植基於分解因數和離散對數雙重難題之公平盲簽章的安全分析

Security of Fair Blind Signature Scheme Based on Factoring and Discrete Logarithms

陳柏岳[*] 林秀峰[#] 陳志瀅[**]

[*]逢甲大學 資訊工程學系 [#]逢甲大學 資訊工程學系 [**]逢甲大學 通訊工程學系

E-mail: m9018333@knight.fcu.edu.tw E-mail: hflin@fcu.edu.tw E-mail: chihchen@fcu.edu.tw

摘要

2002 年，李、林和陳等提出一個植基於分解因數和離散對數的公平盲簽章。本文將指出李等的方法易遭受 Pollard and Schnorr 演算法的攻擊，而產生一般性偽簽。同時我們亦提出修正方法，除保有原來李等方法的特性，又能抵擋 Pollard and Schnorr 的攻擊。

關鍵詞：公平盲簽章、分解因數、離散對數、隱私權、二次剩餘。

1. 前言

自從 David Chaum[2]提出盲簽章系統以來，盲簽章已被應用在許多需要匿名性和隱私權保護的環境中。(例如：電子投票、電子競標、電子付款系統等…)。但是這樣的不可追蹤特性可能被拿來利用從事犯罪活動(例如：勒索[16]或洗錢)。因此，在 1995 年，Makus Stadler、Jean-Maro Pivetean 和 Jan Camenisch[17]為了防止盲簽章的不可追蹤特性可能會被濫用在犯罪行為上，提出了公平盲簽章的觀念，相關的研究論文在[3-8],[11,12],[18]。

由於資訊科技發展迅速，電腦運算能力大幅提升，許多安全性只基於解離散對數或分解因數難題的密碼系統在未來也許會變成時間上的不夠安全。有鑑於此，2002 年，李、林與陳[1]提出一個基於分解因數和離散對數雙重難題的公平盲簽章，此簽章的優點在於其秘密金鑰是以雙重困難度來保護，因而大幅提升了整個系統的安全性，而在其他防止偽簽的部分方面，攻擊者至少需面對分解因數或離散對數問題其中一種的困難度。

本文將指出他們的方法仍有機會遭受 Pollard and Schnorr 演算法[14]的攻擊，而產生一般性的偽簽。同時本文也提出修正的做法，除了保有李等原來方法的特性，且能抵擋 Pollard and Schnorr 的攻擊。

2. 李等公平盲簽[1]的回顧

2.1 二次剩餘的回顧

本節將簡介在李等[1]文以及本文所用到的二次剩餘理論的一些定義和性質。

設 n 為大於 1 的模(modulo)，且整數 a 與 n 互質，記作 $(a,n)=1$。若 $x^2 \equiv a \bmod n$ 有解，則稱 a 為模 n 的二次剩餘(quadratic residue)。反之，稱 a 為模 n 之非二次剩餘(quadratic nonresidue)。我們以 $Z_n=\{0,1,2,...,n-1\}$ 表示模 n 中的最小完全剩餘系(complete residue system)，$Z_n^*=\{0<k<n \mid (k,n)=1\}$ 表示 Z_n 中最大的乘法群。我們由數論書本[10,15]，分別以 n 為奇質數和 n 為二奇質數乘積的情況，得到一些有關二次剩餘的性質如下。

(一)設 n 為奇質數，則

(1) $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ ，其中 $\left(\frac{a}{n}\right)$ 為 Legendre 符號，$\left(\frac{a}{n}\right)=1$ 表示 a 為模 n 的二次剩餘 $\left(\frac{a}{n}\right)=-1$ 表示 a 為模 n 之非二次剩餘。

(2) 若以 $|A|$ 表示集合 A 的基數(cardinal number)，令

$QR_n=\{a\in Z_n^*\mid (\frac{a}{n})=1\}$ ， $QNR_n=\{a\in Z_n^*\mid (\frac{a}{n})=-1\}$ 則 $Z_n^*=QR_n\cup QNR_n$ 且 $|QR_n|=|QNR_n|=\frac{1}{2}(n-1)$。

