網路諮商系統之安全機制設計

蘇品長[1] 郭文雄[2] 劉興漢[1*]

[1]國防大學管理學院資訊管理學系
[2]國防大學理工學院電機電子工程學系

摘　要

「輔導諮商工作」大多為諮商師與被輔導對象以面對面方式進行，隨著網路的普及與便利性，網路諮商系統不啻為一諮商輔導管道之選項。發展網路諮商系統，需考量如何有效保護使用者的隱私、避免其諮商內容及身分資料外洩，故安全性為建立網路諮商系統之重要選項。本研究為密碼系統之應用，以網路諮商與輔導系統為對象，使用橢圓曲線公開金鑰密碼學、盲簽章及網際網路單一簽入機制為基礎，設計網路諮商系統之安全機制；除了能提昇輔導諮商作業效率外，並能確保數位內容的安全，以營造一個安全有效率的電子化輔導諮商環境。

關鍵詞：網路諮商、橢圓曲線密碼系統、盲簽章、單一登入

Design of Security Mechanism for Web-based Counseling Systems

Pin-Chang Su [1], Wen-Hsiung Kuo[2], and Hsing-Han Liu [1*]

[1] *Department of Information Management, Management College, National Defense University*
[2] *Department of Electrical and Electronic Engineering, Chung-Cheng Institute of Technology, National Defense University*

ABSTRACT

Consulting psychology is a consultation process that involves a counselor and a client. A consulting psychologist typically provides specialized service to client individuals in regard to their problems like phobia or anxiety disorders. With the popularity and convenience of the Internet, web-based counseling is fast becoming one of counseling services. This type of counseling (e-counseling) is easily accessible to all those who wish to use it when compared to traditional counseling services as setting appointments. How to effectively protect the client or user's privacy and avoid identity-theft-related data breaches has become a critical issue for an online web counseling system. Thus, this paper presents a single sign-on blind signature scheme based on elliptic curve cryptography (ECC) to achieve a more robust security and efficiency cryptosystem for the accessibility of online counseling. Furthermore, our estimation results indicate that the proposed scheme can achieve excellent performance at web counseling. With such an appropriate design, the scheme will certainly lead to more effective and efficient safeguards for consulting psychology.

Keywords: Web-based Counseling, Elliptic Curve Cryptosystem, Blind-Signature, Single Sing- On

文稿收件日期 104.10.13;文稿修正後接受日期 105.7.7; *通訊作者
Manuscript received October 13, 2015; revised July 7, 2016; * Corresponding author

一、前　言

隨著網際網路的快速發展，網路行為漸漸成為生活的一部分，舉凡工作、學習、休閒、購物等活動皆可透過網路來進行，諮商輔導議題亦不例外；利用網路特質，協助一些不善語言表達、身體不便、交通不便或不願意到輔導機構面對面諮商的一些群體，進行網路諮商。網路諮商是一種在合格且具專業倫理的專業人員協助下透過與當事人的互動，以尋求解決問題與提昇心理效能的專業服務，主要運用的方式是透過網路為媒介，並在專業人員的協助與引導下，逐次探討相關的個人資料與經驗，省視與分析相關問題的癥結與成長障礙，以找出解決的方法與因應之道，進而開發個人潛能、提昇心理的效能。如何善用網路科技，精進網路諮商系統，提升輔導諮商的工作效率，值得研究與探討。

要做好心輔工作首先需要了解到諮商關係與保密原則之間，有著非常緊密的連結。諮商本質上是保密的(Confidential)，它的目的是在協助人們聚焦於其所關注的問題，規劃策略以處理特定的議題，並評鑑執行這些計畫的成功與否。如果當事人沒有隱私，諮商就不能期待他們要透露自己尷尬的事情、一些個人的創傷事件和在治療中的一些資訊，故網路諮商服務系統安全機制之完備與否，為該系統規劃考量選項之一。諮商服務流程一旦由人工作業處理流程轉變於網路的虛擬環境時，如何有效保護當事人的隱私，避免其網路諮商服務內容曝露，為網路諮商系統關鍵的成功因素。

網路諮商系統應具有不受距離因素影響、可即時回應、個案初次受輔較易接受等特色外，網路諮商系統能否被當事人接受，關鍵因素在於系統能否保護當事人的資料安全及隱私[1]，若信賴度不足則很容易讓當事人對其失去信心，影響使用者對該系統的使用態度與意願。故網路諮商系統的安全性問題被列為影響網路諮商系統的外部變數之一[2] [3] [5] [6]。國內的相關學者亦提出諸多網路諮商的探討及應用[4] [7] [8]，對安全的網路諮商系統設計則尚無完整的設計。本研究將就網路諮商過程中使用者的身分認證及諮商資料隱匿的安全性部分，應用密碼學相關技術謀求建立無洩露個人隱私之憂的網路諮商環境。

本文各章節部分安排如下：在第二節，彙整本研究相關文獻及技術之探討。第三節中，提出本研究方法演算法過程。第四節中，分析本方法之安全性分析並與現行諮商作法作效益比較。最後，第五節為本文之結論。

二、文獻探討

本節將就本文所探討的網路諮商與所應用的相關技術－橢圓曲線公鑰密碼系統、盲簽章及網際網路單一登入機制做簡略介紹。

2.1 網路諮商

根據 1998 年全美合格諮商師協會（National Board for Certified Counselor）的定義：「當諮商師與分隔兩地或身處遠方的當事人運用電訊方式在網路上溝通時，所從事之專業諮商與資訊提供之實務工作」，從以上的定義得知，網路諮商是以網路做為中介的溝通平台，讓諮商師與當事人得以不受距離、時間限制等因素得以順利完成諮商服務的方式，當事人可藉由此平台的設置，於諮商的過程中，心理上較不需承受面對一位陌生人（諮商師）做自我表露的壓力，對於個人隱私、禁忌話題，可較坦然的表述。常見的網路諮商方式有電子郵件、文字聊天室與視訊會議等 3 種[1] [2] [3]。國內的網路諮商應用實例方面，於民國 85 年高雄張老師諮商輔導中心首先以電子布告欄系統（BBS），隔年增加以電子郵件的服務，台北市生命線協會亦於民國 86 年起開始提供電子郵件式的諮商服務；台灣大學心理學系更於民國 87 年建立了「心理健康諮詢網」，並開放一般民眾心理健康問題上的諮詢，提供了心理衛生及精神疾病的專業資訊；民國 90 年起張老師以線上聊天的方式提供網路即時諮商服務。

2.2 橢圓曲線公開金鑰密碼系統

自 1978 年美國麻省理工學院的 Rivest 、Shamir 與 Adleman 等三人以數學因數分解的計算難題，提出了第一套非對稱式金鑰密碼系統，命名為 RSA 公開金鑰密碼系統。直至今日，RSA 仍是一套安全的非對稱式密碼系統，但 RSA 的安全強度是有代價的，即它需要大的金鑰長度，隨著電腦計算能力的演進，這種狀況愈加明顯。因此，密碼學研究學者尋

找替代方案，以期能相同安全強度下金鑰長度卻較短，其中之一最有希望的替代方案便是橢圓曲線密碼系統[3]。Miller(1985)[9]及Koblitz(1987)[10]分別提出將橢圓曲線用來實作公開金鑰密碼系統。橢圓曲線的通式為 $y^2+axy+by=x^3+cx^2+dx+e$ 其中 a、b、c、d、e 是實數。在橢圓曲線中，點加法運算是經過特別定義的，除此之外，也另外定義一個無窮遠點 O，假使一條直線與此橢圓曲線相交於三點，則此三點的和為無窮遠點 O。在 Galois Field $E(F_q)$ 中，如果 q 是大於 3 的質數，則橢圓曲線的通式為 $y^2=x^3+ax+b \bmod q$，其中 a，b 為小於 q 的正整數且質數 q 會固定住式程式的上限，並用於模數運算上，且 $4a^3+27b^2\neq 0$ 以避免重根的情形，假設下面兩點 $P(x_1,y_1)$ 及 $Q(x_2,y_2)$ 為橢圓曲線群 中的兩個點，則此橢圓曲線群中的點加法定義如下：。

$$P+O=O+P=P$$

$$x_1=x_2, y_1=-y_2, P=(x_1,x_2)$$
$$Q=(x_2,y_2)=(x_1,-y_1)=-P$$
$$P+Q=O$$

$$\text{if } P\neq Q \text{ then } P+Q=(x_3,y_3)$$
$$\text{in } x_3=\lambda^2-x_1-x_2 \bmod q,$$
$$y_3=\lambda(x_1-x_3)-y_1 \bmod q$$

$$\text{if } x_1\neq x_2 \text{ then } \lambda=(y_2-y_1)/(x_2-x_1)$$

$$\text{if } x_1=x_2 \text{ and } y_1\neq 0$$
$$\text{then } \lambda=(3x_1^2+a)/2y_1$$

