臺東大學綠色科學學刊　第八卷第二期

2018 年，8（2），1 - 14

可選擇連結之匿名分享資訊機制

劉南軒、李維斌、簡楷帆、張辰德

摘要

隨著智慧行動裝置以及線上社交網站的誕生，社群媒體已漸漸地成為網路使用者獲得資訊的來源，越來越多使用者在網路上尋找健康相關的資訊，許多健康相關的社群媒體也開始興起。在健康社群媒體上，病患或是家屬能夠透過經驗分享的方式來幫助擁有類似問題的病患，醫療人員也能藉由病患所分享的經驗來改善自己的治療方式。健康相關資訊是屬於敏感的資料，分享於具有保留與散布特性的社群媒體需要經過匿名的方式才不會造成個人隱私的暴露。然而若是匿名機制不具有連結性，對於其他使用者來說無法觀察完整的病患經驗分享。但若是使用具有連結性的匿名機制使得任何人都能夠追蹤使用者所分享的資訊。因此本論文將提出一個可選擇連結性的匿名分享資訊機制，除了保護使用者分享資訊的匿名性外，也提供使用者在匿名分享的時候能夠選擇是否連結過去匿名分享的資訊。

關鍵字：社群媒體、匿名分享資訊、可選擇連結性

劉南軒，逢甲大學資訊工程學系。E-mail: b020306123@gmail.com

李維斌，逢甲大學資訊工程學系。E-mail: wblee@mail.fcu.edu.tw

簡楷帆，逢甲大學資訊工程學系。E-mail: kaifanchien@gmail.com

張辰德，逢甲大學資訊工程學系。E-mail: chad531206@gmail.com

臺東大綠色科學學刊　2018，8(2)，pp. 1~14

Green Science & Technology Journal

2018 年，8（2），1 - 14

An Anonymous Information Sharing Mechanism with Selective Linkability

Nan-Hsuan Liu & Wei-Bin Lee& Kai-Fan Chien&Chen-Te Chang

Abstract

With the emergence of social networks, social media has become a source of information for Internet users. Users start looking for health-related information through the Internet. And there are more and more health community platforms constructed. With the health community platforms, patients and their family could help other patients with similar problems through experience sharing. Medical personnel could also improve the therapies through the experience shared by patients.

Patients' health-related information are sensitive, sharing information in social media which has the retention and distribution characteristics requires an anonymous approach that does not expose personal privacy. However, if the anonymity mechanism is not linkable, it is impossible for other users to observe the complete sharing of patient experience. But if it uses a linkable anonymous mechanism, anyone can track all the information shared by users. Therefore, this paper has proposed an anonymous information sharing mechanism with selective linkability. In addition to protecting the users' anonymity while sharing information, users can also choose whether to link the shared information while sharing anonymously.

Keywords：Social media, Anonymous information sharing, Selective linkability

---

Nan-Hsuan Liu , Department of Information Engineering and Computer Science。E-mail: b020306123@gmail.com

Wei-Bin Lee, Department of Information Engineering and Computer Science。E-mail: wblee@mail.fcu.edu.tw

Kai-Fan Chien, Department of Information Engineering and Computer Science。E-mail: kaifanchien@gmail.com

Chen-Te Chang, Department of Information Engineering and Computer Science。E-mail: chad531206@gmail.com

一、 緒論

傳統的報章雜誌與電視新聞作為一個單向傳播資訊的媒體，每個使用者被迫只能當一個資訊的接收者。隨著網路以及社群媒體的出現打破了這個限制，除了傳播資訊的種類與內容變得更多元，任何社群媒體的使用者都能夠發表自己的意見參與討論，甚至創造資訊並利用朋友之間的分享機制散佈出去，搖身一變成為事件的主角。除此之外，智慧型行動裝置的出現與普及，更縮短了使用者存取資訊的時間與難度，加速了社群媒體的發展，如今社群媒體已經是生活中不可或缺的一部分。

