路進行大量的檔案秘密分享時；建置集中的資料與認證伺服器，或大量採用 PKI 的架構，其成本的支出可能會高出社群的負擔；此時一個建置會議金鑰架構的對稱式網路，再搭配一些提供數位權利管理的技術，就是良好的著作物發表與分享平台。

1.3 研究目的

因此，本篇論文欲提出一個，將對稱式網路檔案分享、會議金鑰相結合的架構，在享有對稱式網路，檔案傳輸快速便利的情形下，亦能滿足以下第二章文獻整理中，數位權利管理上機密、識別等安全性的需求；而在此提出的系統架構，亦希望能適用於各種會議金鑰分配協定中，因此群組成員數量不同時，在不同的會議金鑰分配協定環境下的效能優劣，是取決於採用協定與成員數量的配適度，而不在本文討論的範圍內。

■ 2. 背景知識

2.1 對稱式網路

利用對稱式（peer to peer）進行檔案分享的架構中，每一個節點既可以是 Client、也可以是 Server，因此有別於主從式架構而能讓使所有節點均能對等的分享資源[6]。對稱式網路通常指的是一種分散式（decentralized）的架構，電腦相互連接並直接溝通與分享資源而不透過伺服器。這些資源包含了系統運算處理能力、記憶體、儲存容量、連網能力。目前對稱式網路中衍生了中控型及分散型兩種架構，以下就其運作結構與差異探討如下：

(1) 中控型對稱式網路

中控型架構的特色，是在其網路中，存在一台建立所有使用者現存檔案索引之資料庫[3]，所有使用者必須連接至該伺服器，進行登入、及後續資料檔案查詢等功能，然後再依據查詢之索引，自行向網路中其他使用者送出下載檔案的需求；其他使用者再接到這樣的需求時，再將該使用者所需的檔案或檔案片段上傳至該使用者。因此，中控伺服器僅負責檔案索引資料庫的維護、更新，以提供使用者查詢。其角色就如同一個媒合者，只提供使用者相互連結的媒介，而不介入後續使用者進行檔案分享的資料傳輸。

(2) 分散型對稱式網路

分散型架構中，並沒有伺服器的存在，所有其上的設備不論其運算能力高低、記憶體容量大小，均具備完全相同的功能，網路中的地位亦完全平等[4]。而使用者要登入網路時，是連接到某一個已經登入的節點（peer），由該節點將使用者登入的訊息逐漸散佈至整個分散型對稱式網路中；另外使用者要進行資料或檔案的搜尋時，亦是透過與使用者有

直接連線的節點，逐漸將搜尋檔案的訊息擴散至整個網路中，而收到搜尋訊息的節點除了將該訊息繼續擴散下去外，會搜尋本身的分享檔案中是否符合原先發出搜尋之使用者的條件，並將符合的結果直接傳回給原先的節點，倘若沒有符合條件的檔案時，則不回應任何訊息。

2.2 會議金鑰

在會議金鑰的相關研究中，有許多金鑰交換的方式，都是自 Diffie 及 Hellman 兩位學者在 1976 年所提出的 Diffie-Hellman 金鑰交換法[7]所衍生出來的，在下面的 2.2.1 節中，將介紹這個重要演算法，以及基於這個金鑰交換法，運用在群組通訊中的 GDH（Group Diffie-Hellman）會議金鑰交換法。

此外，除了金鑰交換的方式以外，以 2.2.2 節將說明金鑰管理架構議題中，學者 Sandro Rafaeli 與 David Hutchison 將會議金鑰的產生及管理架構整理分類[11]，再經由[2]重新定義如下三種：(1) 集中式金鑰分配協定 (Centralized Group Key Management Protocol)，(2) 混合式金鑰分配協定 (Decentralized Architectures)，(3) 分散式金鑰分配協定(Distributed Key Management Protocol)。

