私立東海大學資訊工程與科學研究所

# 碩士論文

指導教授：林 祝 興　博士、周 志 賢　博士

(Dr. Chu-Hsing Lin、Dr. Jue-Sam Chou)

# 階層式金鑰管理方法之設計與應用

# Design and Applications of Hierarchical Key Management Schemes



研究生：李　定　穎　撰

(Ting-Ying Lee)

中　華　民　國　九　十　三　年　六　月

# 摘　　要

**在本篇論文中，我們針對階層式金鑰管理架構作深入的研究與探討，如 Lin 在 1997 年所提出的離散對數階層金鑰架構，以及稍後一些學者所提出的建議以及改進的方法等，並將之配合智慧卡運用於隨選視訊上，實現內容保護、影片分級與使用者管理等機制。**

**但因為智慧卡是屬於低運算能力的設備，因此隨選視訊系統中的運算量必須相當低才行，所以我們也提出以二次剩餘理論為基礎的階層式金鑰架構，其主要的運算只需做一次模數乘法，因此成功地降低智慧卡所需的運算量。**

**關鍵字：階層式金鑰管理、二次剩餘、智慧卡、隨選視訊、內容保護、影片分級、使用者管理。**

# Abstract

In this thesis, we do deep research and discussion to the hierarchical key management structure including of Lin' s discrete logarithm method proposed in 1997 and a lot of scholar's suggestion and improved methods. We also apply it and smart card cooperatively on video on demand (VOD) system to carry out content protection, video classification and user management mechanisms.

But because the smart card is the equipment of low computational ability, the operation amount in the VOD system must be quite low. So, we also propose a hierarchical key management method based on quadratic residues theorem. The main operation amount of this method is just a modular multiplication. Therefore, we reduce the operation amount that smart card need to deal with successfully.

**Keywords:** hierarchical key management, quadratic residues, smart card, video on demand, content protection, video classification, user management.

# 目　　錄

# 圖表目錄

# 第一章 序論

## 第一節 研究背景

隨著數位時代的來臨，對於人類的生活產生很大的改變，其中網際網路扮演著很重要的角色，尤其網路上提供的各種服務正迅速與日常生活結合，使得許多生活上的事務如購物、洽公、休閑娛樂等皆可透過網際網路完成。而未來上網媒介將不會侷限於電腦，各種家電也可做為上網的工具，如每家必備的電視機只要透過 set-top box 將類比與數位訊號做轉換即可上網，業者可以提供多元化的服務，如隨選視訊系統，用戶可購買自己喜愛的頻道或節目，不必受限於業者的安排，購買過多不喜歡的頻道。

然而一旦節目數位化後，許多目前網際網路所存在的安全問題將也將隨之產生。如何保護影片內容不被非法的用戶所截取、如何驗證用戶身份與如何實現影片分級等，將是重要的課題。有鑑於此，本篇論文的研究重心是設計出一個安全合適的隨選視訊架構。而在強調安全性的同時，降低運算成本也是我們的研究重點。

在本研究中我們將利用密碼學相關技術實現隨選視訊內容的保護；為了提供個人化的隨選視訊服務，用戶的身份驗證將是重要的機制，一般認為智慧卡能抵擋個人資料遭篡改或竊取，且可執行簡單的

運算，因此在我們的架構中將使用智慧卡作為個人資訊的儲存體，提供用戶身份驗證。另外在本篇論文中也將針對階層式金鑰管理機制作深入的研究與探討，利用此機制實現影片分級。

## 第二節　論文架構

本篇論文中第一章為序論，第二章介紹在本篇論文中所用到的相關密碼學技術，第三章我們針對相關的研究作介紹，其內容為 Lin [1][4] 所提出的兩個階層式金鑰架構，包括離散對數與橢圓曲線密碼學方法，以及 Lee [2] 針對離散對數方法所提出的兩個攻擊，另外還有 Cho [3] 針對這兩個攻擊所提出的修補方法，以及 Wu [5] 所提出的提升效能的方法，最後我們也將介紹二次剩餘理論。第四章則介紹我們運用階層式金鑰架構所提出的隨選視訊系統架構。第五章中我們詳細介紹我們所提出的階層式金鑰架構新方法。第六章則討論我們所提出的方法的安全性與效能等問題。第七章針對我們所提出的方法提出總結以及導出未來的研究方向。

# 第二章 相關密碼學理論介紹

本章將介紹本論文所用到的密碼學理論，包括單向雜湊函式、RSA、AES 與二次剩餘理論等。

## 第一節 單向雜湊函式

單向雜湊函式（one-way hash function）是密碼學重要的技術，它是一種可以將任意長度的輸入值壓縮成固定長度之輸出值（摘要，Digest）的數學函數或演算法，且若兩個輸入值間只相差些許位元，其輸出值卻會是很大的差距，目前存在的單向雜湊函式演算法有 MD5、SHA-1 [11],…等，由於此演算法為單向的，因此攻擊者或要從輸出值反推得到輸入值在計算上是不可能的, 因此在密碼學中常被拿來當作資訊保護以及防止資料被竄改的技術。

## 第二節 RSA 公開金鑰密碼系統

RSA [19] 公開金鑰密碼系統是在 1978 年由美國麻省理工學院三位教授 Rivest、Shamir 及 Adleman 首先提出一種基於因數分解困難度為基礎的一套公開金鑰密碼系統，可用於加密或簽章，以下我們將介紹產生金鑰對以及、加密與簽章各別之步驟：

### 一、 產生金鑰對

(1) 假設有兩個人 $A$ 與 $B$，其中 $A$ 隨機產生兩個大質數 $p$ 與 $q$。

(2) $A$ 計算 $n = pq$。

(3) $A$ 隨機找出一個滿足 $\gcd(e, f(n)) = 1$ 之整數 $e$，在此 $f(n)$ 為尤拉商數，表示比 $n$ 小且和 $n$ 互質之整數個數，當 $n = pq$ 時，$f(n)$ 之值為 $(p-1)(q-1)$，其中 $(e,n)$ 為公開金鑰。

(4) $A$ 計算私密金鑰 $d$，$d$ 滿足 $ed \equiv 1 (\mathrm{mod}\, f(n))$。

## 二、 加密

金鑰對產生後，$A$ 將公開金鑰 $(e,n)$ 傳送給 $B$，而 $A$ 保有私密金鑰 $d$，則 $B$ 可以利用 $A$ 的公開金鑰 $(e,n)$ 執行加密的動作 $E_e(m) = C = m^e \bmod n$ 將明文 $m$ 加密後傳給 $A$，則 $A$ 利用私密金鑰 $d$ 做解密的動作 $D_d(m) = C^d = (m^e)^d \bmod n = m$

## 三、 簽章

若 $A$ 用自己的秘密金鑰執行 $D_d(m) = S = m^d \bmod n$ 運算則稱為簽章，$B$ 得到 $A$ 所簽署的文件 $S$ 與明文 $m$ 後可以計算 $E_e(S) = S^e = (m^d)^e \bmod n$，若 $m = E_e(S)$ 則代表簽章驗證成功，反之則驗證失敗。

# 第三節 AES 對稱式加密系統

自 1970 年代中期美國公佈 DES 加密法後，DES 開始在全世界蓬勃發展，經過了二、三十年的使用，DES 開始慢慢走向盡頭。因此美國開始對外徵求新一代的加密標準，AES（Advanced Encryption Standard）[12] 於是誕生，經過十幾個演算法的篩選，最後選用 Rijndael 為其演算法，而 Rijndael 之數學理論是基於體 $GF(2^n)$，採用反覆運算來對資料進行加密，其特色為資料長度區塊與金鑰長度是可以變動的。

## 第四節　二次剩餘理論

我們選擇二次剩餘理論作為我們方法的基礎，所以在這個小節我們將簡單的介紹二次剩餘理論 [8] 以及其優點。

假如 $n = pq$，其中 $p$ 與 $q$ 皆為大質數，且 $x^2 \equiv a(\mathrm{mod}\, n)$ 有解，則稱 $a$ 是一個 $\mathrm{mod}\, n$ 的二次剩餘。$QR_n$ 代表所有屬於 $a \bmod n$ 的整數集合；在這個理論即使知道 $a$ 和 $n$，在不知 $p$ 和 $q$ 情況下很難解出 $x$，它的難題是建立在因數分解 $n$ 上[20]，這個難題被稱為二次剩餘問題 (Quadratic Residue Problem)，而相反的只需要一次的乘法運算與一次模數運算便可得到 $QR_n$，因此我們將它運用在我們的方法中，將它視為一個單向函式。