(3) 若 $a,b\in QR_n$ 或 $a,b\in QNR_n$ 則 $ab(\mathrm{mod}\, n)\in QR_n$；若 $a\in QR_n$ 且 $b\in QNR_n$ 則 $ab(\mathrm{mod}\, n)\in QNR_n$。

(4) 設 $0<r<n$，且 $x\in Z_n^*$，則

(a) 若 $n\equiv 3\bmod 4$，則 $|\{x\in QR_n\mid x+r\in QR_n\}|=\frac{1}{4}(n-3)$ 且 $|\{x\in QNR_n\mid x+r\in QR_n\}|=\frac{1}{4}(n+1)$

(b) 若 $n\equiv 1\bmod 4$，則 $|\{x\in QR_n\mid x+r\in QR_n\}|=\frac{1}{4}[n-3-2(\frac{r}{n})]$ 且 $|\{x\in QNR_n\mid x+r\in QR_n\}|=\frac{1}{4}[n+1+2(\frac{r}{n})]$

(5) 因為 $(u,n)=1$，所以 $\{uz\mid z\in Z_n^*\}=Z_n^*$。令 $B=\{uz^2\mid z^2\in QR_n\}$，則

情況 1: 若 $u\in QR_n$，則由 (3) 可知 $B=QR_n$，再由(4)可知

當 $n\equiv 1\bmod 4$ 則有 $\frac{1}{4}[n-3-2(\frac{r}{n})]$ 個 z^2；

當 $n\equiv 3\bmod 4$ 則有 $\frac{1}{4}(n-3)$ 個 z^2，使得 $uz^2+r\in QR_n$

情況 2: 若 $u\in QNR_n$，則由 (3) 可知 $B=QNR_n$，再由(4)可知

當 $n\equiv 1\bmod 4$ 則有 $\frac{1}{4}[n+1+2(\frac{r}{n})]$ 個 z^2；

當 $n\equiv 3\bmod 4$ 則有 $\frac{1}{4}(n+1)$ 個 z^2，使得 $uz^2+r\in QR_n$

從以上的討論可得下列定理

定理：設 $r,u\in Z_n^*$，則在 Z_n^* 中，約有 $\frac{1}{2}(n-1)$ 個 z 使得 uz^2+r 為二次剩餘。

(二)設 $n=pq$，其中 p,q 皆為奇質數，則

(1) $Z_n^*\underset{\text{同構}}{\simeq} Z_p^*\times Z_q^*$ 且 $|Z_n^*|=|Z_p^*||Z_q^*|=(p-1)(q-1)$

(2) 令

(a) $Z_{1,1}=\{a\in Z_n^*\mid (\frac{a}{p})=1\ ,\ (\frac{a}{q})=1\}$

(b) $Z_{1,-1}=\{a\in Z_n^*\mid (\frac{a}{p})=1\ ,\ (\frac{a}{q})=-1\}$

(c) $Z_{-1,1}=\{a\in Z_n^*\mid (\frac{a}{p})=-1\ ,\ (\frac{a}{q})=1\}$

(d) $Z_{-1,-1}=\{a\in Z_n^*\mid (\frac{a}{p})=-1\ ,\ (\frac{a}{q})=-1\}$

則 $Z_n^*=Z_{1,1}\cup Z_{1,-1}\cup Z_{-1,1}\cup Z_{-1,-1}$ ，$|Z_{1,1}|=|Z_{1,-1}|=|Z_{-1,1}|=|Z_{-1,-1}|=\frac{1}{4}(p-1)(q-1)$，且 $a\in Z_n^*$ 是二次剩餘的充要條件為 $a\in Z_{1,1}$。

(3) 設 $c_1\in Z_{1,1}$ ， $c_2\in Z_{1,-1}$ ， $c_3\in Z_{-1,1}$ 和 $c_4\in Z_{-1,-1}$。則由(一)之(3)知，對任意整數 a 可選擇一個適合的參數 c_i $(i=1,2,3,4)$ 使得 $c_ia\in Z_{1,1}$，也就是 c_ia 是模 n 的二次剩餘。例如，若令 $p\equiv 5\bmod 8$ 和 $q\equiv 7\bmod 8$ 兩種形式，則可取 $c_1=1$，$c_2=-1$，$c_3=2$ 和 $c_4=-2$。