在橢圓曲線的求點運算中，若要計算 $2P$ 則等同計算 $P+P$，相同的若要計算 $3P$ 則等同計算 $3P=2P+P$，橢圓曲線的另一個特性為純量相乘，即運算只能做單向的計算，無法再由計算的結果值反推出原始的點，假設一個橢圓曲線是屬於 F_q，而 P 是橢圓曲線 E 上的一個點，給定一個屬於橢圓曲線上的一個點 Q，若要找出一整數 k 使得 $kP=Q$，因為其特殊的點加法運算，破密者除了逐一的窮舉所有可能的點之外，別無他法。直至目前為止，這個問題仍無法於多項式時間內求出解答。橢圓曲線密碼系統的另一個優點是其加密的密鑰長度短，在同樣的安全度之下，僅需要較小的密鑰長度，換句話說，相較於 RSA 在同樣的密鑰長度下，橢圓曲線密碼系統卻可擁有更高的安全性[11]，如表 1[12]。

表 1. RSA 與橢圓曲線密碼系統金鑰長度之比較表

RSA 密碼系統 (bits)	512	1024	2048	3072	7680
橢圓曲線密碼系統(bits)	112	163	224	256	384
金鑰長度比	1：5	1：6	1：9	1：12	1：20

2.3 網路單一登入機制

以網頁為基礎的應用程式(Web-based Application)因具有跨平臺、作業系統特性，使用者僅需使用瀏覽器即可使用，故漸取代傳統 Client-Server 二層式架構，成為目前應用程式開發之主流，但因每個網站開發平臺或驗證方式不同，各有各自的使用者身分認證機制，這對使用者而言，需記憶多組帳號密碼，針對上述使用上不便的問題，單一登入機制 (Single Sign- On,SSO)讓使用者只要經過一組帳號與密碼，就可以存取不同網站之服務，而不需再重複的身分登入驗證動作[13]。網路上著名的單一登入機制如 Microsoft 公司於 1999 年提出.Net Passport 的 Web Service，其採用麻省理工學院的 Kerberos 為其安全架構，採取可信任第三者驗證方式(Trust Third-Party Authentication)對使用者進行身分驗證，用 DES(Data Encryption Standard)對稱式加密演算法來加解密私密金鑰，但.Net Passport 因部份安全漏洞因素，Microsoft 於 1999 年將它做重大更新並易名為 Windows Live ID。

Kerberos 是以對稱式加密方法，隨著公鑰基礎建設(Public Key Infrastructure, PKI)的建立與普及，朱建達等於 2000 年提出以公鑰基礎建設來設計單一登入系統，朱建達[14]在

2000 年便提出以公開金鑰基礎建設設計單一登入系統，所提方法是將系統整合公開金鑰基礎建設，讓使用者先經過「認證伺服器」（AS）驗證之後，取得一份由「憑證中心」（CA）所發的權限屬性票卷，透過此票卷便可向「權限屬性伺服器」（PAS）取得登入「應用伺服器」（V）的帳號、密碼，最後藉由「代理程式」（Agent）將取得的帳號、密碼轉換成為「應用伺服器」（V）可以接受的格式，朱建達所提方法優點是透過 PKI 的機制讓訊息傳遞與資料交換過程中，能夠確保資料完整性、資料來源辨識、資料隱密性、不可否認性等四種重要的安全保障，但此架構至少需要「認證伺服器」、「憑證中心」、「權限伺服器」、「應用伺服器」四個伺服器與「代理程式」，會增加管理上的難度與建置成本提高。

李長庚[15]在 2002 年提出了「一個開放的 Web-Based Single Sign-On 服務架構」，在此架構中，透過專職對外聯繫的服務單位（SSO Embassy），來與其他的單一登入服務系統溝通，並採用以角色為基礎的權限控制機制（Role-Based Access Control, RBAC）與 LDAP（Lightweight Directory Access Protocol）搭配提供權限控制機制，此方法所提的 SSOE（SSO Embassy）是為解決各個單一登入服務網站間資訊交換格式不相容的解決方案，且為了提供使用者更多與外部單一登入服務溝通的選擇，需要實作多個 SSOE 以提供使用者選擇，不過 SSOE 的實作複雜而且困難。

Samar V. [16]在 1999 年提出以 Cookie 實現單一登入，但由於 Cookie 本身的特性與限制， V.Samar 所提的方法只能局限於同一個網域內，2005 年王雅苓[17]提出了「一個新的跨網域單一登入服務架構」，利用建置 Cookie Center 的方法來解決 Cookie 無法跨網域傳遞的限制。在此服務架構中，主要是建基於 Cookie 和 LDAP 之上，並且讓每一個參與單一登入服務的網域，都建置一個 Cookie Center，以便來發出認證的 Cookie 給它們自己網域的使用者，也因為每一個參與單一登入服務的網域，都必須建置一個 Cookie Center，且所有合作的 Cookie Center 皆要向憑證中心來確認使用者身分，故此方法除了增加管理負擔也會加重網路流量的負荷。廖英彥[18]等於 1995 年「網際網路單一登入系統應用」使用 Session Cookie 等方式，提出一種基於網際網路上之單一簽入系統 (Web Based Single Sign-On System) ，讓使用者只要通過一次身份驗證，就可以在不同的網站間進行資料存取，而不必再重覆身份驗證的動作，以提供單一登入身分認證機制。

2.4 Http Cookie 與 Session

在用戶端存取這些網站服務之重要工具—瀏覽器是透過 HTTP 協定(Hypertext Transfer Protocol)來連結網站伺服器，HTTP 是以用戶端的請求(Request)與伺服器回應(Response)模式為基礎，當每次的請求／回應完成後，這雙方的連結就會中斷，因此也稱 HTTP 為無狀態(Stateless)的協定，因為此特性，網站伺服器不知道用戶端上一次做了什麼，這阻礙了互動式網站應用程式的實作。一般使用 Cookie 就是用來解決 HTTP 的無狀態性的方式之一，藉此維護與保存使用者跟網站伺服器會談中的狀態，也就是說使用者登入一個系統，經過認證過程後，如果認證成功，伺服器會將認證字串(Message Authentication code, MAC)以 Cookie 的形式儲存在使用者的電腦中，待使用者再度登入同一個系統時，伺服器會從 Cookie 中取出先前發給使用者的認證字串並進行驗證，而無須使用者再次登入的動作。Cookie 儲存在用戶端中由瀏覽器維護，依存在時間可區分為持續性和暫時性 Cookie。

持續性 Cookie，儲存在使用者的硬碟，除非使用者手動清理或到了過期時間，硬碟 Cookie 不會被刪除，其存在時間是長期的，另外，未加密的 cookie 在傳送過程中，被攔截取得認證資料；即使是加密過的 cookie 被攔截後，也能利用重送攻擊(replay attack)來欺騙伺服器，因此 cookie 的儲存與傳遞的安全議題，也常為人所詬病，用戶端會了安全考量，關閉瀏覽器 Cookie 的功能。