# 第三章 相關階層式金鑰架構研究

本章節中我們將詳細介紹各種階層式金鑰架構，包括 Lin 的離散對數與橢圓曲線密碼學方法、Lee 的攻擊方法、Cho 的修補方法與 Wu 橢圓曲線密碼學改良等方法等，首先我們將先定義稍後章節中所用到的符號：

## 第一節 符號定義

以下所定義之符號，為本文中所用到的符號。

$S$ ：所有群組所形成的集合。

$S_i$ ：集合 $S$ 中的元素，也就是代表每個群組，其中 $1 \le i \le n$。

$ID_l$ ：群組 $S_i$ 的識別碼。

$k_j$ ：群組 $S_i$ 所擁有的群組金鑰。

$r_{ji}$ ：群組 $S_i$ 與群組 $S_j$ 間的關係參數，其中 $i \neq j$。

$x \| y$ ：字串 $x$ 串接字串 $y$。

CA ：一個受信任的角色，負責產生及維護所需的參數。

$E_{key}(X)$ ：以金鑰 $key$ 將資料 $X$ 做加密。

$D_{key}(X)$ ：以金鑰 $key$ 將資料 $X$ 做解密。

$h(X)$ ：代表輸入為 $X$ 的單向雜湊函式值，如 SHA-1。

$EC$ ：代表橢圓曲線。

$X(p_i)$：代表執行$x_i \oplus y_i$運算，其中 $p_i = (x_i, y_i)$ 是一個在橢圓曲線 $EC(Z_p)$ 上的一個點。

## 第二節　階層式金鑰架構

在階層式金鑰架構中如圖 2.2.1 所示，存在 $n$ 個群組的一個集合 $S$，$S = \{S_1, S_2, ..., S_n\}$，每個群組 $S_i$ 皆各自擁有一把群組金鑰 $k_i$，而群組與群組間又存在著"$\succ$"的權限關係；若 $S_j \succ S_i,\ i \neq j$ 則表示群組 $S_j$ 的權限大於群組 $S_i$，並代表 $S_j$ 可以利用本身的金鑰 $k_j$ 產生 $S_i$ 的金鑰 $k_i$，但反過來則不可行。遵循著這個概念先前已經有相當多學者提出各種不同的方法，其基本架構皆包括產生群組金鑰、導出群組金鑰與更新群組金鑰三個階段，至於詳細流程我們將在往後幾節一一做介紹。

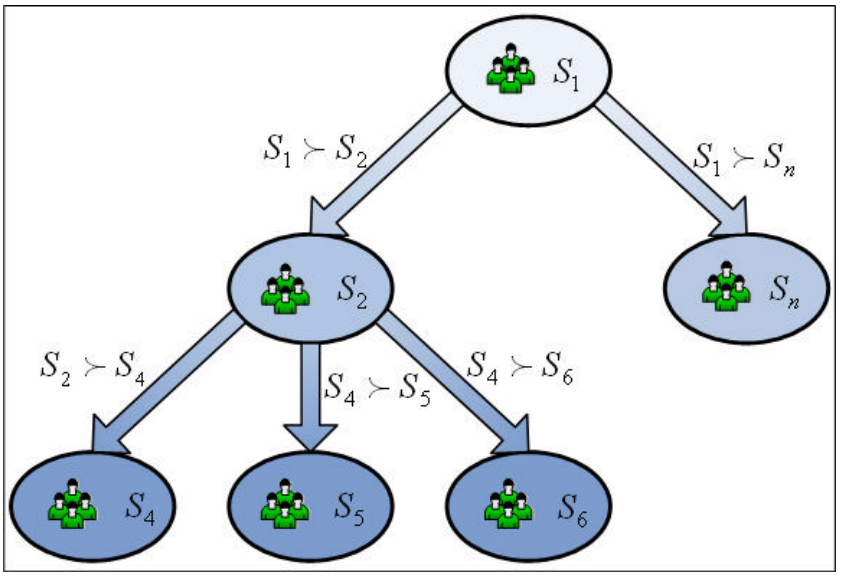


圖 2.1.1、階層式金鑰架構

## 第三節　Lin 的離散對數方法

Lin 在 1997 年提出了一個以離散對數問題為基礎的動態金鑰管理架構，而其架構中也使用 RSA 作為資料保密的演算法，此架構的三個階段說明如下：

**(1)產生群組金鑰階段：**

**步驟一：**CA 隨機選擇一個大質數 $P$，以及原根 $Z \in GF(P)$ 這兩個參數可以被公開，接著 CA 依照 RSA 密碼系統選擇一把私密金鑰 $SK$ 與其對應的公開金鑰 $PK$，並將公開金鑰公佈給所有群組。

**步驟二：**每一個群組 $S_i$ 選擇一把群組金鑰 $k_i$，並用 $PK$ 加密然後將 $E_{PK}(k_i)$ 傳送給 CA。

**步驟三：**CA 利用私密金鑰 $SK$ 解開 $k_i$, $k_i = D_{SK}(E_{PK}(k_i))$，並根據每個群組的關係計算關係參數 $r_{ji}$，例如 $S_j \succ S_i$ 則執行如方程式 (1.2.1) 的計算，其中 $ID_i$ 為群組 $S_i$ 的識別碼。

$$r_{ji} = (Z^{k_j \oplus ID_i} \bmod p) \oplus k_i \qquad (1.2.1)$$

**(2)導出群組金鑰階段：**

若有兩個群組有 $S_j \succ S_i$ 這樣的關係, 則 $S_j$ 可以利用自己的群組金鑰 $k_j$ 和以下的方程式導出 $k_i$。

$$k_i = (Z^{k_j \oplus ID_i} \bmod p) \oplus r_{ji} \qquad (1.2.2)$$

**群組** $S_j$ **必須執行以下三個步驟：**

**步驟一：群組** $S_j$ **向** CA **請求關係參數** $r_{ji}$**。**

**步驟二：**CA **確認是否這是一個合法的請求，若為合法則** CA **將關係參數** $r_{ji}$ **傳送給群組** $S_j$**。**

**步驟三：群組** $S_j$ **執行如方程式** (1.2.2) **的計算，即可獲得群組** $S_i$ **的群組金鑰** $k_i$**。**

**(3)更新群組金鑰階段：**

**步驟一：群組** $S_i$ **選擇一把新的群組金鑰** $k_i^*$ **並將它加密成** $E_{PK}(k_i^*)$ **後傳送給** CA**。**

**步驟二：**CA **將先解開**$k_i^*,\ k_i^* = D_{SK}(E_{PK}(k_i^*))$**，然後計算所有必須更新的關係參數** $r_{ji}^*$**，如方程式** (1.2.3) **所示。**

$$r_{ji}^* = (Z^{k_j \oplus ID_i} \bmod p) \oplus k_i^* \qquad (1.2.3)$$

## 第四節　Lee 提出的兩個攻擊

Lee **在** 1999 **年針對** Lin **的離散對數階層式金鑰管理架構, 提出了兩種情況的攻擊，以下是我們的說明：**

**攻擊一：當群組修改群組金鑰後，若攻擊者能拿到舊的群組金鑰時。**

**假設群組 $S_i$ 將本身的群組金鑰 $k_i$ 更新成 $k_i^*$ 後，如果攻擊者可以獲得舊的群組金鑰 $k_i$，那麼攻擊者可以執行以下兩個步驟而獲得新的群組金鑰 $k_i^*$：**

**步驟一：計算 $r_{ji} \oplus k_i$ 獲得 $Z^{k_j \oplus ID_i} \bmod p$。**

**步驟二：為了獲得群組 $S_i$ 的新群組金鑰 $k_i^*$，攻擊者可以計算 $(Z^{k_j \oplus ID_i} \bmod p) \oplus r_{ji}^*$，其中新的關係參數 $r_{ji}^*$ 為 $(Z^{k_j \oplus ID_i} \bmod p) \oplus k_i^*$。**

