基於雙線性配對之身份基底特定驗證者簽章方法

Identity-Based Strong Designated Verifier Signature Scheme from Pairings

吳宗杉
國立台灣海洋大學
資訊工程系
ilan456@gmail.com

高俊海
國立台灣海洋大學
資訊工程系
sseakao@gmail.com

林韓禹
國立交通大學
資訊工程系
hanyu.cs94g@nctu.edu.tw

黃世豪
佛光大學
資訊學系
hao.430@gmail.com

摘要 **— 以身份辨識為基礎的密碼系統 (Identity-Based Cryptosystems) 由 Shamir 於 1984 年提出。在此系統中，任意第三者 (Third Party) 可由簽署者的身份推導出其公開金鑰，進而驗證所產生簽章的合法性。在 2003 年，Saeednia 等學者率先提出植基於解離散對數問題 (Discrete Logarithm Problem) 之堅固特定驗證者簽章方法，目的在於僅允許簽署者所特定的驗證者才可驗證此簽章，以滿足機密性之需要。同時，特定驗證者具備產生新的簽章副本能力，因此，他無法說服任意第三者相信他所驗證簽章的真確性。本論文以 Waters 所提之身份辨識公開加密方法為基礎，進一步提出植基於雙線性配對 (Bilinear Pairings) 之身份辨識堅固特定驗證者簽章方法，並且滿足不可偽造性、不可轉移性與 來源隱密性等安全性需求。**

關鍵詞 **— 身份辨識、特定驗證者、雙線性配對。**

Abstract **— In 1984, Shamir introduced the identity-based cryptosystem in which any third party can first acquire the signer's public key with his public identity and then verify the resulting signature. In 2003, Saeednia *et al.* proposed the first strong designated verifier signature scheme based on discrete logarithm problem. In their scheme, only the designated verifier can verify the signer's signature, so as to ensure the confidentiality. Besides, the designated verifier has the ability to generate another valid signature transcript intended for himself. Hence, the designated verifier cannot convince any third party of the signature's authenticity. In this paper, we modify Waters's identity-based encryption scheme to propose an identity-based strong designated verifier signature scheme from pairings. Our scheme satisfies the security requirements of unforgeability, non-transferability and source hiding.**

Keywords **— Identity-based, Designated Verifier, Bilinear Pairings**

一、簡介

金鑰必須在具備安全的通道環境下進行傳送，密碼學大師Diffie與Hellman在1976年提出公開金鑰 (Public Key) 密碼學的概念 [6]，此概念為密碼學的研究開闢新的方法。數位簽章機制 (Digital Signature Scheme) [7, 17] 是最為被廣泛被應用的技術之一，主要是利用公開金鑰密碼系統 (Public Key Cryptosystem) [6, 8, 17, 20] 確保簽章加密的完整性 (Integrity)、鑑別性 (Authenticity) [21] 及不可拒絕性 (Non-Repudiation) [11]。大部分公開金鑰的產生方式都是由系統當權者 (System Authority) 所

持有或管理；驗證方式則可透過第三者 (Third Party) 的方式來驗證簽章的合法性，因此簽章者對於自己所產生出來的簽章具有不可否認性的特質，且驗證過程中也必須確保第三者的公平性。但是，從過去研究中發現如電子投票 [16, 19]，似乎不完全能滿足公開金鑰密碼系統中的不可否認性，以及Chaum和Antwerpen於1990年提出的不可否認性簽章機制 (Undeniable Signature Scheme) [5]，對於第三者驗證簽章過程中，無法提供安全的環境。

在1996年，Jakobsson、Sako和Impagliazzo等學者提出特定驗證者簽章 (Designated Verifier Signature, DVS) [11] 機制，此機制率先提出非互動性 (Non-Interactive) 不可否認 (Undeniable) 簽章機制。在DVS中，特定驗證者要能取信於簽章者，並將以簽署好的不可拒絕數位簽章交由特定驗證者來驗證簽章是否具備合法性，由於特定驗證者本身可以經由已收到的簽章，並再次產生與最初DVS具相同特性的DVS，因此非互動性即意味，特定驗證者自我產生的DVS，無法再交由他人驗證，亦無法取信於他人。

