改良分散式 DRM 機制控管 P2P 即時串流服務

古東明
國立雲林科技大學 資訊管理系
koo@yuntech.edu.tw

陳曉琪
國立雲林科技大學 資訊管理系
g9623704@yuntech.edu.tw

***摘要*—P2P 傳輸技術目前相當熱門，因為它能同時讓兩個使用者直接分享彼此的檔案，而不用透過第三方(伺服器)。除此之外，還有許多因素加速 P2P 網路之實用性，這些因素包括可用的頻寬上升、運算能力提高、儲存容量加大及網路資訊激增等。但是，P2P 傳輸技術同時也是惡名昭彰的非法活動溫床，它使得盜版和非法使用變得容易，因此許多使用者利用它來從事違反著作權法的資料交換。為解決 P2P 傳輸架構帶給大眾的不好印象，導入適合 P2P 網路之數位權利管理機制(Digital Rights Management, DRM)是可行的，本研究於現有 P2P 即時串流傳輸架構上，改良分散式 DRM 機制，並導入新型金鑰管理系統。即時串流傳輸架構具有即載即看即丟的特性，能預防數位內容被重複利用，對於本研究所改良之 DRM 機制具有加強效果；而導入新型金鑰管理系統，使得 DRM 機制運作時，惟有使用者缺乏合法解密金鑰時，才會出現警告，其餘時候使用者並不會感受到 DRM 機制之控管，因此能提升使用者對於 DRM 機制的接受度。**

***關鍵詞*—P2P、DRM、金鑰管理系統**

一、緒論

1.1 動機與目的

網際網路無遠弗屆的特性，讓內容的交換越來越便利，為保障創作者或權利擁有者的權益，數位權利管理機制(Digital Right Management, DRM)因應而生。DRM 機制除了保護數位內容免於被非法存取、傳遞之外，還可透過身份驗證功能限制使用者對於數位內容之使用；不僅保障內容提供者的權利，同時也協助使用者避免在未知的情形下產生侵權行為；另外，對於提倡數位內容有價的業者而言，DRM 機制還具備收取與分配權利金之能力。

P2P 技術能讓使用者直接分享彼此的數位內容，而不用透過第三方(伺服器)認證，因此加速了數位內容交換的速度和次數，網路上的使用者也可以透過此技術取得最新的數位資訊。它美好的前景讓眾人不願放棄，但它的特性卻也造成享有著作權之數位內容更容易地在網路上被非法散布，創作者因此對數位內容產業喪失信心。傳統的 DRM 機制具備保護數位內容、控制數位內容使用、驗證合法使用者權利及分配使用權利金等能力，但礙於 P2P 技術匿名傳輸與接收後分享之特徵，故強制將傳統 DRM 系統套用至 P2P 網路，不僅會削弱 DRM 機制之能力，還會降低 P2P 網路之優點。

本研究於現有 P2P 即時串流傳輸架構上，引進改良之 DRM 機制，並導入新型金鑰管理系統。即時串流傳輸架構具有即載即看即丟的特性，能預防數位內容被重複利用，對於本研究所改良之 DRM 機制具有加強效果；而導入新型金鑰管理系統，除了使得內容保護於 P2P 機制下可行外，也使得 DRM 機制運作時，惟有使用者缺乏合法解密金鑰時，才會出現警告，其餘時候使用者並不會感受到 DRM 機制之控管，因此能提升使用者對於 DRM 機制的接受度。

1.2 研究限制

DRM 機制僅能針對欲存取受保護之數位內容的使用者，進行合法與非法存取限定。但對於那些擁有合法權利卻進行非法侵權行為(如側錄數位內容)的使用者，DRM 機制並無法達成有

效的控管，故這並非是 DRM 系統所能涵蓋的範疇。

本研究旨在改良 DRM 機制，著重於有效改善以往 DRM 伺服器與 P2P 網路互相牽制之缺點，對於使用者身份驗證能力及 DRM 機制所涉及之金流部份，並未加以深入研究，故使用者金鑰取得之條件，只簡單以帳密組合驗證合法性。

二、相關技術與文獻探討

本研究預計於現有 P2P 即時串流傳輸架構上，改良分散式 DRM 機制，並導入新型金鑰管理系統。即改良傳統分散式 DRM 機制，以實現 P2P 即時串流網路上內容傳遞之安全控管，並透過新型金鑰管理系統有效地在群組成員變動幅度大之 P2P 網路分配金鑰。在此將針對 P2P 網路、串流傳輸架構、數位權利管理機制(DRM)及金鑰管理系統等研究相關主題深入探討。

2.1 P2P 網路

在 P2P 網路中，資源(CPU、檔案、儲存體)分散在各個 peer 的電腦中，peer 間能直接分享彼此資訊而無需透過第三方(網路伺服器)，因此具備以下優點：

(a). 非集中式：P2P 網路的資源和服務分散在 peer 中，peer 間的資訊傳輸不用透過中央伺服器。

(b). 擴展性：P2P 網路中，peer 的數目與整體網路處理能力成正比，且 peer 數越多資源儲存能力也會相對提昇，能滿足大規模網路應用之需求。

(c). 強韌性：P2P 網路具有自我維護(self-maintain)和自我修復(self-repair)特色，允許 peer 加入與離開而不影響其他 peer；P2P 網路上資源和服務分散在 peer 間，當部分 peer 或網路遭受破壞時，對整體環境的影響很低。

