View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Tamkang University Institutional Repository

應用於跨平台之家庭數位版權協定與安全之研究

李鴻璋
淡江大學資訊管理學系
hclee@mail.im.tku.edu.tw

劉盈妤
淡江大學資訊管理學系
stef1021723517@hotmail.com

摘要

目前商業上提供的平台皆屬於封閉型的系統，不過隨著智慧型手機的普及，消費者偏好在多種平台中使用相同的軟體，跨平台分享將是未來的趨勢主流，在不久的將來跨平台分享數位內容也將建立在家庭當中，引領全球進入嶄新的數位家庭時代。所以如何透過有效的方式來保護數位內容防止非法行為，並提高其安全性將是這個階段所需重視的課題。

之前相關研究中，所提出之協定皆只有改善封閉式檔案傳輸的問題，其主要是在確認數位版權的交易機制，不過並沒有做到安全上的考量。因此在我們所提出的 CUHO 協定，除數位版權分享的目的，並考慮到訊息傳遞安全的重要性，利用了密碼學上的挑戰回應並結合隨機雜湊鎖之理念，將每回合通訊之認證資訊加入隨機亂數以及時間戳記作運算，以達到不可追蹤性以及避免重送攻擊來提高安全性。

關鍵詞：*跨平台;不可追蹤性;家庭數位版權;密碼學;數位內容*

1. 緒論

1.1 研究背景

全球資通訊數位化程度提升，寬頻用戶數逐年增加，帶動發展帶動家庭朝向數位化、網路化、行動化發展，而資通訊網路快速發展將結合家電產品，引領全球進入嶄新的數位家庭時代，有關家庭數位娛樂方面，在數位家庭聯盟持續的推動之下，數位娛樂產品內容分享漸漸成型，未來可朝向跨平台分享為發展方向。在這資訊技術發展快速的時代，不僅許多數位內容都以數位化的方式呈現，加上寬頻、無線網路的普及，數位家庭的概念漸漸由數位家庭聯盟實現中，目前全球較具主導性的技術規格有美國地區的 UPnP / SCP 標準與 Low Works 標準，日本地區的 ECHONET 標準，歐洲地區的 KNX 標準，及中國大陸地區的閃聯（IGRS）標準，在我國也有由系統廠商組成類似的組織，名稱為 SAA 聯盟（Smart Appliance Alliance，智慧家電產業研發聯盟）[2]，相信不久的將來跨平台分享數位內容將在家庭互通的建立，家庭數位版權使用與分享將會落實在每個家庭當中，所以如何透過有效的方式來保護數位內容防止非法行為，並提高其安全性將是這個階段所需重視的課題。

1.2 研究動機與目的

李南逸和陳芸仙[1]提出適合在家庭網路環境運行的數位版權管理系統，透過私密金鑰密碼系統向主要伺服器設備間身分認證的機制，讓家庭網路環境裡的多媒體設備間可以合法的分享彼此的數位內容，不過本研究認為這篇考量的方式安全性不夠高。游子德[5]一個應用於數位家庭的數位版權管理機制，結合身分認證、版權描述語言及數位浮水印…等技術，以確保數位內容的安全性，並以兩段式數位版權管理架構，進行數位內容使用權利的管理，管制數位內容在同一時間點，只有授權給一個設備使用，本研究認為這篇提出的論文只能單一時間單一使用限制太多。上述主要是提及研究性的不足，而現今商業上有許多封閉型平台，會因為軟硬體格式的不同，而無法在不同的平台上可使用，所以我們希望提出一個跨平台的智慧分享平台結合數位家庭的概念，讓數位內容授權在家庭中，也讓數位內容可在家庭中任何撥放器使用，而不需在特定的硬體上撥放。

綜合這些優缺點，本研究使用了應用於跨平台之家庭數位版權協定與安全之研究系統，讓數位內容授權在家庭數位版權系統合法化，利用數位家庭版權架構的數位版權管理系統的跨平台分享，範圍局限於授權的家庭，使用跨硬體平台提供下載服務，讓使用者下載歌曲後可以放置各個撥放器使用，經由家內伺服器下載，再分享給家庭內授權播放器使用。

2. 文獻探討

2.1 封閉型系統與跨平台系統

現今商業上有許多封閉型平台，系統當中主要是透過硬體或軟體做為加解密的依據，所發展出的數位內容為特定的檔案格式與其他平台不相容，這對使用者來說有這非常多限制，像是只能在特定的硬體上撥放使用、會員帳號不可在多個裝置上安裝以及不可同時於兩台電腦使用同一組帳號、密碼登入等等限制，例如 Apple 的 iTunes（FairPlayDRM 系統）[10]、KKBOX [11]，Apple 的 iTunes、KKBOX 與跨平台研究之比較如表 1 所示。