2.2.1 金鑰交換法

(1) Diffie-Hellman 交換法

此交換法是由 Diffie 及 Hellman 所提出一份對密碼學領域影響深遠的論文[7]。這個方法允許兩個欲進行秘密通信的實體，在沒有事先約定下，如何透過不安全的通信方式，產生一把共同持有的秘密金鑰，以供後續秘密通信加密用；可讓任兩個實體設備，在任何人都可監聽的通道中，交換一把秘密安全、僅由雙方共同持有的秘密金鑰。只要選用的參數符合條件，基於離散對數的計算難度，整個交換法是難以在合理的時間內破解的。

(2) GDH 金鑰交換法

Diffie-Hellman 金鑰交換法僅提供兩個實體一個安全有效的溝通方式，並不適用於會議金鑰的多方秘密通信環境中，因此學者 Steiner、Tsudik、Waidner 等人於 1996 的一篇論文[8]中，提出 GDH.2(Group Diffie-Hellman 第二版)，將 Diffie-Hellman 金鑰交換法延伸到多人群組通信的環境下

不論是 D-H 金鑰交換法，或 GDH 金鑰交換法，兩者均著墨於通信的群組成員，如何建立共同的秘密金鑰，而未提出使用者相互認證的方法。因此通信的雙方或多方透過上述的方法建立起一把共同的秘密金鑰，是無法確認所有參與金鑰產生的成員，其身份合法與否。

2.2.2 金鑰管理架構

(1) 集中式金鑰分配協定

在集中式的金鑰分配協議架構中，以一個單一的實體進行整個群組的控制，這個受到所有群組成員所信任的金鑰控制中心（Key Distribution Centre, KDC）負責執行所有的金鑰產生、派送、管理、儲存、更新等工作[11]，其優點在於將群組成員及 KDC 的需求降至最低，增加群組管理的彈性。

(2) 混合式金鑰分配協定

在上述集中式架構中，當 KDC 這個實體無法運作時，整個群組的通訊及其所使用的會議金鑰架構都將隨之停擺，因此 Chen, Tzer-Shyong 及 Mittra 等人提出將龐大群組劃分成數個較小群組的管理方式，以降低單一實體無法運作時的風險[10,12]。

(3) 分散式金鑰分配協定

在這個架構中，沒有明確的 KDC 存在，由群組內所有的成員分享出一些資訊後，藉由特定的程序來產生群組金鑰，也因此在這個架構中，每一位成員都是平等的在同一個時間內，不分先後獲得群組金鑰[9]。

2.3 文獻探討

綜合以上文獻探討，本研究結合中控型對稱式網路與 KDC 之金鑰分配協定作為我們的資訊安全需求的解決方案，其理由如下：

(1) 中控型對稱式網路平台可以解決主從式架構在檔案分享大量資料傳輸中伺服端可能產生的傳輸效能瓶頸。在電子商務的環境下，讓客戶可以快速獲得所需資料檔案，提升使用者滿意度。

(2) 結合集中式或混合式等具有 KDC 之金鑰分配協定，透過分配協定產生及更新金鑰之機制，使群組內的成員持有一把秘密的共同會議金鑰。在檔案秘密分享時可提供資料加密功能，有效避免因傳輸對象不同，使同一份

資料以不同的公開金鑰重複加密的效能耗損。而 KDC 提供群組成員加入、離開群組時，會議金鑰的更新及配送，以搭配中控型對稱式網路執行群組成員管理功能。

這種解決方案可達成下列資訊安全上之三個目的：

(1)身分認證：在對稱式網路中，我們提出一個利用透過群組成員所共同持有的會議金鑰，讓使用者之間在資料傳輸前，先進行相互認證的機制，使資料發送端能確認接收端是否為群組內的成員，而接收端亦能確認發送端是否為偽冒，因此可以抵擋中間人的偽冒攻擊。

(2)保密性：檔案分享時，資料傳遞前先以群組成員所共同持有的會議金鑰加密，此外搭配金鑰分配協定的金鑰變更機制，可達成向前秘密（Forward Secret）與向後秘密（Backward Secret）的需求。