(一) 背景

上網搜尋健康相關資訊可以讓病患在與醫生會診之前做準備以了解會診時接收到的資訊，也能補充在會診時醫生未提供的部分資訊，對於會診與治療的內容和結果，病患也能利用搜尋到的資訊進行驗證與質疑[1]，讓病患更能掌握疾病資訊了解自己的健康狀況。除此之外，網路也為那些行動不便，以及受限於地理因素如偏鄉地區等不易獲得資訊的病患，提供訊息的來源；或是提供一個環境，讓那些患有難以啟齒的疾病而不願露面的病患有一個尋求協助的管道[2]，吸引許多人網尋找健康相關的資訊[3]。

隨著社群媒體的興起，社群媒體的使用者在過去十年間不斷地增加[4]，到 2016 年社群媒體的使用者已多達 20 多億[5]；使用者平均一個人花費在社群媒體上的時間超過六個小時，並且有上升的趨勢[6]；同時根據皮尤研究中心的調查[7]指出，由社群媒體獲得訊息、事件和議題的使用者越來越多，在 2015 年的時候達到了 63%，顯示社群媒體已成為重要的訊息來源。由此可知，社群媒體是一個聽眾多、黏著性高，且被重視的管道。加上 PwC 研究中心的調查結果[8]顯示，有 45%的使用者會參考社群媒體上的健康資訊尋找二次醫療諮詢；56%的中年人利用社群媒體流覽健康資訊；而高達 90%的年輕人相信社群媒體上獲得的健康相關資訊。顯示社群媒體也成了健康資訊的重要來源。

使用者除了可以在社群媒體裡獲取健康資訊，也能夠透過分享自身的健康相關資訊來提升大眾的健康。目前有許多以分享健康資訊為目的的社群網站開始興起，例如讓使用者上傳運動數據與朋友作比較，利用闖關和社交競賽等機制激勵使用者保持運動[9][10]；或是建立一個病友圈，讓病患與家屬能彼此分享患病與照護的經驗，除

了提供擁有相同疾病或是類似病情的病友與家屬作為治療的參考，也能夠提供情緒上的支持，提升病患康復的生活品質，並激勵那些慢性疾病的患者能夠持之以恆地進行健康管理[11][12]；有些社群網站[13][14]則是蒐集病患大量貢獻的健康數據交由不同團體進行研究，開發更優良的治療方式或設備。這些健康社群媒體都以使用者分享健康相關的資訊或數據做為基礎，進而達到維持或促進大眾健康的目的。

(二) 研究動機

然而健康相關資訊屬於個人的敏感性資料，如果沒有妥善處理，將造成個人隱私的洩漏。文獻[15]曾對 2125 名 PatientsLikeMe 會員進行問卷調查，有 76%的使用者擔心他們分享在社群媒體上的健康資訊在不知情的情況下被使用；分別有 74%與 66%的使用者擔心資訊洩漏後會失去醫療照護福利以及工作機會。世界醫師協會白皮書[16]指出，社群媒體具有保留與散布資訊的特性，任何使用者過去所發表的言論或內容都會存留在網路上。曾經有名病患因在社群媒體上發布照片的內容而失去保險給付[17]。而有越來越多的雇主會上網尋找求職者相關的資訊[18]，這些資訊也包括敏感的健康資訊，這些求職者的健康資訊有可能會讓雇主不願意雇用求職者，使他們失去工作機會。由此可知，使用者在社群媒體上分享自身相關的健康資訊，例如：患病的經驗、服用過的藥物或是目前的身體狀況等資訊，都有可能會對使用者的現實生活產生負面的影響，造成使用者不願意在社群媒體上進行健康資訊的分享。然而根據[15]的調查結果顯示，在擁有適當匿名性的保護之下，有高達 94%的受訪者願意分享他們的健康資訊提供醫生研究，進而幫助其他擁有類似病情的病患，改進治療的方式。因此，為了讓社群媒體使用者願意分享其健康相關的資訊，以幫助提昇社會大眾的健康，在社群媒體使用者分享自身的健康資訊時，需要一個匿名的機制保護社群媒體使用者的身份。

