廣義的匿名廣播加密系統

Generalized Anonymous Broadcast Encryption Scheme

丁培毅　　張書瑋　　溫玎蓥

國立台灣海洋大學

Email:{pyting, M96570030, M96570025}@mail.ntou.edu.tw

摘 要 —本文提出一個基於身分識別、廣義的匿名廣播加密系統。由於同時具有廣義性及匿名性。此系統可以應用在成員眾多、需要動態指定存取權限的醫療資料庫系統中。我們首先替 **Boneh** 的 **"空間加密法"** 設計一個維持接收者匿名性的機制，此機制將廣播密文的安全政策藉由接收者的公鑰隱藏起來，接收者可以用自己的私鑰測試是否可解開該密文，如果不能解的話，也無法得知哪些人可解。然後定義此匿名廣播系統的密文不可分辨安全性，假設 **BDDHE** 問題是計算上困難的，我們在標準模型中證明此系統的安全性。

關 鍵 詞 —基於身分識別的加密、廣義的身分識別加密、廣播加密、匿名廣播、標準模型、安全的病歷資料庫。

***Abstract*—In this paper, we propose an identity-based, generalized, anonymous broadcast encryption system. This system can be used in a large scale medical database that requires dynamic assignments of access rights because it is both generalized and anonymous. First we design a mechanism to hide the broadcast targets for Boneh's "Spatial Encryption ". This mechanism hides the policy vector through the target's public key. Any receiver can test the ciphertext to see if he is one of the target receivers. If he is not the target, he will not learn the set of target receivers. Then we define suitable security notion for this anonymous broadcast encryption system. Assuming that BDDHE problem is secure, we prove the security of the system in the standard model.**

***Index Terms:*—Identity-based encryption, Generalized identity-based encryption, Broadcast encryption, Anonymous broadcast encryption, Standard model, Secure medical database.**

一、簡介

在一個基於身分識別的加密 (Identity-Based Encryption, IBE) 系統[16][6]中，使用者用身分識別字串作爲公鑰 (例如 "Alice@xxx.com")，密鑰產生中心(Private Key Generator, PKG) 驗證其身分並授與密鑰。當系統規模較大時，爲了減少 PKG 的工作量，可以使用階層式身分識別加密 (Hierarchical Identity-Based Encryption, HIBE) 系統[14][11]，運用樹狀架構的一組PKG 一層一層往下授權，使用者向底層的 PKG 證實自己的身分以得到密鑰。

在廣播加密系統中，每個廣播者都可以加密信息給任意的使用者集合S，S中的使用者可以用自己的密鑰解開密文[3], [10]，近年來許多相關的研究[2], [13], [1], [7] 主要目標在於縮短金鑰長度、縮短密文長度、降低加解密所需的計算時間、有效率地追蹤洩密者、動態調整系統成員等等，此外也有基於身分識別的廣播加密 (Identity-Based Broadcast Encryption, IBBE) 系統[15]，其好處是公開金鑰長度不會和使用者總人數成正比。

Boneh[8]在2008年提出廣義身分識別加密 (Generalized Identity Based Encryption, GIBE) 系統的概念，GIBE系統中授權關係較爲自由，任何一個成員

都可以把自己部份的能力授權給他人，不像 HIBE 系統中授權只限於樹狀的從屬關係之間，在 GIBE 系統中如果將一個密文加密給一群成員授權能力的交集，即可以提供廣播加密系統的功能。在一個運用 GIBE 系統建構的廣播加密系統中，授權者可解密所有他授權之成員可解的密文，因此加密時可以快速地動態指定存取權限，適合應用在成員眾多的組織結構中，例如: 在中央健保局的醫療資料庫中，其使用成員包含各個醫院、各個專科、各個醫生、病人等等。

在醫療資料庫的應用中，一份病歷資料代表一個病人某一次就診的記錄，這份資料除了病人可以看到內容之外，他的主治醫生、會診醫生、住院醫生、該科主任、醫院主管、衛生機關主管、健保局主管人員都可能有權存取此筆資料。在本文中嘗試運用公開金鑰廣播加密系統的概念來設計這個機制，我們也希望能夠運用有彈性的授權來降低對多個目標廣播時的密文大小和計算量。

如果直接應用現有的廣播加密系統於上述醫療資料庫中，未得到授權的使用者雖然看不到病歷內容，卻可以從廣播密文的接收對象得到部份有用的資訊，因此本文提出了一種基於身分識別的匿名廣義廣播加密系統來解決這個實務上的問題，此處的"匿名性"就是隱藏廣播密文的接收對象。我們由"空間加密系統 (Spatial Encryption System)[8]"著手，此機制具有GIBE 系統的特性，其中每一個使用者的 ID 對應一個多維的仿射空間，每一份文件對應一個空間中的點做爲其安全政策 (security policy)，如果該點位於某一使用者的仿射空間中則該使用者可解此密文。此系統可以更進一步區分爲許多角色 (role)，適合應用於前述醫療資料庫系統中，然而此系統並不具有匿名性，因此我們設計一個隱藏前述安全政策的機制配合空間加密系統運作，進一步保護病歷所有者的隱私，減少密文透露的資訊，使惡意的攻擊者難以由密文中得到任何有用的資訊。我們沿用[8]中最廣義的安全性定義於匿名的廣播系統中，並在標準模型下證明所提出系統的安全性。

第二節介紹相關的定義、假設、以及空間加密系統，第三節爲安全性定義與廣義的匿名廣播加密系統，第四節爲系統安全性的證明，第五節爲結論。

二、基本假設與空間加密系統

令$\mathbb{G}$, $\mathbb{G}_T$爲兩個秩 (order) 爲質數p的循環群，g爲$\mathbb{G}$的生成數。$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ 爲滿足雙線性 (Bilinear)、非退化性 (Non-degenerate)、與可計算性 (Computable) 的雙線性對映 (Pairing)。

