具可追蹤性之無記名憑證應用協定

楊吳泉[1,2] 丁廉原[1] 黃振宗[1] 程凱[2]

[1]義守大學資訊工程學系
[2]義守大學智慧網路科技學系

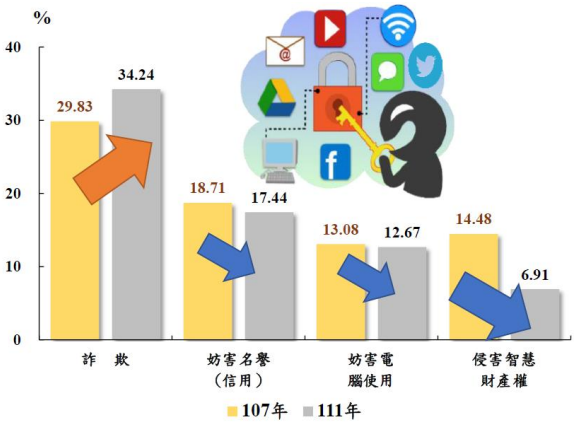
摘要

隨著網際網路的快速發展，其匿名和自由的特性促進了服務和產業的多元化發展，使得使用者能夠方便地獲取各種資訊。然而，這也伴隨著不當的網路行為和犯罪行為的增加，這些行為往往涉及隱匿和偽造身份。為了確保網路空間的安全，需要一種方法來認證使用者的真實身份，從而防止身份隱匿和偽造。本研究基於 Rabadi 的隱式憑證概念，提出了一種新的應用協定—「具可追蹤性之無記名憑證應用協定」。這種協定旨在透過憑證和數位簽章機制，達到實名制和匿名制之間的平衡，不僅提高了冒用身份的門檻，還允許在必要時透過特定方法隱蔽地確認使用者身份，從而在保障網路安全的同時，也尊重了個人隱私權和網路的匿名文化。

關鍵詞：隱式憑證、身分追蹤、橢圓曲線密碼系統

一、前言

在網際網路為人們帶來生活便利性的同時也伴隨著許多不當的網路行為、危及資訊安全，以隱匿或偽造身分的方式進行犯罪行為[1]。根據內政部警政署「警政統計通報(112年第28週)」可以瞭解我國電腦網路犯罪概況(圖1)近5年網路犯罪發生案類以「詐欺」增加4.41%最多，「侵害智慧財產權」減少7.57%改善最多[2]。可得知網路犯罪大多利用網路具有匿名和自由之特性，使得網路犯罪比一般犯罪更為寬廣迅速。在使用許多方便功能的同時，也要阻止攻擊者行為以防止敏感的資訊遭到竊取、竄改，伺服器必須在不被干擾的情況下取得用戶身分，確認使用者身分，又不會暴露全部真實資料。



圖一、111年與107年網路犯罪前4大案類比較 (資料來源: 警政署刑事警察局[2])

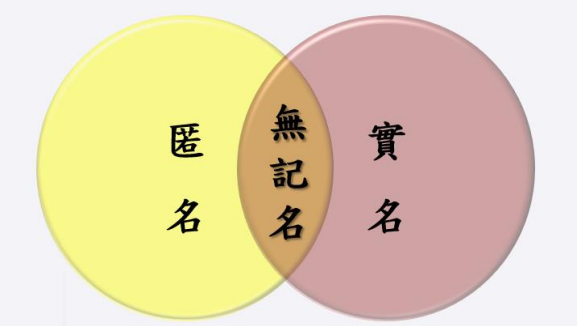
多數隱匿技術本身是用來保護隱私，例如代理(Proxy)隱匿行為是利用轉送等方式將使用者的封包轉成由代理伺服器發送，但是惡意的使用者利用代理隱匿來掩蓋追蹤以進行犯罪。使用實名制對使用者

身分認證可以避免隱匿，但是有侵犯隱私的疑慮，在特定場合並不適用，例如社交網站是一個可溝通的網路平台，毋須每位民眾的真實資料都暴露在公共平台上。

政策方面，網際網路的個人隱私受到重視，世界各國也訂定了相關細則，以國內為例，實施個人資料保護「電腦處理個人資料保護法施行細則」，並修正名稱為「個人資料保護法施行細則」[3]。「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者；處刑法有期徒刑、併科新臺幣罰金。」對於自然人、企業、政府單位若誤觸法條，都將面臨極大的賠償。

為有效解決網際網路身分隱匿與實名制攸關網路自由等爭議問題，本研究擬以一個介於實名制與匿名制之間的使用者「記名制」之理論，使用記名憑證規範認證身分行為，只有特定的單位和特定的方式可以單向追蹤使用者的真實身分，其餘人皆無法追蹤對方的真實身分，同時呈現實名制與匿名制之優勢。