近年來，此議題的簽章方式廣泛受到重視，Galbraith和Mao [8] 提出建構於RSA非互動性不可否認簽章機制應用於多位使用者並具有匿名性 (Anonymity) 和不可見性 (Invisibility) 的特性。Libert和Quisquater [13] 於2004年提出身份辨識不可否認簽章機制，該方法是由Galbraith和Mao所演變而來，並採用雙線性配對的方式完成簽章機制。在 [12] 中，Jakobsson等人亦簡短對「堅固」概念提出見解，結合DVS稱之堅固特定驗證者簽章機制(Strong Designated Verifier Signature, SDVS)，此概念在說明，特定驗證者被要求使用自己的私鑰來驗證簽章的合法性，因此，整個過程中就只有簽章者本身和特定驗證者雙方能擁有已簽訂的數位簽章，而特定驗證者收到該簽章後，亦不能向他人來證明簽章的擁有者。然而，在2003年，Wang [22] 針對上述提出新的見解，認為在Jakobsson等學者所提出的方法中，攻擊者能輕易的偽裝成特定驗證者，使得在接收簽章及驗證簽章過程中不被發現；同年，Saeednia等人 [18] 提出安全性基於離散對數 (Discrete Logarithm) 下的堅固的特定驗證者簽章，主要目的在於不需要第三方的驗證下，簽章驗證者與接收者Bob能在有限的自我運算成本下驗證傳送者Alice所傳送過來的簽章，而無人可以在未得知Bob的私密金鑰下進行簽章驗證過程。

綜合上述我們整理出在SDVS機制中須滿足下列安全性：

(1) 不可偽造性 (Unforgeability)：
在多項式時間 (Polynomial Time) 計算複雜度理論中，攻擊者在沒有獲得驗證者私密金鑰情況下，無法偽造出合法的SDVS，即便是簽章者或是特定驗證者。

(2) 不可轉移性 (Non-Transferability)：
在SDVS中，特定驗證者有能力在有限的計算成本之下，可同時擔任多位被特定者腳色，且產生不同的SDVS，但無法將SDVS轉移給第三者，並取信於第三者。

(3) 來源隱密性 (Source Hiding)：
即便SDVS中的簽章者私密金鑰或是特定驗證者的私密金鑰被取得，也無法從簽章驗證過程中得知簽章者或特定驗證者的身份。

在本論文的第二章中，介紹與本論文有直接相關，且基本的密碼學知識，包含雙線性配對基本數學知識、特色與安全性；介紹身份識別密碼系統的由來與相關應用，以Waters [23]

所提出的身份辨識加密架構方法作介紹；並回顧Jakobsson等人於1996提出的特定驗證者證論(Designated Verifier Proofs) [12]，敘述SDVS各階段的運作。第三章則是針對我們所提出的基於雙線性配對之身份基底特定驗證者簽章方法，主要以Waters所提之身份辨識公開加密方法為基礎，進一步提出植基於雙線性配對 (Bilinear Pairings) 之身份辨識堅固特定驗證者簽章方法，並詳細說明整個簽章過程包含：系統參數階段、簽章產生階段、簽章驗證階段及副本模擬階段，簽章產生過程與驗證等，並針對簽章驗證做正確性推導。第四章為安全性分析，針對本文所提出的簽章進行不可偽造性、不可轉移性及來源隱密性等分析。第五章為本文最後的結論。

二、相關背景知識

(一) 雙線性配對 (Bilinear Pairings)

拜現代數學的快速研究發展之賜，所多過往的計算難題都有新的解決方法。正如 MOV 攻擊法 [14] 一樣，是由 Menezes、Okamoto 和 Vanstone 三人所提出，利用 Weil Pairing 函數的運算特性，能將某些橢圓曲線 (Elliptic Curve) 上的離散對數問題轉至一般已知有限體 (Finite Field) 上的離散對數問題。但是在有限體上要求解離散對數問題則顯得相對容易且有較快的演算法可以得解，因而降低整體使用上的安全度。直到 2000 年 Joux 學者和 2001 年 Boneh 和 Franklin 兩位學者先後再密碼學系統上對雙線性配對函數提出應用後，這樣的情況才有爆炸性的改變。接下來我們將雙線性配對函數與其相關定理有詳細的介紹。

雙線性配對是指兩個循環群 (Cyclic Group) 之間相對應的線性映射 (Bilinear Map) 關係。由於，橢圓曲線上所有點形成的集合，在代數幾何學上會形成「群」(Group) 的關係，因此雙線性配對函數的運算正好能應用於橢圓曲線上。其相關參數與符號如：G 為一序 (Order) 為大質數 q 的循環加法群 (Cyclic Additive Group)，其生成點 (Generator) 為 P，V 則為一序同為大質數 q 的循環乘法群 (Cyclic Multiplicative Group)。在 G 和 V 中解離散對數問題是鄉當困難的，表示方式為 $e: G \times G \to V$ 且對於 $\forall P, Q \in G$ 與 $\forall a, b \in Z$ 滿足下列特性 [3, 26]：