2.2 串流傳輸架構

2.2.1 串流媒體

串流媒體是近來新興的一種網路多媒體傳播方式，它將數位內容壓縮後，經由網際網路穩定地傳送給使用者，使用者在尚未接收到完整的影音資料前，就可以透過播放程式解壓縮開始播放。如圖 1 所示，串流媒體主要包含壓縮模組、串流伺服器與播放工具三個部份：壓縮模組，主要是將龐大的數位內容壓縮成能在網路上傳送的大小，壓縮模組的功能越強，串流的效果就越好；串流伺服器，提供串流的建立、管理與傳送服務；而播放工具，則是負責接收與重組封包、解壓縮以及同步呈現數位內容。

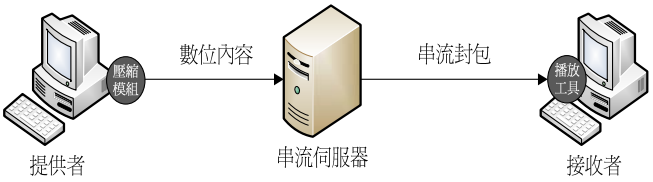

圖 1 串流媒體架構圖[資策會多媒體技術實驗室，2003]

2.2.2 串流媒體分類

串流媒體主要分為即時(On Live)與非即時(On Demand)兩種模式。即時模式意謂媒體來源經壓縮處理後，隨即利用伺服器，經由網路傳送到使用者的播放工具，例如雙向的視訊會議與單向的即時監控；非即時模式意謂媒體來源經壓縮處理後，先存放在串流伺服器中，等待播放工具提出要求後，再經由網路傳送到播放工具上，例如隨選視訊(VOD)。

(a). 即時(On Live)模式

使用者是採用被動式的收播方式，即串流伺服器主動播送數位內容，使用者只能被動的

接收，技術上是採用多點傳播模式(Multicast)，伺服器對於一個資料傳送路徑只建立一條連線，使用者只會接收到同一個數位內容，且使用者若在影音開始傳播之後才加入此連線，是無法再接收先前傳播過的部分。

(b). 非即時(On Demand)模式

使用者是採用主動式的收播模式，可對串流伺服器提出特定數位內容要求，伺服器再配合提供所需的影音資料，此類串流模式技術上是採用單點傳播(Unicast)模式，即伺服器依照個別使用者需求建立各自的連線，但一旦使用者數目增加，伺服器的負擔也會隨之增加。

2.3 數位權利管理機制(DRM)

目前 DRM 機制還沒有公認的定義，主要來自於各界對「數位權利管理(Digital Rights Management)」的價值觀不盡相同，系統需求亦不同[3]，然而大致的概念是一致的，也就是在數位化的環境中，透過數位加密和認證機制，以確保該數位內容無法在未經該數位內容擁有者之授權下，進行散佈、複製和竄改。

2.3.1 DRM 技術

DRM 機制通常是將內容與權利分別管理，其技術主要分為內容保護技術、權利管理兩類，其中權利管理又分成權利描述語言(Rights Expression Language，REL)與使用者存取控制二種，以下將分別論述之。

(a). 內容保護技術

內容保護技術的能力是內容擁有者最感興趣的部分，因此這是數位內容不會被非法盜用最基本的要素；共有金鑰加密演算法(Key Encryption Algorithm)、數位簽章(Digital Signature)與單向雜湊函數(One Way Hashing Function)三種。其中，金鑰加密演算法分為對稱式加密演算法(Symmetric Key Algorithm)，也就是加解密的金鑰相同；與非對稱式加密演算法(Asymmetric Key Algorithm)，即加解密的金鑰不同。實作流程如圖 1 所示，首先將欲加密的內容利用加密金鑰，透過加密演算法處理後，產生加密內容傳送到接收方，接收方唯擁有解密金鑰，才可透過加密演算法反運算還原原始內容[5]。

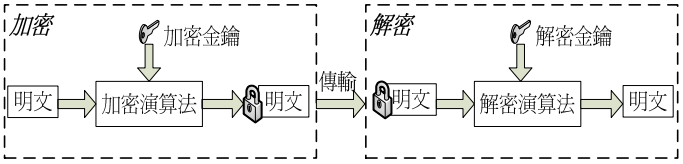

圖 2 金鑰加密演算法實作流程圖

(b). 權利描述語言(REL)