當社群媒體使用者違反社群媒體的規範，或是因發表內容而引起法律糾紛，甚至是使用者透露出想要輕生的念頭時，社群媒體需要知道這些使用者的身份以便對使用者進行究責或是及時拯救使用者以避免悲劇發生，因此在經過社群媒體管理者的判斷後，匿名機制必須有能力揭露社群媒體使用者的真實身份。然而匿名性對使用者而言至關重要，將揭露身份的權力交由單一管理者並不適當；加上社群媒體可能發生複雜的特殊情況，需要多人的討論才能夠做出適當的決定，因此在社群媒體打算揭露使用者的真實身份時，若能透過多個管理者以門檻值的方式合作，將能避免少數不當的管

理者隨意揭露使用者真實身份的風險，也讓所有揭露與否的決定更加公正。

除了揭露社群媒體使用者真實身份的機制之外，還要考慮到匿名機制的連結性。連結性是指不同事物之間如行為、文章、簽章等，其來源是否相同。對於社群媒體來說，如果使用的是具有連結性的匿名機制，代表其他使用者能夠判斷兩則匿名分享的訊息是否由同一發文者所分享；而使用不具有連結性的匿名機制則無法判斷訊息的來源是否相同。也就是說，當社群媒體管理者在不具有連結性的匿名機制中揭露某一個匿名分享資訊的使用者身份時，只有該分享資訊不再有匿名性，而該使用者所分享的其他資訊仍然保持匿名性，管理者若要知道該使用者所分享的其他資訊，則必須重覆揭露其他匿名分享的資訊，確認分享者的身份是否為該使用者；若社群媒體使用的是具有連結性的匿名機制時，因為來自相同使用者分享的資訊會被連結起來，所以當管理者揭露某一個匿名分享資訊的使用者身份時，管理者同時也知道該使用者所分享的其他資訊，而無需重複揭露其他匿名分享資訊的使用者身份。

雖然具有連結性的匿名機制能夠讓社群管理者解開使用者的真實身份後有足夠的資訊進行究責，但是某些情況下只需要使用者的真實身份即可。例如當使用者透露出輕生念頭的時候，為了避免悲劇發生，管理者將揭露該使用者的真實身份。在此種情況下，管理者的首要目標是使用者的真實身份，該使用者過去所分享的資訊對於避免其輕生未必有所幫助。然而在具有連結性的匿名機制下，管理者除了能夠取得使用者的身份，同時也得知該使用者過去所分享的資訊，導致管理者能夠獲得超過完成目標所需的資訊，暴露了使用者的隱私。因此社群媒體管理者在揭露使用者的真實身份時，若能視情況來決定是否進一步進行連結，更能夠保障使用者的隱私。

根據上述的環境，歸納出下列需求：

1. 不可連結之匿名機制：為了提高使用者分享自身健康相關經驗的意願，需要一個匿名機制來保護使用者的隱私，而為了避免社群媒體管理者在揭露使用者身份時獲得額外的資料，此匿名機制必須是不具有連結性。
2. 門檻式揭露身份：當社群媒體使用者有特殊情況發生時，管理者將以門檻式合作的方式揭露使用者的真實身份。
3. 可選擇性連結：當管理者除了使用者的真實身份以外，還需要使用者所分享的資訊進行究責時，管理者能夠更進一步地對該使用者進行連結。

(三)　論文架構

介紹本研究的背景與動機之後，第二章將會介紹使用到的概念與技術，之後在第三章提出可選擇連結之匿名分享資訊機制，第四章是該機制的安全性分析。最後第五章則是提出的結論及對此研究的未來展望。