(4) 設 $r\in Z_n^*$，則：

(a) 當 $p\equiv 1\bmod 4$ 及 $q\equiv 3\bmod 4$ 則

$|\{x\in Z_{1,1}\mid x+r\in Z_{1,1}\}|=\frac{1}{4}[p-3-2(\frac{r}{p})]\times\frac{1}{4}(q-3)$;

$|\{x\in Z_{1,-1}\mid x+r\in Z_{1,1}\}|=\frac{1}{4}[p-3-2(\frac{r}{p})]\times\frac{1}{4}(q+1)$;

$|\{x\in Z_{-1,1}\mid x+r\in Z_{1,1}\}|=\frac{1}{4}[p+1+2(\frac{r}{p})]\times\frac{1}{4}(q-3)$;

$|\{x\in Z_{-1,-1}\mid x+r\in Z_{1,1}\}|=\frac{1}{4}[p+1+2(\frac{r}{p})]\times\frac{1}{4}(q+1)$;

也即在 Z_n^* 中大約有 $\frac{1}{16}(p-1)(q-1)$ 個元素 x 使得 $x+r$ 為一個模 n 之二次剩餘。

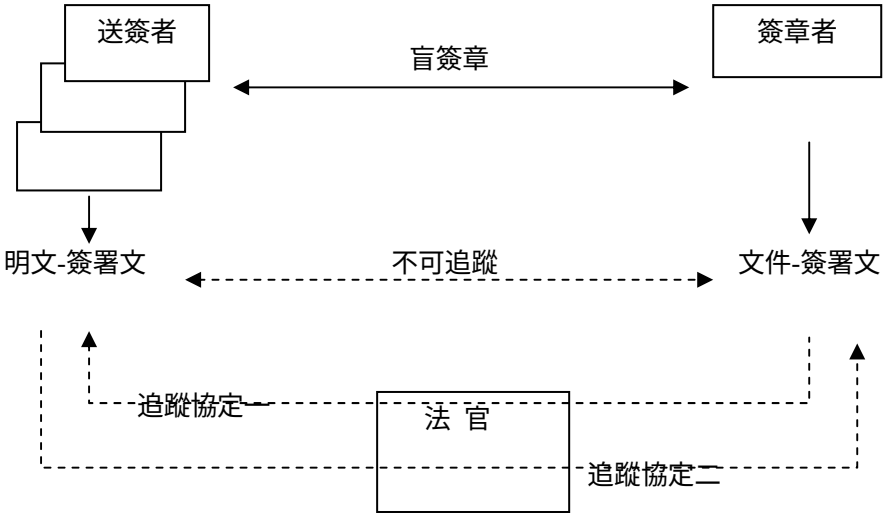
(b) 其餘情況，當 $p\equiv 1\bmod 4$ 且 $q\equiv 1\bmod 4$， $p\equiv 3\bmod 4$ 且 $q\equiv 1\bmod 4$ 或 $p\equiv 3\bmod 4$ 且 $q\equiv 3\bmod 4$ 皆可得到類似的結果，即 Z_n^* 中大約有 $\frac{1}{16}(p-1)(q-1)$ 個元素 x 使得 $x+r$ 為一個模 n 之二次剩餘。

(5) 對任意 $u,r\in Z_n^*$，在 Z_n^* 中有多少個二次剩餘 z^2 能得 uz^2+r 仍為一個二次剩餘?因為 $(u,n)=1$ ， $\{uz\mid z\in Z_n^*\}=Z_n^*$ ， 命 $B=\{uz^2\mid z^2\in Z_{1,1}\}$ 由(7)知， $B=Z_{i.j}$ 的充要條件為 $u\in Z_{i,j}$ $(i,j\in\{1,-1\})$。因此由(9)可知，大約有 $\frac{1}{16}(p-1)(q-1)$ 個二次剩餘 z^2 能使得 uz^2+r 仍為二次剩餘。更進一步推算，在 Z_n^* 中大約有 $\frac{1}{4}(p-1)(q-1)$ 元

素 z 能使得 uz^2+r 為二次剩餘. 此性質將用來說明本文中公平盲簽章的可行性。

2.2 李，林與陳的公平盲簽章

李，林與陳[1]的公平盲簽章，包含了送簽者，簽章者和公正的第三者(稱為法官)三種角色，三者的關係如圖一所示。其演算法，可以詳述如下。



(圖一)