REL 定義數位權利的相關內容，包括權利擁有者資訊、合法使用者資訊以及使用的相關權限與付費條件等。

(c). 使用者存取控制

DRM 透過使用者存取控制技術，驗證取得數位內容之使用者是否擁有合法使用權，並確認合法使用者之數位內容使用期間或次數。

2.3.2 現有 DRM 機制分類

現在的 DRM 機制，普遍利用 DRM 伺服器來實現數位內容傳遞時之 DRM 控管，無論內容提供者或接收者皆會透過 DRM 伺服器分享數位內容，如圖 3。

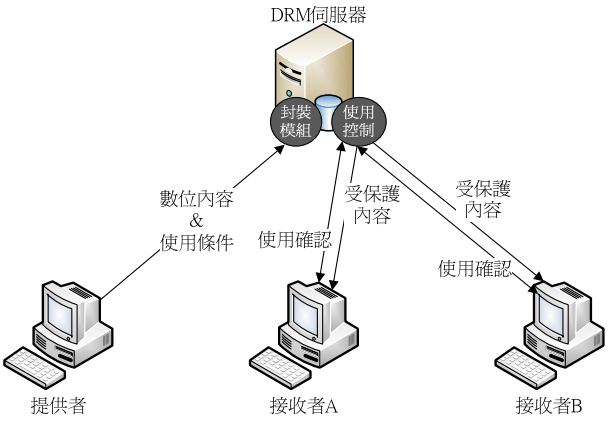

圖 3 Client-Server 架構下之 DRM 機制

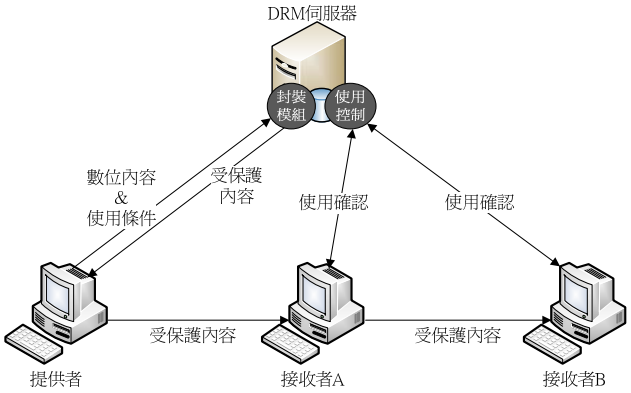

圖 4 P2P 架構下存在 DRM Server 之 DRM 機制

Tetsuya Iwata et al.[2003]將現今使用於 P2P 架構下之 DRM 機制分為存在 DRM Server 之 DRM 機制、分散式之 DRM 機制與半分散式之 DRM 機制三類[7]。

(a). 存在 DRM Server 之 DRM 機制

如圖 4 所示，此架構保留 DRM 伺服器處理相關的 DRM 控管。提供者需將數位內容和使用條件傳送到 DRM 伺服器，由 DRM 伺服器進行封裝作業，封裝好的檔案會先傳送給提供者去進行 P2P 分享；縱使接收者不是透過 DRM 伺服器取得受保護的數位內容，也會在要取得原始數位內容或者被加密的數位內容之使用權之前，啟動內含的控制程序向 DRM 伺服器確認使用權利。

保留 DRM 伺服器的作法，雖然能有效達成 DRM 控管，但卻會破壞 P2P 網路之特性，並造成 P2P 網路擴展性之瓶頸。

(b). 分散式之 DRM 機制

如圖 5 所示，此架構完全去除了第三方(DRM 伺服器)的控管，DRM 功能完全涵蓋在提供者機器內。提供可利用封裝模組將數位內容、使用條件和相對應的控制程序封裝一起，並直接傳送給接收者；接收者在取得原始數位內容或者被加密的數位內容之使用權之前，會啟動內含之控制程序直接向提供者確認使用權利。

完全去除 DRM 伺服器的作法，保留住 P2P 網路擴展性和強韌性兩大優點，但卻難以真實地達到 DRM 機制所有功能，尤其是涉及金流之敏感性問題，且提供者需額外處理使用確認之作業。

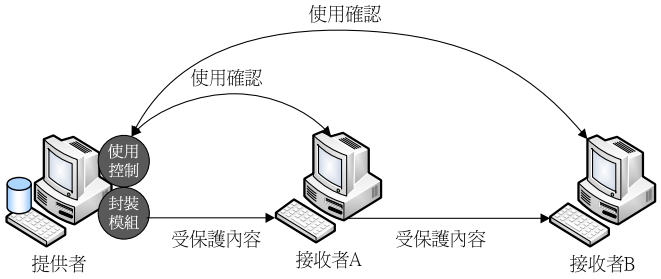

圖 5 P2P 架構下分散式之 DRM 機制

(c). 半分散式之 DRM 機制

如圖 6 所示，此架構混合了前面兩種 DRM 機制之優點，其保留了 DRM 伺服器集中管理認

證作業，而大部份的 DRM 功能則在提供者機器上執行，如使用控制和封裝模組。使用者資料庫由 DRM 伺服器管理，當數位內容驗證程序涉及金流時，提供者可透過 DRM 伺服器之認證模組確認使用者付費狀況，再給予使用確認。