為了讓接收方相信使用者的身分，我們使用公開金鑰架構，使用者尋找可信任的第三方作為憑證管理中心(Certificate Authority，簡稱 CA)，它的功能有提供憑證簽發、註銷與保存。一般來說，CA 發給使用者一個憑證，在 X.509規範中必須包含使用者的身分、發行者名稱、有效日期和演算法等[4]。我們的方案是使用者將使用者自己的 ID 與其他真實資料傳給 CA，CA 基於使用者 ID 產生一個不具實名的憑證，在此我們稱為無記名憑證(Implicit Certificate)。它包含了一個新的公開金鑰和一個「假名」。任何人收到記名憑證都只知道假名而不知道使用者真正的身分，只有 CA 可以連接到使用者真正的身份。如此一來，使用者不僅隱藏自己真實身份，接收方仍然能夠由記名憑證來確信訊息的真實性。



圖二、具可追蹤性無記名憑證考慮呈現實名制與匿名制之優勢

本文藉由網路相關行為之資料蒐集、法規，現有的網路隱匿行為，做為本研究建議方案之用；其次相關知識、文獻，著重於網路隱匿身分行為探討，分析記名方案確實可行；最後，植基在隱式憑證概念下，使用憑證及橢圓曲線 ElGamal 達到記名制的目標，提高偽冒身分門檻，又可對網路隱匿進行防制，暨可達到確認使用者身分，又不會暴露全部真實資料。

二、相關知識與技術

為了實現無記名憑證，我們先介紹現今的憑證和密碼學相關技術，包括公開金鑰基礎建設、橢圓曲線 ElGamal 數位簽章和雙線性配對。

2.1 公開金鑰基礎建設

許多憑證機構的憑證作業會要求申請

憑證時，認證真實身分，因此使用憑證是網路實名制的重要步驟，如網路申報所得稅攸關使用者權益，在網路上必須按照實名要求。

憑證將使用者的個人身分跟公開金鑰鏈結在一起，其中每個 CA 使用者的身分是唯一的，藉以辨識個人身分。公開金鑰基礎建設(Public key Infrastructures, PKI)包含了簽發憑證相關細節，例如法令、CA 以及相關技術環節。憑證目前被視為一個有效解決不安全網路環境的方案，在公開環境且使用者互不相識，所以特別重視使用者的金鑰安全性及真實性。為了證明某一把公鑰確實是某人或某單位所擁有，利用可信任的第三方機構來當作管理中心來證明公鑰的真實性。因此建立一個 CA 來負責簽發電子憑證來證明公鑰效力。大致來說，PKI 的設置使得使用者可以提出認證，並使用公鑰憑證內的公鑰資訊加密訊息傳送給對方。解密時，使用者利用自己的私密金鑰解密。

PKI 也被各國政府拿來做為電子政府的安全基礎建設，以國內為例，我國依照 ITU-T X.509標準建置的階層式 PKI，包含 PKI 的信賴起源(Trust Anchor)政府憑證總管理中心(Government Root Certification Authority, GRCA)，及各政府機關所設立的下屬 CA 所組成，由 GRCA 簽發 CA 憑證給下層的 CA，各下屬憑證與主管機關。以提供網路報稅、電子公路監理、電子發票、醫療系統、電子病歷等[5]。我國政府目前公鑰基礎建設架構如圖三所示。

圖三、目前公鑰基礎建設架構

(資料來源: 政府公開金鑰基礎建設[5])

PKI 元件包含 CA、註冊管理中心、儲存庫。CA 負責簽發公開金鑰憑證，透過對用戶憑證簽署數位簽章來擔保用戶公開金鑰的真實性，以防止惡意人士假冒用戶的公開金鑰。註冊管理中心建立及確認申請人的真實身分，負責執行憑證申請、資料審核；而 PKI 需要儲存庫來存放憑證的相關資訊，包含 CA 所簽發的憑證以及憑證廢止名冊(Certificate Revocation List , CRL)。儲存庫提供 CA 的憑證及廢止的憑證清單的公布、查詢、下載，同時也提供憑證實務作業基準和相關訊息。

2.2 橢圓曲線之 ElGamal 數位簽章

在網路通信中，人們希望在某些重要的文件中附上類似親自簽名的機制，而數位簽章提供了類似「電子蓋章」。希望能由數位簽章來確定訊息來源是特定之當事人所發送。

西元1985年由 Koblitz 與 Miller 同時在不同會議及期刊提出的橢圓曲線公開金鑰密碼學技術[6][7]，不只能應用在密碼學加解密、數位簽章、金鑰交換等，也能應用於大整數分解(factorization)與質數判斷(primality testing)。橢圓曲線在密碼學受到重視的原因，主要因為分布在橢圓曲

線，在相同長度時安全性優於基本模運算(包含離散對數與因式分解)的公開金鑰密碼系統。以目前所知評估的計算複雜度，橢圓密碼曲線160-bit之金鑰安全性相當於金鑰為1024-bit 的 RSA 密碼 [8]。在相同的安全強度下，ECC 的金鑰長度比 RSA、DSA 小且處理速度較快，意即 ECC 每個金鑰位元所能提供的安全性遠超過其他公開金鑰密碼系統，適合在 IC 卡或記憶體有限的裝置上使用。