(1) 雙線性 (Bilinearity)：
$e(aP, bQ) = e(P, Q)^{ab}$。

(2) 非退化性 (Non-Degeneracy)：
若 P 為 G 的生成點，則 $e(P, P)$也會是 V 的生成點，即 $e(P, P) \neq 1$。

(3) 可計算性 (Computability)：
$P, Q \in G_1$，存在一演算法可計算 $e(P, Q)$，使計算的時間複雜度為多項式時間。

在密碼學的研究領域裡，為符合系統安全的需求，通常會有許多計算難題的假設，並且在安全假設上，要在多項式時間內求解這些問題的機率是可以忽略的(Negligible)。以下我們針對在雙線性配對中會用的幾個問題作詳細的定義與說明：

(1) 離散對數問題 (DLP)：
令$b \in Z_q^*$為未知數，給定一大質數n和生成點q，要求得$0 \le x \le q-2$且滿足$g^x \equiv b (\mathrm{mod}\, n)$。$Z_q^*$代表一基底為q的所有實數集合。

(2) 橢圓曲線離散對數問題 (ECDLP)：
在有限體F_p之下，給定橢圓曲線E上的兩相異點P和Q，其中當點的序q若夠大時 (大於160位元)，要求得一整數k且

滿足$Q=kP$是很難的計算難題。

(3) 雙線性Diffie-Hellman問題 (BDHP)：

令$a, b, c \in Z_q^*$為未知數，給定$P, aP, bP, cP \in G_1$，計算abc且滿足$e(P,P)^{abc} \in G_2$為解BDH問題。

(4) 決定Diffie-Hellman問題 (DDHP)：

令$a, b, c \in Z_q^*$為未知數，給定$P, aP, bP, cP \in G_1$，要決定abc且滿足$c \equiv ab \bmod q$為DDH問題。

(5) 計算Diffie-Hellman問題 (CDHP)：

令$a, b \in Z_q^*$為未知數，給定$P, aP, bP \in G_1$，要求得ab且滿足$abP \in G_1$為解CDH問題。

由於利用雙線性配對設計出的演算法，皆有設計簡單與效率上的優勢，因此各類數位簽章等相關研究陸續出現於國內外各重要學術會議與期刊之中 [1, 11]。

(二) 身份識別密碼系統 (Identity-based Cryptosystems)

在 1984 年，Shamir [2] 提出基於身份識別密碼系統 (Identity-based Cryptosystem, IBC) 的概念，該系統以使用者的身份識別來做為它的公開金鑰，例如網址位址 (IP Address)，或是電子郵件 (E-Mail Address)。而使用者的私密金鑰則是由一個可信任的第三公正者 (Trust Third Party) 來產生，也就是所謂的私密金鑰產生者 (Private Key Generator, PKG)。

在 2001 年，Boneh 等人提出第一個可行的基於身份識別之加密技術 (Identity-based Encryption Scheme, IBE) [4]。之後，一些基於身份識別的簽章技術 (Identity-based Signature Scheme) [10, 24, 25]、金鑰交換技術(Key Agreement) 等陸續被提出來。

於 2005 年，Waters [23] 在沒有隨機神諭 (Random Oracle) 環境提出身份辨識加密技術，此加密技術則建構雙線性 Diffie-Hellman 問題 (BDHP) 之下，並有效率的時間內，進行加密行為；以下我們僅針對 Waters 所提出的身份辨識加密 (Identity-based Encryption, IBE) 架構方法作介紹：

令 G 為一個群其序為 p；並存在一雙線性映射 $e: G \times G \rightarrow G_1$；$g$：原根；$H: \{0,1\}^* \rightarrow \{0,1\}^n$；此加密方法主要分為四個階段：系統參數設定、金鑰產生階段、簽章加密階段、簽章解密階段。

【系統參數設定】

該階段的參數有：當權者 (Authority) 將隨機選取三值 $\alpha \in Z_p$、$g \in G$ 和 $g_2 \in G$，並決定 $g_1 = g^\alpha$；此外，再隨機選取一值 $u' \in G$，並從 G 中隨機選取 n-length 向量 $U = (u_i)$。最後，$\{g, g_1, g_2, u', U\}$ 為系統公開參數，而 g_2^α 則為主秘密 (Master Secret)。