**此攻擊可成功的原因是，$Z^{k_j \oplus ID_i} \bmod p$ 這個值在群組更新群組金鑰時完全不會被改變，所以攻擊者可以執行如上述步驟一的運算獲得 $Z^{k_j \oplus ID_i} \bmod p$，接著他可以向 CA 要求關係參數 $r_{ji}^* (= (Z^{k_j \oplus ID_i} \bmod p) \oplus k_i^*)$，並藉著運算 $(Z^{k_j \oplus ID_i} \bmod p) \oplus r_{ji}^*$ 獲得新的群組金鑰 $k_i^*$。**

**攻擊二：當群組間的識別碼 $ID$ 只相差些許位元**

**假設群組 $S_i$ 的識別碼 $ID_i$ 和 $S_l$ 的識別碼 $ID_l$ 只相差些許位元，且 $S_i$ 與 $S_l$ 有著同樣的父節點群組 $S_j$，則 $S_i$ 可以藉由比較 $ID_i$ 與 $ID_l$ 獲得 $(Z^{k_j \oplus ID_l} \bmod p)$。所以 $S_i$ 可以藉由計算 $(Z^{k_j \oplus ID_l} \bmod p) \oplus r_{jl}$ 來破解 $k_l$。**

## 第五節　Cho 的改善方法

**因為 Lee 針對 Lin 的方法提出了兩個弱點，因此 Cho 在 2001 針**

對這個兩個弱點提出了修補方法，其方法與 Lin 的方法相比多了一個參數 $SG$，其產生方式如方程式 (1.4.1) 所示，而其產生關係參數的方法如方程式 (1.4.2) 所示，其中 $SG^{-1}$ 為參數 $SG$ 以 $P$ 為模數的乘法反元素。

$$SG = h(k_j + ID_i) \cdot k_j \bmod f(P) \ , \ f(P) = P - 1 \tag{1.4.1}$$

$$r_{ji} = (Z^{SG} \bmod P) \oplus (k_i \cdot SG^{-1} \bmod P) \tag{1.4.2}$$

Cho 所提出的方法中，雖然 $Z^{SG} \bmod P$ 這個值，在每次群組更新金鑰時也不會改變，但是方程式 (1.4.2) 中 $k_i$ 必須與 $SG^{-1}$ 相乘，所以雖然 $Z^{SG} \bmod P$ 不變，但攻擊者並無從得知參數 $SG$ 的值，當然更無法得知其乘法反元素 $SG^{-1}$，因此若群組 $S_i$ 將群組金鑰更新成 $k_i^*$，攻擊者必須先面臨找出 $SG$ 的問題，所以 Lee 所提出的第一個弱點將不存在。

此方法在產生 $SG$ 的過程中群組的識別碼 $ID_i$ 須與群組金鑰 $k_j$ 相加後做一次單向雜湊函數的運算。由單向雜湊函式特性得知，若單向雜湊函式 $y = h(x)$ 所輸入的兩個值 $x_i$ 與 $x_l$ 差距很小時，其所得到的結果 $y_i$ 與 $y_l$ 的差距卻是相當大，因此可以解決 Lee 所提出比較 $ID_i$ 獲得 $(Z^{k_j \oplus ID_l} \bmod p)$ 進而破解群組金鑰的弱點。

## 第六節　Lin 的橢圓曲線方法

Cho 解決了先前 Lee 所提出的兩個弱點，但其方法多了產生參數 $SG$ 所需的計算，以及尋找參數 $SG$ 的反元素 $SG^{-1}$ 所須花費的時間，因此 Cho 所提出的方法在效能上依舊不理想，因此本節中我們將介紹 Lin 在 2002 年所提出的橢圓曲線密碼學方法。其與先前介紹的方法相同，一樣有三個階段，以下就是這三個階段的說明：

**(1)產生群組金鑰階段：**

**步驟一：**CA 在 $Z_p$ 的範圍中選擇一個橢圓曲線 $EC$，並且產生一個原生點 $G \in EC(Z_p)$，之後找出一個大質數 $q$ 滿足 $q \times G = O$，其中 $O$ 為原點。

**步驟二：**CA 選擇一把私密金鑰 $K$ 並計算其對應的公開金鑰 $P$，$P = K \times G$ 並將 $P$ 與 $q$ 公開出去。

**步驟三：**每一個群組 $S_i$ 選擇一個隨機變數當作本身的群組金鑰 $k_i \in [1, q-1]$，之後計算相對應的公開金鑰 $p_i = k_i \times G = (x_i, y_i)$。

**步驟四：**每個群組各自將自己選擇的金鑰對利用 CA 的公開金鑰 $P$ 加密，然後將 $E_P(k_i)$ 傳送給 CA。

**步驟五：**CA 利用私密金鑰 $K$ 解開 $k_i,\ k_i = D_K(E_P(k_i))$，最後 CA 根據每個群組的關係計算關係參數 $r_{ji}$，例如 $S_j \succ S_i$ 則利用方程式(1.5.1) 計算 $r_{ji}$。

$$r_{ji} = \mathrm{X}((k_j \oplus h(x_i \| y_i)) \times G) \oplus k_i \qquad (1.5.1)$$

**(2)導出群組金鑰階段：**

**若有兩個群組有** $S_j \succ S_i$ **這樣的關係, 則** $S_j$ **可以用自己的金鑰** $k_j$ **以及向** CA **要求的** $p_i$ **與** $r_{ji}$ **用以下的方程式計算產生** $k_i$**。**

$$k_i = \mathrm{X}((k_j \oplus h(x_i \| y_i)) \times G) \oplus r_{ji} \qquad (1.5.2)$$

**(3)更新群組金鑰階段：**

**因為安全的考量，假如群組** $S_i$ **希望更新本身的群組金鑰** $k_i$ **時，** $S_i$ **可以再選擇一把新的金鑰** $k_i^* \in [1, q-1]$ **然後利用** $P$ **加密成** $E_P(k_i^*)$ **後傳送給** CA**。**CA **先解開** $k_i^*,\ k_i^* = D_K(E_P(k_i^*))$**，然後重新計算關係參數** $r_{ji}^*$**，即完成群組** $S_i$ **的群組金鑰更新，如方程式** (1.5.3) **所示。**

$$r_{ji}^* = \mathrm{X}((k_j \oplus h(x_i^* \| y_i^*)) \times G) \oplus k_i^* \qquad (1.5.3)$$

## 第七節　Wu 的橢圓曲線方法

**在** Lin **提出橢圓曲線的方法後，**Wu **認為其運算量依然還有減少的空間，因此** Wu **在** 2003 **年也提出了以橢圓曲線密碼學的方法，但是他將** Lin **的方法做了些微修改。以下是** Wu **的方法：**

**(1)產生群組金鑰階段：**

**步驟一：與** Lin **的方法一樣，**CA **在** $Z_p$ **的範圍中選擇一個橢圓曲線** $EC$**，但是與** Lin **的方法不同的是，**CA **必須針對每個群組** $S_i$ **選擇一個原生點** $G_i$**。**

**步驟二：**CA **選擇一把私密金鑰** $K$ **並計算其對應的公開金鑰** $P$**，** $P = K \times G$ **並將** $P$ **公開。**

**步驟三：每一個群組** $S_i$ **選擇一把群組金鑰** $k_i$**，並用** $P$ **加密然後將** $E_P(k_i)$ **傳送給** CA**。**

**步驟四：**CA **利用私密金鑰** $K$ **解開** $k_i,\ k_i = D_K(E_P(k_i))$**，並根據每個群組的關係計算關係參數** $r_{ji}$**，例如** $S_j \succ S_i$ **則進行如方程式**(1.6.1) **的計算。**

$$r_{ji} = \mathrm{X}(k_j \times G_i) \oplus k_i \tag{1.6.1}$$

**(2)產生群組金鑰階段：**

**若有兩個群組有** $S_j \succ S_i$ **這樣的關係, 則** $S_j$ **可以利用用自己的群組金鑰** $k_j$ **以及向** CA **要求的** $r_{ji}$ **執行以下的方程式運算產生** $k_i$**。**

$$k_i = \mathrm{X}(k_j \times G_i) \oplus r_{ji} \tag{1.6.2}$$

**(3)產生群組金鑰階段：**

**群組** $S_i$ **重新選擇一把群組金鑰** $k_i^*$ **並將它加密成** $E_P(k_i^*)$ **後傳送給** CA**。**CA **先解開** $k_i^*, k_i^* = D_K(E_P(k_i^*))$**，然後為** $S_i$ **選擇**