表一、NIST 推薦的密鑰大小

(資料來源: 美國國家標準局(NIST)[8])

安全性	RSA 金鑰長度	ECC 金鑰長度
2^{80}	1024	160~223
2^{112}	2048	224~255
2^{128}	3072	256~383
2^{192}	7680	384~511
2^{256}	15360	521+

以橢圓曲線離散對數問題為基礎的公開金鑰密碼系統都要制定曲線參數值：

1. 制定欲計算之橢圓曲線$E = E(q; a, b)$, $P = (x_1, y_1), Q = (x_2, y_2)$為曲線上任意兩點接著
   - 選取質數體GF(p)，取q為某質數p，則曲線
   $E: y^2 = x^3 + ax + b\ (mod\ p)$ (1)
   - 選取二元體GF(2^m), q 為 m 次不可分解多項式，則
   $E: y^2 + xy = x^3 + ax^b + b/F_{2^m}$ (2)
2. 計算$g = \#E(F_q)$
3. 選擇$E(F_q)$上的某點 P，使得
   $n = \text{ord}(P)$有大質數因子
   $h = {\#E(F_q)}/{\text{ord}(P)}$ 很小
4. 曲線參數值$(E/F_q, P)$ 代表
   $(q, a, b, g, x(P), y(P), ord(P), h)$。

本系統以橢圓曲線之 ElGamal 數位簽章做為基礎。Alice 將訊息 m 轉成簽章 s 傳給 Bob，其中m為整數且$0 \le m \le n$。

- 曲線參數協定$({E}/{F_q}, P)$
- **金鑰產生**

  1. Alice 隨機選取整數 a 且a 滿足 $gcd(a, g) = 1$，計算$P_a = [a]P$。

  公開金鑰$({E}/{F_q}, P, P_a)$，私鑰值為 a。

- **數位簽章**

  1. Alice 任選一整數 k 且 gcd (k, g)=1
  2.計算$R = [k]P$
  3.計算
  $s^* = k^{-1}\big(m - ax(R)\big) \bmod n$ (3)
  $x(R)$為點 R 之 x 座標
  4.將簽章$s = (m, R, s^*)$傳給 Bob

- **驗證**

  1. Bob 收到$s = (m, R, s^*)$並取得 A 公鑰 $({E}/{F_q}, P, P_a)$
  2.計算
  $V_1 = [x(R)]P_a + [s^*]R,$ (4)
  $V_2 = [m]P$ (5)
  3. $V_1 = V_2$則接受，否則拒絕。

數位簽章最重要的特性在於不可否認性和不可偽造性。只有擁有私密金鑰的人才能夠簽出正確的數位簽章，攻擊者若要偽造簽章必須面臨到橢圓離散對數問題(ECDLP)，在數學計算上難以在有限時間內解出的問題。ElGamal 數位簽章在每次簽署過程中除了使用了私密金鑰外還加入了隨機亂數，所以即使是同一位簽署者對於相同明文依然可以簽署出不同的簽章。

2.3 雙線性配對

雙線性配對函數（Bilinear Pairing）如 Weil Pairing 和 Tate Pairing[9][10]，其定義為兩個循環群之間相對應的線性映射關係，詳細說明如下。

令G_1, G_2為加法群，生成子點 P，形成大小 q 的循環乘法群G_T。令有一函數 $e: G_1 \times G_2 \to G_T$ 能將橢圓曲線上的點映射到乘法群 G_T。這種 Bilinear Pairing 符合如下三個特性：

1. 雙線性(Bilinear)：令點P_1、$P_2 \in G_1$，$Q \in G_2$，則：
   $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$，
   $e(aP, bQ) = e(P, Q)^{ab}$；
   其中a和b屬於Z_q^*
   當這裡的G_T為阿貝爾環(Abelian ring)，G_1, G_2群同態的情況，滿足 $e(aP, Q) = e(P, aQ)$。
2. 非退化性(Non-degenerate)：存在 $P \in G_1$和$Q \in G_2$，使得$e(P, Q) \neq 1$;
3. 可計算性(Computability):任兩點 P,Q，存在有效算法計算$e(P, Q)$。

三、隱式憑證概念

此處介紹 Nader M.Rabadi 提出的隱式憑證方案「Anonymous Group Implicit Certificate Scheme」[11]，在此方案中，Nader 使用隱式憑證[12]和橢圓曲線加密，以實現用戶的匿名性，身份驗證和數據完整性。首先介紹系統初始設定，之後分成金鑰生成、簽署與驗證步驟。

3.1 系統初始設定

一般來說，CA 頒發的認可用戶的唯一公鑰憑證。該認證綁定一個唯一的公鑰。該憑證包含用戶的公鑰，用戶的身份，憑證頒發者的名稱，並使用由 CA 認可該憑證的加密演算法。