二、 先備知識

此章節將介紹本論文提出的匿名機制中所使用的方法與背景知識。首先會介紹群簽章的特性、組成以及需求；最後介紹(t, n)門檻值秘密分享方法的特性，及其如何進行秘密的分享與還原。

(一) 群簽章

群簽章[19]是 David Chaum 等學者於 1991 年所提出的概念，這種簽章能夠讓群體內的成員以群體的名義簽署訊息。任何人都能夠驗證簽章的合法性，但無法得知切確的簽章者身份，只能確定該簽章由群體內的成員所簽署。而當爭議發生的時候，群體內只有管理員有能力撤銷該簽章的匿名性以得知簽章者的真實身份。

一個群簽章的架構由五個步驟所組成：系統設定、憑證產生、簽章、驗證以及揭露身份。系統設定階段會設定一些系統參數，並為每個群體內的成員產生各自的公私金鑰對；憑證產生階段是群體管理員使用自己的私密金鑰以及給予憑證之群體成員的公開金鑰，產生與該群體成員之公開金鑰相對應的簽章憑證；簽章階段利用群體成員的私密金鑰、簽章憑證對訊息進行簽章；驗證階段以群體管理員的公開金鑰、簽署的訊息對相對應的簽章進行驗證，只有產生通過驗證與否兩種結果；揭露身份階段則是以管理者的私鑰對通過驗證的簽章與訊息揭露簽章者的公開金鑰。

一般群簽章會有以下需求：

1. 正確性：必須要讓一個經過誠實合法使用者所產生的簽章能夠被正確地驗證合法性。
2. 不可偽造性：只有群體中的成員能夠產生出合法的群簽章，任何群 體外的人都無法代表該群體簽署訊息。
3. 匿名性：除了群體管理者以外，任何人都無法得知簽章者的真實身份。
4. 可追蹤性：只有群體管理者有能力撤銷該簽章的匿名性，揭露簽章者的真實身份。

(二) (t, n)門檻值秘密分享

Shamir 等學者於 1979 年提出了一個(t, n)門檻值的秘密分享機制[20]，將秘密訊息本身或是用來加密訊息的金鑰分割成 n 個部分發給 n 個秘密的共享者。當需要還原這項秘密訊息的時候，必須集合至少 t 個共享者才能夠正確地還原。

在分發的階段中，秘密的擁有者先建構一個$(t-1)$次方的多項式 $f(x)$，並將欲分享的秘密做為多項式的常數項，接著為 n 個秘密共享者選擇不同的 x_i 並帶入多項式 $y_i = f(x_i)$獲得。最後將秘密分享金鑰(x_i, y_i)透過安全通道分發給秘密的共享者，並且將多項式 $f(x)$銷毀不做記錄。

在還原秘密訊息的階段，首先必須集合至少 t 個共享者的秘密共享金鑰(x_i, y_i)，利用 Lagrange 內插法還原多項式：$f(x) = \sum_{i=1}^{t}(y_i \prod_{j=1, j\neq i}^{t} \frac{x-x_j}{x_i-x_j})$，最後令 $x=0$ 代入 $f(x)$，即可還原秘密訊息。

三、研究方法

此章節將介紹本論文提出的匿名機制的系統架構以及流程與步驟。

(一) 系統架構

在此匿名機制中，有三個角色，分別是社群媒體服務提供商 P_r、社群媒體管理者 M_i 以及社群媒體使用者 U。每種角色所執行的動作如下：

1. 社群媒體管理者(M_i)：負責產生匿名分享的金鑰，以及在特殊情況下揭露與連結匿名分享者的身份。
2. 社群媒體服務提供商(P_r)：負責提供一般社群平台的服務以及系統參數的設定，同時利用(t, n)門檻值秘密分享的方式，將產生匿名分享金鑰以及追蹤的權力授權給社群媒體管理者 M_i 。
3. 社群媒體使用者(U)：向社群媒體管理者申請匿名分享金鑰之後，能夠在社群平台內進行匿名分享資訊。