BDDH (Bilinear Decision Diffie-Hellman) 問題：分辨取樣 x 來自 $\mathcal{P}_{\text{BDDH}}$ 分佈或是 $\mathcal{R}_{\text{BDDH}}$ 分佈，其中 $\mathcal{P}_{\text{BDDH}} := \{a,\ b,\ c \in_R \mathbb{Z}_p^*,\ z = e(g,g)^{abc};\ (g^a,\ g^b,\ g^c,\ z)\}$，$\mathcal{R}_{\text{BDDH}} := \{a,\ b,\ c \in_R \mathbb{Z}_p^*,\ z \in_R \mathbb{G}_T^*;\ (g^a,\ g^b,\ g^c,\ z)\}$。一個機率式多項式時間演算法 $\mathcal{A}(g, g^a, g^b, g^c, z)$ 分辨 BDDH 問題的優勢爲 BDDH $\text{Adv}_{\mathcal{A}}(\lambda) := |\ \Pr[\mathcal{A}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{P}_{BDDH}] - \Pr[\mathcal{A}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{R}_{BDDH}]|$，其中 λ 爲安全參數。

BDDHE (Bilinear Decision Diffie-Hellman Exponent) 問題：分辨取樣 $\boldsymbol{x}$ 來自 $\mathcal{P}_{\text{BDDHE}}$ 分佈或是 $\mathcal{R}_{\text{BDDHE}}$ 分佈，其中 $\mathcal{P}_{\text{BDDHE}} := \{\alpha \in_R \mathbb{Z}_p^*, h \in_R \mathbb{G}^*, z = e(g,h)^{\alpha^n};\ (g^{\alpha^{[0,n-1]}}, g^{\alpha^{[n+1,2n]}}, h, z)\}$，$\mathcal{R}_{\text{BDDHE}} := \{\alpha \in_R \mathbb{Z}_p^*, h \in_R \mathbb{G}^*, z \in_R \mathbb{G}_T^*;\ g^{\alpha^{[0,n-1]}}, g^{\alpha^{[n+1,2n]}}, h, z\}$，其中符號 $g^{\alpha^{[a,b]}}$ 代表 $(g^{\alpha^a}, g^{\alpha^{a+1}}, \cdots, g^{\alpha^b})$，$a,\ b \in \mathbb{Z}$ 且 $a \leq b$。一個機率式演算法 $\mathcal{A}(g, g^{\alpha^{[0,n-1]}}, g^{\alpha^{[n+1,2n]}}, h, z)$ 分辨 BDDHE 問題的優勢爲 BDDHE $\text{Adv}_{\mathcal{A},n}(\lambda) := |\ \Pr[\mathcal{A}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{P}_{BDDHE}] - \Pr[\mathcal{A}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{R}_{BDDHE}]|$，其中 λ 爲安全參數。

空間加密系統

Boneh 用一個密文長度固定的 n 維空間加密系統[8] 實現 GIBBE 系統，其靈感來自固定密文長度的 HIBE 系統[5]，安全性則基於 BDDHE 問題。

符號

- $\boldsymbol{v} = (v_1, v_2, ..., v_n)^T \in \mathbb{Z}_p{}^n$ 代表 n 維的行向量
- 由群 $\mathbb{G}$ 元素構成的 n 維向量 $g^{\boldsymbol{v}} := (g^{v_1}, g^{v_2}, ..., g^{v_n})^T \in \mathbb{G}^n$。在不知道向量 $\boldsymbol{v}$ 的情況下，給

定 $g^{\boldsymbol{v}}$ 和一個 n 維向量 $\boldsymbol{w} = (w_1, w_2, ..., w_n)^T$，任何人可以很容易計算出 $\mathbb{G}$ 中的元素 $g^{\langle \boldsymbol{v}, \boldsymbol{w} \rangle} = (g^{v_1})^{w_1} \cdot (g^{v_2})^{w_2} \cdot \ldots \cdot (g^{v_n})^{w_n}$，其中 $\langle \boldsymbol{v}, \boldsymbol{w} \rangle := \boldsymbol{v}^T \boldsymbol{w}$ 代表兩個 n 維向量的內積

- $\text{Aff}(M, \boldsymbol{x}) \subseteq {\mathbb{Z}_p}^n$ 代表 d 維仿射空間 $\{M\boldsymbol{y} + \boldsymbol{x} : \boldsymbol{y} \in {\mathbb{Z}_p}^d\}$，其中 $M \in {\mathbb{Z}_p}^{n \times d}$，$\boldsymbol{x} \in {\mathbb{Z}_p}^n$

系統環境

- 系統參數：$\mathbb{G}$、$\mathbb{G}_T$ 爲兩個秩爲質數 p (安全參數 $\lambda = \lceil \log\, p \rceil$) 的循環群，$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 爲一個雙線性對映。秘密參數包含 $a_0 \in \mathbb{Z}_p$、$\boldsymbol{a} \in {\mathbb{Z}_p}^n$、$b \in \mathbb{Z}_p$，公開參數包含 g、$g^{a_0} \in \mathbb{G}$，$t = e(g, g)^b \in \mathbb{G}_T$ 和一個向量 $g^{\boldsymbol{a}} \in \mathbb{G}^n$。
- 每一個使用者的角色 ρ 對應一個 d 維仿射空間 V_ρ := $\text{Aff}(M_\rho, \boldsymbol{x}_\rho)$，其密鑰 K_{V_ρ} =(g^r, $g^{b + r a_0 + r\langle \boldsymbol{x}_\rho, \boldsymbol{a} \rangle}$, $g^{r {M_\rho}^T \boldsymbol{a}}$), r 是從 $\mathbb{Z}_p^*$ 中隨機挑選的元素。
- 每一個密文的安全政策 π 對應一個 n 維向量 $\boldsymbol{x}$。
- 布林函數

$$\text{open}(\rho, \pi) = \begin{cases} 1, & \text{若 } \boldsymbol{x} \in V_\rho \\ 0, & \text{其它} \end{cases}$$