一、參數設定

步驟一：簽章者任意選取一個質數 $p=4p_1q_1+1$，$p_1=2p_2+1$，$q_1=2q_2+1$ 其中 p_1，p_2，q_1 和 q_2 皆為大質數，並選取一個元素 g 其模 p 之秩 (order) 為 p_1q_1，即 $g^{p_1q_1}\equiv 1 \bmod p$。

步驟二：簽章者任意選取一個秘密金匙 x $(0<x<p_1q_1)$，計算 $y\equiv g^{x^2} \bmod p$，並公佈 y 為公開金匙。

步驟三：對外公佈 y、p 和 g，並且經由一個安全的管道將 p_1 和 q_1 秘密的傳送給法官。

二、盲簽章

步驟一：送簽者依據公開格式選定明文 M 並選擇一個亂數 u $(0<u<p_1q_1)$，計算 $\bar{M}\equiv Mu \bmod p_1q_1$，傳送文件 $\bar{M}$ 給簽章者要求簽署。

步驟二：簽章者收到文件 $\bar{M}$ (簽章者對 $\bar{M}$ 文件內容是盲目的)後，隨機選擇二個數 a 和 t_1。

步驟三：簽章者選擇一個參數 $\bar{c}$ 使得 $\bar{c}(1-a^2)$ 在模 p_1q_1 為二次剩餘，並計算 $b\equiv\sqrt{\bar{c}(1-a^2)} \bmod p_1q_1$。

步驟四：簽章者計算 $t\equiv at_1 \bmod p_1q_1$ 和 $\bar{r}\equiv g^{\bar{c}t^2+t^{-2}} \bmod p$。

步驟五：簽章者求出滿足下列關係式的 $\bar{s}$ 和 $\bar{k}$。

$$t^{-1}\bar{r}+\bar{c}t\bar{k}\equiv bx\bar{M}+ax\bar{s} \bmod p_1q_1 \qquad (2.1)$$

$$a^{-1}t^{-1}\bar{k}-a^{-1}t\bar{r}\equiv a^{-1}b\bar{s}x\bar{c}^{-1}-x\bar{M} \bmod p_1q_1 \qquad (2.2)$$

註：將 (2.1) 平方 +(2.2) 平方 $\times\bar{c}a^2$，可得到 $(t^{-2}+\bar{c}t^2)(\bar{r}^2+\bar{c}\bar{k}^2)=(b^2+\bar{c}a^2)x^2(\bar{M}^2+\bar{c}^{-1}\bar{s}^2)$，因此可得到

$$g^{(t^{-2}+\bar{c}t^2)(\bar{r}^2+\bar{c}\bar{k}^2)}=g^{\bar{c}x^2(\bar{M}^2+\bar{c}^{-1}\bar{s}^2)} \text{ 或}$$

$$\bar{r}^{\bar{r}^2+\bar{c}\bar{k}^2}=y^{\bar{c}\bar{M}^2+\bar{s}^2}。$$

步驟六：簽章者將文件 $\bar{M}$ 的簽署文 $(\bar{r},\bar{k},\bar{s},\bar{c})$ 回傳給送簽者。

步驟七：送簽者收到 $(\bar{r},\bar{k},\bar{s},\bar{c})$ 後，驗證 $y^{\bar{c}\bar{M}^2+\bar{s}^2}\equiv\bar{r}^{\bar{r}^2+\bar{c}\bar{k}^2} \bmod p$ 是否成立。

步驟八：簽章者傳送 $\bar{r}$ 給法官。

以上簽章法的詳細描述可參考[1]。

三、抽取簽章

步驟一：送簽者任意選擇兩個整數 $\bar{a}$ 和 c。

步驟二：送簽者計算 $r\equiv\bar{r}^{\bar{a}} \bmod p$，

$M\equiv\bar{M}u^{-1} \bmod p_1q_1$，

$A\equiv c^{-1}\bar{a}^{-1}(\bar{c}\bar{M}^2+\bar{s}^2)^{-1}(\bar{r}^2+\bar{c}\bar{k}^2) \bmod p_1q_1$ 和