【金鑰產生階段】

令 v 為 n bit 字串長度的身份 (Identity)；v_i 為身份的第 i bit；$r \in_R Z_p$，使用者計算出

$$d_v = (g_2^\alpha (u' \prod_{i \in v} u_i)^r, g^r),$$

為使用者的私密金鑰。

【加密階段】

當身份者 A 欲對訊息 $M \in G_1$ 進行加密時，需選取一值 $t \in_R Z_p$，並針對 M 進行加密動作，計算

$$C = (e(g_1, g_2)^t M, g^t, (u' \prod_{i \in v} u_i)^t),$$

C 則為加密後的文件。

【解密階段】

收到密文 C，並令 $C=(C_1, C_2, C_3)$ 以及身份者 A 之後，便可以進行解密。首先令 $d_A=(d_1, d_2)$，並計算

$$C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)}$$

$$=(e(g_1, g_2)^t M)$$

$$\frac{e(g, (u'\prod_{i\in v} u_i)^{rt})}{e(g_2, g_2)^t e((u'\prod_{i\in v} u_i)^{rt}, g)}$$

$$= (e(g_1, g_2)^t M)\frac{e(g^r, (u'\prod_{i\in v} u_i)^t)}{e(g_2^{\alpha}(u'\prod_{i\in v} u_i)^r, g^t)}$$

$$=M$$

最後則將原加密過的文件 C 解密回明文 M。

(三) 特定驗證者簽章機制 (Designated Verifier Signature Scheme)

在此我們簡單敘述 Jakobsson 等人於 1996 提出的特定驗證者證論(Designated Verifier Proofs) [12]：

【系統參數階段】

此方法共定義兩個角色：簽章者 U_a、特定驗證者 U_b。U_a 選 $x_a \in Z_q^*$ 為私鑰，計算公鑰

$y_a = g^{xa} \bmod p$；

U_b 選 $x_b \in Z_q^*$ 為私鑰，計算公鑰

$y_b = g^{xb} \bmod p$。

其他參數定義如下：p, q：兩個大質數，使得 $q|(p-1)$；g 為子群 (Subgroup) G_q 的生成點其序為 q；s 為簽章者的數位簽章 $s = m^{xa} \bmod p$；m 為訊息 (Message) ；H 為雜湊函數。

【簽章產生階段】

U_a 隨機選取三個變數 $w, r, t \in Z_q$ ，並計算

$c = g^w y_b^r \bmod p$；

$G = g^t \bmod p$；

$M = m^t \bmod p$；

$h = H(c, G, M)$；

$d = t + x_a(h + w) \bmod q$，

U_a 將 DVS (w, r, G, M, d) 傳送給 U_b。

【簽章驗證階段】

U_b 收到 DVS (w, r, G, M, d) 後，計算

$c = g^w y_b^r \bmod p$；

$h = H(c, G, M)$，

並驗證

$Gy_a^{h+w} = g^d \bmod p$；

$Ms^{h+w} = m^d \bmod p$。

若上述兩等式分別相等，則表示 DVS 通過 U_b 的驗證為合法簽章。

【副本模擬階段】

U_b 隨機選取三個變數 $d, \alpha, \beta \in Z_q$ ，並計算

$c = g^{\alpha} \bmod p$；

$G = g^d y_a^{-\beta} \bmod p$；

$M = m^d s^{-\beta} \bmod p$；

$h = H(c, G, M)$；

$w=\beta-h \bmod q$；

$r = (\alpha-w)\, x_a^{-1} \bmod q$。

最後 DVS (d, α, G, M, r) 為對於訊息 m 而

言，則為另一個合法的 DVS。

三、我們提出的方法

本文我們以 Waters 所提之身份辨識公開加密方法為基礎，進一步提出植基於雙線性配對之身份辨識堅固特定驗證者簽章方法；此簽章方式不同於傳統數位簽章具有可公開驗證性，特定驗證者簽章只允許被指定的驗證者可以驗證簽章的正確性，並確保簽章者的隱私性，安全性則建構於雙線性配對。

在此新方法中簽章處理過程有簽章者與特定驗證者雙方。而新方法建構於雙線性配對下亦能有效滿足不可偽造性、不可轉移性、來源隱密性等安全性考量，本章節將我們提出的新簽章技術分為四階段，分別如下所述：

【系統參數階段】

$\boldsymbol{G}_1$ 為一序大質數 q 加法群，其生成點為 p，$\boldsymbol{G}_2$ 則為一個序同為大質數 q 的乘法群；g：生成點；h：雜湊函數；而 $e: \boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ 為雙線性映射且會滿足雙線性配對特色。系統管理者 (System Authority) 依序產生下列各參數值：