(3)安全性：在認證的步驟中，具備可以抵擋重送攻擊之機制。

■ 3. 研究方法

3.1 系統架構

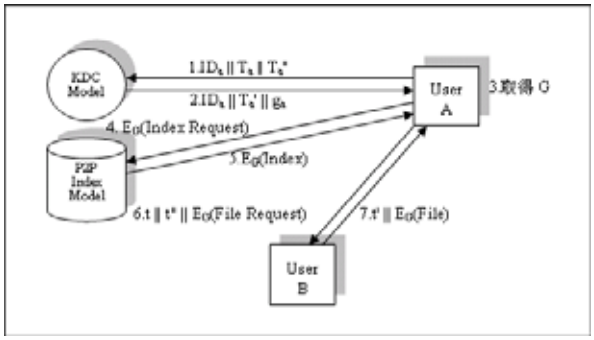

圖 1 會議金鑰之對稱式網路中心運作圖

本論文所提出的系統架構稱為「會議金鑰之對稱式網路中心（Conference Key P2P Network Center）」，在這個對稱式網路中，使用者利用由 KDC 所核發的會議金鑰，以加密的方式索取所需檔案的來源節點索引清單，而在所有的檔案資料分享中，亦均以會議金鑰予以加密（如圖 1）。整個架構包含以下兩項功能模組：

(1)P2P Index Model：負責系統所有分享檔案索引清單建立更新、異動維護之管理功能；並依群組使用者需求提供檔案來源之節點索引清單，維繫對稱式網路檔案秘密分享、資料交換功能之運作。

(2)KDC Model：提供群組成員管理；及使用者加入、離開群組之申請提出，使用者認證資訊的產生與核發；或已加入群組使用者於建立會議金鑰或索取檔案索引清單前的認證。此外亦負責執行會議金鑰運算產生、建置派送、更新異動功能，這也是下面即將討論的重點。

3.2 參數定義

p、g：可公開的正整數，p 為一大質數，並符合 p > g，g 為 p 之原根。

ID*i*：由 KDC 所核發給使用者 *i*，用以稽核群組成員身分的資訊。

T*i*：由使用者 i 產生的時戳，在進行認證時，可藉以抵抗中間人攻擊及重送攻擊。

H(M)：將訊息透過雜湊函數運算，取得雜湊值。

S_i：由KDC與使用者*i*雙方約定秘密持有之數值，用以產生會議金鑰。

G：由全體群組成員共同持有之秘密會議金鑰。

E_{key} (M)：將訊息透過對稱式加密函數，以key金鑰加密。

3.3 會議金鑰之產生

若整個群組有 n 位成員，則會議金鑰由 KDC 依下列步驟所產生：

(1)將所有使用者的S_i值之連續乘積為 g 之指數。

(2)所得之數取 p 之同餘，即為會議金鑰G（如下式）。

$$G = g^{\prod_{i=1}^{n} S_i} \pmod{p} \qquad (1)$$

3.4 金鑰派送

在本文所提出的對稱式網路的環境架構中，並不要求每一位使用者在產生金鑰時，均可以同時連線並同時取得用以運算出會議金鑰G的相關值，而是使用者在登入對稱式網路時，再將相關值傳送至使用者端，以下就是使用者 a 在登入「會議金鑰之對稱式網路中心」之 KDC 時，認證與金鑰派送的步驟：

(1)當使用者登入時，產生一時戳 Ta。

(2)使用者 a 以 Sa 為金鑰，將 Ta 透過對稱式加密函數加密後，為 g 之指數，所得數再取 p 之同餘，最後所得之雜湊值是為 Ta'（如下式）。

$$T_a' = H\left(g^{E_{S_a}(T_a)} (\text{mod } p)\right) \quad (2)$$

(3)再以 Sa 為金鑰，將 Ta'透過對稱式加密函數加密後，為 g 之指數，所得數取 p 之同餘，最後所得之雜湊值是為 Ta"（如下式）。

$$T_a'' = H\left(g^{E_{S_a}(T_a')} (\text{mod } p)\right) \quad (3)$$

(4)使用者 a 將 IDa、Ta、Ta"傳送至 KDC Model。

$$ID_a \| T_a \| T_a'' \quad (4)$$

(5)KDC 根據 IDa 提取 Sa，並以前述步驟(2)、(3)方式，計算出 Ta'、Ta"，比對自使用者 a 所送來的 Ta"是否相符，若相符則 KDC 確認該用戶端身份確為其所宣稱的使用者 a。