首先，令 E 為橢圓曲線，P 為 E 上的一點，質數 n 為 P 的序。設$c_A \in [1, n-1]$作為 CA 的私密金鑰，$C_A = c_A P$為公開金鑰。，CA 對某群組 j 生成私密金鑰 $u_j \in [1, n-1]$，公開金鑰 $U_j = u_j P$。CA 也對此群組產生隱式憑證I_j，該隱式憑證I_j包含群組最低限度的身分標識、CA 的身分以及憑證的有效期限。H 代表安全雜湊函數且輸出長度為 $|H|$。CA 計算 $e_j = H(I_j || U_j)$。

使用者向 CA 註冊申請憑證，CA 將使用者分配到資料庫的使用者群組裡。令群組 j 裡的使用者身分表示為i，CA 進行以下步驟：

1. 產生使用者 i 的私鑰 $\{b_i, t_i\}$和公鑰 $B_i = b_i P$。
2. 產生使用者 i 的簽章
   $s_i = e_j u_j + b_i^{-1} c_A + t_i u_j \bmod n$。 (6)

最後，CA 儲存使用者 i 的私鑰$\{b_i, t_i\}$、公鑰B_i、 CA 的簽章 s_i、CA 的公鑰C_A、群組的公鑰U_j，和使用者所在的群組隱式憑證 I_j。

3.2 金鑰生成與簽署步驟

令 M 表示為使用者在通訊網路中的訊息，其中包含了時間戳記作為重送攻擊的保護。當使用者 i 準備好廣播 (Broadcasts) M 時，進行以下步驟：

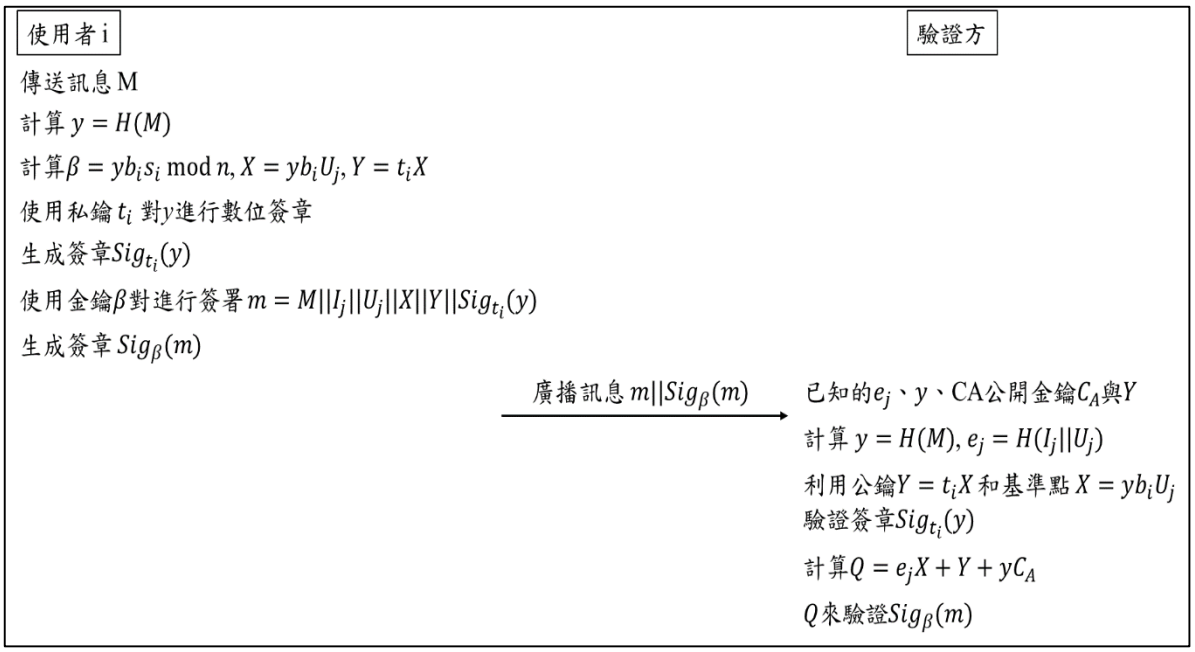
1. 計算 $y = H(M)$。
2. 計算 $\beta = y b_i s_i \bmod n$，$X = y b_i U_j$，$Y = t_i X$。$X$為曲線上的一個基準點。
3. 使用私鑰 t_i 對 y 進行數位簽章演算法，

此方案中採用 Elliptic Curve DSA。假設 X 為簽署 y 時 $E(F_q)$上的一個基準點，則生成簽章$Sig_{t_i}(y)$

4. 使用金鑰 β 對進行簽署 $m = M||I_j||U_j||X||Y||Sig_{t_i}(y)$，生成簽章 $Sig_\beta(m)$
5. 使用者廣播訊息 $m||Sig_\beta(m)$

驗證方可以利用已知的e_j、y、CA 公開金鑰C_A與Y來構築使用者私鑰 β相對應的公鑰$\beta P = e_jX + Y + yC_A = Q$來驗證簽章，其步驟如下：