$B\equiv\bar{a}^{-1}M^2(\bar{c}\bar{M}^2+\bar{s}^2)^{-1}(\bar{r}^2+\bar{c}\bar{k}^2)-c^{-1}r^2 \bmod p_1q_1$，並將 $(\bar{a},r,A,B)$ 秘密地傳送給法官，要求法官求解 (s,k)。

步驟三：法官收到 $(\bar{a},r,A,B)$ 後，確認 $r\equiv\bar{r}^{\bar{a}} \bmod p$ 成立。

步驟四：法官任意選擇一個整數 s $(0 < s < p_1q_1)$，使得 $As^2 + B$ 為模 p_1q_1 的二次剩餘。

步驟五：法官解二次剩餘方程式 $k^2 \equiv As^2 + B \bmod p_1q_1$，可得四個根 k_1, k_2, k_3, k_4 並任取一根為 k，將 (s,k) 秘密地回傳給送簽者。

步驟六：送簽者及驗證者可以驗證 $y^{cM^2+s^2} \equiv r^{r^2+ck^2} \bmod p$ 式子是否成立。若是，則簽署文 (r,s,k,c) 為明文 M 的合法盲簽署文，反之則否。

在[1]中，李，林與陳證明了以上所求得的簽章 (r,s,k,c) 確為一公平盲簽章，並且證明其安全性植基於分解因數和離散對數雙重難題。然而，在下一節中，我們將指出李，林與陳的作法並無法抵擋 Pollard 與 Schnorr 演算法[14]的攻擊。

3. Pollard 與 Schnorr[14]演算法的攻擊

任何有敵意的攻擊者，對任意信息 M，可由下列步驟得到對於 M 的偽簽：

步驟一：任意選兩正整數 t, c

步驟二：計算 $r = y^t \bmod p$

步驟三：由 Pollard & Schnorr 的演算法[14]求解方程式 $s^2 - tck^2 = tr^2 - cM^2 \bmod p_1q_1$ 中的 s, k。

因為由步驟三所得到 s 與 k 滿足 $s^2 + cM^2 = t(r^2 + ck^2) \bmod p_1q_1$，故滿足驗證式 $y^{cM^2+s^2} = y^{t(r^2+ck^2)} = r^{r^2+ck^2} \bmod p$。因此，得到對任意信息 M 的偽簽章 (r,k,s,c) 而使法官與簽章者無法追蹤。

4. 修正方法

針對上述李，林與陳[1]之公平盲簽章的缺陷，在本節中，我們將提出一個改良的作法並確保改良後的作法能夠抵擋 Pollard 與 Schnorr 演算法的攻擊。

一、參數設定：與原來方法相同，只是選取適合的質數 $p_1 \equiv 3 \bmod 8$ 與 $q_1 \equiv 7 \bmod 8$。並選取 $c_1 = 1 \in Z_{(1,1)}, c_2 = -2 \in Z_{(1,-1)}, c_3 = 2 \in Z_{(-1,1)}, c_4 = -1 \in Z_{(-1,-1)}$。

二、 盲簽章

步驟一~二：與原來相同。

步驟三：簽章者可選擇一參數 $\bar{c} \in \{1,-2,2,-1\}$ 使得 $\bar{c}(1-a^2)$ 在模 p_1q_1 為二次剩餘並計算 $b = \sqrt{\bar{c}(1-a^2)} \bmod p_1q_1$，且滿足 $0 \le b \bmod p_1 < \frac{1}{2}p_1$ 及 $0 \le b \bmod q_1 < \frac{1}{2}q_1$。

步驟四：簽章者計算 $t = at_1 \bmod p_1q_1$ 和 $\bar{r} = g^{\bar{c}t^2 + t^{-2}} \bmod p$。

步驟五：簽章者求出滿足下列關係式的 s_1, k_1。

$$t^{-1}\bar{r} + \bar{c}tk_1 \equiv bx\bar{M} + axs_1 \bmod p_1q_1 \quad (4.1)$$

$$a^{-1}t^{-1}k_1 - a^{-1}t\bar{r} \equiv a^{-1}bs_1x\bar{c}^{-1} - x\bar{M} \bmod p_1q_1 \quad (4.2)$$