(6)當KDC確認使用者身份後，將所有使用者的 S_i 值之連續乘積除以Sa之後為 g 之指數，所得數再取 p 之同餘，即為會議金鑰相關值 g a（如下式）。

$$g_a = g^{\frac{\prod_{i=1}^{n} S_i}{S_a}} (\text{mod } p) \quad (5)$$

(7)KDC 將 IDa、g a、Ta'傳送給使用者 a。

$$ID_a \| T_a' \| g_a \quad (6)$$

(8)使用者比對由 KDC 傳送之 Ta'是否與自己送出的相符，若相符則驗證 KDC 身份未遭偽冒，此時將 g a 的 Sa 次方取 p 之同餘，即得會議金鑰 G（如下式）。

$$g_a^{S_a} (\text{mod } p) = \left(g^{\frac{\prod_{i=1}^{n} S_i}{S_a}} (\text{mod } p) \right)^{S_a} (\text{mod } p) \quad (7)$$

$$\equiv g^{\left(\frac{\prod_{i=1}^{n} S_i}{S_a}\right) * S_a} (\text{mod } p) = G$$

3.5 金鑰更新

在本文提出的架構中，當群組內使用者異動時，會議金鑰亦必須隨之更新，以達到向前秘密與向後秘密的安全性需求，以下便為本文所提出之金鑰更新方式

3.5.1 使用者加入會議金鑰變更流程

當一位使用者 n+1 加入群組時，KDC 會依據下列步驟來進行會議金鑰之更新：

(1)當KDC同意使用者n+1 的加入群組時，必須透過安全管道核發該位使用者一個IDn+1與一組秘密數值 S_{n+1}。

(2)KDC通知所有其他群組成員，舊會議金鑰 G 停用，協調出新的 S_i 值，並要求每一位成員重新登入對稱式網路中。

(3)計算新的會議金鑰 G'，在成員重新登入完成驗證後，傳送給該成員（含新加入使用者）新的會議金鑰相關值，以計算出新的會議金鑰 G'（如下式）。

$$G' = g^{\prod_{i=1}^{n+1} S_i} (\text{mod } p) \quad (8)$$

3.5.2 使用者離開金鑰變更流程

當使用者 n 因故必須退出群組時，會議金鑰之對稱式網路中心會依據下列步驟來進行會議金鑰之更新：

(1)KDC通知所有其他群組成員，舊會議金鑰 G 停用，協調出新的 S_i 值，並要求每一位成員重新登入對稱式網路中。

(2)計算新的會議金鑰 G'，在成員重新登入完成驗證後，傳送給該成員（含新加入使用者）新的會議金鑰相關值，以計算出新的會議金鑰 G'（如下式）。

$$G' = g^{\prod_{i=1}^{n-1} S_i} (\text{mod } p) \quad (9)$$

3.6 使用者相互驗證

當使用者 a 根據自 P2P Index Model 所獲得的索引清單，向擁有檔案的另一位使用者 b 索取檔案時，認證步驟如下：

(1)使用者 a 產生一時戳 t，並以會議金鑰 G，將 t 透過對稱式加密函數加密後，為 g 之指數，所得數再取 p 之同餘，最後所得之雜湊值是為 t'（如下式）。