一個新的原生點 $G_i^*$ 並重新計算新的關係參數 $r_{ji}^*$，如方程式 (1.6.3) 所示。

$$r_{ji}^* = \mathrm{X}(k_j \times G_i^*) \oplus k_i^* \tag{1.6.3}$$

# 第四章 隨選視訊應用

我們將第三章所介紹的以橢圓曲線密碼學為基礎的階層式金鑰管理架構配合智慧卡，提出了隨選視訊的應用，並利用此金鑰架構的特性，實現影片分級、內容保護等機制，以下我們將詳細介紹我們的隨選視訊系統。

## 第一節 系統架構

### 一、 系統架構簡介

在我們的系統中，首先我們將影片依照 Saskatchewan [21] 的影片分級法分為六個層級如圖 3.1.1 所示，稱為層級類別，這六個層級類別分別為：

1. 成人類別（A，Adult）。
2. 限制級類別（R，Restricted）。
3. 18 歲或 18 歲以上或 18 歲以下可由父母陪同觀賞（18A）。
4. 14 歲或 14 歲以上或 14 歲以下可由父母陪同觀賞（14A）。
5. 父母陪同觀賞的類別（PG，Parental Guidance）。
6. 普遍級（G，General）。

除了以上依照觀賞者年齡所做的影片層級分類外，我們也將影片

依照其內容分為數個類別如圖 3.1.1 所示，稱為內容類別，包括動作電影、愛情電影、綜藝節目、教育性節目等。當然系統業者可以隨時依需要加入或移除某些影片類別，且每一種影片種類並不一定要涵蓋上述六個影片層級，例如圖 3.1.1 中，教育性節目所涵蓋最高的影片層級為 14A 而不是成人類別，而每個影片群組 $V_{ij}$ $(1 \le i \le 6、1 \le j \le n)$ 皆必須屬於一個層級類別與一個內容類別，如 $V_{42}$ 影片群組屬於 14A 層級類別與愛情電影內容類別。

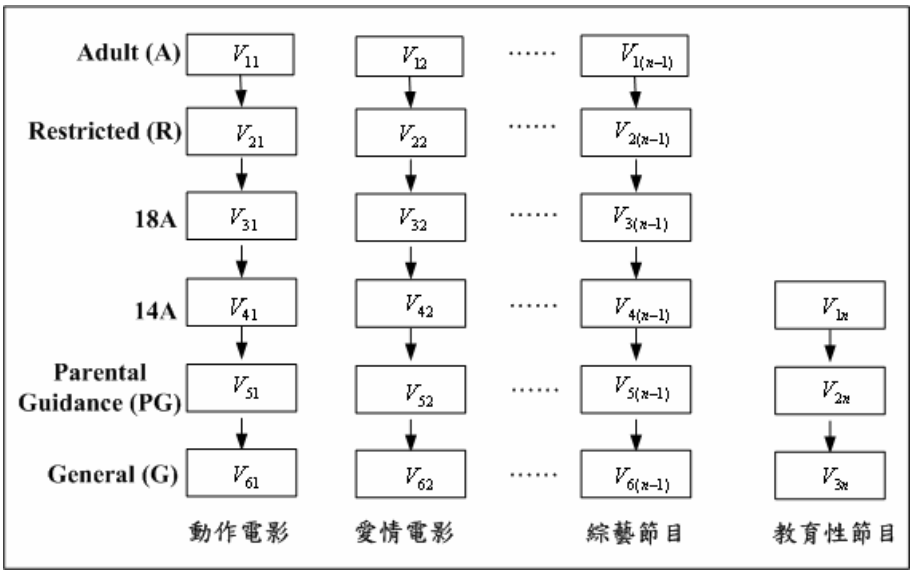


圖 3.1.1、隨選視訊系統影片群組分類

## 二、 系統建立

在隨選視訊系統建立之前，系統管理者必須選擇或產生一些系統運作所需的參數，並在客戶選擇完欲購買的影片類別後，負責將這些參數存入智慧卡中交給客戶。這個階段的流程與金鑰管理架構的群組

金鑰產生階段流程很類似，但為了符合我們的隨選視訊系統，所以必須做些許的改變，例如在系統第一次執行時，所有影片群組的金鑰必須由系統管理者選定，以下是我們針對系統建立階段的說明：

**步驟一：**管理者在 $Z_p$ 的範圍中選擇一個橢圓曲線 $EC$，並選擇一個原生點 $G \in EC(Z_p)$，之後尋找一個大質數 $q$ 滿足方程式 $q \times G = O$，其中 $O$ 為原點。

**步驟二：**管理者為每個影片群組產生一把秘密金鑰 $k_{V_{ij}} \in [1, q-1]$ $(1 \le i \le 6$、$1 \le j \le n)$，接著利用方程式 (3.1.1) 算出其對應的公開金鑰 $p_{V_{ij}}$。

$$p_{V_{ij}} = k_{V_{ij}} \times G \tag{3.1.1}$$

**步驟三：**根據每個 $V_{lj} \succ V_{ij}$ $(l = i+1)$ 的影片群組關係，管理者利用方程式 (3.1.2) 計算其關係參數 $r_{V_{lj}V_{ij}}$。

$$r_{V_{lj}V_{ij}} = X((k_{V_{lj}} \oplus h(x_{Vij} || y_{Vij})) \times G) \oplus k_{V_{ij}} \tag{3.1.2}$$

## 三、 使用者選擇影片群組

**步驟一：**使用者 $U$ 選擇其欲購買的影片群組。

**步驟二：**管理者根據每個使用者選擇一把金鑰 $SK_U$，這把金鑰為秘密金鑰。

**步驟三：**根據使用者購買的影片群組，系統管理者利用秘密金鑰

$SK_U$ 加密所有相關的關係參數 $r_{V_{lj}V_{ij}}$。我們以符號 $E_{SK_U}(r_{V_{lj}V_{ij}})$ 表示利用對稱式加密演算法如 AES [12] 以及秘密金鑰 $SK_U$ 加密 $r_{ji}$。加密之後，管理者將 $E_{SK_U}(r_{V_{lj}V_{ij}})$ 分成兩半，第一半以 $E_{SK_U}(r_{V_{lj}V_{ij}})\_1$ 表示，第二半以 $E_{SK_U}(r_{V_{lj}V_{ij}})\_2$ 表示。

**步驟四：**系統管理者將所有加密過後的第二半關係參數值 $E_{SK_U}(r_{V_{lj}V_{ij}})\_2$（$i \le l \le 6$）存入智慧卡中，而第一半 $E_{SK_U}(r_{V_{lj}V_{ij}})\_1$ 則由管理者保存。

**步驟五：**根據系統建立階段之步驟四所提的方法計算使用者的私密金鑰 $SK_u$ 與 $V_{ij}$（使用者選擇購買的影片類別中，位於最高的類別，如圖 3.2.1 所示。）之影片群組金鑰 $k_{V_{ij}}$ 的關係參數 $r_{UV_{ij}}$。接下來，管理者利用私密金鑰 $SK_U$ 將 $r_{UV_{ij}}$ 加密，一樣將 $E_{SK_U}(r_{UV_{ij}})$ 分成兩半，將第二半 $E_{SK_U}(r_{UV_{ij}})\_2$ 存入智慧卡中，第一半 $E_{SK_U}(r_{UV_{ij}})\_1$ 由管理者保存。

**步驟六：**管理者為每張智慧卡產生一組 $PINCODE_U$。$PINCODE_U$ 是一組存取智慧卡的密碼，使用者在觀看影片前須先鍵入正確的 $PINCODE_U$ 才可以存取秘密金鑰 $SK_U$。

## 四、 使用者如何觀看影片

在 $V_{lj} \succ V_{ij}$ 這樣的關係限制中，假如使用者想要觀賞類別 $V_{ij}$ 的影片時，那麼他必須使用類別 $V_{lj}$ 的類別金鑰 $k_{V_{lj}}$ 解出類別 $V_{ij}$ 的類別金鑰 $k_{V_{ij}}$，他必須執行如下的步驟。