此匿名機制的流程可以分為系統設定階段、申請分享金鑰階段、分享資訊階段、驗證階段以及追蹤與連結階段。在系統設定階段，由社群媒體服務提供商進行系統參數的設定，並且將產生匿名分享金鑰以及追蹤的權力授權給社群媒體管理者 M_i ；社

群媒體使用者 U 要匿名分享資訊之前，都必須執行申請分享金鑰階段，向社群媒體管理者 M_i 申請，再由 t 位管理者合作產生匿名分享所需的金鑰，使用者才能夠在分享訊息階段中進行匿名分享訊息；驗證階段則是進行匿名分享訊息的驗證，確認訊息的合法性；最後若是發生特殊情況需要追蹤或是進一步需要連結時，則由 t 位社群媒體管理者 M_i 合作，進行訊息作者的身份揭露與連結。

(二)　系統流程與步驟

以下將對本論文提出的可選擇連結之匿名分享資訊機制的流程進行詳細的步驟說明。

1. 系統設定階段

我們假設此系統已經包含一個 Public Key Infrastructure 負責維護社群媒體服務提供商 P_r 以及社群媒體使用者 U 的公私鑰，其中社群媒體服務提供商 P_r 的私密金鑰 x_{pr}，公開金鑰為 $y_{pr} = g^{x_{pr}} \pmod p$；社群媒體使用者 U 的私密金鑰 x_i，公開金鑰為 $y_U = g^{x_U} \pmod p$。p、q 為滿足 $q|p-1$ 的兩個大質數。

此階段由社群媒體服務提供商 Pr 進行系統的設定，步驟如下：

步驟一、計算 $D_{pr} = g^d \pmod p$，其中 $d \in Z_q$ 為隨機選擇數。

步驟二、計算 $\widetilde{x_{pr}} = x_{pr} + d \pmod q$。

步驟三、將 $\widetilde{x_{pr}}$ 作為追蹤的金鑰，並透過 (t,n)-*Threshold Secret Sharing* 的方式分享給所有的管理者 M_i，步驟如下：

(1) 建立 $(t-1)$ 次多項式 $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + \widetilde{x_{pr}} \pmod q$，其中 $a_{t-1}, \ldots, a_1 \in Z_q$。