表1　Apple 的 iTunes、KKBOX 與跨平台研究之比較

	獨家授權		跨平台系統
	KKBOX	iTunes	
特點	會員制 付費享受歌曲的模式 會員在期間可離線播放歌曲	曲目制 單/多曲下載付費模式	單/多曲下載付費模式 跨平台多撥放器使用模式
商業模式	無曲目擁有權	曲目擁有權	曲目擁有權 能夠開放式多家授權
版權發行者	單一	單一	可多家
撥放器	帳號僅能安裝在三台裝置而且不能同步	帳號僅能安裝在五台裝置可同步	授權狀態下皆可多台同步撥放
軟體可擴充性	限制	限制	開放

2.2 相關研究

家庭數位版權管理系統近來有許多學者提出，此節我們將介紹之前學者所提出的家庭數位版權管理系統。

2.2.1 游子德所提機制

2008 年游子德[5]提出應用於家庭架構之數位版權管理系統，主要是對於使用者合理使用數位內容的系統加以探討。此論文提出兩段式的管控機制，利用憑證授權使用時段的方式，達到數位內容可以在任何時間、任何地點及任何設備之合理使用的目的。此機制系統架構圖，以圖 1 表示，運作流程分為六個階段，以下以圖 2~圖 7 表示。相關符號定義如表 2 所示。

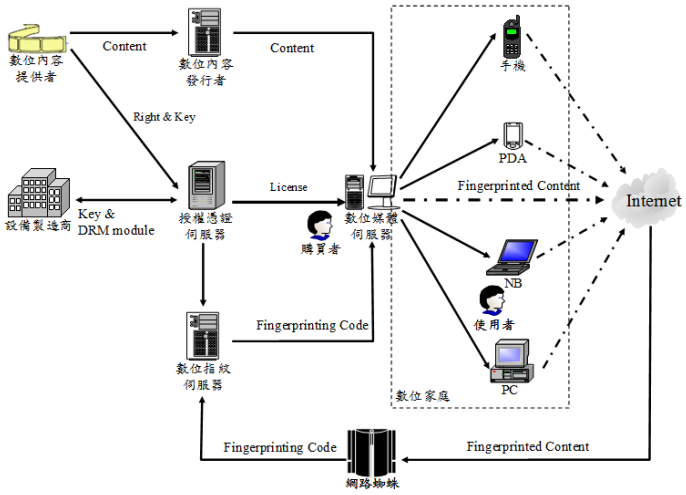

圖1　系統架構圖

表2　符號定義

符號	定義
E[Data]	用公鑰系統對資料 (Data) 加密
E(Data)	用私鑰系統對資料 (Data) 解密
H(Data)	對資料 (Data) 進行雜湊函數運算
C	數位內容
R	數位內容的使用權利
L	授權憑證，包含使用權利 R 和加密金鑰 K_C
ID_C	數位內容的識別碼
ID_U	使用者的識別碼
ID_B	購買者的匿名識別碼 ID_B= $H(ID_U \| s)$
P_B	購買者的付款資訊
ID_S	媒體伺服器的識別碼
ID_{P_x}	媒體播放器 x 的識別碼
ID_{Fp}	數位內容的數位指紋識別碼
ID_L	數位內容的授權憑證識別碼

KS	數位內容的加密金鑰種子 $KS=H(SK_{CP})$
K_C	數位內容加密金鑰 $K_C=H(KS \| H(C))$
PK_{CP}, K_{CP}	數位內容提供者的公鑰及私鑰
PK_{LS},SK_{LS}	授權憑證伺服器的公鑰及私鑰
PK_M, SK_M	設備製造商的公鑰及私鑰
PK_U, SK_U	使用者的公鑰及私鑰
PK_B, SK_B	購買者的公鑰及私鑰
PK_S, SK_S	媒體伺服器的公鑰及私鑰
K_{P_x}	媒體播放器 x 的金鑰
$K_{S\_P_x}$	媒體伺服器與媒體播放器 x 的共享金鑰
TR_x	媒體播放器 x 要求數位內容的授權使用時間
TS_x	媒體播放器 x 的電子時戳
s	隨機產生的亂數
$\|$	連結符號