暫時性 Cookie，暫存記憶體，一旦使用者將瀏覽器關閉後即消失，其存在時間是短暫，又稱為 Session Cookie[16]，Session 的功能和 Cookie 類似，都是用來記錄使用者的狀態與資訊，不同點在於 Cookie 的是存在用戶端而 Session 是存在伺服器端，由於 Session 的資訊是儲存在伺服器端，因此也常應用在使用者身分認證。Session 在一段時間沒有再繼續互動或是用戶執行登出功能，Session 工作階段

就會結束，為了能持續維持狀態與記錄這些資訊，Session 搭配 Cookie 來使用，使瀏覽器必須使用網址改寫(URL Rewriting)的方式來傳送 Session ID，也讓攻擊者有機會從網址列中取得某些資訊，進行進程追蹤，造成資訊安全問題。

2.5 盲簽章

David Chaum [18]以 RSA 的方法提出盲簽章機制，而電子匿名投票選舉即是利用這個方法確保投票者的身分達到隱匿效果。運用密碼學中數位簽章之特性，使用公鑰與私鑰的特性對訊息做加密、解密，做為送簽者與需求者間確認之用。舉例來說，如同投票人「送簽者」請選委會「簽章者」在一封經彌封的選票信件上蓋鋼戳，鋼戳的戳記印痕會經由外層的信封複印至內層的選票，以證明此選票之合法性戳記，再將此封內含有選票信件回覆給具合法身分的投票人，投票人於收到蓋有戳記的選票後，先檢查信封是否仍處於彌封狀態，再將選票自信封中取出，此選票帶有選務中心鋼戳的戳記，以證明此張選票之合法性。投票人在此選票上自行圈選後寄往開票中心，但該選票上不會記錄投票人身分或地址，寫上寄往開票中心的地址，如此完成匿名投票的步驟[19]，盲簽章過程敘述如下：

(1) 盲簽章是簽章者植基於 RSA 方法選定*(n, e)*、*d* 分別為公鑰與私鑰，送簽者想要將訊息 M 送給簽章者簽章，卻不願讓簽章者知悉訊息 M 的內容。送簽者隨機挑選一整數 R 為盲因子，滿足條件 $GCD(R,n)=1$ 計算 $M'=(R^e \times M) \bmod n$ 將 M' 傳給簽章者。

(2) 簽章者收到 M' 後，以其私鑰 d 計算 $S'=(M')^d \bmod n$ 將 S' 回傳給送簽者，於簽章過程中，簽章者完全不知道所簽章的資料內容。

(3) 送簽者：

$$S'=(R^e \times M)^d \bmod n$$

$$S'=(R^{ed} \times M^d) \bmod n$$

$$S'=(R \times M^d) \bmod n$$

送簽者利用之前所選擇的盲因子 R，對此簽章做除盲化的動作 R^{-1}，將收到的 S' 內之盲因子移除，以得到簽章者對訊息 M 的簽章 d ：

$$S=M^d \pmod n$$

(4) 需求者得到 $S=M^d \pmod n$，需求者可以使用簽章者的公鑰 e 來驗證 S 的有效性以還原訊息 M，若驗證成立則代表該簽章為簽章者對訊息 M 的有效簽章。

$$S^e=(M^d)^e \pmod n$$

由上述可知，送簽者在簽章者不知訊息內容情況下簽署，以得到其簽章，主要特性有二：簽章章不知所簽署訊息內容，是盲化(blindness)的；其次是公即公布訊息內容，也無法追蹤訊息之間的關係[20][21][22]。

三、單一登入之網路諮商系統安全機制設計

本方法以橢圓曲線密碼系統為基礎，架構的成員計有使用者 U、驗證主機 AS、諮商網站 A、諮商網站 B、諮商師 I、J 等，系統架構使用案例圖如圖 1，各成員於使用網路諮商系統前，網路諮商系統各階段成員須先註冊成為合法使用者。各系統成員如使用者、諮商師亦須以個人資訊，選定帳號、密碼後向驗證主機註冊使用權限，註冊後，驗證主機計算出各成員之公、私鑰，系統使用符號表如表 2。

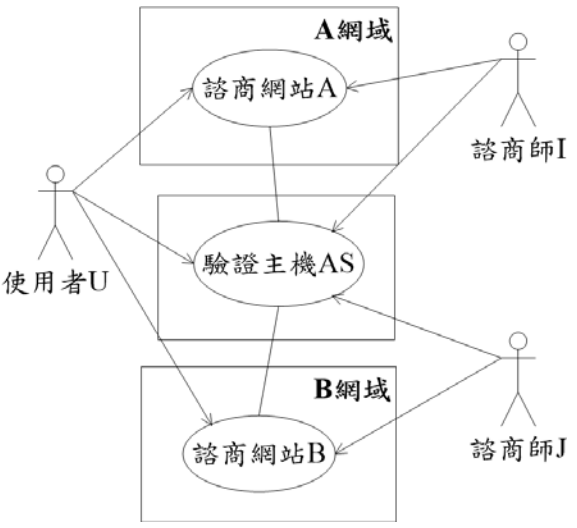

圖 1. 系統架構使用案例圖

表 2. 系統使用之符號說明

項目	符號	說明	項目.	符號	說明
1.	AS	驗證主機	12.	K_{mn}	認證雙方共同之隱匿金鑰
2.	A	諮商網站 A	13.	$h(\ )$	單向無碰撞雜湊函數
3.	B	諮商網站 B	14.	n_n 、k_n	成員選擇亂數值，不公開
4.	U	使用者	15.	a, b	網站 A,B 自選秘密整數值
5.	I	諮商師（A 網站）	16.	γ_n 、β_n	隱藏會議金鑰值
6.	J	諮商師（B 網站）	17.	X_n	隱匿值，$X_{\mathrm{N}}=\left(x_{N_1}, y_{N_2}\right)$
7.	id_n	各方成員的帳號	18.	sk_n	會議金鑰
8.	Q_n	各方成員的公鑰	19.	R_n	成員產生之簽名檔
9.	d_n	各方成員的私鑰	20.	s_n	驗證訊息之雜湊值
10.	m	明文訊息	21.	α	盲化後訊息
11.	C_n	加密後之密文	22.	m' 、s'、r	解盲化後訊息

備註：$_n$ 為系統中的各方成員，如 AS、A、B、U、I、J 等

3.1 系統初始

驗證中心 AS 在有限域 F_q 上選取一條安全的橢圓曲線(q 為一個 224bit 以上之大質數)上選一階數（order）為 n 的基點 G，使得 $nG=O$，其中 O 為此橢圓曲線之無窮遠點。驗證中心 AS、諮商網站 A 使用 SHA-256 之單向雜湊函數 $h(\ )$，AS 計算公開金鑰 Q_{AS} 後公布 E、G、n、Q_{AS} 及 $h(\ )$。

$$Q_{AS}=d_{AS}G$$

系統內成員依此方法計算所屬公開金鑰 Q_n

$$Q_n=d_nG \tag{1}$$

3.2 服務請求階段

(1) 使用者 U 向諮商網站 A 請求登入服務。

(2) 諮商網站 A 檢查使用者 U 的記憶體中是否存有諮商網站 A 所簽發之會議金鑰 sk_A ，如果有，則允許使用者 U 登入；如果無，則進行下一步驟，服務請求階段如圖 2。