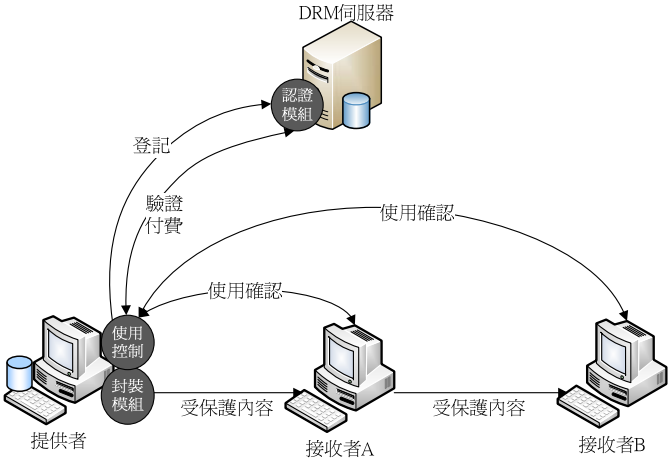

圖 6 P2P 架構下半分散式之 DRM 機制

2.4 新型金鑰管理系統

針對動態群組密金鑰管理的方式，現在普遍採用以樹狀結構為基礎的群播金鑰管理機制，此機制雖然存在諸多優點，但卻也存在一些缺點[10]，使其不適用於 P2P 網路。Chin-Chen Chang et al.[2008]提出新型金鑰管理系統，成功解決上述傳統以樹狀結構為基礎的群播金鑰管理機制的缺點，且它在群組成員變動時金鑰更新的計算複雜度為 O(1)[11]，我們發現這個演算法非常適用於 P2P 網路成員變動幅度大之特性。

2.4.1 新型金鑰管理系統概念

新型金鑰管理系統概念如圖 7 所示。在此金鑰管理機制下，每個合法的接收者只持有一把解密金鑰，因此不需額外識別金鑰功能，這邊值得注意的是，各個接收者所持有的解密金鑰皆不同；而提供者也只持有一把加密金鑰，此加密金鑰是透過中國餘式定理，由各接收者的解密金鑰計算得出，提供者所提供的數位內容皆由此唯一的加密金鑰加密；此金鑰管理系統最大的特色在於，它採用一對多的金鑰演算法，接收者各自擁有與他人不同的解密金鑰，所以當群組成員變動時，唯有提供者所持有的加密金鑰需重新計算，接收者依然使用原先的解密金鑰；而加入 P2P 網路的駭客(非合法使用者)縱使截取到加密過的內容，也無法取得相對應的金鑰。

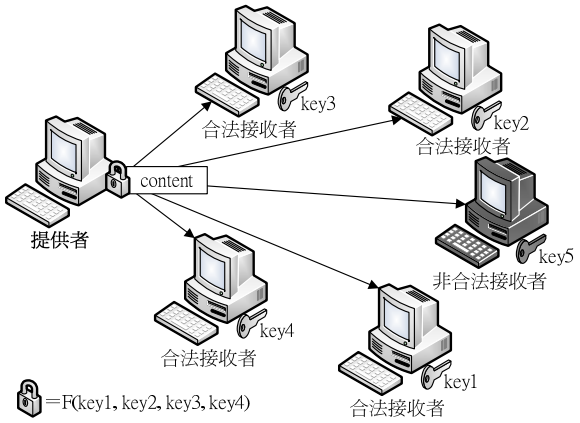

圖 7 新型金鑰管理系統概念圖

2.4.2 金鑰的產生與加解密

(a). 解密金鑰的產生：隨機產生一組質數(p_i, q_i)，傳送給接收者作為解密金鑰，每個接收者得到的質數組合皆不同。

(b). 加密金鑰的產生：利用公式(1)和公式(2)運算出一組加密金鑰(P, Q)，爾後的數位內容皆透過此加密金鑰加密保護。

$$P = \prod_{i=t_2}^{t_k} p_i \,,\; P_i = \frac{P}{p_i} \,,\; P_i P_i' \equiv 1 \bmod p_i \qquad (1)$$

$$Q = \prod_{i=t_2}^{t_k} q_i \,,\; Q_i = \frac{Q}{q_i} \,,\; Q_i Q_i' \equiv 1 \bmod q_i \qquad (2)$$

(c). 加密內容：執行數位內容 m 的加密動作時，會先隨機選擇 r_i，透過公式(3)運算出 d_i，接著再透過公式(4)和公式(5)運算出加密之數位內容(R, D)，並將(R, D)傳送給所有接收者，接收者所接收到的加密內容(R, D)皆相同。

$$d_i = r_i \oplus m \qquad (3)$$

$$R = \sum_{i=0}^{k_r} r_i P_i P_i' \bmod P \quad (4)$$

$$D = \sum_{i=0}^{k_r} d_i Q_i Q_i' \bmod Q \quad (5)$$

(d). 解密內容：接收者利用解密金鑰(p_i, q_i)，透過公式(6)和公式(7)運算出(r_i, d_i)，將 (r_i, d_i) 透過公式(8)運算，便能解回原先受保護的數位內容 m。

$$r_i = R \bmod p_i \quad (6)$$

$$d_i = D \bmod q_i \quad (7)$$

$$m = ri \oplus d_i \quad (8)$$

三、研究方法與架構

P2P 傳輸技術目前相當熱門，因為它能同時讓兩個使用者直接分享彼此的檔案，而不用透過第三方(伺服器)；但是，P2P 傳輸技術同時也是惡名昭彰的非法活動溫床，它使得盜版和非法使用變得容易，因此許多使用者利用它來從事違反著作權法的資料交換，為解決 P2P 傳輸架構帶給大眾的不好印象，導入適合 P2P 網路之 DRM 機制是可行的。本研究將試圖改善 Tetsuya Iwata et al.[2003]所提出的分散式之 DRM 機制，為加強 DRM 控管能力及不降低使用者接受度，預計導入新型金鑰管理系統，改善傳統金鑰管理系統於成員變動幅度大的 P2P 網路下之實作不易，使得在 P2P 網路下，針對數位內容加密保護成為可行。