(1) 數位內容封裝階段:如圖 2 所示

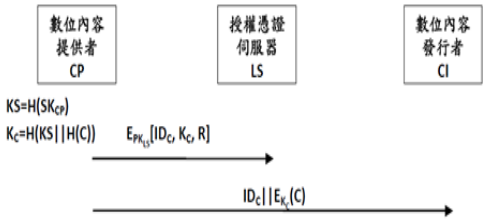

圖2 數位內容封裝階段

(2) 數位家庭註冊階段:如圖 3 所示

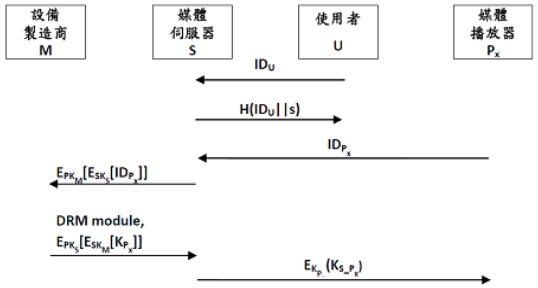

圖3 數位家庭註冊階段

(3) 購買者註冊階段:如圖 4 所示

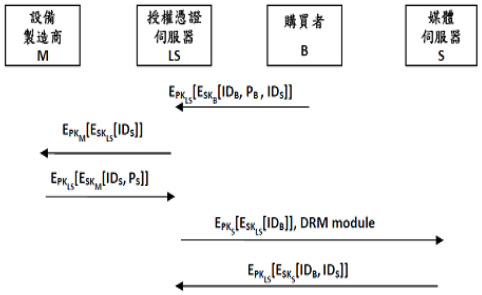

圖4 購買者註冊階段

(4) 數位內容購買階段:如圖 5 所示

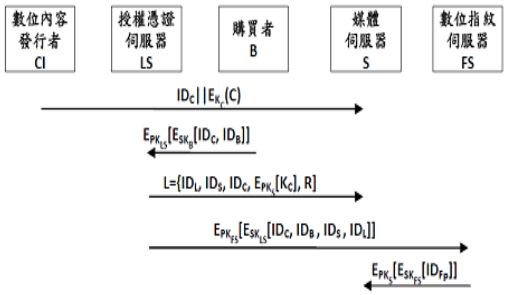

圖5 數位內容購買階段

(5) 數位內容使用階段:如圖 6 所示

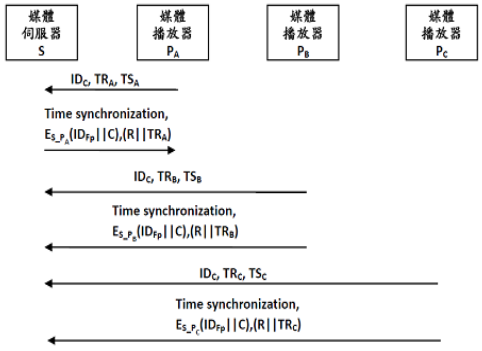

圖6 數位內容使用階段

(6) 數位內容追蹤階段:如圖 7 所示

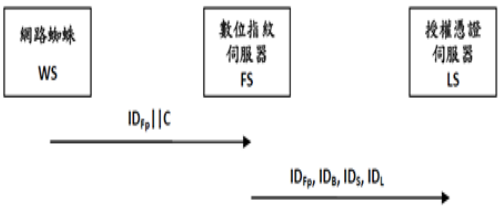

圖7 數位內容追蹤階段

3. CUHO-具跨平台、不可追蹤性之家庭數位版權管理機制

此章節將介紹本篇論文所提的機制，而我們將此機制稱為 CUHO。其原因取機制中的跨平台(Cross-platform)、不可追蹤性(Untraceability)及家庭數位版權管理(HOme-scoped digital rights management)的各個英文單字字首。

3.1 簡介

在跨平台分享過程中，藉由相互挑戰回應達到雙向鑑別，並結合隨機雜湊鎖之理念，將每回合跨平台分享之認證資訊加入隨值數作運算，以達到不可追蹤性。數位內容提供者與數位內容發行者之間簽訂合約(以 XrML 的文件形成)，授權憑證伺服器確保二者依照合約履行，也利用 DRM 這項技術原本用於保護音樂、影片不被盜拷，透過加密的方式，來保護圖文、影音，不被非法存取或利用。本文所提之數位版權管理系統，結合密碼學、XrML、身分認證及雙向鑑別…等技術，以確保數位內容的安全性不被非法使用。