(3) 諮商網站 A 選擇一橢圓曲線 E 上的一個點 N_A，選一祕密參數值 $a\in Z_q$，計算 X_A：

$$X_A=aN_A=\left(x_{N_A}, y_{N_A}\right) \tag{2}$$

a、N_A 及 X_A 均不公開。

(4) 諮商網站 A 將 X_A 加密 C_A 與 C_{U}，分別傳送給驗證主機 AS 與使用者 U，計算式：

$$C_{\mathrm{A}}=\left\{aG, \mathrm{X}_A+aQ_{\mathrm{AS}}\right\} \tag{3}$$

$$C_A=\left\{C_{A1}, C_{A2}\right\} \tag{4}$$

$$C_{A1}=aG \qquad C_{A2}=X_A+aQ_{AS} \tag{5}$$

連同 id_U、C_A、目前網址 url_A 傳至驗證主機 AS，如圖 2 服務請求階段循序圖。

(5)

$$C_{\mathrm{U}}=\left\{aG, \mathrm{X}_A+aQ_{\mathrm{U}}\right\} \tag{6}$$

$$C_U=\left\{C_{U1}, C_{U2}\right\} \tag{7}$$

$$C_{U1}=aG \qquad C_{U2}=X_A+aQ_U \tag{8}$$

將 id_U 、C_U 、url_A 傳至使用者 U。

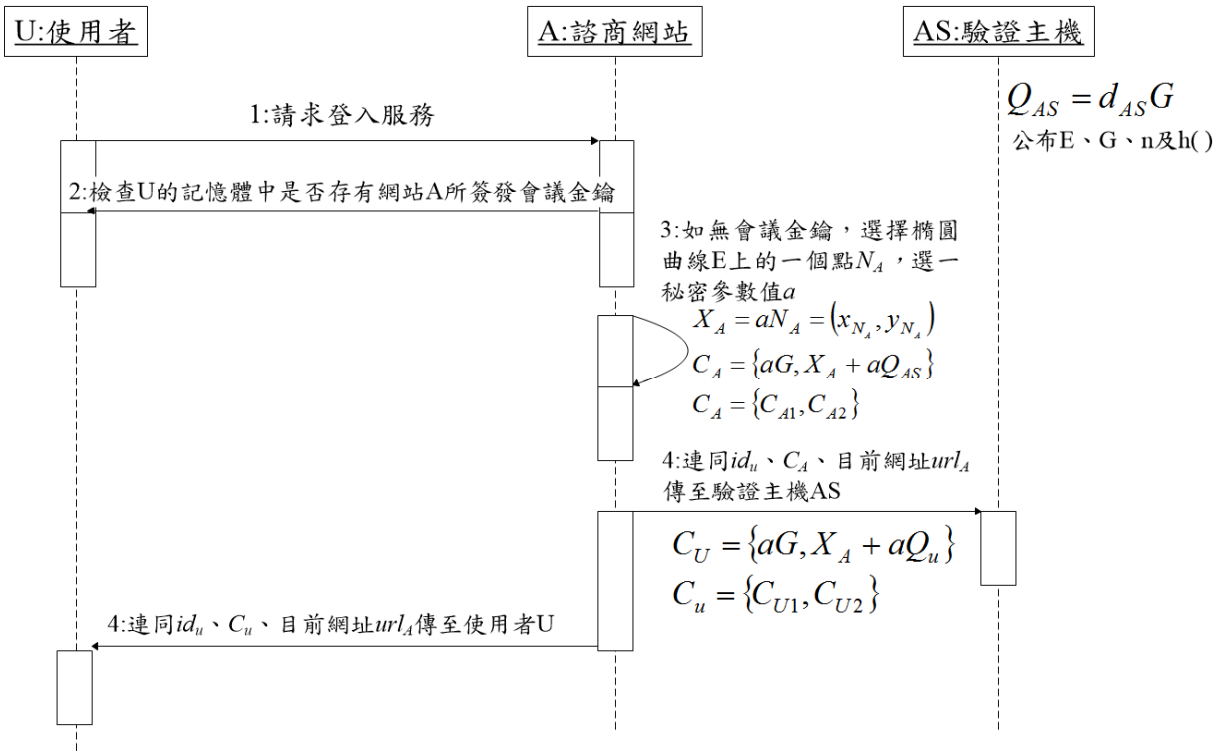

圖 2. 服務請求方式循序圖

3.3 會議金鑰簽發與驗證階段

驗證主機之會議金鑰簽發與諮商網站驗證階段循序圖如圖 3，本階段說明如下：

(1) 驗證主機 AS 於收到諮商網站之 id_U 、C_A 、url_A 後，先確認使用者 U 的記憶體中是否存有驗證主機 AS 所簽發會議金鑰 sk_{AS} ?如果沒有則執行身分驗證；如果有則執行步驟（2）。

(2) 如果驗證主機 AS 驗證使用者 U 的身分已註冊驗證成功，則簽發兩支會議金鑰，一支 sk_{AS} 予使用者；另一支 sk_A 授予諮商網站 A。

(3) 驗證主機 AS 記錄使用者 U 登入諮商網站 A 之相關資訊，以備未來登出諮商網站 A 時的使用資訊。

(4) 驗證主機 AS 將諮商網站 A 所傳來的 C_A ，$C_A=\{C_{A1},C_{A2}\}$ 以私鑰 d_{AS} 解密還原 x_{N_A} ：

$\because C_{A1}=aG \quad C_{A2}=X_A+aQ_{AS}$ (如式 3)

$$C_{A2}-d_{AS}C_{A1}=X_A+aQ_{AS}-d_{AS}(aG) \quad (9)$$

$$=X_A+aQ_{AS}-\mathrm{Q}_{AS}a \quad (10)$$

$$=X_A=(x_{N_A},y_{N_A})$$

(5) 驗證主機 AS 將上一步驟求得之 x_{N_A} 與會議金鑰 sk_A 做互斥或（XOR）運算，產生 γ_A ：$\gamma_A=sk_A\oplus x_{\mathrm{N_A}}$ (11)

(6) 驗證主機 AS 將會議金鑰 sk_A 做單向雜湊函數運算，計算 $\beta_A=h(sk_A)$ (12)

(7) 驗證主機 AS 將 id_U 、γ_A 、β_A 傳回給諮商網站 A。

(8) 諮商網站 A 以 x_{N_A} 和驗證主機 AS 傳來之 γ_A 值做互斥或（XOR）運算，求得 $sk_A^{'}$ 與驗證主機 AS 傳來之 sk_A 做比對是否相符 $sk_A^{'}\overset{?}{=}sk_A$

$$sk_A^{'} = x_{N_A} \oplus \gamma_A$$
$$= x_{N_A} \oplus (sk_A \oplus x_{N_A}) \quad (13)$$

(9) 諮商網站 A 將 $sk_A^{'}$ 以雜湊函數進行運算，與 β_A 做比對是否相符

$$\beta_A{}' \stackrel{?}{=} \beta_A$$
$$\beta_A{}' = h(sk_A^{'}) \quad (14)$$

(10) 諮商網站 A 若比對 γ_A 與 β_A 值無誤，即表示使用者 U 已通過驗證主機 AS 之驗證，再與使用者端U檢查與本身計算之 $h(x_{N_A})$ 是否符合?若符合則表示該使用者為原請求服務者 U，諮商網站 A 簽發該會議金鑰 sk_A 授予使用者 U，並允許其服務請求，登入諮商網站 A。