1. 計算 $y = H(M), e_j = H(I_j||U_j)$
2. 利用公鑰$Y = t_iX$ 和基準點 $X = yb_iU_j$ 驗證簽章$Sig_{t_i}(y)$
3. 通過計算$Q = e_jX + Y + yC_A$來建構使用者的公鑰，並利用 Q 來驗證 $Sig_\beta(m)$



圖四、金鑰生成與簽署步驟

四、可追蹤無記名協定架構

在過去，已有許多學者對使用者身分的匿名提出方法。例如在2001年 Rivest 等人提出「How to leak a secret」[13]。利用環簽章的簽署者身分之不可確定性來隱藏使用者的真實身分，藉以達到匿名性。然而這些文獻的協定滿足了使用者匿名性，卻未能追蹤使用者身分。若有惡意的使用者利用匿名之特性進行不法行為，我們將難以追查使用者身分。

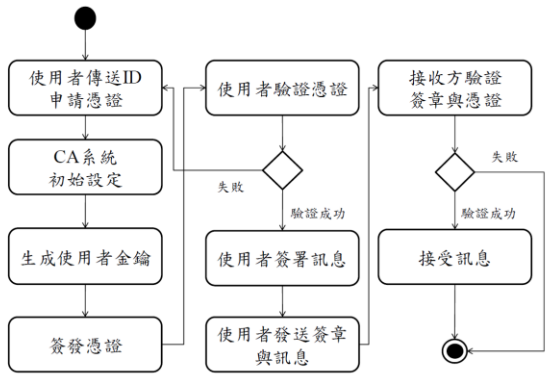
一般社交網站與其他開放式線上平台，使用者的身分資訊毋須暴露在公共平台上。因我們的方案具有匿名性，使用者在網站發言時可以保護自己的真實資料；當使用者在網站上抹黑或毀謗他人，當事人與警方可以請 CA 揭示使用者真正的身分。

我們提出的方案主要有三個角色，分

別為可信任的第三方 CA、使用者 Alice、接收方 Bob [14]。CA 角色是可以信賴的第三者(Trusted Third Party, TTP)，若 CA 造假或是洩漏用戶隱私，例如重複簽署同一使用者金鑰，系統無法預防。其流程為系統初始設定、CA 簽發憑證、使用者數位簽署與驗證階段。參數定義如表二所示，系統流程圖如圖五所示，流程步驟詳述於各小節。

表二、系統架構參數列表

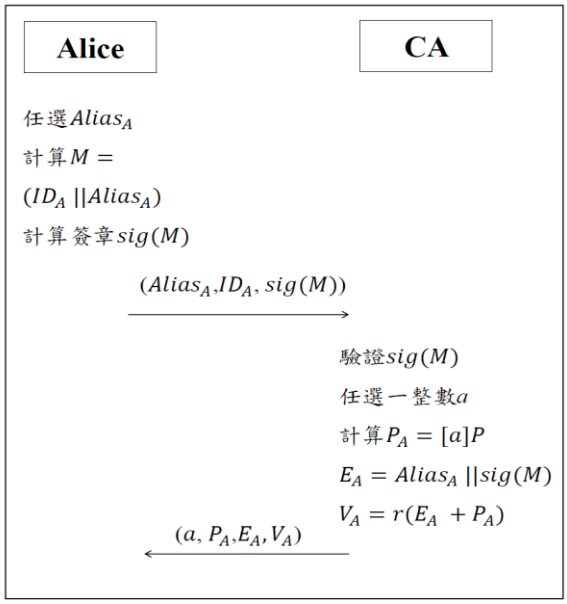
ID_A	使用者的身分
$Alias_A$	使用者登錄憑證的假名
$sig(M)$	使用者對自己身分的數位簽章
P	橢圓曲線上的一基準點
P_{CA},r	CA 的公、私鑰
P_A,a	使用者的公、私鑰。
(E_A,V_A)	使用者的憑證



圖五、系統架構動態圖

4.1 系統初始設定

使用者首先需要跟 CA 申請公、私鑰和憑證，必須事先擁有憑證才能進行往後的簽署階段，如圖五所示。Alice 用自己的真實資訊向 CA 註冊申請記名的憑證並登錄一個使用者名稱 $Alias_A$。Alice 對自己的身分資訊 $M = (ID_A \,||Alias_A)$ 進行數位簽章，如 ECDSA，計算出簽署文 $sig(M)$ 發送給 CA。CA 本身往往藉由階層式認證及自簽憑證存放於公開資料庫具以辨識身分，通常事先下載儲存。初始階段若欲在 Alice 及 CA 間實施中間人攻擊，往往需在內部網路偽造網站，並作 IP 偽造，這部分需藉由資安內部管控加強，此外，也需事先偽造 CA 自簽憑證，難以實施。