(2) 將 x_i 帶入多項式得到 Secret Sharing 的私密金鑰 $y_i = f(x_i)$，其中 x_i 代表管理者 M_i 的 ID。

(3) 在安全通道下發給每個管理者 M_i 相對應的 Secret Sharing 的私密金鑰 y_i。

(4) 服務提供商 Pr 將多項式 $f(x)$ 銷毀不作記錄。

步驟四、計算 $\widetilde{y_{pr}} = g^{\widetilde{x_{Pr}}^{-1}} \pmod p$。

步驟五、公布 p、q、g、y_{pr}、$\widetilde{y_{pr}}$ 和 D_{pr} 作為系統參數。

2. 申請分享金鑰階段

使用者U進行匿名分享資訊之前會向管理者M_1申請分享金鑰，管理者M_1會與其他$(t-1)$個管理者M_i合作，產生新的匿名分享金鑰。

步驟一、使用者U計算$\widetilde{y_U} = \widetilde{y_{pr}}^{x_U} \pmod p$。

步驟二、使用者U將y_U和$\widetilde{y_U}$傳送給管理者M_1。

步驟三、管理者M_1將y_U傳送給其他管理者M_i。

步驟四、每位管理者M_i收到y_U後進行以下步驟：

(1) 計算$r_i \equiv g^{k_i} \pmod p$，其中$k_i \in Z_q$為隨機選擇數。

(2) 計算$e_i \equiv {y_U}^{k_i} \pmod p$。

(3) 計算$\widetilde{y_{pr_i}} \equiv \widetilde{y_{pr}}^{k_i} \pmod p$。

(4) 將r_i、e_i和$\widetilde{y_{pr_i}}$傳送給管理者M_1。

步驟五、管理者M_1收集完所有r_i、e_i和$\widetilde{y_{pr_i}}$進行以下步驟：

(1) 計算$R \equiv \prod_{i=1}^{t} r_i \pmod p$。

(2) 計算$E_1 \equiv \prod_{i=1}^{t} e_i \pmod p$。

(3) 計算$E_2 \equiv \widetilde{y_U} \cdot \prod_{i=1}^{t} \widetilde{y_{pr_i}} \pmod p$。

(4) 計算$\tilde{E} = h(E_1 \| E_2 \| R)$，其中$h(\cdot)$為一對一的單向雜湊函數。

(5) 將$\tilde{E}$傳送給其他管理者M_i。

步驟六、每位管理者M_i收到$\tilde{E}$後進行以下步驟：

(1) 計算

$$s_i \equiv k_i - \tilde{E} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \pmod q$$

(2) 將s_i傳送給管理者M_1。

步驟七、管理者M_1收集完所有s_i進行以下步驟：

(1) 計算$\tilde{S} \equiv \sum_{i=1}^{t} s_i \pmod q$。

(2) 將分享金鑰$(E_1, E_2, \tilde{E}, \tilde{S})$回傳給使用者$U$。

使用者U可以透過以下步驟來驗證分享金鑰$(E_1, E_2, \tilde{E}, \tilde{S})$的正確性：

(1) 計算$R_v \equiv g^{\tilde{S}} (y_{pr} \cdot D_{pr})^{\tilde{E}} \pmod p$。

(2) 計算$\tilde{E}_v = h(E_1 \| E_2 \| R_v)$。

(3) $\tilde{E}_v =? \tilde{E}$。

3. 分享資訊階段

當使用者U要匿名分享訊息m，會使用分享金鑰$(E_1, E_2, \tilde{E}, \tilde{S})$對訊息$m$進行匿名簽章，供社群媒體管理者驗證其分享資訊的合法性，步驟如下：

步驟一、計算$\alpha \equiv g^{\tilde{S}}(y_{pr} \cdot D_{pr})^{\tilde{R}} \ (mod\ p)$。

步驟二、計算$r \equiv R^{a} \ (mod\ p)$，其中$a \in Z_q$為隨機選擇數。

步驟三、計算$e = h(m \| r)$。

步驟四、計算$s \equiv a - ex_U \ (mod\ q)$。

步驟五、完成後的簽章為$\sigma = ((E_1, E_2, \tilde{E}, \tilde{S}), e, s)$。

4. 驗證階段

任何人都能夠利用以下步驟驗證簽章$\sigma = ((E_1, E_2, \tilde{E}, \tilde{S}), e, s))$對訊息$m$的合法性：

步驟一、　計算$R \equiv g^{\tilde{S}}(y_{pr} \cdot D_{pr})^{\tilde{E}} \ (mod\ p)$。

步驟二、計算$V \equiv E \cdot R^{-1} \ (mod\ p)$。

步驟三、計算$r_v \equiv V^{e} R^{s} \ (mod\ p)$

步驟四、計算$e_v = h(m \| r_v)$。

步驟五、檢查$e_v =? e$，若相等表示此簽章為合法的匿名簽章。

5. 追蹤與連結階段

為了得知兩個簽章$\sigma = ((E_1, E_2, \tilde{E}, \tilde{S}), e, s)$與$\sigma'' = ((E''_1, E''_2, \tilde{E}'', \tilde{S}''), e'', s'')$是否由同一使用者所產生，管理者首先檢驗兩份簽章的合法性。若兩份簽章皆通過驗證，管理者M_1會與其他$(t-1)$個管理者M_i合作，對兩份簽章進行連結，步驟如下：