隨機選取 $\alpha \in_R Z_q$ 和 $g_2 \in_R \boldsymbol{G}_1$，計算

$$g_1 = g^{\alpha} \quad , \tag{1}$$

令 g_2^{α} 為主秘密 (Master Secret)，

並將值回傳給 U_i，其 i 泛指所有使用者的變數，如 U_s 是簽章者 $(i = s)$，U_v 驗證者 $(i = v)$；最後，U_i 收到後計算兩組私密金鑰

$$x_{i_1} = g_2^{\alpha} h(id_i)^{k_i} \quad ; \tag{2}$$

$$x_{i_2} = g^{k_i} \quad , \tag{3}$$

其中 $k_i \in_R Z_q$ ；並將 (g, g_1, g_2) 公開。

【簽章產生階段】

該階段共有兩位參予者簽章者 U_a、特定驗證者 U_v；U_a 隨機選取 $t, w \in_R Z_q$ ，並計算

$$S = (e(g_1^{h(m)} x_{a_1}, g^t), x_{a_2}^t) \tag{4}$$

$$R = (g_1^t \cdot e(g_1, g_2)^w, g^w, h(id_v)^w) \tag{5}$$

U_a 將訊息 m 和 SDVS (S, R) 傳送給 U_v。

【簽章驗證階段】

U_v 收到 m 和 SDVS (S, R) 後，令 $S = (s_1, s_2)$ 和 $R = (r_1, r_2, r_3)$，並驗證

$$s_1 = e(h(id_a), s_2) e(g^{h(m)} g_2, r_1 \frac{e(x_{v_2}, r_3)}{e(x_{v_1}, r_2)}) \tag{6}$$

等式 (6) 成立，表示 SDVS 通過驗證，為合法簽章；反之，亦為非法簽章；以下針對驗證式 (6) 推導其正確性：

$$e(h(id_a), s_2) e(g^{h(m)} g_2, r_1 \frac{e(x_{v_2}, r_3)}{e(x_{v_1}, r_2)})$$

$$= e(h(id_a), s_2)$$

$$e(g^{h(m)} g_2, r_1 \frac{e(g^{k_i}, r_3)}{e(g_2{}^{\alpha} h(id_i)^{k_i}, r_2)})$$

由式 (2)、(3) 得知。

$$= e(h(id_a), s_2)$$

$$e(g^{h(m)} g_2, r_1 \frac{e(g^{k_i}, h(id_v)^w)}{e(g_2{}^{\alpha} h(id_i)^{k_i}, g^w)})$$

由式 (5) 得知。

$$= e(h(id_a), s_2)$$

$$e(g^{h(m)}g_2, r_1 \frac{e(g^{k_i}, h(id_v)^w)}{e(g_2{}^{\alpha}, g^w)e(h(id_i)^{k_i}, g^w)})$$

$$= e(h(id_a), s_2)$$

$$e(g^{h(m)}g_2, r_1 \frac{e(g, h(id_v))^{k_i w}}{e(g_2{}^{\alpha}, g^w)e(h(id_i), g)^{k_i w}})$$

$$= e(h(id_a), s_2)e(g^{h(m)}g_2, r_1 \frac{1}{e(g_2{}^{\alpha}, g^w)})$$

$$= e(h(id_a), s_2)e(g^{h(m)}g_2, \frac{g_1^t e(g_1, g_2)^w}{e(g_2{}^{\alpha}, g^w)})$$

$$= e(h(id_a), s_2)e(g^{h(m)}g_2, \frac{g_1^t e(g^{\alpha}, g_2)^w}{e(g_2{}^{\alpha}, g^w)})$$

$$= e(h(id_a), s_2)e(g^{h(m)}g_2, \frac{g_1^t e(g, g_2)^{\alpha w}}{e(g_2, g)^{\alpha w}})$$