$$t' = H\left(g^{E_G(t)} (\text{mod } p)\right) \quad (10)$$

(2)再以會議金鑰 G，將 t'透過對稱式加密函數加密後，為 g 之指數，所得數再取 p 之同餘，最後所得之雜湊值是為 t"（如下式）。

$$t'' = H\left(g^{E_G(t')} (\text{mod } p)\right) \quad (11)$$

(3)使用者 a 將 t、t"連同檔案下載需求送至使用者 c。

(4)使用者 b 同樣以步驟(2)、(3)方式計算出 t'、t"後，比對使用者 a 所傳送之 t"是否相符，若相符則可確認使用者 a 為合法群組成員。

(5)使用者 b 將計算之 t'連同第一份所欲傳送之加密後的檔案資料，一併傳送回使用者 b。

(6)使用者 a 比對收到之 t'與原先計算之 t'是否相符，若相符則確認使用者 b 為合法群組成員，並開始後續之檔案分享程序。

在上述的步驟中，由於使用者相互認證所採用的運算方式類似，因此與 3.4 節相同的，基於離散對數與雜湊函數的破解難題，攻擊者難以在合理的時間範圍與有限的資源下，以 t、t'或 t'、t"推算 G。

■ 4. 安全性分析

4.1 保密性

就本文提出的架構中，保密性除了在資料傳輸及索引清單傳送的過程中，以會議金鑰進行加密外，另外特別需提出討論的，就是在金鑰產生或更新的階段中，竊聽者是否能推算破解出會議金鑰；以及當成員異動時，是否能滿足會議金鑰中，向前秘密（Forward Secret）與向後秘密（Backward Secret）的需求。

在金鑰派送時，是由KDC將與群組成員用以運算出會議金鑰的 $g_i = g^{\frac{\prod_{i=1}^{n} S_i}{S_i}} \pmod{p}$，傳送給每一位不同的成員，竊聽者僅能獲得不同的$g_i$值，欲推算破解出會議金鑰 G，仍必須面對離散對數的破解難題，而本機制與GDH交換法相比，並無逐一傳遞訊息的步驟，且本機制中，使用者登入「會議金鑰之對稱式網路中心」時間點並不一致，因此攻擊者在單位時間內，所能獲得的資訊與GDH相比更少，因此可以推論，本機制在金鑰派送過程的安全性，不遜於GDH金鑰交換法。

當群組新增一位使用者U_{n+1}時，為了符合向前秘密的保密性，KDC必須與全體其他使用者協調新的S_i值，再依照金鑰產生的程序，重新計算g_i值，然後將新的g_i傳送給包含新使用者的全體群組成員，以計算出新的會議金鑰 G'，此時即使這位新成員U_{n+1}可蒐集所有在金鑰更新時，KDC與其他使用者往來傳輸的資訊，仍無法破解出先前的會議金鑰 G。

當使用者U_n離開群組時，為了符合向後秘密的保密性，KDC亦必須與其他的使用者協調新的S_i值，因此這位離開的成員亦無法以先前的會議金鑰 G 及竊聽而得來的相關資訊，推算破解出新的會議金鑰 G'。

4.2 身份認證

在本文所提出的架構中，當使用者與 KDC 通信以取得會議金鑰時；或使用者與使用者相互分享檔案資訊時，均包含相互進行身份認證的機制，本節將以中間人攻擊為例，說明以本架構之身份認證機制，抵擋偽冒身份之攻擊。

當 3.4 節金鑰派送的階段中，任一位可以竊聽獲得 Ta、Ta'、Ta"，以及原先 p、g 公開參數的攻擊者，當欲逆推 Sa 時，由於 Ta'、Ta"均為同餘 p 之後的雜湊值，因此攻擊者首先必須面臨雜湊函數的破解難題，即使攻擊者破解雜湊值，欲以 Ta、$g^{E_{S_a}(T_a)} \pmod{p}$ 推算 Sa 時，必須面對對稱式加密函數的破解問題；若欲以 $g^{E_{S_a}(T_a)} \pmod{p}$、$g^{E_{S_a}(T_a')} \pmod{p}$ 推算 Sa 時，則同時必須面對對稱式加密函數與離散對數的破解難題，因此在 3.2 節所假設的環境，且所選用的對稱式加密函數與雜湊函數本身強度足夠之狀況下，攻擊者難以在合理的時間範圍與有限的資源破解 Sa。

如果群組內的一位合法使用者 b 欲對使用者 a 發動中間人攻擊（Man-in-the-Middle Attack），對 a 而言，由於 b 無法破解 Sa 值，因此在 3.4 節步驟(8)中，使用者 a 會發現 KDC 遭到偽冒，因此無法成功。