圖六、系統初始設定

CA 獲取 Alice 公鑰並驗證簽章 $sig(M)$，若驗證正確則 CA 依據 Alice 提供的資料生成私鑰 a、公鑰 $P_A = aP$，憑證 $E_A = Alias_A \,\|\, sig(M), V_A = r(E_A + P_A)$。CA 將金鑰對 $\{a, P_A\}$ 和憑證 $\{E_A, V_A\}$ 傳送給 Alice，將 Alice 的身分相關資訊以及簽章 $sig(M)$ 儲存到硬體設備。

Alice 收到金鑰對 (a, P_A) 及憑證 (E_A, V_A) 後，驗證 (E_A, V_A) 是否為合法的憑證 $e(V_A, P) = e((E_A + P_A)), P_{CA})$。

4.2 使用者簽章及驗證

使用者簽章步驟如下：Alice 接收到

憑證和金鑰後，對於欲發送的訊息 m 進行數位簽章，如圖六所示。

首先先任選一整數k且 $\gcd(k,g)=1$，雖然使用者的公開金鑰和私密金鑰都是同一對，但是每次簽署訊息都需要一個新的隨機亂數。簽章計算如下列步驟：

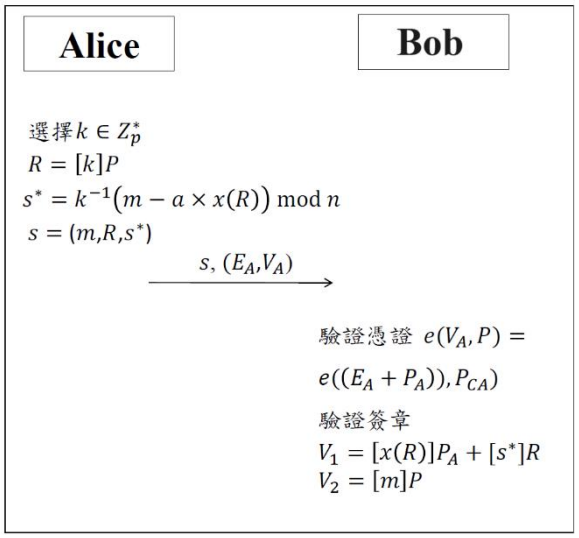
$$\begin{cases} R=[k]P \\ s^*=k^{-1}\big(m-a\times x(R)\big) \bmod n \end{cases} \quad (7)$$

最後使用者發送數位簽章$s=(m,R,s^*)$,憑證(E_i,V_i)。

驗證過程是接收方收到數位簽章s並取得使用者之公鑰$(E/F_q,P,P_i)$，進行驗證憑證和簽章：首先確認 $e(V_A,P)=e((E_A+P_A)),P_{CA})$，並檢查$V_1=V_2$?

$$\begin{cases} V_1=[x(R)]P_i+[s^*]R \\ V_2=[m]P \end{cases} \quad (8)$$

若$V_1=V_2$，則訊息就會被接受；否則就會被拒絕。



圖七、簽署與驗證階段

對於協定的應用舉兩個例子如下，應用一：一般社交網站與其他開放式線上平台，因為隱式憑證具有使用者匿名性，使用者在網站發言時可以隱藏自己的真實資料；但是當使用者在網站上抹黑或毀謗他人，當事人與警方可以請 CA 找出使用者真正的身分。應用二：常見的線上購物或其他電子商務，店家首要關心的是能否順利收到錢或電子現金是否有效，對於使用者的真實資料為其次，因此下訂單的消費者可利用隱式憑證來保有匿名特性，若是消費者違反合約，那麼店家可請 CA 揪出消費者真正的身分來進行制裁。

五、安全性分析

對我們所提出的方案做安全性分析，包括正確性、匿名性、不可偽造性、可追蹤性、重放攻擊及不可否認性等部分。效能部分，牽涉到各類雙線性配對演算法實作，本文不探討。相關分析及比較如下：

5.1 正確性

憑證驗證證明：

$$\begin{aligned} e(V_A,P)&=e((E_A+P_A),P_{CA}) \\ e(V_A,P)&=e(r(E_A+P_A),P) \\ &=e\big((E_A+P_A),rP\big) \\ &=e\big((E_A+P_A),P_{CA}\big) \end{aligned} \quad (9)$$

簽章驗證證明：$V_1=V_2$

$$\begin{aligned} V_1&=[x(R)]P_A+[s^*]R \\ &=[x(R)][a]P+\big[k^{-1}\big(m-ax(R)\big)\big][k]P \\ &=[a\times x(R)+m-a\times x(R)]P \\ &=[m]P \\ &=V_2 \end{aligned} \quad (10)$$

5.2 匿名性

CA 把含有 Alice 真實身分之部分加密並嵌入憑證。Alice 將訊息附於憑證一同發送，Bob 能夠從憑證$e(V_A,P)=e((E_A+P_A),P_{CA})$驗證使用者公鑰之合法性，Bob 驗證過程中並無法知道有關對方的身分線

索。假如 Bob 試圖攻擊憑證$E_A = Alias_A \| sig(M)$來獲得對方身分，則將面對解橢圓曲線離散對數問題；同時，除了 CA 外其他人難以獲得ID_A，攻擊者無法從憑證(E_A, V_A)識別特定當事人的真實身分，因此我們的系統達到匿名性。