$$= e(h(id_a), s_2)e(g^{h(m)}g_2, g_1^t)$$

由式 (1) 得知。

$$= e(h(id_a), g^{tki})e(g^{h(m)}, g_1^t)e(g_2, g_1^t)$$

$$= e(h(id_a), g^{tki})e(g^{h(m)}, g_1^t)e(g_2, g^{\alpha t})$$

$$= e(h(id_a), g)^{tki} e(g, g_1)^{h(m)t} e(g_2, g)^{\alpha t}$$

$$= e(h(id_a), g)^{tki} e(g, g)^{h(m)\alpha t} e(g_2, g)^{\alpha t}$$

由式 (1) 得知。

$$= e(h(id_a), g)^{tki} e(g_1, g)^{h(m)t} e(g_2, g)^{\alpha t}$$

$$= e(h(id_a)^{ki}, g^t)e(g_1^{h(m)}, g^t)e(g_2{}^{\alpha}, g^t)$$

$$= e(g_1^{h(m)}, g^t)e(g_2{}^{\alpha}h(id_a)^{k_i}), g^t)$$

$$= e(g_1^{h(m)}x_{a_1}, g^t)$$ 由式 (4) 得知。

$$= s_1$$

【副本模擬階段】

U_v 選取 $s_2{}^*, r_1{}^*, r_2{}^*, r_3{}^* \in_R \boldsymbol{G}_1$，計算

$$s_1^* = e(h(id_a), s_2^*)e(g^{h(m)}g_2, r_1^* \frac{e(x_{v_2}, r_3^*)}{e(x_{v_1}, r_2^*)})$$

(7)

最後 (S^*, R^*) 對於訊息 m 而言，若等式 (7) 成立，表示 SDVS 通過驗證，為另一個合法簽章；以下針對驗證式 (7) 推導其正確性：

其正確性推導如下：

$$e(h(id_a), s_2^*)e(g^{h(m)}g_2, r_1^* \frac{e(x_{v_2}, r_3^*)}{e(x_{v_1}, r_2^*)})$$

$$= e(h(id_a), s_2^*)$$

$$e(g^{h(m)}g_2, r_1^* \frac{e(g^{k_i}, r_3^*)}{e(g_2{}^{\alpha}h(id_i)^{k_i}, r_2^*)})$$

$$= e(h(id_a), s_2^*)$$

$$e(g^{h(m)}g_2, r_1^* \frac{e(g^{ki}, h(id_v)^{w^*})}{e(g_2{}^{\alpha}h(id_i)^{k_i}, g^{w^*})})$$

$$= e(h(id_a), s_2^*)$$

$$e(g^{h(m)}g_2, r_1^* \frac{e(g^{k_i}, h(id_v)^{w^*})}{e(g_2{}^{\alpha}, g^{w^*})e(h(id_i)^{k_i}, g^{w^*})})$$

$$= e(h(id_a), s_2^*)$$

$$e(g^{h(m)}g_2, r_1^* \frac{e(g, h(id_v))^{kiw^*}}{e(g_2{}^{\alpha}, g^{w^*})e(h(id_i), g)^{k_i w^*}})$$

$$= e(h(id_a), s_2^*)e(g^{h(m)}g_2, r_1^* \frac{1}{e(g_2{}^{\alpha}, g^{w^*})})$$

$$= e(h(id_a), s_2^*)e(g^{h(m)}g_2, \frac{g_1^{t^*} e(g_1, g_2)^{w^*}}{e(g_2{}^{\alpha}, g^{w^*})})$$

$$= e(h(id_a), s_2^*)e(g^{h(m)}g_2, \frac{g_1^{t^*} e(g^{\alpha}, g_2)^{w^*}}{e(g_2{}^{\alpha}, g^{w^*})})$$

$$=e(h(id_a),s_2^*)e(g^{h(m)}g_2,\frac{g_1^{t^*}e(g,g_2)^{\alpha w^*}}{e(g_2,g)^{\alpha w^*}})$$

$$=e(h(id_a),s_2^*)e(g^{h(m)}g_2,g_1^{t^*})$$

$$=e(h(id_a),g^{t^*k_i})e(g^{h(m)},g_1^{t^*})e(g_2,g_1^{t^*})$$

$$=e(h(id_a),g^{t^*k_i})e(g^{h(m)},g_1^{t^*})e(g_2,g^{\alpha t^*})$$

$$=e(h(id_a),g)^{t^*k_i}e(g,g_1)^{h(m)t^*}e(g_2,g)^{\alpha t^*}$$

$$=e(h(id_a),g)^{t^*ki}e(g,g)^{h(m)\alpha t^*}e(g_2,g)^{\alpha t^*}$$

$$=e(h(id_a),g)^{t^*k_i}e(g_1,g)^{h(m)t^*}e(g_2,g)^{\alpha t^*}$$

$$=e(h(id_a)^{k_i},g^{t^*})e(g_1^{h(m)},g^{t^*})e({g_2}^{\alpha},g^{t^*})$$

$$=e(g_1^{h(m)},g^{t^*})e({g_2}^{\alpha}h(id_a)^{ki}),g^{t^*})$$

$$=e(g_1^{h(m)}x_{a_1},g^{t^*})$$

$$={s_1}^*$$

四、安全性分析

本文所提出基於雙線性配對之身份識別特定驗證者簽章機制，其安全性皆基於解 ECDLP 與 BDHP 之安全性，並具備不可偽造性、不可轉移性與來源隱密性等分析。以下我們依序針對每一種方法提出五種安全性分析，茲分述如下：