四個演算法運作如下：

- **Setup**(λ, n)：產生公開的系統參數 p、$\mathbb{G}$、$\mathbb{G}_T$，$g \in_R \mathbb{G}^*$ 和秘密參數 a_0、$b \in_R \mathbb{Z}_p$，$\boldsymbol{a} \in_R {\mathbb{Z}_p}^n$，計算 $t := e(g, g)^b$，輸出公開參數 PP := (p, $\mathbb{G}$, $\mathbb{G}_T$; g, g^{a_0}, $g^{\boldsymbol{a}}$, t) 和系統管理者密鑰 $K_\top$:= (g, g^b, $g^{\boldsymbol{a}}$) $\in \mathbb{G}^{n+2}$，$\top$ 代表最上層的 PKG。
- **Delegate**(PP, V_1, K_{V_1}, V_2)：兩個子空間 V_1 := $\text{Aff}(M_1, \boldsymbol{x}_1)$、$V_2$:= $\text{Aff}(M_2, \boldsymbol{x}_2)$ 且 V_2 是 V_1 的子空間，必存在 $d \times d$ 矩陣 T 和 d 維向量 $\boldsymbol{y}$ 滿足 $M_2 = M_1 T$、$\boldsymbol{x}_2 = \boldsymbol{x}_1 + M_1 \boldsymbol{y}$，授權者擁有 K_{V_1}，可以用下列步驟計算空間 V_2 對應的密鑰 K_{V_2}，首先計算 $\hat{K}_{V_2}$:= (g^r, $g^{b + r a_0 + r\langle \boldsymbol{x}_1, \boldsymbol{a} \rangle} \cdot g^{r \boldsymbol{y}^T M_1^T \boldsymbol{a}}$, $g^{r T^T M_1^T \boldsymbol{a}}$) = ($g^r$, $g^{b + r a_0 + r\langle \boldsymbol{x}_2, \boldsymbol{a} \rangle}$, $g^{r M_2^T \boldsymbol{a}}$)，再將其隨機化，挑選 $s \in_R \mathbb{Z}_p^*$ 並計算 K_{V_2} := ($g^r \cdot g^s$, $g^{b + r a_0 + r\langle \boldsymbol{x}_2, \boldsymbol{a} \rangle} \cdot g^{s(a_0 + \langle \boldsymbol{x}_2, \boldsymbol{a} \rangle)}$, $g^{r M_2^T \boldsymbol{a}} \cdot g^{s M_2^T \boldsymbol{a}}$) = ($g^{r+s}$, $g^{b + (r+s)(a_0 + \langle \boldsymbol{x}_2, \boldsymbol{a} \rangle)}$, $g^{(r+s) M_2^T \boldsymbol{a}}$)，$K_{V_2}$ 即爲 V_1 授權給 V_2 的密鑰。
- **Encrypt**(PP, $\boldsymbol{x}$, m)：令信息 m 爲群 $\mathbb{G}_T$ 中的一個元素，挑選 $s \in_R \mathbb{Z}_p^*$ 計算密文 $\boldsymbol{c}$:= (c_1, c_2, c_3) := (g^s, $g^{s(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)}$, $m \cdot t^s$)
- **Decrypt**(PP, V, K_V, $\boldsymbol{x}$, c_1, c_2, c_3)：其中 $\boldsymbol{x} \in V$，ρ 即爲 V，π 即爲 $\boldsymbol{x}$，若滿足 $\text{open}(\rho, \pi)$ 爲眞，首先執行授權演算法 Delegate(PP, V, K_V, $\text{Aff}(0, \boldsymbol{x})$) 得到密鑰 $K_{\{\boldsymbol{x}\}}$:= (k_1, k_2) := (g^r, $g^{b + r(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)}$)，依照下式即可解回信息 m:

$$\frac{c_3 \cdot e(c_2, k_1)}{e(c_1, k_2)} = \frac{m \cdot t^s \cdot e(g, g)^{rs(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)}}{e(g, g)^{sb + rs(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)}} = m$$

上述系統中安全政策向量 $\boldsymbol{x}$ 是附在密文上公佈的，我們在下節中將修改此系統，使得只有可解密的使用者可得到 $\boldsymbol{x}$。

三、基於身分識別的廣義匿名廣播加密系統

以下先規範匿名廣播加密系統的性質，定義其安全性，然後修改空間加密系統使其具備匿名性：

廣義的匿名廣播加密系統：

- 系統中所有成員皆可自行加密並廣播信息密文，廣播者不限於特定的成員。
- 加密者可任意挑選一個成員的集合 S，使在 S 內的成員可解密，而不在 S 內的成員不能解密。
- 密文必須具有匿名性，只有在集合 S 內的成員知道哪些人可解密，而不在 S 內的成員則否。
- 允許透過授權的機制將部份解密能力委託他人行使，被授權者可解密的密文，其授權者也可解密。
- 兩個沒有階層從屬授權關係的成員，可授權給同一人。意即 A 和 B 都可授權給 C，C 可解的密文 A 和 B 都能解，但 A 能解的密文 B 不一定能解，反之亦然。

以下安全定義及系統中，都假設使用者的身分識別字串 ID 必須經過一個單向且有效率的演算法得到對應的仿射空間 V := $\text{Aff}(M, \boldsymbol{x})$，其中 M 是一個 $n \times n$ 的矩陣，$\boldsymbol{x}$ 是一個 n 維的行向量，由 ID 計

算 Aff$(M, \boldsymbol{x})$ 是容易的 (可在多項式時間內算出)，而由 Aff$(M, \boldsymbol{x})$ 求得對應的 ID 是計算上困難的。

安全性定義：

以下是一個質疑者 $\mathcal{C}$ 和攻擊者 $\mathcal{A}$ 間的賽局，如果任何有效率的攻擊者 $\mathcal{A}$ 於此賽局的優勢都可以忽略，則此系統在匿名 (Anonymous) 的廣播設定、選擇性 (Selective) ID、與選擇明文攻擊 (Chosen Plaintext Attack, CPA) 的情境下是安全的，我們稱之爲 (Anon, Sel, CPA)-secure。

環境設定：$\mathcal{C}$ 先挑選空間維度 n、質數 p 和兩個秩爲 p 的循環群 $\mathbb{G}, \mathbb{G}_T$ 並傳送給 $\mathcal{A}$，$\mathcal{A}$ 挑選兩個身分識別字串的集合 $S_0 = \{\mathrm{ID}_{0,1}, \mathrm{ID}_{0,2}, \ldots, \mathrm{ID}_{0,k}\}$，$k < n$、$S_1 = \{\mathrm{ID}_{1,1}, \mathrm{ID}_{1,2}, \ldots, \mathrm{ID}_{1,k'}\}$，$k' < n$ 並傳送 (S_0, S_1) 給 $\mathcal{C}$，$\mathcal{C}$ 挑選 $\boldsymbol{x}_0 \in \cap_{i=1}^{k} V_{0,i}$, $\boldsymbol{x}_1 \in \cap_{i=1}^{k'} V_{1,i}$，$V_{i,j}$ 爲 $\mathrm{ID}_{i,j}$ 所對應的仿射空間，$\mathcal{C}$ 挑選其它的公開參數 PP 並傳送給 $\mathcal{A}$。