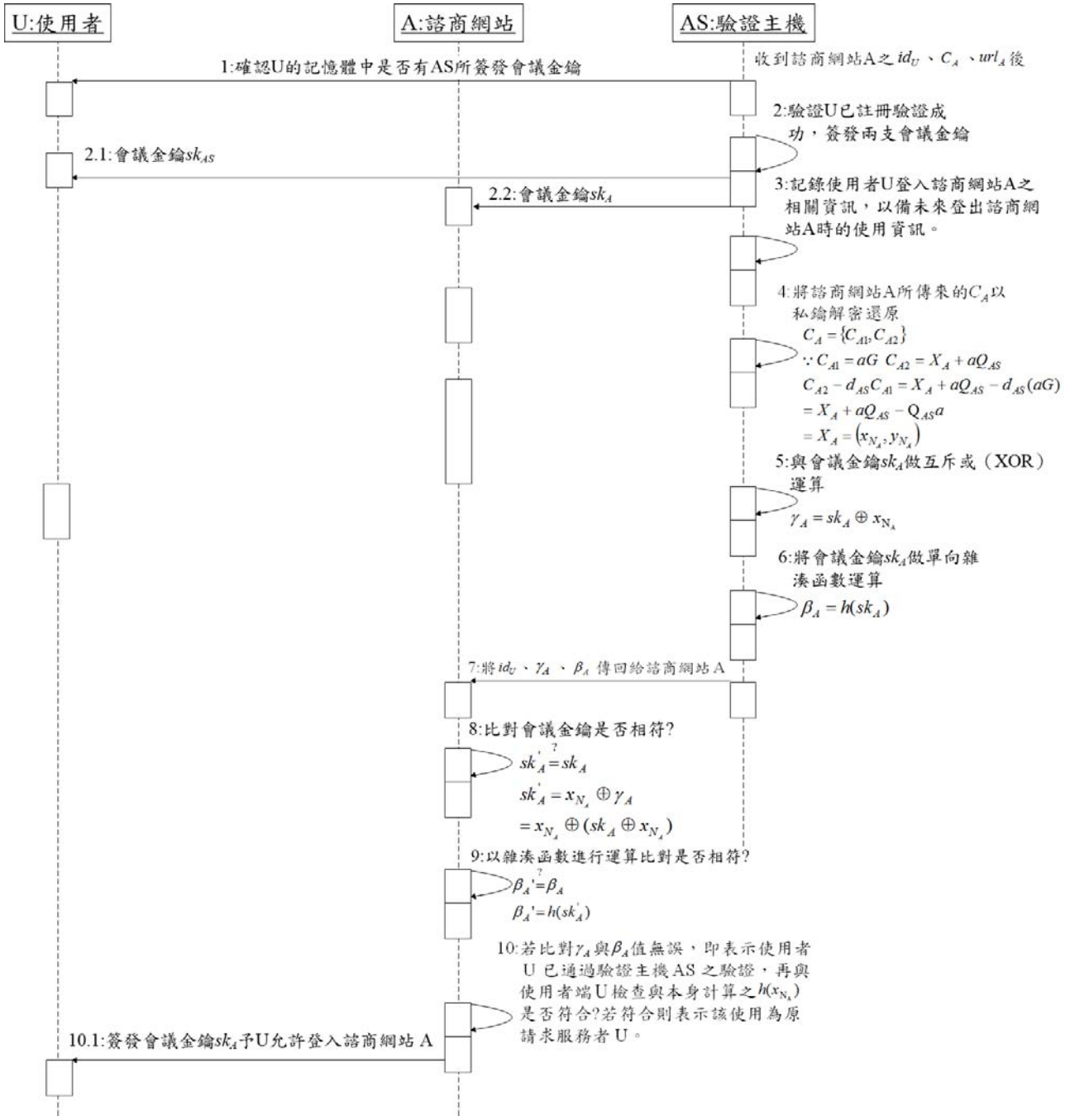

圖 3. 會議金鑰簽發與驗證階段循序圖

3.4 諮商師與使用者驗證階段

諮商師 I 以登入諮商網站 A 後獲得之 sk_A 與 f_A 做互斥或（XOR）運算後得 $f_A^{'}$，並傳給使用者如下所示：

諮商師 I 計算： $f_A^{'} = sk_A \oplus f_A$ (15)

驗證 $sk_A^{'} \stackrel{?}{=} sk_A$

使用者 U 檢查： $f_A \stackrel{?}{=} f_A^{'} \oplus sk_A$ (16)

$$f_A \stackrel{?}{=} (sk_A \oplus f_A) \oplus sk_A \quad (17)$$

$$f_A \stackrel{?}{=} f_A$$

$$f_A \stackrel{?}{=} h(x_A) \quad (18)$$

若是則代表諮商師 I 為來自諮商系統 A 之合法授權；同理，諮商師 I 亦可檢查使用者 U 之 Cookie 中的 f_A，以確認其是否為原請求服務者 U。

3.5 傳送簽密諮商訊息階段

在上一階段驗證成功後，諮商師 I 與使用者 U 以 Diffie-Hellman 計算交換金鑰，傳給對方以相互驗證對方身分，循序圖如圖 4 所示，步驟說明如下：

(1) 諮商師 I 計算： $\mathrm{K_{IU}} = \mathrm{d_I} \cdot Q_\mathrm{U}$ (19)

使用者 U 計算： $\mathrm{K_{UI}} = \mathrm{d_U} \cdot Q_\mathrm{I}$ (20)

(2) 雙方計算：

$$\mathrm{X_{IU}} = \mathrm{d_I} \cdot \mathrm{K_{UI}} = \mathrm{d_I} \cdot d_\mathrm{U} \cdot G \stackrel{?}{=} \mathrm{X_{UI}} \quad (21)$$

$$\mathrm{X_{UI}} = \mathrm{d_U} \cdot \mathrm{K_{IU}} = \mathrm{d_U} \cdot d_\mathrm{I} \cdot G \stackrel{?}{=} \mathrm{X_{IU}} \quad (22)$$

如果驗證相符，則確認對方身分。

(3) 使用者 U 將諮商訊息明文 m 編碼為橢圓曲線 E 上點 M，計算密文 C_M、s_U、$\mathrm{R_U}$ 傳給諮商師 I：

$$C_\mathrm{M} = \{\mathrm{k_U}G, \mathrm{M} + \mathrm{k_U}Q_\mathrm{I}\} \quad (23)$$

$$s_\mathrm{U} = \mathrm{k_U^{-1}}h(m)d_\mathrm{U} \quad (24)$$

$$\mathrm{R_U} = \mathrm{k_U}G \quad (25)$$

(4) 諮商師 I 將收到 C_M 後計算：

$$\mathrm{M} = \mathrm{M} + \mathrm{k_U}Q_\mathrm{I} - \mathrm{d_I}\mathrm{k_U}G \quad (26)$$

$$= \mathrm{M} + \mathrm{k_U}Q_\mathrm{I} - Q_\mathrm{I}\mathrm{k_U} = \mathrm{M}$$

得明文點 M 並轉值為 m，再以 s_U、$\mathrm{R_U}$ 驗證上述明文之真確性，計算式：

$$\mathrm{R_U} \cdot s_\mathrm{U} \quad (27)$$

$$= \mathrm{k_U}G \cdot \mathrm{k_U^{-1}}h(m)d_\mathrm{U} \stackrel{?}{=} h(m)Q_\mathrm{U} \quad (28)$$

3.6 諮商個資轉介盲簽章階段

如果個案經諮商師 I 輔導後，判斷其個案（使用者 U）有必要轉介另一諮商單位或適合領域諮商網站 B 之諮商師 J 做輔導時，轉介前需將受輔導對象諮商資訊轉交，使用基於 ECC 之盲簽章方式[23]，以確保使用者 U 之個資簽署過程中盲化與不可追蹤性等，本機制步驟如下：

(1) 諮商網站 A 盲化使用者 U 之個資訊息

諮商網站 A 計算

$$\alpha = m \cdot d_A \cdot Q_\mathrm{A} \quad (29)$$

將 α 值傳給驗證主機 AS。

(2) 驗驗證主機 AS 簽署盲化訊息

選擇秘密整數 $n_\mathrm{AS} \in Z_q$，檢查 α、n_AS 者是否已在清單內並使用，如果是則重選 n_AS，否則計算

$$r = n_\mathrm{AS} \cdot \alpha \quad (30)$$

$$s = (n_\mathrm{AS} + d_{AS}) \cdot \alpha \quad (31)$$

將 α、r、s 傳給諮商網站 A。

(3) 諮諮商網站 A 解盲化階段

計算 $s' = s - m \cdot d_A \cdot Q_{AS}$ (32)

計算 $m' = d_A(d_A - 1) \cdot m$ (33)

將 m'、s'、r 傳給諮商網站 B。

(4) 諮諮商網站 B 驗證盲簽章階段

諮商網站 B 使用驗證主機 AS 之公鑰 Q_{As}

驗證 $r = s' - m' \cdot Q_{As}$ (34)