5.3 不可偽造性

現有一攻擊者 Eve 取得 Alice 的公開金鑰P_A，對訊息m偽造 Alice 的簽章。Eve 必須找出含有訊息的兩個有效簽章R和s^*來偽造 Alice 的簽章。

Eve 選擇 R 來計算s^*，她需有$[m]P = [x(R)]P_A + [s^*]R$，換言之，$s^* = ([m]P - [x(R)]P_A)R^{-1}$，而$R = [k]P$的變化取決於使用者任意選擇的亂數，這表示 Eve 要偽造簽章必須計算橢圓離散對數問題(ECDLP)，這是非常困難的。我們設計使用者記名制系統，基於解橢圓離散對數問題困難度的假設，(R, s^*)為m之合法簽署文。由於 Eve 對m並無控制能力，想要偽造簽署文(m, R, s^*)，必須擁有使用者亂數k才有辦法偽造簽章，故本系統數位簽章仍屬安全。因此設計的系統達到簽章不可偽造性。

5.4 可追蹤性

過去的文獻大多是隱匿用戶身分，而未考量匿名的潛在危險。可追蹤記名協定的特性在於每個人都可以驗證憑證的合法性，但是不知道誰是真正的持有人，只有 CA 知道持有人的真實身分。當持有人從事不法行為，法院要求 CA 需追蹤出持有人真實身分時，CA 藉由憑證中之E_A內容，檢查使用者的簽章$sig(M)$來確認出 Alice 的真實身分。CA 對憑證(E, V)解密含有真實資訊的E_A還原出使用者的真實資料，因此我們的系統有達到可追蹤性。

5.5 不可否認性

假設法院要求 CA 公開嫌犯 Alice 的資料做為物證當參考，於是 CA 使用者 Alice 的真實身分交給法院做證物。為了以防有任何一方做偽證或否認公告結果與自己所持有之憑證不相符的情況，憑證內需要一個強力的證據使得任何一方皆無法偽造及抵賴結果。我們將情況分為 CA 不誠實以及使用者不誠實兩種情況探討。

第一種情況是使用者不誠實，Alice 欲否認自己的罪刑，遂聲稱 CA 公告的結果與自己持有之憑證不相符來脫罪，則 CA 公告憑證所含有使用者的數位簽章$sig(M)$及身分資訊$M = (ID_A \| Alias_A)$。$sig(M)$為初始 Alice 對自己身分資訊$M = (ID_A \| Alias_A)$生成的簽章，具有簽章之不可偽造性，讓 Alice 無從抵賴身分。

第二種情況是 CA 不誠實， CA 作偽證不利於 Alice。Alice 亦可使用$sig(M)$和 CA 公告的結果進行比對。雖然 CA 可以驗證 Alice 的數位簽章$sig(M)$，卻無法偽造 Alice 的簽章，即 Alice 的簽章$sig(M) \neq$ CA 偽造的簽章$sig'(M)$， CA 亦無法將 Alice 的身分認證給其他人。

以上兩種情況都可以進行抵禦，使得結果更具有公信力，任何一方都無從否認，因此我們的系統達到身分之不可否認性。

5.6 重放攻擊

重放攻擊(Replay attack)一般用以癱瘓系統服務，主要傳送大量系統可接受的

服務請求而不回應導致系統癱瘓。就目前使用者簽章及驗證過程，首先攻擊者必須事先取得 Alice 的傳送內容與簽章，在加以重送，便有一定困難，最重要是可以藉由檢查簽章內容，即使正確若是內容重複丟棄即可，系統不用額外等待回應，重送攻擊的疑慮可忽略。當然也可加上 Nonce 檢查回應，加強系統防護。

5.7 比較

本文是基於橢圓離散對數及雙線性配對且具備了保護使用者的身分遭辨識與竊取，對應使用者真正資訊的參數是秘密不被公開的，協定中的參數是可以控制但不被偽造的；另一方面在必要時刻，法院可傳喚 CA 提供物證公布憑證持有人的真實資訊，對應使用者資訊的參數是無法被偽造且使用者不可否認，使得本論文協定更具有公信力。我們將表達一些安全性的項目，並使用表三來顯示過去文獻的方案與本論文方案之間的比較。

表三、本論文與其他協定之功能性比較

	Rivest et al Scheme [13]	Rabadi Scheme [11]	Z. Chen et al Scheme [15]	Proposed Scheme
A1	✓	✓	✓	✓
A2	✓	✓	✓	✓
A3		✓	✓	✓
A4				✓