第一次詢問階段：$\mathcal{A}$ 向 $\mathcal{C}$ 詢問多次授權給身分識別字串 ID′ (對應仿射空間 V') 的密鑰，$\mathcal{C}$ 執行 Delegate(PP, $\top$, $K_\top$, V') 並傳送 $K_{V'}$ 給 $\mathcal{A}$，但是 $\mathcal{A}$ 不能詢問子集合 S_0 與 S_1 內的身分識別字串的密鑰。

質疑階段：$\mathcal{A}$ 挑選兩個信息 m_0、m_1 傳送給 $\mathcal{C}$，$\mathcal{C}$ 隨機挑選 $\beta \in \{0, 1\}$，計算 $\boldsymbol{c}^*$:= Encrypt(PP, $\boldsymbol{x}_\beta$, m_β)，並回傳給 $\mathcal{A}$。

第二次詢問階段：$\mathcal{A}$ 再向 $\mathcal{C}$ 詢問多次授權給身分識別字串 ID″ (對應仿射空間 V'') 的密鑰，$\mathcal{A}$ 不能詢問子集合 S_0 與 S_1 內的身分識別字串的密鑰。

猜測階段：$\mathcal{A}$ 輸出 β'，如 $\beta' = \beta$ 則 $\mathcal{A}$ 贏得此賽局。

上述的賽局中 $\mathcal{A}$ 必須在拿到公開參數前先指定 ID 的集合 S_0 與 S_1，稱爲選擇性 ID 的攻擊模型 [4]；只提供 $\mathcal{A}$ 加密引擎而沒有提供 $\mathcal{A}$ 解密引擎，是所謂的選擇明文攻擊。對於一個非匿名的廣播加密系統，賽局中 $\mathcal{A}$ 只需要挑一個共同的識別字串集合 S，亦即 S_0 必須等於 S_1，否則 $\mathcal{A}$ 可以輕鬆地由廣播的對象分辨密文中的明文。

攻擊者 $\mathcal{A}$ 在 $\mathcal{V}$ 賽局 (當 $\mathcal{A}$ 攻擊一個設定參數爲 SP 的加密系統 $\mathcal{S}$) 中的優勢爲 $\mathcal{V}\mathrm{Adv}_{\mathcal{A}\longleftrightarrow(\mathcal{S},\mathrm{SP})}(\lambda) := |\Pr[\mathcal{A} \text{ wins } \mathcal{V}] - \Pr[\mathcal{A} \text{ loses } \mathcal{V}]|$。假如對於所有的設定參數 SP 和所有的機率式多項式時間的攻擊者 $\mathcal{A}$，優勢 $\mathcal{V}\mathrm{Adv}_{\mathcal{A}\longleftrightarrow(\mathcal{S},\mathrm{SP})}(\lambda)$ 是一個 λ 的可忽略函數，則稱此廣播加密系統 $\mathcal{S}$ 是 $\mathcal{V}$-secure。

匿名的空間加密系統 四個演算法如下：

環境設定 Setup(λ , n)：產生一個雙線性對映 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ ，$\mathbb{G}$、$\mathbb{G}_T$ 爲兩個秩爲質數 p ($\lceil \log p \rceil = \lambda$) 的循環群，$h : \mathbb{G}_T \longrightarrow \mathbb{Z}_p$ 爲一 1-1 之編碼函式，n 是空間維度。挑選 $g \in_R \mathbb{G}^*$，產生秘密參數 a_0、b、$b_1 \in_R \mathbb{Z}_p$，$\boldsymbol{a}$、$\boldsymbol{a}_1 \in_R {\mathbb{Z}_p}^n$，然後計算 $t := e(g, g)^b$、$t_1 := g^{b_1}$，輸出公開參數 PP := (p, $\mathbb{G}$, $\mathbb{G}_T$; g, g^{a_0}, $g^{\boldsymbol{a}}$, $g^{\boldsymbol{a}_1}$, t, t_1) 和管理者密鑰 $K_\top$:= (g, g^b, $g^{\boldsymbol{a}}$, b_1, $\boldsymbol{a}_1$)。

一個識別字串 ID 對應的仿射空間爲 V = Aff$(M, \boldsymbol{x})$，密鑰爲 K_V = (g^r, $g^{b+ra_0+r\langle \boldsymbol{x},\boldsymbol{a}\rangle}$, $g^{rM^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x},\boldsymbol{a}_1\rangle}$, $g^{b_1M^T\boldsymbol{a}_1}$) 其中 b 、b_1 是管理者的秘密，r 是從 $\mathbb{Z}_p^*$ 中隨機挑選的一個數。