如果上式驗證成立，則諮商網站 B 則可確認盲化訊息確為驗證主機 AS 簽署過，上述 3.4 至 3.6 循序圖如圖 4 與圖 5 所示。

Proof： $r = s' - m' \cdot Q_{As}$

$$= s - m \cdot d_A \cdot Q_{AS} - d_A(d_A - 1) \cdot m \cdot Q_{As}$$

$$= s - m \cdot d_A \cdot Q_{AS} - d_A d_A \cdot m \cdot Q_{As} + d_A \cdot m \cdot Q_{As}$$

$$= s - d_A \cdot d_A \cdot m \cdot Q_{As}$$

$$= (n_\mathrm{AS} + d_{AS}) \cdot \alpha - d_A \cdot d_A \cdot m \cdot Q_{As}$$

$$= (n_\mathrm{AS} + d_{AS}) m \cdot d_A Q_A - d_A \cdot d_A \cdot m \cdot Q_{As}$$

$$= n_{AS} \cdot m d_A Q_A + d_{AS} \cdot m d_A Q_A - d_A d_A \cdot m Q_{As}$$
$$= n_{AS} \cdot m \cdot d_A \cdot Q_A + d_{AS} \cdot m \cdot d_A \cdot d_A \cdot G$$
$$- d_A \cdot d_A \cdot m \cdot d_{As} \cdot G$$
$$= n_{AS} \cdot m \cdot d_A \cdot Q_A$$
$$= n_{AS} \cdot \alpha \quad (\text{如式 } 30) \ = r$$

3.7 跨網站諮商之身分認證階段

使用者 U 經通知應轉介另一諮商單位或適合領域之諮商師 J（隸屬諮商網站 B）做輔導時，讓使用者 U 導向另一諮商網站 B，無須要求當事人重新登入諮商網站 B，本機制步驟如下：

(1)服務請求階段

Step 1.使用者轉向諮商網站 B 請求服務。

Step 2.諮商網站B檢查使用者U的記憶體中是否存有諮商網站 B 所簽發之會議金鑰 sk_B ，如果有，則允許使用者 U 登入；如果無，則進行如式(2)至(6)產生 C_B 連同使用者 U 的 id_U 、網址 url_B 傳至驗證主機 AS 進行驗證。

(2)會議金鑰簽發與驗證階段

Step 1 驗證主機 AS 於收到諮商網站之 id_U 、C_B 、url_B 後，先確認使用者 U 的記憶體中是否存有驗證主機 AS 所簽發會議金鑰 sk_{AS} ？如果沒有則執行身分驗證；如果有，則執行下一步驟。

Step 2 如果驗證主機 AS 驗證使用者 U 的身分已註冊驗證成功，則簽發兩支會議金鑰，一支 sk_{AS} 授予使用者；另一支 sk_B 授諮商網站 B。

Step 3 驗證主機 AS 記錄使用者 U 登入諮商網站 B 之相關資訊，以備未來登出諮商網站 B 時的使用資訊。

Step 4驗證主機AS與諮商網站B依式(8)至(12)產生相關驗證參數，諮商網站B若比對 α_B 與 β_B 值無誤，即表示使用者 U 已通過驗證主機 AS 之驗證，再與使用者端 U 檢查的 f_B 與本身計算之 $h(x_{N_B})$ 是否符合？若符合則表示該使用者為原請求服務者 U，諮商網站 B 簽發該會議金鑰 sk_B 授予使用者 U，並允許其服務請求，登入諮商網站 B。