3.1 DRM 機制改良

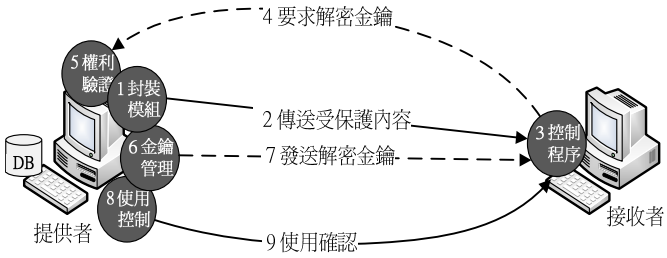

圖 8 改良之 DRM 機制

1. 提供者定義數位內容之權利規則，及使用者被授權的程度，並透過封裝模組封裝一起。
2. 提供者將受保護內容傳送給 P2P 群組成員，此時受保護內容會經由 P2P 轉傳特徵分散出去。
3. 接收者在取得原始數位內容之前，會先啟動內含之控制程序，控制程序會先判斷接收者端是否擁有數位內容相對應之解密金鑰，擁有解密金鑰則會試圖做解密動作。當未擁有解密金鑰，或擁有解密金鑰但無法成功解密時，皆會執行步驟 4。
4. 接收者提供驗證資料，向提供者要求解密金鑰。
5. 提供者透過權利驗證模組，連結資料庫驗證使用者資料，當使用者資料合法則執行步驟 6，不合法則給予錯誤訊息。
6. 提供者透過金鑰管理模組產生一組新的解密金鑰，儲存於使用者資料庫；並重新計算加密金鑰。
7. 提供者發送解密金鑰給合法的接收者，一旦接收者收到解密金鑰，則控制程序會再次試圖做解密動作。值得注意的是，接收者除非擁有合法驗證資料且合法被授權使用內容，否則解密動作不會成功。
8. 使用控制模組會根據提供者之定義，定時啟動執行使用確認作業。

9. 唯擁有合法解密金鑰的使用者，才能通過來自使用者傳送之使用確認作業。一旦發現使用者解密金鑰已失效(如到期)，則使用者端的控制程序會通知使用者無法繼續解密作業，並結束數位內容之使用。

3.2 新型金鑰管理系統導入

將新型金鑰管理系統導入 P2P 網路後，配合群組成員加入與退出時的金鑰管理作業程序如圖 9 所示。

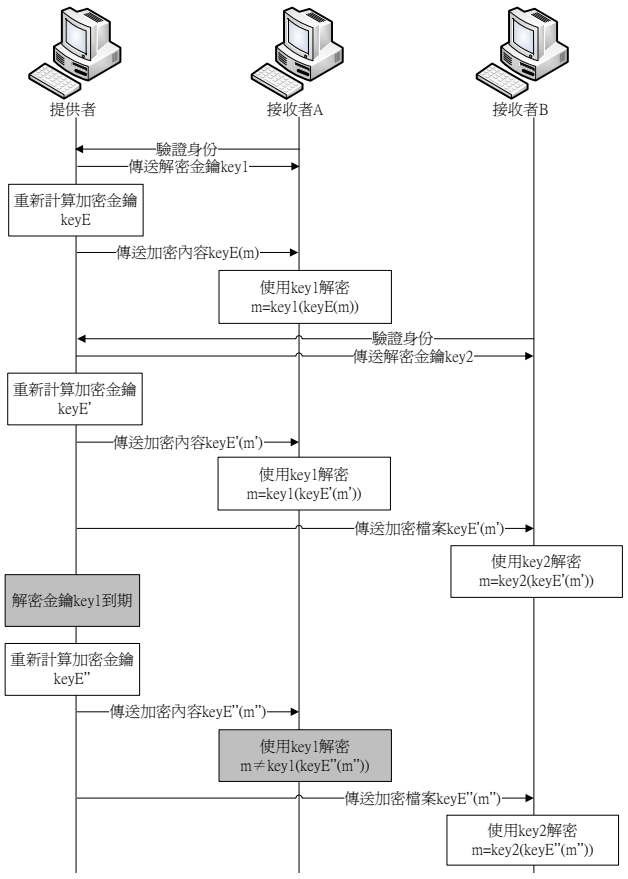

圖 9 新型金鑰系統群組成員加入與退出程序

四、系統實作

本研究採用 NetBeans IDE 應用軟體作為開發環境，利用 Java JXTA 相關類別和方法開發 P2P 基本網路，而播放軟體則採用 Open Source Goalbit 4.1 版。