**步驟一：**使用者將智慧卡插入 set-top box 中的讀卡機中，然後輸入他的 $PINCODE_U$，以確保它是合法的使用者，接著選擇他希望觀賞的影片類別。

**步驟二：**在 set-top box 中的終端程式自動與管理者連繫，並且決定任何參數是否需要更新，這些參數包含關係參數與金鑰等。假如需要更新，則 set-top box 的終端程式將自動將所接收到的資料放入智慧卡中取代舊有的資料。（這部份我們將於更換金鑰階段做詳細討論。）

**步驟三：**終端程式將幫助使用者向管理者要求影片群組 $V_{ij}$ 的群組金鑰 $p_{Vij}$，以及第一半的加密關係參數值 $E_{SK_U}(r_{UV_{ij}})\_1$，之後終端程式把這些參數都傳給智慧卡。

**步驟四：**智慧卡首先將兩半經過加密的關係參數 $E_{SK_U}(r_{UV_{ij}})\_1$ 以及 $E_{SK_U}(r_{UV_{ij}})\_2$ 組合在一起，形成 $E_{SK_U}(r_{UV_{ij}})$。接著智慧卡利用存在智慧卡中的私密金鑰 $SK_U$ 解開 $E_{SK_U}(r_{UV_{ij}})$

獲得 $r_{UV_{ij}}$，然後利用 $p_{V_{ij}}(=(x_{V_{ij}}, y_{V_{ij}}))$、$r_{UV_{ij}}$ 以及他所擁有的私密金鑰 $SK_U$ 計算類別 $V_{lj}$ 的金鑰 $k_{V_{lj}}$ 如下方程式所示。

$$k_{V_{ij}} = X((SK_U \oplus h(x_{V_{ij}} \| y_{V_{ij}})) \times G) \oplus r_{UV_{ij}} \quad (3.1.3)$$

步驟五：重複步驟二到步驟四的動作一層一層解出影片群組金鑰，直到合適的影片群組金鑰 $k_{V_{lj}}$ 被解出為止。

## 五、 使用者如何更換金鑰

為了安全的考量，每一個影片群組或使用者的金鑰經過一段時間必須做更新, 因此若使用者 $U$ 要更換金鑰時, 必須執行以下的動作：

步驟一：管理者首先為使用者 $U$ 產生一把新的金鑰 $SK_U^*$。

步驟二：管理者重新計算所有與類別 $V_{ij}$ 有關的關係參數，並且利用新的私密金鑰 $SK_U^*$ 加密 ，最後把它分為兩半然後先保留這些參數，另外管理者也須將 $SK_U^*$ 利用舊的私密金鑰 $SK_U$ 做加密 $E_{SK_U}(SK_U^*)$。

步驟三：管理者在使用者觀賞影片時，必須先提醒使用者智慧卡中的資料必須更新，由終端程式接收這些新的參數，包括 $E_{SK_U}(SK_U^*)$，首先將新的秘密金鑰 $SK_U^*$ 利用舊的秘密金鑰解出。接著將舊的參數取代掉，此更新參數動作

在觀賞影片階段之步驟二中有提到。

**步驟四：**智慧卡確認舊的參數已經被新的參數所取代，此階段即完成。

若為影片群組類別 $V_{ij}$ 要做群組金鑰更新的動作，則進行以下的步驟：

**步驟一：**管理者首先為使用者 $V_{ij}$ 產生一把新的金鑰 $k_{V_{ij}}{}^{*}$。

**步驟二：**管理者重新計算所有與類別 $V_{ij}$ 有關的關係參數，並且利用使用者的祕密金鑰 $SK_U$ 加密 ，最後把它分為兩半然後先保留這些參數。

**步驟三：**管理者在使用者觀賞影片時，必須先提醒使用者智慧卡中的資料必須更新，由終端程式接收這些新的參數。接著將舊的參數取代掉。

**步驟四：**智慧卡確認舊的參數已經被新的參數所取代，此階段即完成。

## 第二節　範例說明

為了更容易了解，在本節我們將舉一個實際的例子說明我們所提出的隨選視訊架構，如圖 3.2.1 所示，在圖 3.2.1 中使用者 $U$ 選擇購買了三種節目，包含動作電影、愛情電影以及教育性節目，而在各個

種類的節目中使用者 $U$ 所選擇的層級也有所不同如動作電影類 $U$ 是選擇購買 Restricted 層級 $V_{21}$ 以下的影片類別，而愛情電影類部分則是選擇購買 18A 層級 $V_{32}$ 以下的影片類別。

因此管理者必須為使用者 $U$ 再計算其與$V_{21}$、$V_{32}$ 以及 $V_{2n}$ 三個影片類別的關係參數 $r_{UV_{21}}$、$r_{UV_{32}}$ 以及 $r_{UV2n}$，接著利用私密金鑰 $SK_U$ 加密這些關係參數，最後管理者將第二部份加密過後的關係參數 $E_{SK_U}(r_{UV_{21}})\_2$、$E_{SK_U}(r_{UV_{32}})\_2$ 以及 $E_{SK_U}(r_{UV2n})\_2$ 存入智慧卡，然後才發給使用者。

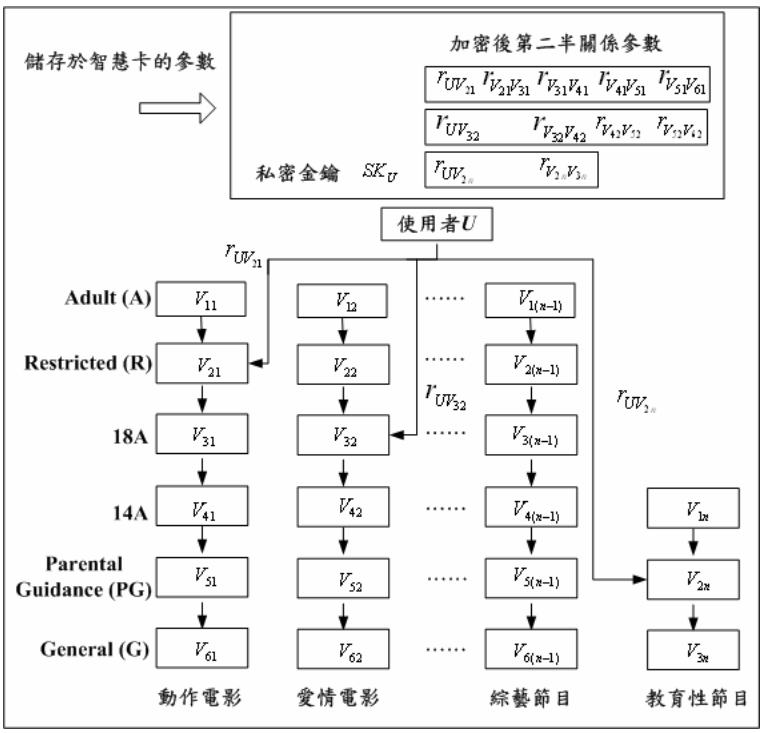


圖 3.2.1、隨選視訊系統使用者影片群組選擇

當使用者想要觀賞的影片是位於類別 $V_{42}$ 中時，他必須進行以下的動作：

**步驟一：使用者** $U$ **將智慧卡插入** set-top box **的讀卡機中，然後輸入他的** $PINCODE_U$ **以驗證他的身分。**

**步驟二:終端程式幫助使用者向管理者要求參數** $p_{V_{32}}$ **與** $p_{V_{42}}$ **以及第一半的加密關係參數** $E_{SK_U}(r_{UV_{32}})\_1$ **與** $E_{SK_U}(r_{V_{32}V_{42}})\_1$**，終端程式收到後將這些參數送到智慧卡中。**

**步驟三：智慧卡將** $E_{SK_U}(r_{UV_{32}})\_1$ **與** $E_{SK_U}(r_{UV_{32}})\_2$ **結合起來形成** $E_{SK_U}(r_{UV_{32}})$**，將** $E_{SK_U}(r_{V_{32}V_{42}})\_1$ **與** $E_{SK_U}(r_{V_{32}V_{42}})\_2$ **結合起來形成** $E_{SK_U}(r_{V_{32}V_{42}})$**，然後智慧卡利用已經存在智慧卡中的私密金鑰** $SK_U$ **解開** $E_{SK_U}(r_{UV_{32}})$ **與** $E_{SK_U}(r_{V_{32}V_{42}})$ **獲得** $r_{UV_{32}}$ **與** $r_{V_{32}V_{42}}$**。**