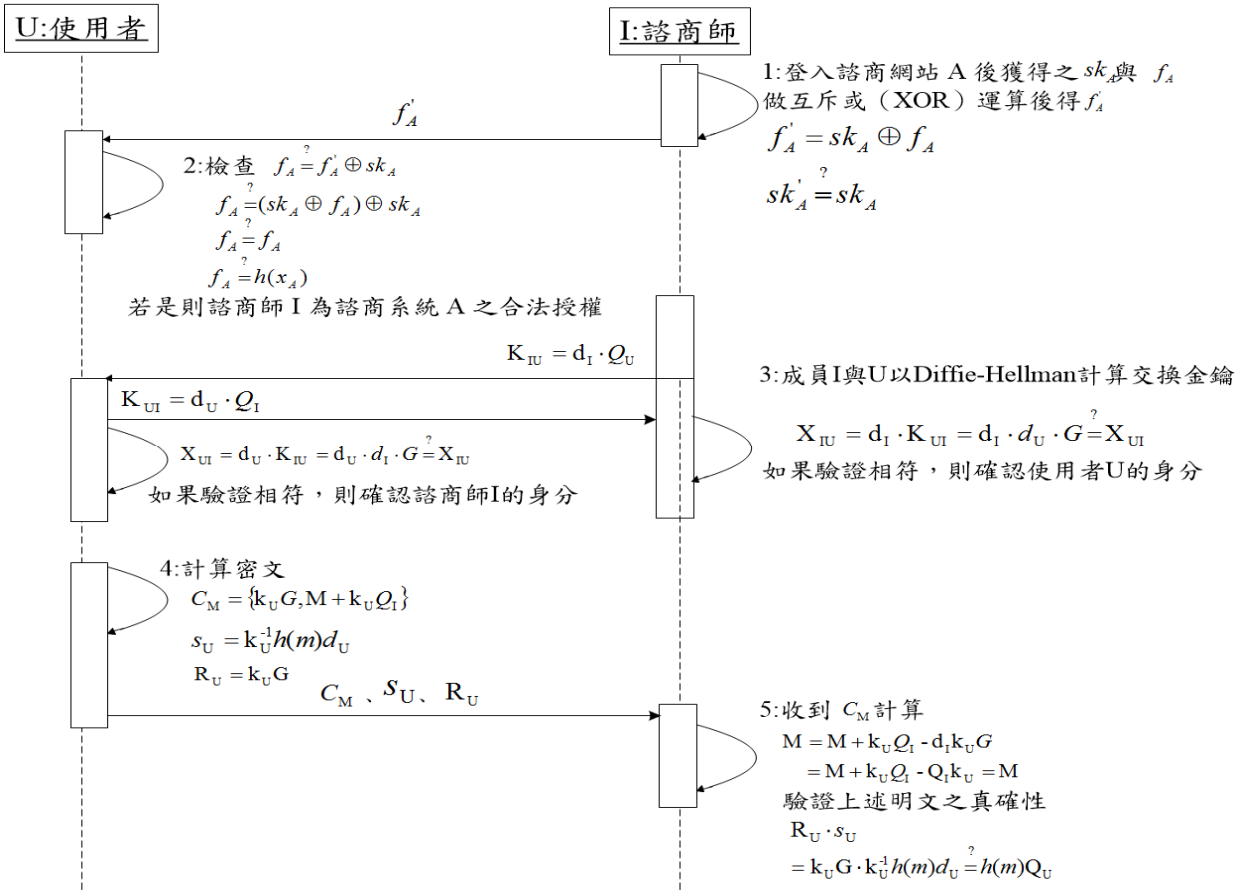

圖 4. 身分驗證與傳送簽密訊息循序圖

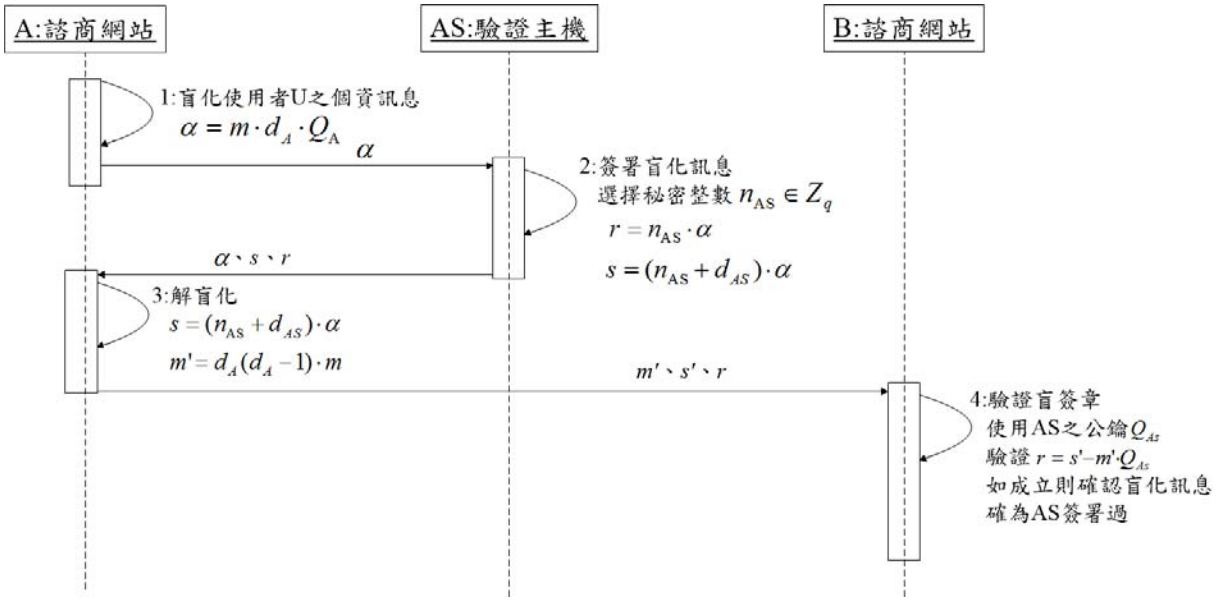

圖 5. 諮商個資轉介盲簽章循序圖

3.8 登出作業

使用者於登出網站時，可分為正常使用情形下登出與未執行登出（非正常作業）兩種，分別說明之：

(1)使用者於登出諮商網站時，諮商網站會將其請求重導至驗證主機進行簽出動作，依原本使用者登入諮商網站所記錄之資訊，將原本簽發給各成員之會議金鑰 *sk* 廢止，完成登出動作。

(2)使用者未執行登出而逕行關閉瀏覽器或操作逾時：如果使用者未執行登出動作，因會議金鑰有其時間限制，當超過時間限制（timeout），會議金鑰會自動失效，或使用者直接關閉瀏覽器，則存於記憶體中的會議金鑰亦會自動清除。

四、安全性分析

本研究之安全機制利用橢圓曲線離散對數難題、盲簽章等，以確保諮商內容之隱匿性等安全需求，安全性分析與本系統特點分別說明如下：

4.1 保密性

是指資料不得被未經授權的個人、實體或程序所取得或揭露的特性。其確保了訊息在成功地送達目的地之後，所有的訊息交換都是保密的。本研究的方法是設計網路諮商服務內容在網路中傳送時，使用通訊對方之公鑰將訊息加密，如式（2）至（8）所示，若攻擊者想在通訊過程中竊取，則攻擊者須破解橢圓曲線離散對數之難題[24]。

4.2 真確性

指的是訊息在傳遞過程中不能被破壞或干擾，通訊的內容在通訊節點間傳遞的過程中確認沒有被改變，也就是訊息在的處理過程中不能被加入、刪除或修改。

本研究中系統內各方成員須先向金鑰產製中心驗證主機註冊及身分確認，以獲得其公鑰（如 Q_{AS}）與身分認證簽章，本研究使用簽密法，系統內成員會自行驗算傳過來的訊息之正確性，將 C_M、s_U、R_U 如式（23）至（28）所示驗證上述明文之真確性，若攻擊者想要竄改簽章偽造，則必須面對橢圓曲線離散對數問題，故驗證過程中詐偽的行為會被偵測出來。

4.3 不可否認性

公開金鑰密碼系統中，系統每位成員的公鑰與其密鑰有其唯一的對應關係，換句話說，只有該成員所擁有的密鑰才能對應到該成員

的公鑰，因此藉由此金鑰對可以達到鑑別成員身分的功能如式（2）至（8）。本研究各階段中成員於使用系統前，皆須完成註冊及身分確認，才能獲得其憑證與公鑰，且在運用其身分時，須使用由驗證主機所給予之公鑰等參數資料進行相互身分驗證，因此各階段成員身分都有確認性。

數位簽章機制中，簽章產生機制必須使用簽署者的密鑰，簽章驗證機制則要使用簽署者的公鑰，才能驗證該簽章的有效性。因此，如果驗證者利用公鑰驗證所收到數位簽章為有效時，則表示此簽章與電子文件的確是由具有該公鑰的成員所簽署，將解開之明文 m，再以 s_U 、R_U 驗證，如式（27）至（28）。

4.4 盲化與不可追蹤性

盲簽章是指簽章雖然對某個訊息簽章，但並不知道所簽訊息的內容，也就是說對簽章者而言，訊息被盲化處理過。在本文者，諮商網站 A 為諮商訊息擁有者（欲轉介諮商訊息），驗證主機 AS 為簽章者，盲簽章過程包括：

- 訊息盲化：諮商網站 A 將訊息 m 進行盲化處理得 $\alpha = m \cdot d_A \cdot Q_A$ 再傳給驗證主機如式（29）所示。
- 盲化訊息簽章：驗證主機 AS 應用數位簽章方法對盲化訊息進行簽章 α、r、s 如式（30）至（31），並將其簽章後訊息送回給諮商網站 A。
- 解盲化：諮商網站 A 將驗證主機 AS 傳回之盲簽章訊息（α、r、s），從盲簽章（r、s）中解盲化得到驗證主機 AS 的簽章如式（30）（31）所示，通過除去盲因子的方法徙到 m'、s'、r 如式（32）（33），再傳給諮商網站 B。
- 驗證簽章：諮商網站 B 使用驗證主機 AS 之公鑰驗證 r，如果驗證成立，如式(34)，則諮商網站 B 則可確認盲化訊息確為驗證主機 AS 簽署過。

綜整本架構具盲簽章的特質:

(1) 盲化：訊息的內容對簽章者來說是盲化的，簽章者看不到消息的內容。

(2) 不可追蹤性。簽章者僅知 α、r、s，即使簽名者保留有關數據，仍難以找出 α、r、s 之間的內在聯繫，不可對訊息 m 的擁有者進行追蹤。

諮商訊息經由盲化後，在傳送過程中僅驗證中心 AS 能簽署經盲化諮商訊息，且不會介入存取內容，讓使用者不必擔心因網路諮商驗證中心 AS 的疏失，而導致諮商內容曝光，且僅有諮商驗證中心才可以產生合法的盲簽章，因為偽造者無法知道簽章者產生簽章的私密金鑰，因此無法偽造出盲簽章。

4.5 身分識別與單一登入

系統所有成員在註冊階段至驗證主機 AS 完成註冊並取得公鑰與會議金鑰後，即可利用 AS 所賦予之公鑰及會議進行相互身分認證，如式（11）至（14）。

身分識別指的是系統定義使用者 ID 所依據的規則，本研究架構中認證訊息當中包含傳送者與接收者之 ID，以及只有正確身分雙方才會共同持有之通訊金鑰，因此一旦雙方完成身分認證，即可確認對方身分如式（19）至（22）。

本研究架構驗證主機與諮商網站角色分離，驗證主機 AS 用來簽發會議金鑰、盲化訊息簽署之系統，不受制任一系統。驗證主機 AS 產生新的會議金鑰授予各成員，攻擊者無法由之前認證過程所產生的會議金鑰以假冒身分。

4.6 效益分析

心理諮商的服務主要為面對面的諮商，藉由網路諮商讓諮商師與受輔導對象可以不受時間與空間的限制，滿足雙方的需求[24]，綜整傳統諮商方式與網路諮商系統兩者特性分析比較如表 3，本研究參酌表 4 之運算量分析[25] [26]，彙製本研究時間複雜度運算參考表（如表 5），以整體效益而言，證明本研究不僅能達到安全性要求，也能減少計算成本，減輕系統因執行安全機制之資源負擔[27]，以利後續相關網路諮商系統安全機制之相關領域研究運用。