4.1 內容使用規則定義模組

此模組在提供者欲分享數位內容時被啟動，主要用來協助提供者定義受保護內容的使用規則，詳細運作流程請參照圖 10。

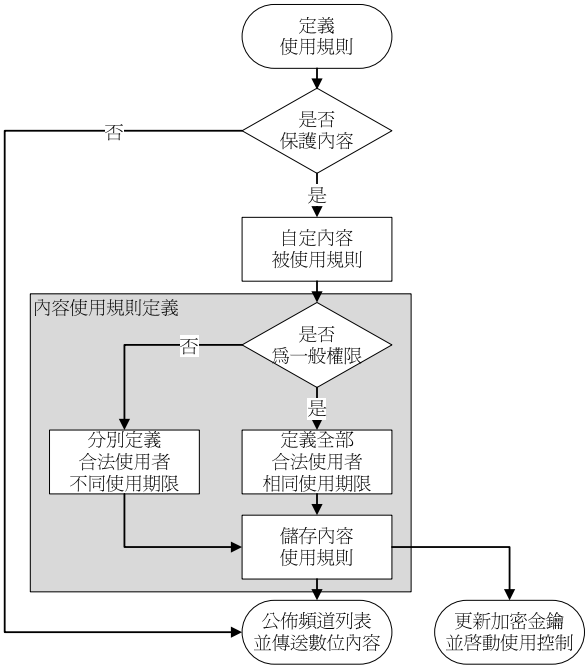

圖 10 內容使用規則定義模組

4.2 使用者權利驗證模組

此模組在提供者接收到使用者驗證資料時被啟動，主要用來協助提供者驗證使用者身份，並觸發金鑰管理模組，去更新金鑰，詳細運作流程請參照圖 11。

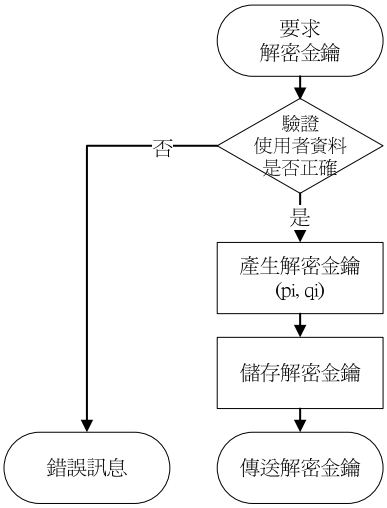

圖 11 使用者權利驗證模組-提供者端

4.3 金鑰管理模組

此模組協助提供受保護頻道內容的提供者自行定義接收群解密金鑰的有效性(更新或保留)，詳細運作流程請參照圖 12。

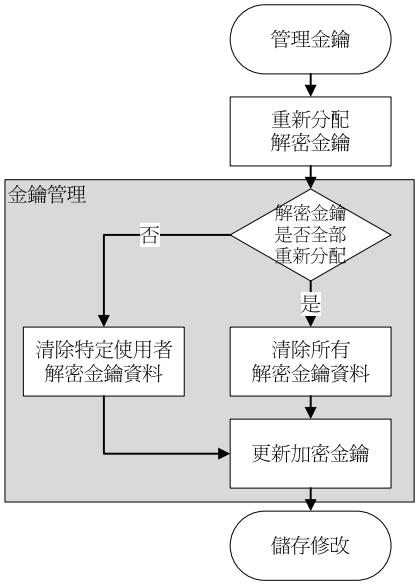

圖 12 金鑰管理模組

4.4 使用者控制程序模組

此模組除了在接收者欲開啟受保護頻道內容時被啟動外，也在接收到使用確認訊息時被啟動，主要用來協助使用者解密加密內容，詳細運作流程請參照圖 13。

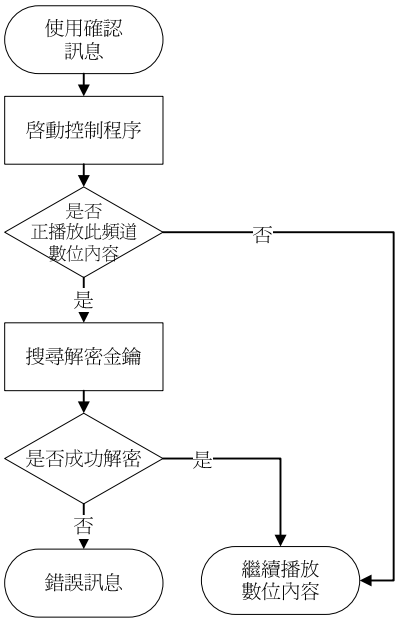

圖 13 使用者控制程序模組

4.5 內容使用控制模組

此模組在提供者發佈受保護頻道資訊時被啟動，詳細運作流程請參照圖 14。

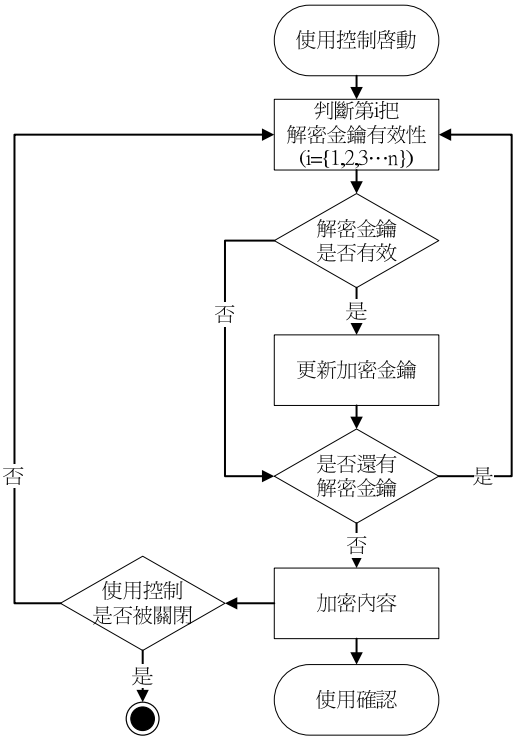

圖 14 內容使用控制模組

五、實驗與分析報告

完成系統實作後，必須透過實驗測試本系統相關績效，以分析本系統的可行性。本系統目標為 P2P DRM 機制之改良，考量現實網路環境中包含許多複雜難以量化因素，因此本研究透過 Testbed@TWISC 網路安全測試平台，設計實驗環境之網路拓樸、網路速度及電腦數量。