(一) 不可偽造性 (Unforgeability)：

此分析主要在說明假設攻擊者欲偽造 SDVS 中的 S 簽章。從式 (4) 中我們可以知道簽章 S 包含簽章者兩組私密金鑰 x_{a_1} 和 x_{a_2}，既為只有簽章者才知道私密金鑰。另外，在此攻擊當中亦會面臨到 ECDLP 與 BDHP 困難；因此，SDVS 中的 S 簽章只容許簽章者本身才能產生，任何能都不能產生或偽造，因此攻擊者無法偽造有效的 SDVS。

而在【簽章驗證階段】推導過程中式，我們亦能發現，s_1 替換為 $e(g_1^{h(m)}x_{a_1},g^t)$，當中即包含簽章者的私鑰 x_{a_1}，而該私鑰只有簽章者所擁有，如有攻擊者企圖偽造 s_1'使得 $s_1=s_1'$亦不可行；此外在式 (4)，$s_2=x_{a_2}^t$，同樣也包含簽章者的另一把私鑰，若攻擊者企圖偽造 s_2'使得 $s_2=s_2'$亦不可行，同樣仍面臨 ECDLP 與 BDHP 困難。

(二) 不可轉移性 (Non-Transferability)：

此分析在說明特定驗證者如何再產生一個有效的 SDVS。從【簽章產生階段】中我們可知道 U_a 自行選取兩組值，並計算出式 (4) 和式 (5) 後傳送給 U_v 驗證，U_v 收到後驗證式 (6) 是否成立，若成立則 (S, R) 即為有效的 SDVS，反之則無效；其 SDVS 推導驗證過程可參考【簽章產生階段】。

在【副本模擬階段】中，U_v 自選取四組變數：$s_2^*, r_1^*, r_2^*, r_3^* \in_R \boldsymbol{G}_1$，並計算出式 (7)，產生另一組 (S^*, R^*) 簽章，即對訊息 m 而言，為合法的 SDVS;也因為 U_v 可以自行選取變數並產生合法的 SDVS，所以當然無法將自行產生的 SDVS 取信於任意第三者，因為特定驗證者所公開出來的 SDVS 可能不是原來的 SDVS，而是 U_v 自己另外計算出來的。因此，特定驗證者無法將所收到的 SDVS 轉移給第三者驗證。

(三) 來源隱密性 (Source Hiding)：

此分析是由不可轉移性 (Non-Transferability) 所衍生出來另一個安全性議題，說明給定一個 SDVS，很難去分辨真正的簽署者。因為不論 U_a 或 U_v 皆能產生合法的 SDVS，但實際上真正有用的 SDVS 乃 U_a 所產生，U_v 雖為特定驗證者，執行驗證 U_a 所給定的 SDVS，但透過【副本模擬階段】，我們能了解可以 U_v 自行產生合法 SDVS 但卻無法實際派上用場，而任意第三者也無法從 SDVS 辨識到底是 U_a 或 U_v 所產生的。換言之，SDVS 具備保護簽章者身份的特性。

五、結論

特定驗證者簽章技術在密碼學領域中尚屬於新應用，目的在於簽章者將已簽署好的文件，交付給簽章者所特定的驗證者進行簽章驗證，而簽章者對於自己所產生出來的簽章具有身份辨識作用，即無法對自己的簽章進行否認；而特定驗證者雖可同時進行多個簽章驗證，亦可自行產生 SDVS，但基於不可轉移性，使得就算特定驗證者自行產生出合法的 SDVS，但仍不具任何效力；最後簽章驗證結束後，亦無法對簽章的產生者與特定簽章者做身份辨識，即為保護簽章者與特定簽章者的隱私性。