授權 Delegate(PP, V_1, K_{V_1}, V_2)：V_1 = Aff$(M_1, \boldsymbol{x}_1)$、V_2 = Aff$(M_2, \boldsymbol{x}_2)$，若 $V_2 \subseteq V_1$ 則 V_1 可以授權給 V_2。K_{V_1} := (g^r, $g^{b+ra_0+r\langle \boldsymbol{x}_1,\boldsymbol{a}\rangle}$, $g^{rM_1^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x}_1,\boldsymbol{a}_1\rangle}$, $g^{b_1{M_1}^T\boldsymbol{a}_1}$)，因爲 V_2 是 V_1 的子空間，所以必存在矩陣 T 和向量 $\boldsymbol{y}$ 使得 $M_2 = M_1T$, $\boldsymbol{x}_2 = \boldsymbol{x}_1 + M_1\boldsymbol{y}$ ，授權者擁有 K_{V_1}，可以用下列步驟計算空間 V_2 對應的密鑰 K_{V_2}，首先計算 $\hat{K}_{V_2}$:= (g^r, $g^{b+ra_0+r\langle \boldsymbol{x}_1,\boldsymbol{a}\rangle} \cdot g^{r\boldsymbol{y}^TM_1^T\boldsymbol{a}}$, $g^{rT^TM_1^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x}_1,\boldsymbol{a}_1\rangle} \cdot g^{b_1\boldsymbol{y}^TM_1^T\boldsymbol{a}_1}$, $g^{b_1T^TM_1^T\boldsymbol{a}_1}$) = ($g^r$, $g^{b+ra_0+r\langle \boldsymbol{x}_2,\boldsymbol{a}\rangle}$, $g^{rM_2^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x}_2,\boldsymbol{a}_1\rangle}$, $g^{b_1{M_2}^T\boldsymbol{a}_1}$)，再將其隨機化，挑選 $s \in_R \mathbb{Z}_p^*$ 並計算 K_{V_2} := ($g^r \cdot g^s$, $g^{b+ra_0+r\langle \boldsymbol{x}_2,\boldsymbol{a}\rangle} \cdot g^{s(a_0+\langle \boldsymbol{x}_2,\boldsymbol{a}\rangle)}$, $g^{rM_2^T\boldsymbol{a}} \cdot g^{sM_2^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x}_2,\boldsymbol{a}_1\rangle}$, $g^{b_1{M_2}^T\boldsymbol{a}_1}$) = ($g^{r+s}$, $g^{b+(r+s)(a_0+\langle \boldsymbol{x}_2,\boldsymbol{a}\rangle)}$, $g^{(r+s)M_2^T\boldsymbol{a}}$, $g^{b_1\langle \boldsymbol{x}_2,\boldsymbol{a}_1\rangle}$, $g^{b_1{M_2}^T\boldsymbol{a}_1}$)，$K_{V_2}$ 即爲 V_1 授權給 V_2 的密鑰。

匿名廣播加密 Encrypt(PP, S, m)：m 爲打算廣播的信息，爲簡化起見以下假設信息 m 爲群 $\mathbb{G}_T$ 中的一個元素(實作時通常將信息以無失眞的方式編碼爲 $\mathbb{G}_T$ 中的元素)，S 爲廣播對象的身分識別字串之集合，亦即 $S = \{\mathrm{ID}_1, \mathrm{ID}_2, ..., \mathrm{ID}_k\}$，$k < n$，如前一節所述每一 ID_i 可以適當地對應到一個仿射空間 V_i = Aff$(M_i, \boldsymbol{x}_i)$。加密者可以下列步驟計算密文 $\boldsymbol{c}$：

1) 找到一個安全政策 π 及其對應的向量 $\boldsymbol{x} = (x_1, x_2, ..., x_n)$ 滿足 $\boldsymbol{x} \in \cap_{i=1}^{k} V_i$ 且 $\Pr[\boldsymbol{x} \in \cup_{\mathrm{ID}_j \notin S} V_j]$ 可忽略。
2) 隨機挑選一個向量 $\boldsymbol{y}_m \in_R \mathbb{Z}_p{}^n$ 和整數 $u \in_R \mathbb{Z}_p$。
3) 計算 $\boldsymbol{v}_i := M_i \boldsymbol{y}_m + \boldsymbol{x}_i$，$i = 1, 2, ..., k$。
4) 計算 $r_{1,i} := e(g^{\langle \boldsymbol{v}_i, \boldsymbol{a}_1 \rangle}, g^{b_1})^u = e(g^{b_1 \langle \boldsymbol{v}_i, \boldsymbol{a}_1 \rangle}, g^u) \in \mathbb{G}_T$，$i = 1, 2, ..., k$。
5) 挑選 $(key, r_2, ..., r_n) \in \mathbb{Z}_p{}^n$ 滿足 $key \equiv \langle R_i, \boldsymbol{v}_i \rangle \pmod{p}$，$R_i := (h(r_{1,i}), r_2, ..., r_n)$，$i = 1, 2, ..., k$。
6) 隨機挑選 $s \in \mathbb{Z}_p$，計算
$$(c_1, c_2, c_3) := (g^s,\ g^{s(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)},\ m \cdot t^s)$$
7) 令 $R := (r_2, r_3, \ldots, r_n)$，$\mathcal{SE}$ 爲一個安全的對稱式加密系統，計算 $\boldsymbol{x}_e := \mathcal{SE}_{key}(x_1 \parallel x_2 \parallel ... \parallel x_n)$。

信息 m 的密文爲 $\boldsymbol{c} := (\boldsymbol{y}_m, g^u, R, \boldsymbol{x}_e, c_1, c_2, c_3)$

步驟 6 爲空間加密演算法的加密方法。步驟 2 ～ 5 和 7 的設計是爲了使廣播加密系統具有匿名性，若將一個密文的安全政策 π 及其對應的向量 $\boldsymbol{x}$ 直接公開，任何人皆可判斷 $\boldsymbol{x}$ 是否屬於一個識別字串對應的仿射空間，從而得知廣播的對象。

步驟 7 運用一個單次密鑰 key 將 $\boldsymbol{x}$ 加密起來而不直接公開；步驟 2 ～ 5 藉由公開 $(\boldsymbol{y}_m, g^u, R)$，使 S 集合內的使用者都用自己的密鑰計算出此密文之單次密鑰 key，而不在 S 內的使用者則否。步驟 5 爲解一個 n 元聯立方程式，k 必須小於 n，否則無解。步驟 2 ～ 4 使得每次加密時，即使集合 S 內的成員不變，步驟 5 聯立方程式的係數仍會不同，而解聯立方程式得到的單次密鑰 key 亦不相同。

實際應用時集合 S 必須將所有可解密的上層 ID 都放進來，由於在醫療資料庫的應用中 ID 的設計爲一個路徑，如：臺大醫院\眼科\．．．，因此只需要沿著路徑，就可把上層 ID (臺大醫院、臺大醫院眼科、．．．) 都放入集合 S 內。

匿名廣播解密 Decrypt(PP, V_i, K_{V_i}, $\boldsymbol{c}$)：如果密文 $\boldsymbol{c}$ 的安全政策 π 所對應的向量 $\boldsymbol{x} \in V_i$，則此演算法可以解出正確明文 m，V_i 爲集合 S 中使用者 ID_i 所對應的仿射空間，K_{V_i} 爲 ID_i 之密鑰，解密步驟如下：