5.1 適當金鑰長度實驗

5.1.1 產生解密金鑰平均計算時間

此實驗目的在於評估金鑰長度是否會影響金鑰產生的平均時間，進而找出最適的解密金鑰長度，統計結果如圖 15 所示。

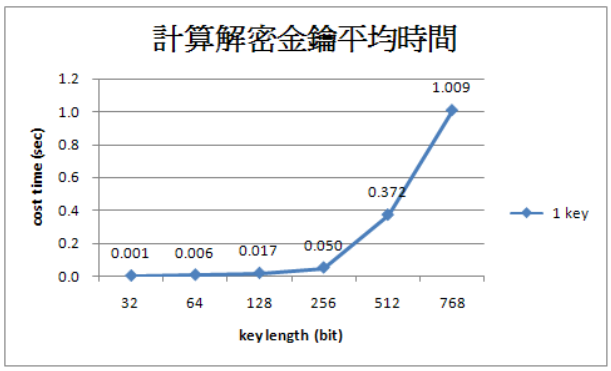

圖 15 計算解密金鑰平均時間折線圖

5.1.2 解密金鑰數量計算

此實驗目的在於評估金鑰長度至少多長，才能達到機率上的相對安全。利用質數定理推算出 6 種不同長度可能的質數數量，再透過圖 15 所統計的每把解密金鑰平均產生時間，推算出計算 6 種不同長度之所有質數產生的時間，結果如表 1。

表 1 金鑰數量統計表

金鑰長度 (bit)	$x = 2^{bit}$	金鑰數量-質數數量 $\pi(x) - \pi(x - 1)$ $\pi(x) = x / \ln x$	解密金鑰組合 (pi, qi) {i= 1, 2, 3…n} 2 * C(x, 2)	預估計算時間 (年)
32	2^{32}	93694476	$4389327369 * 10^{6}$	0
64	2^{64}	$2046140408 * 10^{9}$	$2093345283 * 10^{27}$	10^{9}
128	2^{128}	$1902570869 * 10^{28}$	$1809887954 * 10^{65}$	10^{17}
256	2^{256}	$3249952431 * 10^{66}$	$5281095400 * 10^{141}$	10^{57}
512	2^{512}	$1885305082 * 10^{143}$	$1777187625 * 10^{295}$	10^{135}
768	2^{768}	$1456308549 * 10^{220}$	$1060417295 * 10^{449}$	10^{212}

5.1.3 實驗小結

經由以上產生解密金鑰平均計算時間和解密金鑰數量計算兩個實驗，得出 64bit、128bit 和 256bit 的解密金鑰長度都是適合本系統的，但金鑰長度往往也關係著加解密的效率，通常金鑰長度與加解密的效率成反比，因此還得配合加解密速度才能判斷適當的金鑰長度。

5.2 封包加解密效能實驗

對於密碼系統而言，除了金鑰管理很重要外，加解密的效能也很重要。而除了金鑰長度會影響加解密效能外，密碼系統的演算法也與加解密效能息息相關。

5.2.1 加解密封包平均計算時間

執行本實驗目的為二：(1)找出金鑰長度與加解密效能間的關係。(2)使用者人數(解密金鑰數量)與加解密效能間的關係，此關係於演算法相關，加密效能的統計結果如圖 16 所示，解密效能的統計結果如圖 17 所示。

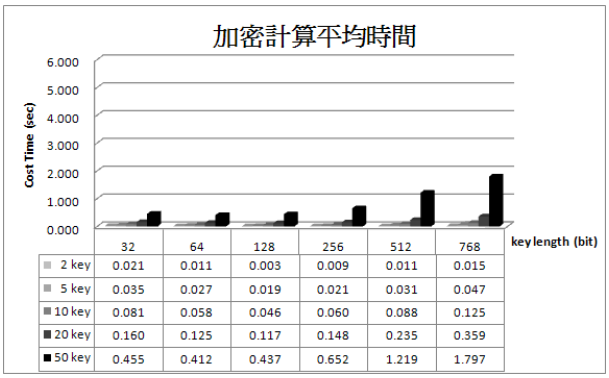

圖 16 加密計算平均時間長條圖

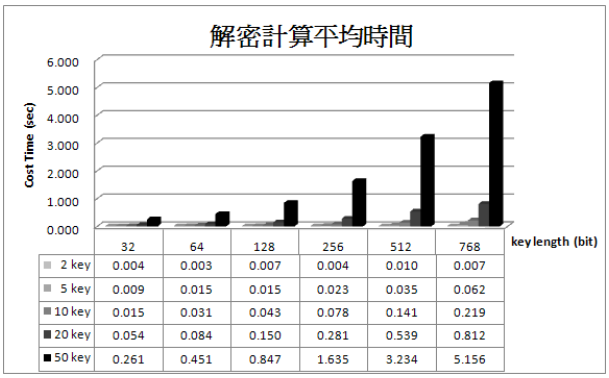

圖 17 解密計算平均時間長條圖

5.2.3 實驗小結

經由以上封包加解密平均計算時間實驗，再配合先前產生解密金鑰平均計算時間和解密金鑰數量計算兩個實驗，我們可得出 64bit 與 128bit 的解密金鑰長度是較佳的，而基於機率上的相對安全原則，判斷 128bit 的金鑰長度是個很好的選擇。