步驟一、　管理者M_1將E_2和E''_2傳送給其他管理者M_i。

步驟二、　每位管理者M_i收到E_2和E''_2進行以下步驟：

1. 計算$E_{2_i} \equiv E_2^{\,y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i}} \ (mod\ p)$。
2. 計算$E''_{2_i} \equiv E''_2{}^{\,y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i}} \ (mod\ p)$。

步驟三、　將E_{2_i}和E''_{2_i}回傳給管理者M_1。

步驟四、　管理者M_1收集完所有E_{2_i}和E''_{2_i}進行以下步驟：

(1) 計算$R \equiv g^{\tilde{S}}(y_{pr} \cdot D_{pr})^{\tilde{E}} \ (mod\ p)$

(2) 計算$y_{U_1} \equiv R^{-1} \prod_{i=1}^{t} E_{2_i} \ (mod\ q)$。

(3) 計算$R'' \equiv g^{\tilde{S}''}(y_{pr} \cdot D_{pr})^{\tilde{E}''} \ (mod\ p)$

(4)　計算$y_{U_2} \equiv R''^{-1} \prod_{i=1}^{t} E''_{2_i} \ (mod\ q)$。

(5) 比較$y_{U_1} =? y_{U_2}$，若相等，代表σ與σ''的簽章者是同一人。

四、安全性分析

(一) 正確性

一個合法使用者所產生的簽章$\sigma = ((\tilde{S}, \tilde{E}, \widetilde{S'}, \widetilde{E'}, A, B), s'', e'', h(m))$，必能夠被正確地驗證合法性，在本論文的方法中，若簽章是經過誠實合法的方式產生，則必能滿足關係式$\alpha_U{}^{s''} \cdot DH_U{}^{e''} \cdot g^{h(m)} \equiv e'' \pmod p$，其證明如下：

$\alpha_U{}^{s''} \cdot DH_U{}^{e''} \cdot g^{h(m)} \equiv e'' \pmod p$

$\equiv \alpha_U{}^{k''} \cdot g^{h(m)}$

$\equiv e'' \pmod p$。

(二) 不可偽造性

在系統中，使用者若想要匿名分享訊息時，必須擁有簽章憑證才能夠產生合法的匿名簽章，而簽章憑證必須成為群體中的合法成員，才能夠在申請簽章憑證的階段中才能夠獲得簽章憑證。因此，非群體成員的攻擊者只能透過偽造的方式來產生簽章憑證。

然而要產生簽章憑證必須知道服務提供商 P_r 的私密金鑰 X_{Pr}，在我們的假設之中，群體成員中的任何人包括管理者，其私密金鑰是絕對無法被攻擊者所得知。而在「申請簽章憑證階段」或是「連結匿名簽章階段」中，由許多管理者合作還原服務提供商 P_r 的私密金鑰 X_{Pr} 皆以指數的方式傳送，即使攻擊者獲得傳送的資料內容，也無法還原出私密金鑰 X_{Pr}，其難度相當於解離散對數之難題。故不是該群體成員中的攻擊者，無法偽造簽章憑證，也無法產生合法的匿名簽章。

(三) 匿名性

使用者的匿名簽章$\sigma = ((\tilde{S}, \tilde{E}, \widetilde{S'}, \widetilde{E'}, A, B), s'', e'', h(m))$之中，只有$\tilde{E}$與 B 包含簽章者的身份資訊，然而攻擊者若想要自$\tilde{E}$與 B 計算出簽章者的真實身份，其難度等同於解離散對數之難題，攻擊者無法有效計算出簽章者的真實身份，故簽章者保有其匿名性。

(四)　(t, n)門檻值可追蹤性

本論文的方法是利用 Diffie–Hellman 的方式將簽章者的身份加密，必須擁有服務提供商 P_r 的私密金鑰 x_{Pr} 才能夠揭露簽章者的身份。而群體管理員們能夠透過秘密分享的方式，蒐集 t 位管理員的秘密共享金鑰來還原提供商 P_r 的私密金鑰 x_{Pr}。