步驟六：簽章者求出兩整數 $\bar{s}, \bar{k} \in Z^*_{p_1q_1}$ 滿足 $\bar{s}^4 = s_1^2 \bmod p_1q_1$ 及 $\bar{k}^4 = k_1^2 \bmod p_1q_1$。

註：將 (4.1) 平方 +(4.2) 平方 $\times \bar{c}a^2$，可得到 $(t^{-2} + \bar{c}t^2)(\bar{r}^2 + \bar{c}k_1^2) = (b^2 + \bar{c}a^2)x^2(\bar{M}^2 + \bar{c}^{-1}s_1^2)$，或 $(t^{-2} + \bar{c}t^2)(r^2 + \bar{c}\bar{k}^4) = (b^2 + \bar{c}a^2)x^2(\bar{M}^2 + \bar{c}^{-1}\bar{s}^4)$。由此可得 $r^{\bar{r}^2 + \bar{c}\bar{k}^4} = y^{\bar{c}\bar{M}^2 + \bar{s}^4} \bmod p$。

步驟七：簽章者將文件 $\bar{M}$ 的簽署文 $(\bar{r}, \bar{k}, \bar{s}, \bar{c})$ 回傳給送簽者。

步驟八：送簽者收到 $(\bar{r}, \bar{k}, \bar{s}, \bar{c})$ 後，驗證 $y^{\bar{c}\bar{M}^2 + \bar{s}^4} = \bar{r}^{\bar{r}^2 + \bar{c}\bar{k}^4} \bmod p$ 是否成立。

步驟九：簽章者傳送 $\bar{r}$ 給法官。

三、抽取簽章

步驟一：送簽者任意選擇兩個整數 $\bar{a}$ 和 $c, c \in \{1,-1,2,-2\}$。

步驟二：送簽者計算 $r \equiv \bar{r}^{\bar{a}} \bmod p$，$M \equiv \bar{M}u^{-1} \bmod p_1q_1$，$A \equiv c^{-1}\bar{a}^{-1}(\bar{c}\bar{M}^2 + \bar{s}^4)^{-1}(\bar{r}^2 + \bar{c}\bar{k}^4) \bmod p_1q_1$ 和 $B \equiv \bar{a}^{-1}M^2(\bar{c}\bar{M}^2 + \bar{s}^4)^{-1}(\bar{r}^2 + \bar{c}\bar{k}^4) - c^{-1}r^2 \bmod p_1q_1$，並將 $(\bar{a}, r, A, B)$ 秘密地傳送給法官，要求法官求解 (s,k)。

步驟三：法官收到 $(\bar{a}, r, A, B)$ 後，確認 $r \equiv \bar{r}^{\bar{a}} \bmod p$ 成立。

步驟四：法官任意選擇一個整數 s $(0 < s < p_1q_1)$，使得 $As^4 + B$ 為模 p_1q_1 的二次剩餘。

步驟五：法官解二次剩餘方程式 $k^4 = As^4 + B \bmod p_1q_1$，可得四個根 k_1, k_2, k_3, k_4 並任取一根為 k，將 (s,k) 秘密地回傳給送簽者。

步驟六：送簽者及驗證者可以驗證

$y^{cM^2+s^4} = r^{r^2+ck^4} \bmod p$ 式子是否成立。若是，則簽署文 (r,s,k,c) 為明文 M 的合法盲簽署文，反之則否。

根據以上改良作法所得的公平盲簽章 (r,s,k,c) 之正確性和公平性的証法與李等李等原來的方法完全類似，讀者可以參考[1]。在下一節裡，我們將證明我們的改良作法不但保有李等方法的所有安全性外，也能抵擋 Pollard 與 Schnorr 演算法的攻擊。

4.3 公平盲簽章的特性

4.3.1 正確性

假使送簽者依照上述過程取得公平盲簽章的盲簽署文，則所取得的盲簽署文是正確合法的。

證明：

$$\begin{aligned} k^4 &\equiv As^4 + B \bmod p_1q_1 \\ &\equiv c^{-1}\bar{a}^{-1}(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4)s^4 \\ &\quad + \bar{a}^{-1}M^2(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4) - c^{-1}r^2 \bmod p_1q_1 \\ &\equiv c^{-1}\bar{a}^{-1}(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4)(cM^2+s^4) \\ &\quad - c^{-1}r^2 \bmod p_1q_1 \end{aligned}$$