**步驟四:智慧卡利用參數** $p_{V_{32}}(=(x_{V_{32}}, y_{V_{32}}))$**、** $p_{V_{42}}(=(x_{V_{42}}, y_{V_{42}}))$**、** $r_{V_{32}V_{42}}$ **與** $k_u$ **計算** $k_{V_{32}}$ **與** $k_{V_{42}}$**，其計算方式如下方程式所示。**

$$k_{V_{32}} = X((SK_U \oplus h(x_{V_{32}} || y_{V_{32}})) \times G) \oplus r_{UV_{32}} \tag{3.2.1}$$

$$k_{V_{42}} = X((k_{V_{32}} \oplus h(x_{V_{42}} | y_{V_{42}})) \times G) \oplus r_{V_{32}V_{42}} \tag{3.2.2}$$

**步驟五：**set-top box **利用** $k_{V_{42}}$ **解開被加密的影片，使用者** $U$ **就可以觀賞影片了。**

**在以上的例子中，我們假設使用者** $U$ **是一個成年人。但在另一個情況中假如使用者是一個未滿** 14 **歲的小孩，那麼父母則可為他選擇合適的影片層級，換句話說他只能利用他的智慧卡觀賞** Parental

Guidance **層級以下的影片，因此我們可以利用金鑰管理架構，實現影片分級的機制。**

# 第五章 以二次剩餘理論為基礎之階層式金鑰管理方法

為了提高隨選視訊系統的效能，我們將降低智慧卡的運算負擔，因此這個章節中我們將說明我們如何利用二次剩餘理論降低階層式金鑰架構的運算量，同時我們的方法也是目前為止所提出的各種方法中效能最好的。與先前 Lin 所提出的方法一樣，本法亦有三個階段如下所示：

## 第一節 方法介紹

**(1) 產生群組金鑰：**

**初始步驟：本步驟只出現在系統第一次建立的時候，當系統建立完成後，則不需再進行此步驟，其包含以下兩個動作：**

**1.** CA **產生一把金鑰** $SK$ **然後透過安全通道傳給所有的群組** $S_i$。CA **選擇兩個大質數** $p$ **和** $q$ **分別滿足** $(p+1)|4$ **和** $(q+1)|4$，**並且計算** $n = pq$。

**2.** CA **計算所有的** $QR_p$ **和** $QR_q$，**然後利用** $SK$ **將** $QR_p$ **和** $QR_q$ **加密。最後** CA **將** $E_{SK}(QR_p, QR_q)$ **傳送給所有的群組。**