3.2 研究架構

系統架構圖如圖 8 所示

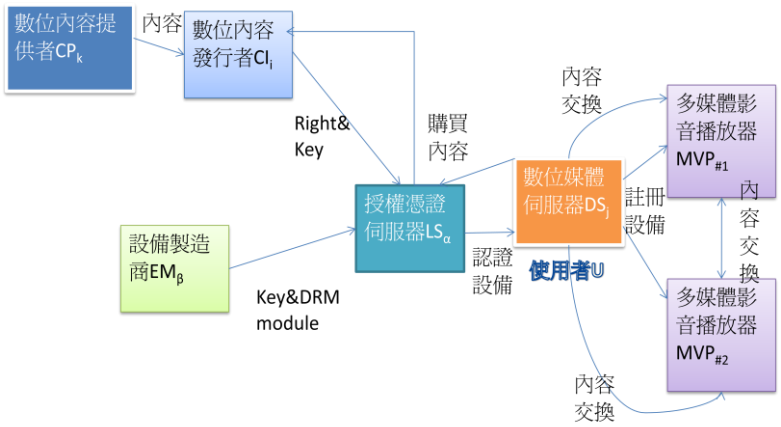

圖8 系統架構圖

3.3 六個角色的關係及應用

3.3.1 數位內容提供者

提供者提供數位版權內容給發行者，其提供者可以傳給多個發行者，提供者與發行者之間簽訂合約(以 XrML 的文件形成)，授權憑證伺服器確保二者依照合約履行。

3.3.2 數位內容發行者

透過網路，發行者向提供者購買數位版權內容（以 XrML 的文件形成），並負責進行儲存管理與分享，建立一個數位內容的傳輸管道，發行者必須定義購買者使用權限(以 XrML 的文件形成)，使用金鑰加密，將該購買者的使用權限安全的傳送到購買者家中的媒體伺服器(購買者透過家中的媒體伺服器向發行者購買或是利用 IC 卡媒介傳送到媒體伺服器)。發行者上必須有編碼以提供給媒體伺服器向授權憑證伺服器查核，當使用者要播放曲目時，媒體伺服器傳送伺服器 ID、播放的曲目以及發行者名稱以及購買者使用契約權限給授權憑證伺服器檢查，契約中有內容發行者的簽章，所以授權憑證伺服器可以審核是否有使用權利。

3.3.3 設備製造商(軟硬體)

負責生產數位媒體伺服器以及多媒體影音播放器設備，透過授權憑證伺服器與數位媒體伺服器進行金鑰驗證，使用金鑰與 DRM module 保護並安全傳送數位內容。

3.3.4 授權憑證伺服器

授權憑證伺服器主要分成兩種認證過程

一、驗證數位版權內容

當購買者要播放影音時，數位媒體伺服器要透過授權憑證伺服器檢查提供者與發行者之間的契約，確認數位版權內容是否一致。透過媒體伺服器傳送伺服器 ID、播放的曲目以及發行者名稱以及購買者使用契約權限的認證，確認是否具有使用權利以及追蹤數位內容不合理的存取。

二、驗證設備

授權憑證伺服器必須驗證數位媒體伺服器是為合法的設備製造商所生產，以確保數位內容發行者可以安全傳送數位內容到數位媒體伺服器。

3.3.5 數位媒體伺服器

數位媒體伺服器例如:iTunes、MOD 數位機上盒等等設備，在數位家庭網路中，用來認證撥放器設備，媒體伺服器必須透過授權憑證伺服器認證其設備，一個數位家庭中可以有多台媒體伺服器，而一台媒體伺服器可以供多台播放器使用，媒體伺服器必須儲存撥放器對它註冊資訊以及已購買加密數位內容，媒體伺服器與播放器之間有共享金鑰，作為媒體伺服器與播放器交換內容的憑證。

3.3.6 多媒體影音播放器

系統可以支援多媒體影音播放器，已達到跨平台的目的，例如 RMVB、iPad、iPod 等等經註冊過後的設備，使用時播放器必須向伺服器註冊，並且具唯一性，播放器只能註冊在一個數位家庭內，如果多家註冊只保留最後一次註冊那家，註冊後伺服器會產生共享金鑰，作為數位內容解密之用途，播放器其主要用途為讀取和撥放數位內容。播放器之間交換數位內容，必須透過媒體伺服器認證，確定是為註冊播放器才可交換內容。

3.4 系統流程

我們將 CUHO 認證分為四個主要階段：數位設備與內容確認的流程、家庭數位內容購買階段、家庭數位內容播放階段、及多媒體影音播放器內容交換階段。符號定義如表 3 示。XrML 以圖 9 和圖 10 表示。

表3 符號定義

符號	定義
CP_k	數位內容提供者 k(Content Provider)
CI_i	數位內容發行者 i(Content Issuer)

EM_β	設備製造商 β (Equipment Manufacturer)
LS_α	授權憑證伺服器 α (License Server)