1) $\hat{\boldsymbol{v}}_i = M_i \boldsymbol{y}_m + \boldsymbol{x}_i$
2) 計算 $\hat{r}_{1,i} = e(g^{b_1 \langle \hat{\boldsymbol{v}}_i, \boldsymbol{a}_1 \rangle}, g^u)$。
3) 計算 $\hat{key} \equiv \langle \hat{R}_i, \hat{\boldsymbol{v}}_i \rangle \pmod{p}$，$\hat{R}_i = (h(\hat{r}_{1,i}), r_2, ..., r_n)$。
4) 用 $\hat{key}$ 解密 $\boldsymbol{x}_e$ 得到 $\hat{x}_1 \parallel \hat{x}_2 \parallel ... \parallel \hat{x}_n$，還原 $\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$。
5) 令 $\hat{V}_{\boldsymbol{x}} = \mathrm{Aff}(0, \hat{\boldsymbol{x}})$ 執行授權演算法 Delegate(PP, V_i, K_{V_i}, $\hat{V}_{\boldsymbol{x}}$)，得到
$$K_{\{\hat{\boldsymbol{x}}\}} := (k_1, k_2) = (g^r,\ g^{b + r(a_0 + \langle \hat{\boldsymbol{x}}, \boldsymbol{a} \rangle)})$$
6) 代入下式可解出 $\hat{m}$
$$\frac{c_3 \cdot e(c_2, k_1)}{e(c_1, k_2)} = \frac{m \cdot t^s \cdot e(g, g)^{rs(a_0 + \langle \boldsymbol{x}, \boldsymbol{a} \rangle)}}{e(g, g)^{sb + rs(a_0 + \langle \hat{\boldsymbol{x}}, \boldsymbol{a} \rangle)}} = \hat{m}$$

正確性：

1) 若 $\boldsymbol{x} \in V_i$ 則 $\hat{\boldsymbol{v}}_i = M_i \boldsymbol{y}_m + \boldsymbol{x}_i = \boldsymbol{v}_i$。
2) $\hat{r}_{1,i} = e(g^{b_1 \langle \hat{\boldsymbol{v}}_i, \boldsymbol{a}_1 \rangle}, g^u) = e(g^{b_1 \langle \boldsymbol{v}_i, \boldsymbol{a}_1 \rangle}, g^u) = r_{1,i}$。
3) $\hat{R}_i = (h(\hat{r}_{1,i}), r_2, ..., r_n) = (h(r_{1,i}), r_2, ..., r_n) = R_i$，$\hat{key} \equiv \langle \hat{R}_i, \hat{\boldsymbol{v}}_i \rangle = \langle R_i, \boldsymbol{v}_i \rangle \equiv key$。
4) 因爲 $\hat{key} = key$ 所以 $\hat{\boldsymbol{x}} = \boldsymbol{x}$。
5) 從解密的步驟 6 可知，當 $\hat{\boldsymbol{x}} = \boldsymbol{x}$ 時，$\hat{m} = m$。

因此當 $\boldsymbol{x} \in V_i$ 則可解出正確的明文 m。

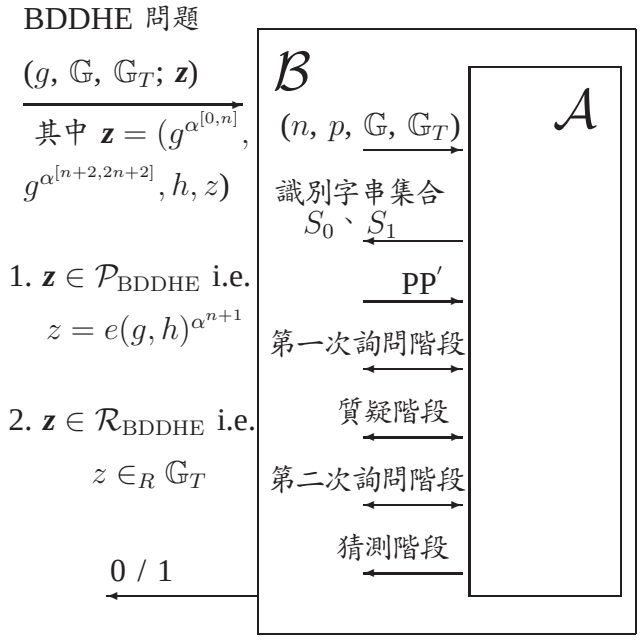
四、安全性證明

定理 1. 在一個 (Anon, Sel, CPA) 賽局中，對於任何攻擊匿名的廣播加密系統 $\mathcal{S}$ 的機率式多項式時間攻擊者 $\mathcal{A}$，存在一個分辨 BDDHE 問題的演算法 $\mathcal{B}$，執行的時間大約跟 $\mathcal{A}$ 相同，使得 $\mathrm{BDDHE\ Adv}_{\mathcal{B}, n+1}(\lambda) = \frac{1}{2} \cdot (\mathrm{Anon, Sel, CPA})\mathrm{Adv}_{\mathcal{A} \longleftrightarrow (\mathcal{S}, n)}(\lambda)$

證明：

如圖一所示，在一個匿名的廣播加密系統中，我們可證明若存在一個攻擊者 $\mathcal{A}$ 在 (Anon, Sel, CPA) 賽局中對系統 $\mathcal{S}$ 有不可忽略的優勢，則可以建構一個演算

法 $\mathcal{B}$ 對 BDDHE 問題有不可忽略的優勢，由於空間限制，且此證明由[8]之證明衍生出來，此處省略此證明，詳細證明請見論文完整版[9]。 ∎



圖一、匿名廣播加密系統安全性證明之攻擊模型

係定理 2. 若 BDDHE 問題是計算上不可分辨的，則廣義的匿名廣播加密系統 $\mathcal{S}$ 是 (Anon, Sel, CPA)-secure。

在一個 (Anon, Sel, CPA) 賽局中，一個攻擊匿名廣播加密系統 S 的攻擊者 $\mathcal{A}$ 收到 $\boldsymbol{c}^*$ 後，挑選 ID_a、$\mathrm{ID}_b \in S_0$，如果他可以判斷 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$，則代表識別字串集合 S_0 可解密文 $\boldsymbol{c}^*$，反之識別字串集合 S_1 可解。因此，爲了補強定理 1 ，必須證明不存在演算法 $\mathcal{A}$ 可分辨是否 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$。