**步驟一：每一個群組解開收到的資料** $E_{SK}(QR_p, QR_q)$ **並且從中選**

擇一數當成一把群組金鑰 $k_i \in QR_p \cap QR_q$。

**步驟二：**然後將群組金鑰加密並傳送 $E_{SK}(k_i)$ 給 CA。

**步驟三：**CA 解開收到的訊息 $E_{SK}(k_i)$ 可以獲得 $k_i$，之後 CA 利用方程式 (4.1.1) 計算 $QR_n$，也就是 $a_i$。

$$a_i = k_i^2 \bmod n \tag{4.1.1}$$

**步驟四：**對所有 $S_j \succ S_i$ 的群組，CA 利用方程式 (4.1.2) 計算他們的關係參數 $r_{ji}$。

$$r_{ji} = h(k_j \oplus a_i) \oplus k_i \tag{4.1.2}$$

以上步驟如下圖 4.1.1 所示。

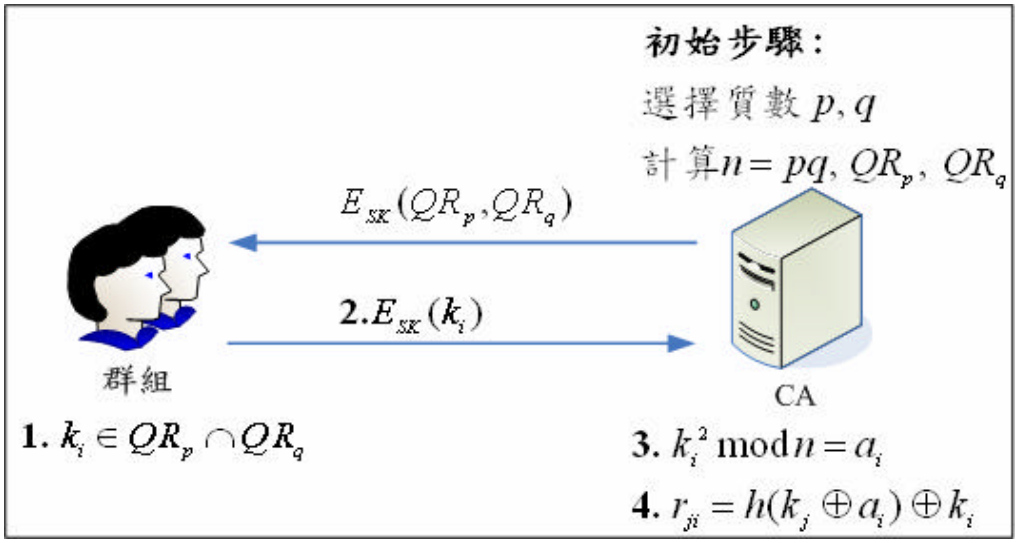


圖 4.1.1、產生群組金鑰

**(2) 導出群組金鑰：**

對所有 $S_j \succ S_i$ 這樣的關係，$S_j$ 可以利用方程式 (4.1.3) 計算出群組 $S_i$ 的群組金鑰 $k_i$。

$$k_i = h(k_j \oplus a_i) \oplus r_{ji} \qquad (4.1.3)$$

**步驟一：** $S_j$ **向** CA **要求所需的參數** $a_i$ **與** $r_{ji}$**。**

**步驟二：**CA **傳送** $a_i, r_{ji}$ **給** $S_j$**。**

**步驟三：** $S_j$ **執行如方程式** (4.1.3) **的運算，算出** $k_j$**。**

**以上步驟如下圖** 4.1.2 **所示。**

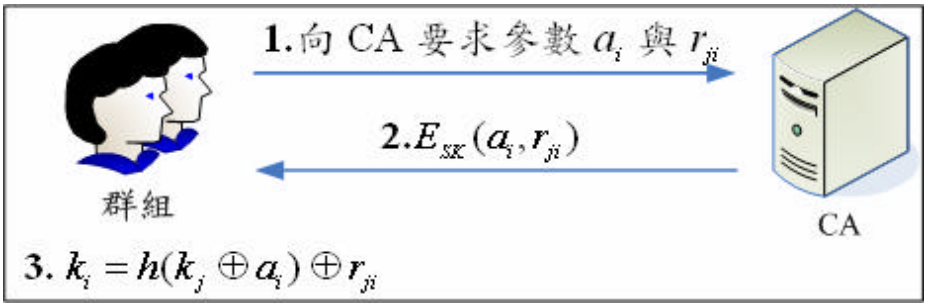


**圖** 4.1.2**、導出群組金鑰**

**(3) 更新群組金鑰**

**步驟一：** $S_i$ **重新選擇一把新的金鑰** $k_i^* \in QR_p \cap QR_q$**。**

**步驟二：** $S_i$ **利用** $SK$ **加密後傳送** $E_{SK}(k_i^*)$ **給** CA**。**

**步驟三：**CA **將計算一個新的二次剩餘數** $a_i^*$**，** $a_i^* (= (k_i^*)^2 \bmod n)$**。**

**步驟四：**CA **重新計算所有關係參數如方程式**(4.1.4)**。**

$$r_{ji}^* (= h(k_j \oplus a_i^*) \oplus k_i^*) \qquad (4.1.4)$$

**以上步驟如圖** 4.1.3 **所示。**

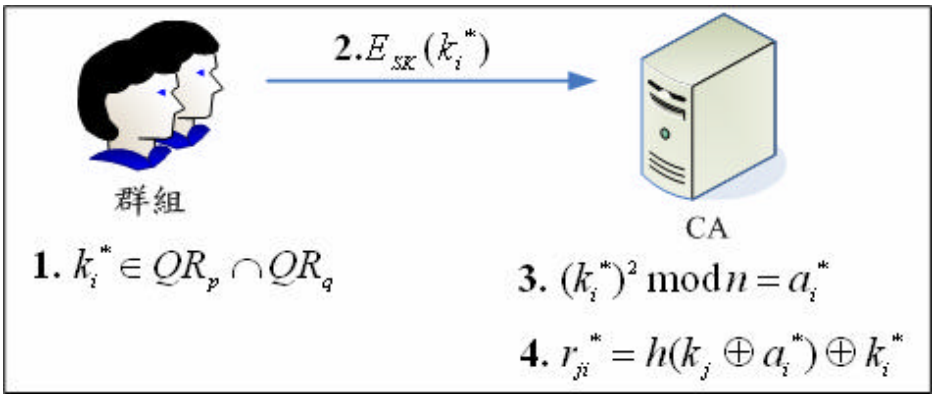


**圖 4.1.3、更新群組金鑰**

## 第二節　安全性分析

**在本章節我們提出一些針對我們所提方法的攻擊，但經過分析後我們可證明攻擊者無法成功破解我們的方法。**

**攻擊一：反向攻擊**

**我們假設** $S_j \succ S_i$ **，但** $S_i$ **想要破解** $k_j$ **那麼他可以做如方程式** (4.3.1) **的計算得到** $h(k_j \oplus a_i)$ **，但是群組金鑰** $k_j$ **由單向雜湊函式所保護，若要得到** $k_j$ **他必須面對破解單向雜湊函式的難題，因此此攻擊方式無法成功。**

$$h(k_j \oplus a_i) = r_{ji} \oplus k_i \tag{4.3.1}$$

**攻擊二：內部成員蒐集參數攻擊**

**有一個群組** $S_i$ **擁有** $m$ **個父節點群組如圖** 4.3.1 **所示, 我們以** $S_j$ **,** $S_{j+1}$ **, …,** $S_{j+m}$ **表示。那麼在群組** $S_i$ **裡的使用者可以蒐集所有的關係參數** $r_{ji}$ **,** $r_{j(i+1)}$ **,..,** $r_{j(i+m)}$ **。然後，他可以得到**

$h(k_{j+v} \oplus a_i), v = 1,2,...,m$ 但他必須面對破解單向雜湊函式的難題，因此這個攻擊無法成功。

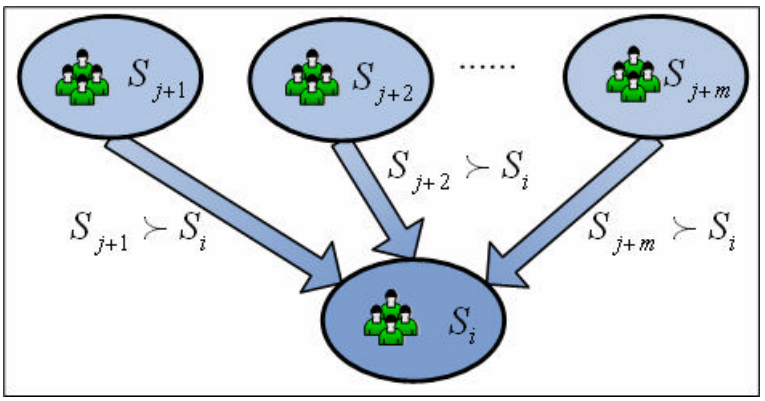


圖 4.2.1、內部成員蒐集攻擊

**攻擊三：外部成員蒐集參數攻擊**

我們考慮另一個情況，有一個外部攻擊者（也就是不屬於任何群組），若他要進行如攻擊二的攻擊時，他將會面對比攻擊二更加困難的問題，因為攻擊者本身並沒有群組金鑰 $k_i$。

**攻擊四：群組聯合攻擊**

假設 $S_j$ 有兩個子節點 $S_i$ 和 $S_l$，而兩個群組中各有一個使用者要聯合起來破解 $k_j$ 如圖 4.3.2 所示，則他們可以計算方程式 (4.3.2) 和方程式 (4.3.3)，但是他們將面對一個和攻擊二一樣的問題。

$$r_{ji} = h(k_j \oplus a_i) \oplus k_i \qquad (4.3.2)$$

$$r_{jl} = h(k_j \oplus a_l) \oplus k_l \qquad (4.3.3)$$

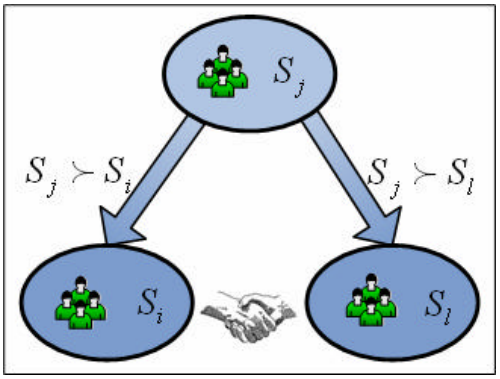


圖 4.2.2、群組聯合攻擊

**攻擊五：子節點間的攻擊**

另一個情況是有兩個群組 $S_i$ 和 $S_l$ 有著同一個父節點 $S_j$ 如圖4.3.3所示，而 $S_i$ 想要破解 $S_l$ 的群組金鑰 $k_l$。在群組 $S_i$ 裡的攻擊者只擁有 $k_i$ 以及可以獲得 $r_{ji}$ 與 $r_{jl}$，但從這些資訊並無法直接破解 $k_l$，因為他將面對一個和攻擊一一樣的難題，所以攻擊者無法破解 $S_l$ 的群組金鑰。

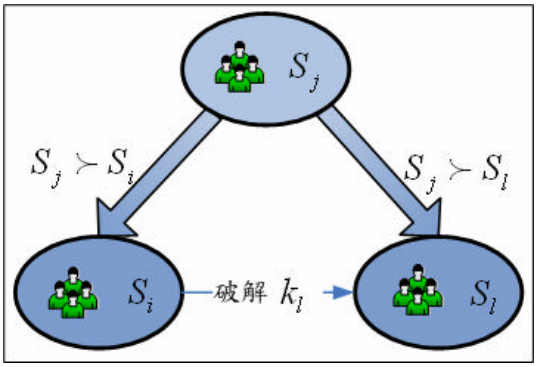


圖 4.2.3、子節點間的攻擊

**攻擊六：利用 $a_i$ 直接破解 $k_i$**

基於二次剩餘問題，這個破解方式將會面臨因數分解的問題，因此此破解方式將不會成功。

**攻擊七：Lee 所提出的兩個攻擊**

**攻擊一：當群組修改群組金鑰後，若攻擊者能拿到舊的群組金鑰時。**

**在** $r_{ji} = h(k_j \oplus a_i) \oplus k_i$ **中的** $a_i$ **在每次群組** $S_i$ **把他的群組金鑰** $k_i$ **修改成** $k_i^*$ **時都會由** CA **重新計算，因此這個弱點將不存在。**

**攻擊二：當群組間的識別碼** $ID$ **只相差些許位元。**

**在我們的式子** $r_{ji} = h(k_j \oplus a_i) \oplus k_i$ **中並沒有使用群組的識別碼** $ID_i$ **做為參數，因此這個弱點不存在。**

## 第三節　效能比較

**這一節中我們將討論我們方法的效能，其中我們將與** Lin **橢圓曲線方法，以及** Wu **的橢圓曲線方法做比較，我們皆假設最差的情況，而為了容易討論，我們首先定義了一些符號，以下說明這些符號以及其所代表的意義：**

$T_{MUL}$ **：執行一次** 1024-bit **模乘法運算所需的時間。**

$T_H$ **：執行一次** 160-bit **單向雜湊函式運算所需的時間。**

$T_{EC\_MUL}$ **：執行一次** 160-bit **橢圓曲線模乘法運算所需的時間。**

**根據**[10]**，我們可以知道** $T_{EC\_MUL} \approx 29T_{MUL}$ **。**

在此金鑰管理方法第一次建立時，包含一個初始步驟，此步驟由 CA 計算出所有的二次剩餘數 $QR_p$ 和 $QR_q$，而此動作必須計算 $(p-1)+(q-1)$ 次的模乘法，因此所需的計算量為 $((p-1)+(q-1))T_{MUL}$。由於我們將此方法運用於隨選視訊系統中，而初始步驟只需由管理者在隨選視訊系統第一次建立的同時執行一次，所以並不影響後續用戶選擇影片、觀賞影片與更新金鑰等步驟的運算量，因此在與 Lin 和 Wu 的效能比較中，我們不考慮此步驟。