DS_j	數位媒體伺服器 j(Digital Server)
$MVP_{\#n}$	多媒體影音播放器 n (Multimedia Video Player) 多個多媒體影音播放器歸同一個數位媒體伺服器管理
ID_C	數位內容的識別碼
ID_{CPk}	數位內容提供者 k 的識別碼
ID_{CI_i}	數位內容發行者 i 的識別碼
$ID_{LS\alpha}$	授權憑證伺服器 α 的識別碼
ID_{DSj}	數位媒體伺服器 j 的識別碼
$ID_{MVP_{\#n}}$	多媒體影音播放器 n 的識別碼
X_i	數位內容發行者向數位內容提供者購買數位版權內容的某特定契約 i，為簡化起見，發行者與提供者指的是協定假說下所討論的對象 (簽訂合約以 XrML 的文件形成)
KS_k	數位內容提供者 k 之數位內容加密種子 $KS_k=H(SK_{CP_k})$
K_C^k	數位內容加密種子 KS_k 對數位內容 C 產生之加密金鑰 $K_C^k=H(KS_k//H(C))$
r	隨機亂數
t_m	時間戳記
R_C	內容發行者定義購買者使用權限的某次購買契約 C，為簡化起見，發行者與購買者指的是協定假說下所討論的對象 (簽訂合約以 XrML 的文件形成)
PK_{LS_α}, SK_{LS_α}	授權憑證伺服器 α 的公鑰及私鑰
PK_{DSj}, SK_{DSj}	數位媒體伺服器 j 的公鑰及私鑰
$PK_{MVP_{\#n}}$, $SK_{MVP_{\#n}}$	多媒體影音播放器 n 的公鑰及私鑰
$K_{DSj\_MVP\#n}$	數位媒體伺服器 j 對多媒體影音播放器 n 在註冊時產生出共享金鑰 $K_{DSj\_MVP\#n}=H(SK_{DSj}//n//r)$
ID_L	短期授權憑證 L 內容裡的 ID
T_L	短期授權憑證 L 的到期日
L	授權憑證 L 數位媒體伺服器 j 向授權憑證伺服器 α 請求播放數位內容 C 時，授權憑證伺服器 α 檢查確認後傳送授權憑證 L 給數位媒體伺服器 j 當作驗證，其內容包括授權憑證 L 的內容為 $(ID_L, ID_{DSj}, ID_C, R_C, T_L, E_{PK_{DSj}}(K_C^k))$
//	連結符號

```
<license>
  <grant>
        <keyHolder> CPk</keyHolder>
        <ProviderID>IDCPk </ProviderID>
        <IssuerID>IDCli </IssuerID>
        <cx:print/>
        <offline>no</offline>

<validityInterval>2014/06/30</validityInterval>
        <digitalResource>
          <fidID> IDC</fidID>
        </digitalResource>
    </grant>
    < Conform >
          <dsig:Signature>
          <!—CPk 與 CIi 雙方的簽章值-->
          </dsig:Signature>
    </ Conform >
</license>
```

圖9 數位內容發行者向提供者購買數位版權內容 X_i

```
<license>
  <grant>
        <keyHolder>DSj </keyHolder>
        <ProviderID>IDCPk </ProviderID>
        <IssuerID>IDCli </IssuerID>
        <cx:print/>
        <offline>no</offline>
        <validityInterval>2013/12/31 </validityInterval>
        <digitalResource>
          <fileID> IDC</fileID>
        </digitalResource>
    </grant>
    <Conform>
          <dsig:Signature>
          <!—CPk 的簽章值-->
          </dsig:Signature>
    </Conform>
</license>
```