但是，若要將此密碼系統用於即時串流機制上，針對每一個傳輸的封包做加密的動作，對於影片的流暢度而言是不佳的。因此，本研究所實作的系統，增加一個 CheckTime 的功能，供提供者設定平均加密的時間。即 CheckTime = 1 時，為對每一分鐘所產生的封包做加密的動作，當使用者無法解密此封包時，便會顯示錯誤訊息，通知使用者無法再播放數位內容。

5.3 DRM 機制分析

表 2 改良之 DRM 機制與傳統 DRM 機制比較

分類	Client-Server 架構下之 DRM 機制	P2P 架構下分散式之 DRM 機制	P2P 架構下改良之 DRM 機制
權利監督	良好	N/A	尚可
權利規則定義	良好	差	尚可
伺服器計算負荷	差	良好	尚可
P2P-非集中式	N/A	良好	良好
P2P-擴展性	N/A	良好	良好
P2P-強韌性	N/A	良好	良好
提供者接受度	良好	尚可	良好
接收者接受度	差	差	尚可
備註	N/A，無此功能。 差，表示只初步具備此功能，但不敷使用。 尚可，表示基本功能皆具備，且能有效使用。 良好，表示整體功能完善，包含一些進階功能。		

六、結論

本研究貢獻在於改良傳統分散式 DRM 機制，使其適用於現有 P2P 即時串流傳輸架構上，並視 P2P 網路群組成員變動幅度大之特性，導入合適之新型金鑰管理系統。

改良之 DRM 機制在 DRM 能力、系統效能、P2P 優勢及使用者接受度的分析上，整體來看的確優於傳統的 DRM 機制。在 DRM 機制控管能力方面，本研究所提出的 P2P 架構下改良之 DRM 機制，雖然延續 P2P 架構下分散式之 DRM 機制的作法，將 DRM 伺服器能力分散至提供者端，但導入新型金鑰管理系統，協助提供者變相的達成監控使用權功能，雖然無法較傳統 DRM 伺服器優良，但是已能達成基本的 DRM 能力。而在 P2P 網路優點的保留方面，傳統 Client-Server 架構下之 DRM 機制，並無法任何 P2P 優勢，因為其所有的檔案分享都得透過第三者(伺服器)；而本研究所提出的 P2P 架構下改良之 DRM 機制，將 DRM 伺服器的能力分散在提供者端，並不會因為 DRM 伺服器的效能或安全問題，而破壞掉造成 P2P 網路強韌性，因此在 P2P 優勢的保留上皆是良好的。

誌謝

本研究部分經費來自國科會98年度專題研究計畫NSC 98-2221-E-224-033與【網路安全測試平台(Testbed@TWISC)之建置、推廣與應用】NSC 98-2219-E-006-001，特此致謝。

參考文獻

[1] 沈榮津等編著，2007，2007 台灣數位內容產業年鑑，經濟部工業局數位內容產業推動服網。

[2] 官振鵬，呂沐錡，2008，"應用於 P2P 網路中以社群為基礎之階層式數位權利管理機制"，電腦與通訊，124 期，頁 95-100，2008 月 06 日。

[3] 陳星吏，2003，架構一個以角色為金鑰管理基礎的企業數位版權管理系統雛型，國立交通大學，碩士論文。

[4] Renato Iannell, 2001, "Digital Rights Management (DRM) Architectures", D-Lib Magazine, vol. 7, Number 6, June.

[5] Mark Stamp, 2003, "Digital rights management: the technology behind the hype", Journal of Electronic Commerce Research, vol. 4, pp. 102-112.

[6] Park, Jaehong, Ravi Sandhu, 2002, "Towards Usage Control Models:Beyond Traditional Access Control", Monterey, California, SACMAT, June 3-4, pp. 57 64.

[7] Tetsuya Iwata et al., 2003, "A DRM system suitable for P2P content delivery and the study on its implementation", The 9th Asia-Pacific Conference on Communications, Harbin, China, December 15-19.

[8] Jae-Youn Sung, Jeong-Yeon Jeong, Ki-Song Yoon, 2006, "DRM Enabled P2P Architecture" , The 8th International Conference, February 20-22, pp.487-490.

[9] Xi Chen, 2007, "Secure Media Distribution in P2P Networks" The First International Symposium on Data, Privacy, and E-Commerce, November 1-3, pp. A212-214.

[10] 鄭富國，2006，"階層結構中金鑰管理之研究"，國立中興大學，博士論文。

[11] Chin-Chen Chang, Yi-Fang Cheng, Iuon-Chang Lin, 2008, "A novel key management scheme for dynamic multicast communications." International Journal of Communication Systems, vol. 22, Issue 1, pp. 53-66, August 15.

[12] Sun Microsystems Inc., 2007, JXTA Java Standard Edition v2.5: Programmers Guide.