A1. 身分保護；

A2. 簽章及身分之不可偽造性；

A3. 有效追查使用者真實身分；

A4. 真實身分的不可否認性；

六、結論

我們分析過去網路身分匿名之技術及相關法律，發現多數研究著重於隱匿用戶身分，其缺點在於利用隱匿及竄改身分的網路犯罪會對追緝造成困難。實施實名制認證使用者之身分可以規範網路犯罪行為，卻可能衍生其他問題，如侵害隱私。我們希望保護身分隱私的同時不因侵犯隱私之疑慮而有損民眾的接受意願。因此本研究提出一個具可追蹤性之無記名憑證應用協定，基於公開金鑰基礎建設及橢圓密碼學技術保護身分隱私，並保存身分記錄來強化身分的可追蹤性。

本研究實現匿名性、身分認證之需求和身分的不可否認性。使用者對憑證中心註冊自己的真實身分，由憑證中心做背書簽發一個不具實名的憑證。研究中是以認定 CA 角色是可以信賴的第三者(Trusted Third Party, TTP)，若 CA 造假，例如重複簽署同一使用者金鑰，系統無法預防。另外，若 CA 有洩露用户隱私的情事發生的話，本系統也無法預防。

本研究將身分的紀錄嵌入至憑證中，隱藏真實資料來保護個人身分隱私，任何人皆能夠驗證憑證的正確性，但是他無法從憑證的資訊直接辨識出特定之當事人；一旦持有人利用隱匿進行網路犯罪行為，憑證中心可透過記錄留存追蹤持有人之身分資訊，並且避免了證據不足使得持有人脫罪的情況。不僅達到匿名制隱匿身分之特性，更實現實名制的可追蹤性，同時兼顧網路的便利和安全，符合網路自由權和辨識身分之需求。

參考文獻

[1]楊吳泉等人, ”網際網路隱匿與竄改身

分之行為態樣及其防治技術研究期末報告”, 國家通訊傳播委員會研究報告，https://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=1812, 2011.11。

[2]警政署統計室, "警政統計通報(112年第28週)," https://www.npa.gov.tw/ch/app/data/doc?module=wg057&detailNo=1128133397835681792&type=s , 2023.07。

[3]全國法規資料庫, 個人資料保護法施行細則, https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050022 , 2016.03。

[4] ITU-T X.509, “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks,” https://www.itu.int/rec/T-REC-X.509-201910-I/en, 2019.

[5]台灣政府公開金鑰基礎建設, https://grca.nat.gov.tw/index2.html, 查詢時間: 2024.03.20。

[6]Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation 48 (177): 203–209, JSTOR 2007884, 1987.

[7]Miller, "Use of elliptic curves in cryptography", CRYPTO 85, pp. 417–426, 1985

[8]National Institute of Standards and Technology(NIST), http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-57Part1_3-8-07.pdf, 查詢時間: 2020.07.18。

[9]A. Joux, “The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems,” in Proceedings Fifth Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Springer-Verlag , 2002.

[10] D. Boneh, B. Lynn and H. Shacham, “Short Signatures from the Weil Pairing,” Advances in Cryptology-Asiacrypt’01, LNCS 2248, pp. 514-532, Springer, 2001.

[11] Nader M. Rabadi, ”Anonymous Group Implicit Certificate Scheme,” in Consumer Communications and Networking Conference (CCNC), 2010.

[12] D. R. L. Brown, R. P. Gallant and S. A. Vanstone, "Provably secure implicit certificate schemes," in the Proc. of the 5th International Conference on Financial Cryptography, 2002.

[13] R.L. Rivest, A. Shamir and Y. Tauman, “How to leak a secret,” Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.552-565, Springer-Verlag, 2001.

[14] 楊吳泉、黃振宗, “基於隱式憑證之可追蹤記名協定”，第24屆全國資訊安全會議, 2014.05。

[15] Z. Chen, S. Chen, H. Xu and B. Hu, "A security scheme of 5G ultra dense network based on the implicit certificate", Wireless communication and mobile computing, vol. 2018.

Traceable Alias Protocol based on Implicit Certificate

Wu-Chuan Yang[1,2], Lien-Yuan Ting[1], Zhen-Zong Huang[1], Kai Chain[2]

[1]Department of Information Engineering, I-Shou University

[2]Department of Intelligent Network Technology, I-Shou University

Abstract

With the rapid development of the Internet, its anonymity and freedom have fostered the diversification of online applications in services and industry development, allowing users to easily access a wealth of convenient information. However, this has also led to numerous improper online behaviors, including crimes committed through hiding and falsifying identities. For safety and the verification of true identities, implementing an online real-name system to prevent hiding and falsification of identities is an important aspect. Yet, this system faces controversies regarding the culture of online anonymity and individual privacy rights. To balance safety and convenience, this study is based on Rabadi's concept of implicit certificates, proposing a "Traceable Anonymity Certificate Application Protocol." This protocol aims to find a middle ground between real-name and anonymity systems by integrating certificate and digital signature mechanisms. Besides standardizing identity verification behaviors and raising the threshold for identity impersonation, it also allows for the concealment of users' real identities to achieve anonymity. In case of disputes, users' identity information can be verified through specific methods.

Key words：Implicit Certificates, Identity tracing, Elliptic Curve Cryptography