引理 3. 假設 BDDH 問題是計算上不可分辨的，對於所有機率式多項式時間的演算法 $\mathcal{A}$ ，給定 (PP, $\boldsymbol{y}_m$, g^u, R, V_a, V_b) 判斷 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$ 或 $\langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle$ 是計算上不可分辨的。

證明: 假設存在一個機率式多項式時間的演算法 $\mathcal{A}$，滿足 $|\ \Pr[\mathcal{A}(\mathrm{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle] - \Pr[\mathcal{A}(\mathrm{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle]\ | \geq \epsilon$ ，亦即假設 $\mathcal{A}$ 有不可忽略的優勢可以成功地由公開的密文及 ID_a、ID_b 的仿射空間 V_a、V_b 判斷是否 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$，運用 $\mathcal{A}$ 我們建構一個可以分辨 BDDH 問題的演算法 $\mathcal{B}$ 如下：

模擬者 $\mathcal{B}$ 從一個 BDDH 問題得到 p、$\mathbb{G}$、$\mathbb{G}_T$ 和 (g^a, g^b, g^c, z)。首先 $\mathcal{B}$ 挑選 $g^{a_0} \in_R \mathbb{G}$、$g^{\boldsymbol{a}} \in_R \mathbb{G}^n$、$t \in_R \mathbb{G}_T$、$a_2, a_3, ..., a_n \in_R \mathbb{Z}_p$，然後計算公開參數 PP := $(p, \mathbb{G}, \mathbb{G}_T; g, g^{a_0}, g^{\boldsymbol{a}}, g^{\boldsymbol{a}_1} := (g^a, g^{a_2}, ..., g^{a_n}), t, t_1 := g^{b_1} = g^b)$

針對任意的 ID_a、ID_b，$\mathcal{B}$ 挑選 $\boldsymbol{y}_m \in_R {\mathbb{Z}_p}^n$、令 $g^u := g^c$，根據 $\boldsymbol{v}_i = M_i\ \boldsymbol{y}_m + \boldsymbol{x}_i$ 計算 $\boldsymbol{v}_a := (v_{a1}, v_{a2}, ..., v_{an})$、$\boldsymbol{v}_b := (v_{b1}, v_{b2}, ..., v_{bn})$，其中 M_i 爲 $n \times n$ 的矩陣，$\boldsymbol{x}_i \in {\mathbb{Z}_p}^n$。$\mathcal{B}$ 計算 $\alpha := \langle (v_{a2}, v_{a3}, ..., v_{an}),\ (a_2, a_3, ..., a_n)\rangle$, $\beta := \langle (v_{b2}, v_{b3}, ..., v_{bn}),\ (a_2, a_3, ..., a_n)\rangle$，因爲 $r_{1,a} = e(g^{b_1\langle \boldsymbol{v}_a, \boldsymbol{a}_1\rangle}, g^u) = e(g,g)^{(v_{a1}a+\alpha)b_1u} = (e(g,g)^{ab_1u})^{v_{a1}} \cdot (e(g,g)^{b_1u})^{\alpha} = (e(g,g)^{abc})^{v_{a1}} \cdot e(g^b, g^c)^{\alpha}$ 且 $r_{1,b} = e(g^{b_1\langle \boldsymbol{v}_b, \boldsymbol{a}_1\rangle}, g^u) = e(g,g)^{(v_{b1}a+\beta)b_1u} = (e(g,g)^{ab_1u})^{v_{b1}} \cdot (e(g,g)^{b_1u})^{\beta} = (e(g,g)^{abc})^{v_{b1}} \cdot e(g^b, g^c)^{\beta}$ ，如果 $z = e(g,g)^{abc}$ 則 $r_{1,a} = z^{v_{a1}} \cdot e(g^b, g^c)^{\alpha}$、$r_{1,b} = z^{v_{b1}} \cdot e(g^b, g^c)^{\beta}$，所以 $\mathcal{B}$ 計算 $h(r_{1,a}) = h(z^{v_{a1}} \cdot e(g^b, g^c)^{\alpha})$、$h(r_{1,b}) = h(z^{v_{b1}} \cdot e(g^b, g^c)^{\beta})$。

$\mathcal{B}$ 挑選 $R := (r_2, r_3, ..., r_n) \in {\mathbb{Z}_p}^{n-1}$ 滿足 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$，並將 (PP, $\boldsymbol{y}_m, g^u, R, V_a, V_b$) 傳送給 $\mathcal{A}$。若 $\mathcal{A}$ 輸出 $\zeta \in \{0,1\}$ 則 $\mathcal{B}$ 也輸出 ζ。

BDDH 攻擊者的優勢如下：

1) $z = e(g,g)^{abc}$: $\Pr[\mathcal{B}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{P}_{BDDH}]$ = $\Pr[\ \mathcal{A}(\mathrm{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle]$
2) $z \in_R \mathbb{G}_T$: $\Pr[\mathcal{B}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{R}_{BDDH}]$ = $\Pr[\mathcal{A}(\mathrm{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle]$

$\Rightarrow$ BDDH $\mathrm{Adv}_{\mathcal{B}}(\lambda)$:=

$$|\ \Pr[\mathcal{B}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{P}_{BDDH}] - \Pr[\mathcal{B}(\boldsymbol{x}) = 1 : \boldsymbol{x} \in_R \mathcal{R}_{BDDH}]\ | =$$
$$|\ \Pr[\mathcal{A}(\mathrm{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 :$$

$$\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle] - \Pr[\mathcal{A}(\text{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle] \mid \geq \epsilon$$

在 BDDH 問題很困難的假設下，BDDH $\text{Adv}_{\mathcal{B}}(\lambda)$ 爲一個可忽略的函數，因此不存在演算法 $\mathcal{A}$ 使得 $\mid \Pr[\mathcal{A}(\text{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle] - \Pr[\mathcal{A}(\text{PP}, \boldsymbol{y}_m, g^u, R, V_a, V_b) = 1 : \langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle] \mid \geq \epsilon$ ，ϵ 爲一個不可忽略的函數。 ∎