因此本文主要針對基於雙線性配對安全性下，結合身份辨識密碼系統的金鑰管理特性，與特定驗證者簽章機制中不可否認性特色，提出基於雙線性配對之身份基底特定驗證者簽章方法，簽章者利用自己的私鑰產生 SDVS 與 ECDLP 與 BDHP 困難之下，使得該簽章具有不可偽造性；SDVS 驗證時簽章者會指定特定驗證者驗證簽章，亦只有被指定到的特定驗證者會相信簽章的真確性，但基於不可轉移特性，既使特定驗證者自行產生新的 SDVS，亦不能向第三者證明該簽章的可信度；而在整個 SDVS 過程中，除簽章者與特定驗證者之外，其他人亦無法從 SDVS 得知簽章者的真實身份，以保護簽章者的隱私性。

六、參考文獻

[1] F. Bao, R. Deng and H. Zhu, “Variations of Diffie-Hellman problem”, In Proceedings of ICICS 2003, LNCS 2836, Springer-Verlag, pp. 301-312, 2003.

[2] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing”, In Proceedings of CRYPTO 2001, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.

[3] D. Boneh, B. Lynn and H. Shacham, “Short signatures from the Weil pairing”, Advances in Cryptology – ASIACRYPT 2001, LNCS 2248, pp. 516-534, 2001.

[4] J. C. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman groups”, PKC 2003, LNCS 2567, Springer-Verlag, pp. 18-30, 2003.

[5] D. Chaum and H. Van Anterpen, “Undeniable signature”, Advances in Cryptology – CRYPTO’90, Springer-Verlag, pp. 212-216, 1990.

[6] W. Diffie and M. Hellman, “New directions in cryptography”, IEEE Transitions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, 1976.

[7] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[8] S. Galbraith and W. Mao, “Invisibility and anonymity of undeniable and confirmer signatures”, The Cryptographers’ Track at the RSA Conference 2003 (CT-RSA 2003), LNCS 2612, Springer-Verlag, pp. 80-97, 2003.

[9] M. Girault, “Self-certified public keys”, Advances in Cryptology – EUROCRYPT’91, Springer-Verlag, pp. 491-497, 1991.

[10] F. Hess, “Efficient identity based signature schemes based on parings”, Selected Areas in Cryptography – SAC’2002, LNCS 2595, Springer-Verlag, pp. 310-324, 2003.

[11] IEEE Standard Specifications for Public-key Cryptography, IEEE 1363-2000, 2000.

[12] M. Jakobsson, K. Sako and R. Impagliazzo, “Designated verifier proofs and their applications”, Advances in Cryptology – EUROCRYT’96, Springer-Verlag, pp. 143-154, 1996.

[13] B. Libert and J. J. Quisquater, “Identity based undeniable signatures”, The Cryptographers’ Track at the RSA Conference 2004 (CT-RSA 2004), LNCS 2964, Springer-Verlag, pp. 112-125, 2004.

[14] A. Menezes, T. Okamoto and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, IEEE

Transactions on Information Theory, Vol. 39, pp. 1639-1646, 1993.

[15] B. Meng, S. Wang and Q. Xiong, "A fair non-repudiation protocol", In Proceedings of the 7th International Conference on Computer Supported Cooperative Work in Design (CSCW'02), Brazil, pp. 68-73, 2002.

[16] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet", In Proceedings of the 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS'01), California, pp. 188-190, 2001.

[17] R. Rivest, A. Shamir and L. Adlema, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[18] S. Saeednia, S. Kremer and O. Markowitch, "An efficient strong designated verifier signature scheme", In Proceedings of the 6th International Conference on Information Security and Cryptology (ICISC 2003), Seoul, Korea, pp. 40-54, 2003.

[19] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", Advances in Cryptology – CRYPTO'99, Springer-Verlag, pp. 149-164, 1999.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology – CRYPTO'84, Springer-Verlag, pp. 47-53, 1984.

[21] W. Stallings, Cryptography and Network Security: Principles and Practices, 4th. Ed., Pearson, 2005.

[22] G. Wang, "An attack on not-interactive designated verifier proofs for undeniable signatures", Cryptology ePrint archive, http://eprint.iacr.org/2003/243.pdf,2003.

[23] B. Waters, "Efficient identity-based encryption without random oracles", Advances in Cryptology – EUROCRYPT 2005, Springer-Verlag, pp. 114-127, 2005.

[24] X. Yi, "An identity-based signature scheme from the Weil pairing", IEEE Communications Letters, Vol. 7, No. 2, 2003.

[25] X. Yi, "Efficient ID-based key agreement from Weil pairing", Electronics Letters, Vol. 39, No. 2, pp. 206-208, 2003.

[26] F. Zhang and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings", The 8th Australasian Conference on Information Security and Privacy, pp. 312-323, 2003.