圖10 內容發行者定義購買者使用權限的契約 R_C

一、針對數位版權/伺服器在此文件檔案中之權限，產生一個較短之 XrML 權限檔

二、此權限檔只記錄該數位內容在相對應文件檔案之可進行的權限內容

三、權限檔內含數位內容識別碼、對文件檔案使用之權利、權限有效日期(發行者與提供者簽訂使用期限、短期授權憑證)以及可否離線使用數位內容

四、將此 XrML 權限檔及簽章值傳送給授權憑證伺服器驗證

3.4.1 數位設備與內容確認的流程

數位設備與內容確認的流程分為三個階段。

一、數位內容封裝階段：如圖 11 所示

(1) 數位內容提供者將 ID_C、K_C^k 以及某特定契約 X_i 傳送給授權憑證伺服器當作授權憑證。

(2) 數位內容提供者將數位內容封裝後傳給數位內容發行者。

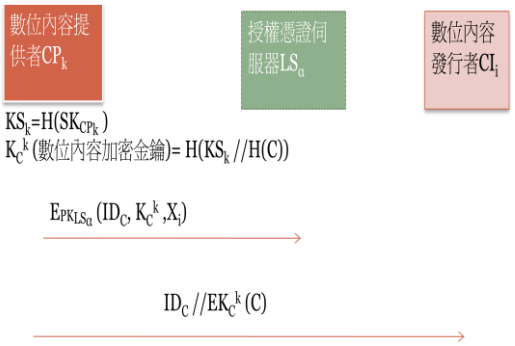

圖11 數位內容封裝階段

二、數位媒體伺服器註冊階段：如圖 12 所示

（1）數位媒體伺服器透過授權憑證伺服器驗證數位媒體伺服器。

（2）設備製造商確認數位媒體伺服器是否為合法的設備製造商所生產。

（3）確認後，才能確保數位內容發行者可以安全傳送數位內容到伺服器。

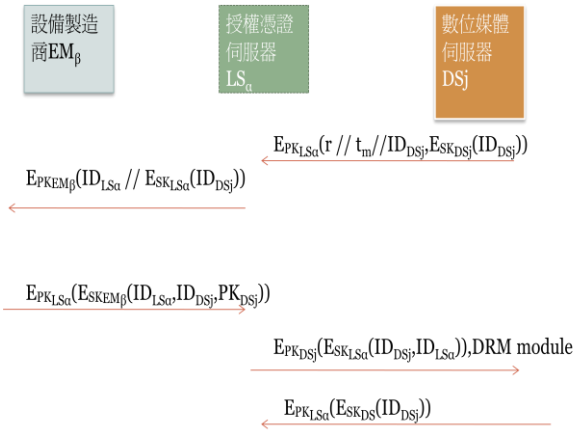

圖12 數位媒體伺服器註冊階段

三、多媒體影音播放器註冊階段：如圖 13 所示

（1）多媒體影音播放器向數位媒體伺服器註冊之前，必須先透過授權憑證伺服器向設備製造商驗證播放器是否為合法的設備製造商所生產。

（2）驗證後，多媒體影音播放器即可向數位媒體伺服器註冊，註冊後伺服器會產生共享金鑰，並傳送給播放器，作為數位內容解密之用途。

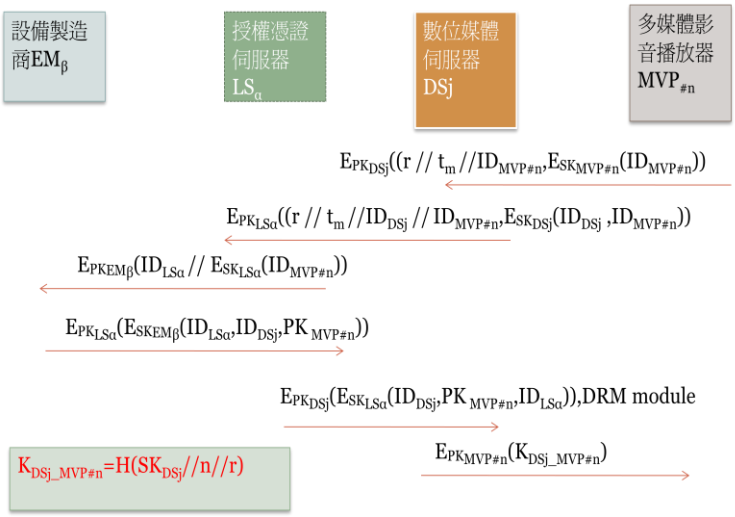

圖13 多媒體影音播放器註冊階段

3.4.2 家庭數位內容購買階段：如圖 14 所示

（1）數位媒體伺服器向授權憑證伺服器驗證伺服器為哪個合法伺服器。

（2）確認後，再將要購買的 ID_C 透過授權憑證伺服器向發行者購買。

（3）數位內容發行者再將封裝的數位內容、購買者使用權限契約 R_C 傳送給數位媒體伺服器。

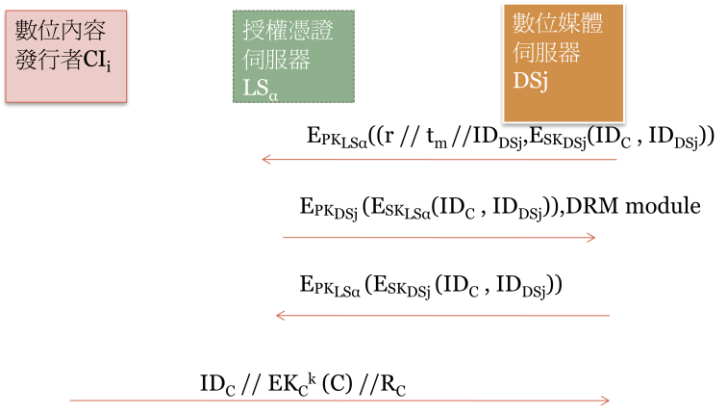

圖14 家庭數位內容購買階段

3.4.3 家庭數位內容播放階段

家庭數位內容播放階段分為兩個階段。

一、家庭數位內容播放階段 Case 1: 如圖 15 所示