因此，在私密金鑰無法被得知的假設之下，只有群體的管理者能夠透過(t, n)門檻值的方式撤銷該簽章的匿名性，揭露簽章者的真實身份。

五、結論

在社群媒體分享健康資訊時，社群媒體是否擁有適當的身份保護將影響使用者分享健康資訊的意願，因此本論文提出一個匿名機制保護使用者的身份。

為了讓使用者更彈性地決定是否匿名分享資訊時是否具有連結性，本論文利用可重新申請憑證的方式讓使用者能夠決定是否與之前匿名分享的資訊作連結。而為了提昇重新申請機制的可用性，在申請簽章憑證階段採取(t, n)門檻值管理員合作的方式產生憑證，避免某些管理員不在線上而無法完成申請憑證階段的問題產生。

參考文獻

[1] Caiata-Zufferey, Maria, et al. (2010)."*Online health information seeking in the context of the medical consultation in Switzerland.*" Qualitative Health Research 20, 1050-1061.

[2] Griffiths, F., Lindenmeyer, A., Powell, J., Lowe, P., & Thorogood, M. (2006). *Why are health care interventions delivered over the internet? A systematic review of the published literature.* Journal of medical Internet research, 8(2).

[3] Fox, S., & Duggan, M. (2013). Health online 2013. Health, 1-55.

[4] Perrin, A. (2015). Social Media Usage: 2005-2015.

[5] We are social: Digital in 2016. Available: http://wearesocial.com/uk/special-reports/digital-in-2016

[6] Nielsen. (2011). State of the media: The social media report. Nielsen.

[7] Pew Research Center: Internet, Science & Technology. “The Evolving Role of News on Twitter and Facebook.” Available: http://www.journalism.org/files/2015/07/Twitter-and-News-Survey-Report-FINAL2.pdf (retrieved: 05/26/2016)

[8] PwC Health Research Institute, “Social media ‘likes’ healthcare: From marketing to social business.” Available: http://download.pwc.com/ie/pubs/2012_social_media_likes_healthcare.pdf

[9] Fitocracy[Online]. Available: https://www.fitocracy.com/ (retrieved: 05/26/2016)

[10] SocialRace[Online]. Available: https://www.socialrace.cc/ (retrieved: 05/26/2016)

[11] HealthKeep[Online]. Available: https://www.healthkeep.com/ (retrieved: 05/26/2016)

[12] CarePages[Online]. Available: https://www.carepages.com/ (retrieved: 05/26/2016)

[13] PatientsLikeMe[Online]. Available: https://www.patientslikeme.com/ (retrieved: 05/26/2016)

[14] SmartPatients[Online]. Available: https://www.smartpatients.com/ (retrieved: 05/26/2016)

[15] Social Networking Sites and the Continuously Learning Health System: A Survey. URL: http://nam.edu/wp-content/uploads/2015/06/VSRT-PatientDataSharing.pdf

[16] World Medical Association. (2012). JDN Social Media and Medicine [White Paper].URL: http://www.wma.net/en/30publications/35whitepapers/JDN_Social_media_white_paper_2012.pdf

[17] Depressed woman loses benefits over Facebook photos. URL: http://abcnews.go.com/Technology/AheadoftheCurve/woman-loses-insurance-benefits-facebook-pics/story?id=9154741

[18] Social Networking Privacy: How to be Safe, Secure and Social. URL: https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social#hindering-job-seekers

[19] Chaum, D., & Van Heyst, E. Group signatures. (1991). *In Workshop on the Theory and Application of of Cryptographic Techniques*, Springer Berlin Heidelberg, 257-265.

[20] Shamir, A. *“How to share a secret.” Communications of the ACM*, 22(11), 612-613.