表 3. 現行諮商與網路諮商方式兩者特性分析比較

特性	一般諮商方式	網路諮商方式
互動模式	面對面或電話諮商，可獲得立即回應。	透過網路諮商系統所提供功能，使雙方藉由文字、影像等做回應。
互動時間	雙方需約定共同時間，時間上協調不易	需電腦、網路設備，雙方可身處兩地，時間協調較容易。
非語言訊息	諮商師可藉由觀察個案表情、語氣及肢體動作做判斷。	諮商師無法觀察個案外在情緒現做判斷，僅能由其用字遣詞揣測個案動機。
匿名性	當面且須留下身分資料給諮商師，部分當事人較難克服心理障礙。	完全經電腦認證、加密，資料隱密性高，對首次接受諮商者較能接受。
方便性	雙方距離、交通方式及往返時間等，對忙碌、行動障礙者不便。	可在家或有電腦上網環境即可，雙方時間安排上較有彈性。
效率性	人工作業，作業時程冗長。	自動化作業，接受與轉介個案快速。
完整性	晤談結束後，諮商師需再額外記錄晤談內容。	晤談內容即時寫入資料庫，方便日後個案查詢與案例追蹤。
資訊能力	不需要。	需具中文打字、上網等能力。

表 4. 時間複雜度運算之相互關係參考表

符號	運算時間
T_{ECMUL}	$\approx 29\ T_{MUL}$
T_{ECADD}	$\approx 5\ T_{MUL}$
T_{INVS}	$\approx 240\ T_{MUL}$
T_{EXP}	$\approx 240\ T_{MUL}$
T_{ADD}	可忽略不計

表 5. 本研究時間複雜度運算參考表

運算階段	時間複雜度
驗證主機解密運算	$T_{ECADD}+ T_{ECMUL} \approx 34\ T_{MUL}$
簽密諮商訊息	$T_{MUL}+ T_{ECMUL} \approx 30\ T_{MUL}$
解簽密諮商訊息	$2T_{ECMUL} + T_{MUL} \approx 29\ T_{MUL}$
驗證諮商訊息簽章	$T_{MUL}+ T_{ECMUL} \approx 30\ T_{MUL}$
盲化諮商訊息	$T_{MUL}+ T_{ECMUL} \approx 30\ T_{MUL}$
簽章盲化諮商訊息	$3T_{ECMUL} \approx 87 T_{MUL}$
解盲化諮商訊息	$T_{MUL}+ T_{ECMUL} \approx 30\ T_{MUL}$
驗證盲簽章	$T_{ECADD}+ T_{ECMUL} \approx 34\ T_{MUL}$

五、結論

本研究以網路諮商系統為探討對象，以橢圓曲線密碼學為基礎，結合盲簽章機制，設計具單一登入之網路諮商系統之安全機制，綜整本研究效益略述如下：

(1) 以橢圓曲線密碼系統加密諮商訊息與執行簽章，以更少的密鑰長度達到 RSA 相同的安全強度[28]。
(2) 諮商師與受輔導對象雙方可由通訊金鑰進行雙方身分認證。
(3) 使用者在會議金鑰的有效期限內，被轉介至另一諮商單位時，允許直接登入另一諮商網站（諮商輔導單位），不需再重新經過身分認證等程序。
(4) 以盲簽章的方式將資料隱匿功能，並防止過程中偽冒與竄改情事之發生，使諮商訊
息的轉介具盲化與不可追蹤性。

參考文獻

[1] 宋文松，線上輔導與諮商系統之可行性
研究，中原大學資訊管理研究所碩士論文，桃園，2003。
[2] 徐啟氤，以科技模式探討網路諮商使用意願之影響因素，國立暨南國際大學資訊管理學系碩士論文，南投，2005。
[3] 文美華，網路諮商機構實施電子郵件諮

商之實務經驗、困難及因應方式與網路諮商倫理行為之探討，國立屏東教育大學教育心理與輔導學系碩士論文，屏東，2006。

[4] 李伯偉，WiMAX 行動諮商系統，國立高雄第一科技大學資訊管理學系碩士論文，高雄，2008。

[5] 莊博凱，影響台南縣市國中生使用網路諮商相關因素之研究，長榮大學社會工作學系碩士論文，台南，2007。

[6] 許毓隆，以科技接受模式探討網路諮商專家系統虛擬實境服務之接受程度，世新大學企業管理研究所碩士論文，台北，2009。

[7] 張維中，網路諮商系統之設計與實作，國立暨南國際大學資訊管理學系碩士論文，南投，2004。

[8] 蘇品長、郭文雄，“單一登入之網路諮商系統安全機制探討”，2010 國際聯合研討會—第十二屆「網際空間：資安、犯罪與法律社會」學術暨實務研討會，2010。

[9] Miller, V. S., “Use of Elliptic Curve in Cryptography,” Advance in Cryptography- Crypto ’85, pp. 417-426, New York, 1985.

[10] Kobiltz, N. , “Elliptic Curve Crypto-systems,” Mathematics of Commutation, Vol. 48, pp. 203-209, 1987.

[11] Tsai, C.H. and Su, P.C., “ECC-Based Cryptosystem for Multi-Document Fail-Stop Signature with Encryption Scheme” ,Journal of Internet Technology, Vol.16, No.3, pp. 462-475, 2015.

[12] 蘇品長，植基於 LSK 和 ECC 技術之公開金鑰密碼系統，長庚大學電機工程研究所博士學位論文，桃園，2007。

[13] 林裕峰，跨網域之校務單一登入系統，交通大學理學院網路學習學程碩士論文，新竹，2008。

[14] 朱建達，建立於公開金鑰基礎建設的單一簽入系統，交通大學資訊科學研究所碩士論文，新竹，2001。

[15] 李長庚，一個開放的 Web-Based Single Sign-On 服務架構，交通大學資訊管理研究所碩士論文，新竹，2002。

[16] Samar, V., "Single sign-on using cookies for Web applications ", Proceedings of the IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises , pp.158-163, 1999.

[17] 王雅苓，一個新的跨網域單一登入服務架構"，交通大學資訊管理研究所碩士論文，新竹，2005。

[18] 廖英彥，網際網路單一登入系統應用，世新大學資訊管理系碩士論文，台北，2005。

[19] Chaum, D., “Blind signatures for untraceable payments,” Advances in Cryptology- CRYPTO'82, pp. 199-203, New York, 1983.

[20] 李秉禮，具選票驗證之匿名電子投票機制，佛光大學資訊研究所碩士論文，宜蘭，2007。

[21] 郭文雄，設計具自我認證之國軍網路申訴制度安全機制探討，國防大學資訊管理學系碩士論文，桃園，2010。

[22] 蘇品長、蔡建華、郭文雄、林明慶、楊倫青，“具自我認證之國軍網路申訴機制探討”，國防管理學報，第 32 卷，第 1 期，第 59-72 頁，2011。

[23] Jeng, F.G ,Chen T.L and Chen, T. S, “An ECC-Based Blind Signature Scheme”, International Journal of Networks, Vol. 5, No. 8, pp. 921-928,August 2010.

[24] Chester, A., and Glass, C. A.," “-line counseling: A descriptive analysis of therapy services on the Internet “. British Journal of Guidance &Counseling , 34(2), pp.145-160 . 2006.

[25] Kavitha Ammayappan , Atul Negi , V. N. Sastry and Ashok Kumar Das, “An ECC-Based Two-Party Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks”, Journal of Computers Vol 6, No 11, pp. 2408-2416,2408-2416, Nov 2011.

[26] Thu, A.A. and Mya, K.T., “Implementation of an Efficient Blind Signature Scheme”, International Journal of Innovation, Management and Technology, Vol. 5, No. 6, pp. 443-448, December 2014.

[27] Liu, D. C. & Chen, L. C. , “Using Model Checking to Ensure Transaction Fairness in E-Commerce Protocols, Proceedings of Business and Information“,

Kitakyushu, Japan, paper number: 8027,BAI 2010.

[28] A., Riele, H., Timofeev, A., and Zimmermann, P., “Factorization of a 768-bit RSA modulus “, 30th Annual Cryptology Conference, Advances in Cryptology – CRYPTO, pp.333-350. 2010.