由加密演算法 Encrypt(PP, S, m) 可以看出 key 跟信息 m 與 (c_1, c_2, c_3) 是完全獨立的，因此證明時演算法 $\mathcal{A}$ 不需要知道 (m, c_1, c_2, c_3)。此外計算 key 時不需要公開參數 $(g^{a_0}, g^{\boldsymbol{a}}, t)$，所以我們直接挑選 $g^{a_0} \in_R \mathbb{G}$、$g^{\boldsymbol{a}} \in_R \mathbb{G}^n$、$t \in_R \mathbb{G}_T$，而不需先挑選 $a_0 \in_R \mathbb{Z}_p$、$\boldsymbol{a} \in_R {\mathbb{Z}_p}^n$、$b \in_R \mathbb{Z}_p$ 再計算 g^{a_0}、$g^{\boldsymbol{a}}$、$t = e(g, g)^b$。

BDDH 假設比 BDDHE 假設弱，亦即若存在一個演算法 $\mathcal{A}$ 可分辨 BDDH 問題，則存在一個演算法 $\mathcal{B}$ 可分辨 BDDHE 問題。$\mathcal{B}$ 從一個 BDDHE 問題中得到 (g, $\mathbb{G}$, $\mathbb{G}_T$; $g^{\alpha^{[0,n-1]}}$, $g^{\alpha^{[n+1,2n]}}$, h, z)，傳送 (g, $\mathbb{G}$, $\mathbb{G}_T$; $g^a := g^\alpha$, $g^b := g^{\alpha^{n-1}}$, $g^c := h$, z) 給 $\mathcal{A}$，若 $\mathcal{A}$ 可分辨 $z = e(g, g)^{abc}$ 或 $z \in_R \mathbb{G}_T$ 則 $\mathcal{B}$ 可分辨 $z = e(g, h)^{\alpha^n}$ 或 $z \in_R \mathbb{G}_T$。

密文 $\boldsymbol{c}$ 中無法直接得到識別字串的集合 S，而上面證明中如果沒有密鑰 K_{V_a}、K_{V_b} 則在多項式時間內判斷 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$ 或 $\langle R_a, \boldsymbol{v}_a\rangle \not\equiv \langle R_b, \boldsymbol{v}_b\rangle$ 是計算上不可分辨的，推得可解密 $\boldsymbol{x}_e$ 的密鑰 key 具有私密性，因爲假設存在一個演算法可在多項式時間算出 $key \equiv \langle R_i, \boldsymbol{v}_i\rangle$，$i \in \{1, 2, ..., k\}$，則可判斷是否 $\langle R_a, \boldsymbol{v}_a\rangle \equiv \langle R_b, \boldsymbol{v}_b\rangle$。

若 $\mathcal{SE}$ 爲一個在弱於 BDDHE 假設 (例如 BDDH 假設) 下安全的對稱式加密系統，則我們的系統在 BDDHE 問題是困難的假設下是安全的。

在一個具有適應式 (Adaptive) 安全性的賽局中，$\mathcal{C}$ 可以自由地決定公開參數，$\mathcal{A}$ 在質疑階段時才挑選並傳送 S_0, S_1 給 $\mathcal{C}$。[12] 中提出一種折衷的半靜態 (Semi-Static) 安全性，並提出一種雙金鑰的系統設計方法，可以把具有半靜態安全性的廣播加密系統，轉換爲具有適應式安全性的廣播加密系統，本文中的系統也可以做類似的擴充。

五、結論

本論文基於 Boneh 的“空間加密法” 設計一個隱藏廣播對象的機制，成爲一個具有匿名性、基於身分識別的廣義廣播加密系統，這個系統可以應用在需要動態指定可解密者的醫療資料庫系統中。假設 BDDHE 問題是計算上困難的，本文在標準模型下證明此匿名廣播系統的安全性。

六、致謝

本論文相關研究承蒙中華電信研究所 (計畫編號:TL-98-1501) 及行政院國科會 (計畫編號:NSC 97-2221-E-019-014) 經費補助, 得以順利完成, 特此致謝。

七、參考文獻

[1] N. Attrapadung and H. Imai, “Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations”, in *Asiacrypt’05*, LNCS 3788, pp. 100–120, 2005.

[2] N. Attrapadung, K. Kobara, and H. Imai, “Sequential key derivation patterns for broadcast encryption and key predistribution schemes”, in *Asiacrypt’03*, LNCS 2894, pp. 374–391, 2003.

[3] S. Berkovits, “How to broadcast a secret”, in *Eurocrypt’91*, LNCS 547, pp. 535–541, 1991.

[4] D. Boneh. and X. Boyen, “Efficient selective-ID secure identity based encryption without random oracles”, in *Eurocrypt’04*, LNCS 3027, pp. 223–238, 2004.

[5] D. Boneh, X. Boyen, and E. Goh, “Hierarchical identity based encryption with constant size ciphertext”, in *Eurocrypt’05*, LNCS 3494, pp. 440–456, 2005.

[6] D. Boneh and M. K. Franklin, “Identity based encryption from the Weil pairing”, in *SIAM Journal on Computing*, 32(3), pp. 586–615, 2003.

[7] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys”, in *Crypto’05*, LNCS 3621, pp. 258–275, 2005.

[8] D. Boneh and M. Hamburg, "Generalized identity based and broadcast encryption schemes", in *Asiacrypt'08*, LNCS 5350, pp. 455–470, 2008.

[9] S. W. Chang, "Generalized anonymous broadcast encryption scheme", in http://140.121.140.23/cgi-bin/cdrfb3/gsweb.cgi?o=dstdcdr, 2009.

[10] A. Fiat and M. Naor, "Broadcast encryption", in *Crypto'93*, LNCS 773, pp. 480–491, 1994.

[11] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography", in *Asiacrypt'02*, LNCS 2501, pp. 548–566, 2002.

[12] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems", in *Eurocrypt'09*, LNCS 5479, pp. 171–188, 2009.

[13] M. T. Goodrich, J. Z. Sun, and R. Tamassia, "Efficient tree-based revocation in groups of low-state devices", in *Crypto'04*, LNCS 3152, pp. 511–527, 2004.

[14] J. Horwitz and B. Lynn, "Towards hierarchical identity-based encryption", in *Eurocrypt'02*, LNCS 2332, pp. 466–481, 2002.

[15] R. Sakai and J. Furukawa, "Identity-based broadcast encryption", in *Cryptology ePrint Archive*, Report 2007/217, available at http://eprint.iacr.org/2007/217.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes", in *Crypto'84*, LNCS 196, pp. 47–53, 1984.