（1）當購買者要播放影音時，伺服器要透過授權憑證伺服器檢查 R_C

（2）當使用者要播放曲目時，伺服器會去檢查有沒有短期授權憑證 L。

（3）此案例伺服器有短期授權憑證 L，多媒體播放器就可以直接播放，不需透過授權憑證伺服器檢查。

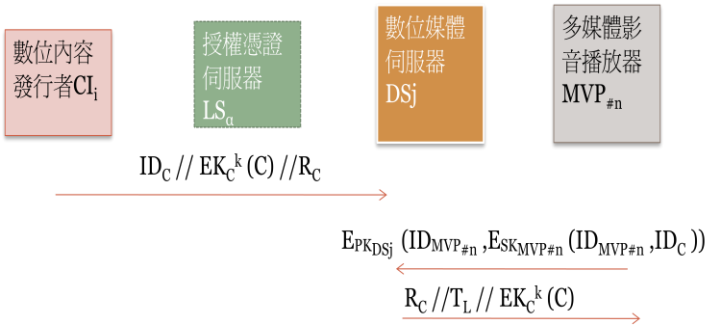

圖15 家庭數位內容播放階段 Case 1

二、家庭數位內容播放階段 Case 2: 如圖 16 所示

（1）與 Case 1 相同

（2）與 Case 1 相同

（3）此案例數位媒體伺服器沒有短期授權憑證 L，伺服器傳送 ID_{DSj}、ID_C、ID_{CIi} 以及 R_C 給授權憑證伺服器檢查，以取得短期授權憑證 L。

（4）數位媒體伺服器取得短期授權憑證 L 後，數位媒體伺服器將 L 的到期日 T_L 、R_C 以及封裝的數位內容傳送給多媒體影音播放器進行撥放。

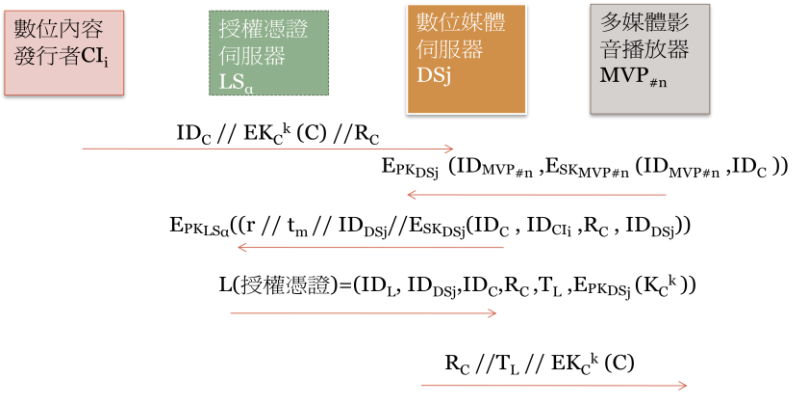

圖16 家庭數位內容播放階段 Case 2

3.4.4 多媒體影音播放器內容交換階段: 如圖 17 所示

(1) 多媒體影音播放器之間交換數位內容，必須透過媒體伺服器認證，確定是為此數位媒體伺服器註冊，多媒體播放器才可交換數位內容。

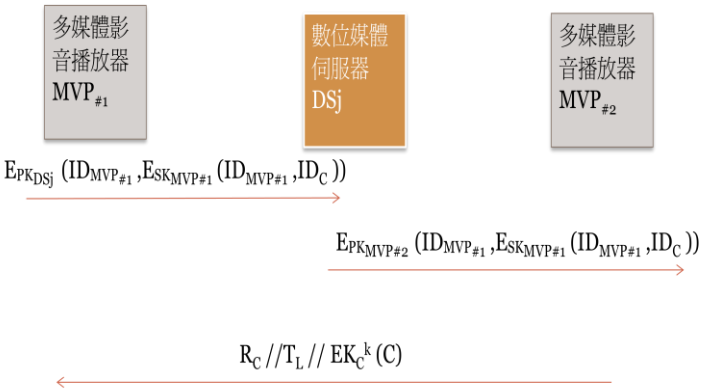

圖17 多媒體影音播放器內容交換階段

4. 分析與討論

4.1 安全性分析

本論文所提機制，根據家庭數位版權管理系統之安全需求，在此作分析：

一、不可追蹤性(Untraceability):授權憑證伺服器與數位媒體伺服器進行通訊時，每回合的認證資訊皆加入隨機亂數進行運算，使溝通訊息具隨機性，由於每次傳送的資料都不相同且沒有相關，攻擊者無法從中得知關連性也無法進行預測或追蹤。

二、重送攻擊(Replay Attack):攻擊者偽裝成合法的數位媒體伺服器與多媒體影音播放器是無效的，因為每回合皆有隨機產生之亂數加入運算，並且加入時間戳記；而且就算是同一個 ID_{DSj} 每次亂數處理後，每次都不一樣，每回合皆會更新。

三、合理使用(Using Reasonable):為了達到任何時間、任何地點、任何設備皆可使用的合理保障，所以對於此系統可同時於兩台設備使用同一組帳號、密碼登入，並且無限制播放器硬體格式；此外，還提供短期授權憑證，可讓使用者在時間內不需重複認證。