因此

$$ck^4 + r^2 \equiv \bar{a}^{-1}(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4)(cM^2+s^4) \bmod p_1q_1$$

所以

$$\begin{aligned} r^{r^2+ck^4} &\equiv r^{\bar{a}^{-1}(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4)(cM^2+s^4)} \bmod p \\ &\equiv \bar{r}^{(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4)(cM^2+s^4)} \bmod p \\ &\equiv y^{(cM^2+s^4)} \bmod p \end{aligned}$$

4.3.2 公平性

其公平性如同原方法，請參考[1]

5. 安全性分析

攻擊一、Pollard-Schnorr 攻擊：攻擊者任選一整數 v，計算 $r = y^v \bmod p$ 對任意信息 M

分　析：利用 Pollard-Schnorr 的演算法求出下列方程式的 A, B

$$A^2 + cM^2 = vr^2 + vcB^2 \bmod p_1q_1$$

但攻擊者必須另外解出 $s^2 = A \bmod p_1q_1$ 及 $k^2 = B \bmod p_1q_1$ 而面臨因數分解 p_1q_1 的難題。

攻擊二、在沒有法官的協助下，簽章者嘗試完成追蹤協定一或追蹤協定二，簽章者利用記錄下來的 $(\bar{M},\bar{k},\bar{r},\bar{s},\bar{c})$ 和送簽者事後公佈的 (M,k,r,s,c) 計算

$$\bar{a} \equiv (\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(cM^2+s^4)(ck^4 + r^2)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4) \bmod p_1q_1$$

，藉由檢驗 $r \equiv \bar{r}^{\bar{a}} \bmod p$ 是否成立，追蹤 $(\bar{M},\bar{k},\bar{r},\bar{s},\bar{c})$ 和 (M,k,r,s,c) 的關係。

分　析：假如簽章者使用這一個方法嘗試做追蹤的動作，是不可行的，其原因可由下列定理說明。

定　理：對任意一組 $(\bar{M},\bar{k},\bar{r},\bar{s},\bar{c})$ 與 (M,k,r,s,c)，若

$$\bar{a} \equiv (\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(cM^2+s^4)(ck^4 + r^2)^{-1}(\bar{r}^2+\bar{c}\bar{k}^4) \bmod p_1q_1$$

，則 $r \equiv \bar{r}^{\bar{a}} \bmod p$ 皆成立(此定理說明了我們的公平盲簽章演算法具有不可追蹤性)。

證　明：

$$\begin{aligned} \bar{r}^{\bar{a}} &\equiv \bar{r}^{(\bar{r}^2+\bar{c}\bar{k}^4)(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(cM^2+s^4)(ck^4+r^2)^{-1}} \\ &\equiv y^{(\bar{c}\bar{M}^2+\bar{s}^4)(\bar{c}\bar{M}^2+\bar{s}^4)^{-1}(cM^2+s^4)(ck^4+r^2)^{-1}} \\ &\equiv y^{(cM^2+s^4)(ck^4+r^2)^{-1}} \\ &\equiv r^{(ck^4+r^2)(ck^4+r^2)^{-1}} \\ &\equiv r \bmod p \qquad \text{Q.E.D} \end{aligned}$$

攻擊三、在沒有法官的協助下，送簽者嘗試從 $(\bar{M},\bar{k},\bar{r},\bar{s},\bar{c})$ 抽取出 (M,k,r,s,c)。

分　析：送簽者必須知道 p_1 和 q_1 值才能得到 (s,k) 滿足 $k^4 \equiv As^4 + B \bmod p_1q_1$，因為 Pollard-Schnorr[14]演算法只能求解二次方程 $x^2 + ay^2 = b \bmod p_1q_1$ 中的 x, y 值，無法解四次方程 $x^4 + ay^4 = b \bmod p_1q_1$ 中的 x, y 之值。因此，送簽者必須面對分解因數問題。