對一位群組以外的非法攻擊者而言，由於 Sa 是難以破解的，因此如欲從 g a 來破解 G，亦必須面對解離散對數的難題。

而在 3.6 節使用者與使用者檔案分享傳輸前，相互認證的階段中，由於所採用的運算方式與 3.4 節類似，因此基於對稱式加密函數、雜湊函數與離散對數的破解難題，攻擊者亦難以在合理的時間範圍與有限的資源下，以 t、t'或 t'、t"推算 G

4.3 安全性

由於在 3.4 節使用者與 KDC 認證；及 3.6 節使

用者相互認證的階段中，本機制是採用時戳來做為認證的參數之一，因此在認證的過程中，可有效抵擋重送攻擊。

■ 5. 結論

在網際網路盛行、資訊爆炸的時代中，已無可避免面臨效能與頻寬不足的困境，透過對稱式網路技術，再結合適當的安全功能，是可以避免對稱式網路侵犯智慧財產權的爭議。

在本文所提出，對稱式網路檔案分享、會議金鑰相結合的架構，希望在享有對稱式網路，檔案傳輸快速便利的情形下，能提供數位權利管理等相關領域中所需的機密、識別等安全性需求。而在某些需要高度機密或隱私的環境中，本架構所納入的會議金鑰亦能在高度效能的對稱式網路中，提供良好的傳輸保密功能。

另外因應不同應用環境中，群組成員數量的不同，本架構在設計上，亦能符合不同種類之集中式或混合式金鑰分配協議，以期在各種應用領域上更新金鑰時，都能在安全性與效能上取得一良好的平衡。

參考文獻

1.林詠修(民國 91 年 6 月),「安全群播中高效能更新邏輯樹群組金鑰協定」,私立元智大學資訊工程研究所碩士論文。

2.王偲穎(民國 94 年 6 月),「動態會議金鑰分配機制之研究」,私立世新大學資訊管理研究所碩士論文。

3.劉怡玟(民國 93 年 7 月),「點對點檔案分享軟體使用行為之研究」,國立中山大學傳播管理研究所碩士論文。

4.陳榮林(民國 92 年 6 月),「點對點傳輸之著作權侵問題—以美國法為中心」,國立交通大學科技法律研究所碩士論文。

5.資策會電子商務研究所(2005, November 18),創市際市場研究顧問公司【調查聯盟線上資料】,來源：http://www.find.org.tw/0105/cooperate/cooperate_disp.asp?id=102

6.教育部,網路與通訊【線上資料】(2005, December 14)，來源：http://content.edu.tw/junior/computer/ks_mc/chapter/ch12/c12_01.htm。

7.Diffie, W. and Hellman, M.E.(1976)，"New Direction in Cryptography"，IEEE Trans.On Information Theory，Vol. IT-22, No. 6，pp. 644-654.

8.Steiner, Michael, Tsudik, Gene, and Waidner, Micheal(1996)，"Diffie-Hellman Key Distribution Extended to Group Communication"，*3rd ACM Conference on Computer and Communication Security*，pp. 31-37.

9.Trappe, W.，Wang, Y.，and Liu, K.J.R.(2005)，"Resource-Aware Conference Key Establishment for Heterogeneous Networks"，*ACM Transactions on Networking*，Vol. 13，No. 1，pp. 134-146.

10.Chen, Tzer-Shyong，Huang, Kuo-Hsuan，and Chung, Yu-Fang(2004)，"Modified Cryptographic Key Assignment Scheme for Overcoming the Incorrectness of the CHW Scheme"，*2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (IEEE'04)*，pp. 569-572.

11.Rafaeli, Sandro and Hutchison, David(2003)，"A Survey of Key Management for Secure Group Communication"，*ACM Computing Surveys (CSUR)*，Vol. 35，No. 3，pp. 309-329.

12.Mittra, S.(1997)，"Iolus: A Framework for Scalable Secure Multicasting"，*Processing of the ACM SIGCOMM*，Vol. 27，pp. 277-288.