4.2 比較分析

在此小節，我們將第二章相關研究中各學者所提機制及本論文所提之 CUHO 機制作比較分析及討論。在游子德[5]的方法當中，雖然改善了使用者隱私權以及無限制硬體格式的問題，不過方法當中限制了媒體播放器使用數位內容時，必須依使用時段授權給不同的媒體播放器，一個時間點只能授權給一個媒體播放器，這樣限制對於使用者是不方便的；除此之外，在這個方法當中可支援出版/發行者數目以及營運平台的數目都是單一個並沒有考慮到多個可支援出版/發行者數目以及營運平台的數目，這是此篇比較大的問題。綜合以上優缺點，本論文 CUHO 機制將單一可支援出版/發行者數目以及營運平台的數目修改為多個可支援出版/發行者數目與多個營運平台的數目，並且在登入系統上沒有限制經授權的播放器同時登入，在溝通過程中，也將隨機產生之亂數和時間戳記加入運算，避免重送攻擊，除此之外，此系統每個階段皆具不可追蹤性。在本論文中，提供了短期授權憑證，這是游子德[5]所提機制中沒有提及的，短期授權憑證可以提供多媒體影音播放器要播放時，可以更加快速，可讓使用者在時間內不需重複認證。

表4 相關研究之安全性比較表

	游子德所提機制	本論文 CUHO 之機制
數位版權機制	有	有
固定 ID 身分暴露	暴露	未暴露
撥放器分享	可	可
多台家內撥放器可否同時撥放	不可	可
不可追蹤性	X	O
跨平台	可	可
營運平台/可支援出版/發行者數目	單	多
抵禦重送攻擊	O	O
短期授權憑證	X	O

5. 結論

目前在家庭數位版權系統的實際應用上，主要需考量的議題包含安全性及隱私保護等方面。在安全性及隱私保護方面，我們使用隨機雜湊鎖結合挑戰回應機制達到跨平台

具不可追蹤性，本研究也因應現今商業上許多封閉型系統會因為軟硬體格式的不同，而無法在不同的平台上可使用，因此使用了跨平台的概念，利用數位家庭版權架構的數位版權管理系統中的跨平台分享，讓數位內容不需在特定的硬體上撥放使用，此外，也將跨平台數位內容授權在家庭數位版權系統中。另外，將每回合通訊之認證資訊加入隨機亂數以及時間戳記作運算，使溝通訊息具隨機性且無關連性，達到不可追蹤性與避免重送攻擊。相較於游子德[5]所提的方法，如表 4 所示，本研究 CUHO 增加了跨平台、不可追蹤性、防止固定 ID 身分暴露、短期授權憑證及抵禦重送攻擊等特點，有效提高家庭數位版權系統認證的安全性。

參考文獻

[1] 李南逸、陳芸仙，《適用於家庭網路之數位版權管理系統》，碩士論文，南台科技大學資訊管理系，2010。

[2] 林漢鴻 ，全球商業經營管理學報，全球商業經營管理學報 數位家庭之設計標準及發展趨勢，第四期 101.09 page 109-117，2012。

[3] 張釋心，《植基於智慧卡之企業矩陣型組織的數位版權管理系統》，碩士論文，淡江大學，2011 。

[4] 張老師的 Blog！網址： http://blog.lishin.tcc.edu.tw/plog/post/11/1396，數位家庭產業分析，二月 20, 2009, 上網日期： 2012/11/25。

[5] 游子德，《應用於數位家庭架構之數位版權管理系統》，碩士論文，佛光大學資訊學系，2008。

[6] 楊佳泰，《以 XrML 為基礎之多媒體數位版權管理機制之研究》，碩士論文，國立中正大學資訊工程研究所，2005。

[7] 陳欣郁，《產業供應鏈下具不可追蹤及雙向鑑別之 RFID 認證之研究》，碩士論文，淡江大學，2012。

[8] 陳昭珍，網址：http://datf.iis.sinica.edu.tw/Announcement/04DRM/1.pdf，數位出版的商業模式與版權管理，上網日期： 2012/11/31。

[9] 戴智斌， Music Online PPT 2005，上網日期：2012/11/31.

[10] APPLE，網址：http://www.apple.com/tw/, 上網日期：2012/10/31.

[11] KKBOX，網址：http://tw.kkbox.com/index.html, 上網日期： 2012/10/31.

[12] Kalman, G. ,Right Management Infrastructure for Home Content,Mobile and Wireless Communications Summit, 16th IST,IEEE,P1-5 July 2007.

[13] Popescu, B.C., Crispo, B., Tanenbaum, A.S and Kamperman , F. L. A. J., A DRM Security Architecture for Home Networks, The 4th ACM Workshop On Digital Rights Management. ,2004.

[14] XrML Elements 網址：http://msdn.microsoft.com/zh-tw/library/cc542560(v=VS.85).aspx , 10/26/2012，上網日期：2013/1/2.

[15] Zhang, Zhiyong, Huang, Tao, Niu, Danmei ,and Zhang, Lili ,Usage Control Model for Digital Rights Management in Digital Home Networks ,JOURNAL OF MULTIMEDIA, VOL. 6, NO. 4, AUGUST 2011.