在表格一中，我們可以發現我們的方法比 Lin 和 Wu 的方法所需的時間減少許多，特別是在導出群組金鑰的階段最差的狀況只需要 $nT_H$ 的時間，因為群組 $S_i$ 只需要執行如方程式 $r_{ji} \oplus h(k_j \oplus a_i)$ 的運算，最差的狀況必需做 $n$ 次，而此方程式最主要的時間花費是在執行單向雜湊函式 $h(\ )$ 運算。

在產生群組金鑰的階段，我們假設存在 $n$ 個群組，因此 CA 必須方程式 $k_i^2 \bmod n$ 計算屬於每個群組的參數 $a_i$，以及利用方程式 $r_{ji} = h(k_j \oplus a_i) \oplus k_i$ 計算關係參數（群組 $S_j$ 與群組 $S_i$ 間的關係參數 $r_{ji}$），所以此階段需要 $n(T_{MUL}+T_H)$ 的時間。

在修改群組金鑰階段，CA 也需要執行如產生群組金鑰階段一樣的步驟，因此此階段所需要的時間也是 $n(T_{MUL}+T_H)$，總而言之我們的方法與 Lin 與 Wu 的方法相比是相當有效率的。

**表 4.3.1、時間複雜度比較**

| | **Lin 的方法** | **Wu 的方法** | **我們的方法** |
|---|---|---|---|
| **產生群組金鑰階段** | $(58n+29)T_{MUL}$ | $29nT_{MUL}$ | $n(T_{MUL}+T_H)$ |
| **導出群組金鑰階段** | $(58n+29)T_{MUL}$ | $29nT_{MUL}$ | $nT_H$ |
| **更新群組金鑰階段** | $(58n+29)T_{MUL}$ | $29nT_{MUL}$ | $n(T_{MUL}+T_H)$ |

# 第六章 結論

## 第一節 研究成果討論

在我們的隨選視訊系統中，使用 Lin 的橢圓曲線階層式金鑰方法，並運用了智慧卡提出了一個影片分級的機制。在這個隨選視訊系統中，業者可自行將影片作分類，並依照 Saskatchewan 的影片分級法做影片分級。使用者可依據自己的喜好，選擇欲購買的影片類型，並依照業者所定的價格付費，當使用者欲觀賞影片時，只要將智慧卡插入 set-top box 的讀卡機中，並輸入密碼便可選擇其所購買的影片。

本系統最大的特色為，以使用者的觀點，父母可為小孩挑選適合其年齡的影片，如教育性的節目，如此可避免小孩觀賞到限制級的節目，也就是影片分級。在業者方面，其可以隨時加入或移除一種或多種影片種類，如此對於系統管理將更有彈性。

由於我們利用 Lin 所提出的橢圓曲線方法設計隨選視訊系統，雖然其運算量已比早期的方法降低，但事實上還是需要相當的時間，因此我們試著研究新方法，我們選擇使用二次剩餘的方法，由於二次剩餘每次運算只需要一次模乘法，業者只需要預先將所需的二次剩餘數 $QR_p$ 與 $QR_q$ 計算出來並保存著，之後，在金鑰產生與修改階段只需要 $T_{MUL}+T_H$ 的時間，而在導出金鑰的階段甚至只需要執行一次雜湊

函式運算的時間 $T_H$，因此我們所提出的改良方法可以使系統效能大幅提升。

## 第二節　未來研究方向

在我們的隨選視訊系統中，每位使用者都需各自擁有一張智慧卡，但再某些情況中，如使用者單位視為一個群組，那麼其所須擁有的智慧卡數勢必等於其群組成員數，因此我們未來將朝向多人可共同擁有同一張智慧卡作研究與探討。換句話說，未來我們將針對智慧卡中必須處理的存取控制問題作研究，不同使用者所能存取的智慧卡權限皆不相同。讓每一個群組只需保存一張智慧卡，可依照成員的不同提供不同的影片供之觀賞。

在階層式金鑰管理方法方面，未來我們將針對，群組的加入與移除作研究，例如新群組加入後群組與群組間的關係如何做有效率的調整，也是未來的研究重點。

# 參考文獻


[1] C. H. Lin, “Dynamic key management schemes for access control in a hierarchy,” *Computer Communications*, 20, 1997, pp.1381-1385.

[2] N. Y. Lee and T. Hwang, “Research note Comments on ‘dynamic key management schemes for access control in a hierarchy’,” *Computer Communications*, 22, 1999, pp.87-89.

[3] H. H. Cho, Y. H. Park, J. S. Lee, H. S. Jang and K. H. Rhee, “A Proposal of Secure Efficient Dynamic Hierarchical Key Management Structure,” *The Second Workshop on Information Security Application 2001* pp.357-362

[4] C. H. Lin and J. H. Lee, “An Efficient Hierarchical Key Management Scheme Based on Elliptic Curves,” *Journal of Interdisciplinary Mathematics*, Vol. 5, No. 3, October 2002, pp.293-301.

[5] M. C. Wu, T. S. Chen, J. L. Liu and J. H. Wen, “Access Control System based on the Elliptic Curve Cryptosystem,” *Proceedings of International Conference on Informatics, Cybernetics, and Systems 2003*, pp. 1335-1340.

[6] C. H. Lin, J. S. Chou, T. Y. Lee, “A Secure Scheme for Users Classification and Contents Protection in Video-on-demand Systems,” *Proceedings of International Conference on Informatics, Cybernetics, and Systems 2003*, pp.1347-1352.

[7] C.C. Chang, S.M. Tsu, “Remote scheme for password authentication based on theory of quadratic residues,” *Computer Communications*, 18, 1995, pp.936–942.

[8] K. H. Rosen, “Elementary Number Theory and Its Applications,” *Addison-Wesley*, Reading, MA (1988).

[9] K.J. Tan, H.W. Zhu, “Research note A conference key distribution scheme based on the theory of quadratic residues,” *Computer Communications*, 22, 1999, pp.735–738.

[10] Neal Koblitz, Alfred Menezes and Scott Vanstone, “The State of Elliptic curve Cryptography,” *Design, Codes and Cryptography*, 19, 2000, pp.173-193.

[11] Draft FIPS 180-2, Secure Hash Standard (SHS), U.S. Doc/NIST, May 30, 2001.

[12] Draft FIPS 197, Advanced Encryption Standard (AES), U.S. Doc/NIST, Nov 26, 2001.

[13] N. Koblitz, A. Menezes and S. Vanstone, “The State of Elliptic curve Cryptography,” *Design, Codes and Cryptography*, 19, 2000, pp.173-193.

[14] N. Koblitz, “A Course in Number Theory and Cryptography,” *New York, NY:Spring-Verlag*, Second edition, 1994.

[15] A. Menezes, “Elliptic curve Public Key Cryptosystems,” *Kluwer Academic Publishers*, 1993.

[16] D. A. Tran, K. A. Hua, S. Sheu, " A new caching architecture for efficient video-on-demand services on the internet," *Proceedings Symposium on Applications and the Internet*, 2003, pp.172 -181.

[17] Finqing Zhao; C.-C.J. Kuo, " Video-on-demand server system design with random early migration," *Proceedings of the 2003 International Symposium on Circuits and Systems*, Volume: 2, 2003, pp. 640 -643.

[18] L. Harn, L. Y. Lin, "A Cryptographic Key Generation Scheme for Multi-Level Data Security," *Computer and Security* 9, 1990, pp.539-546.

[19] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol.21, No. 2, 1978, pp.120-126.

[20] W. Patterson, "Mathematical Cryptology for Computer Scientists and Mathematicians," *Rowman*, 1987.

[21] The Saskatchewan Film Classification by "http://www.saskjustice.gov.sk.ca/film_&_video/default.shtml".