攻擊四、攻擊者欲由公開金匙 $y \equiv g^{x^2} \bmod p$ 求得密秘金匙 x。

分　析：很明顯地，攻擊者必須面對解

離散對數問題和分解因數雙重難題。

攻擊五、攻擊者欲偽造明文 M 的簽署文，他試圖找出一組參數 (k,r,s,c) 以滿足驗證式子

$$y^{cM^2+s^4} \equiv r^{r^2+ck^4} \bmod p$$。

分　析：首先，若攻擊者任意選擇三個數當作 k，r 和 c。然後從驗證式中求出 s，則攻擊者必須面對解離散對數問題和分解因數問題。同樣地，如果攻擊者任選 k，s 和 c 或 s，　r 和 c 欲從驗證式子中求出 r 或 k，攻擊者還是必須面對解離散對數問題和分解因數問題。

攻擊六、替代攻擊法(Substitution Attack[13])

假設攻擊者已擁有明文 M 的盲簽署文 (k,r,s,c)。他嘗試利用這一組資訊，在不需求出秘密金匙 x 之情況下，偽造另一明文 M' 的盲簽署文 (k',r',s',c')。

分　析：攻擊者先令 $c'=c$。再選擇一個亂數 v 並計算

$$r' = r^{v^2} = g^{(ct^2+t^{-2})v^2} \bmod p$$

。接著令 $M'=\pm Mv$ 或 $\pm sv$，$s'=\pm sv$ 或 $\pm Mv$，則

$$(ct^2+t^{-2})v^2(r'^2+ck'^4) = x^2(cM'^2+s'^4)$$
$$= v^2x^2(cM^2+s^4)$$
$$= (ct^2+t^{-2})v^2(r^2+ck^4) \bmod p_1q_1$$

。因此可得

$$r'^2+ck'^4 = r^2+ck^4 \bmod p_1q_1$$

。然而，攻擊者為了解出 k' 滿足

$$k'^4 \equiv (r^2+ck^4-r'^2)c^{-1} \bmod p_1q_1$$

必須面對分解因數問題。

攻擊七、同態攻擊法(Homomorphism Attack [9])

假設攻擊者擁有明文 M_1，M_2 和 M_3 的盲簽署文 (k_1,r_1,s_1,c_1)，(k_2,r_2,s_2,c_2) 和 (k_3,r_3,s_3,c_3)，其中 $r_3 \equiv r_2 \cdot r_1 \bmod p$，攻擊者利用這三組盲簽署文和驗證式試圖求出秘密金匙 x。

分　析：攻擊者利用三組盲簽署文可得到下列三個驗證式：

$$\bar{a}_1(t_1^{-1}+\bar{c}_1t_1^2)(r_1^2+c_1k_1^4) = x^2(c_1M_1^2+s_1^4) \bmod p_1q_1 \quad (5.1)$$

$$\bar{a}_2(t_2^{-1}+\bar{c}_2t_2^2)(r_2^2+c_2k_2^4) = x^2(c_2M_2^2+s_2^4) \bmod p_1q_1 \quad (5.2)$$

$$\bar{a}_3(t_3^{-1}+\bar{c}_3t_3^2)(r_3^2+c_3k_3^4) = x^2(c_3M_3^2+s_3^4) \bmod p_1q_1 \quad (5.3)$$

由此，他可以進一步計算

$(5.1)\times(r_2^2+c_2k_2^4)(r_3^2+c_3k_3^4)+(5.2)\times(r_1^2+c_1k_1^4)(r_3^2+c_3k_3^4)-(5.3)\times(r_1^2+c_1k_1^4)(r_2^2+c_2k_2^4)$，而得到下列的結果

$$\begin{aligned}0 &\equiv x^2(c_1M_1^2+s_1^4)(r_2^2+c_2k_2^4)(r_3^2+c_3k_3^4)\\ &+x^2(c_2M_2^2+s_2^4)(r_1^2+c_1k_1^4)(r_3^2+c_3k_3^4)\\ &+x^2(c_3M_3^2+s_3^4)(r_2^2+c_2k_2^4)(r_1^2+c_1k_1^4) \bmod p_1q_1\\ &\equiv x^2(r_1^2+c_1k_1^4)(r_2^2+c_2k_2^4)(r_3^2+c_{31}k_3^4)(x^{-2}(\bar{a}_1(t_1^{-2}\\ &+\bar{c}_1t_1^2)(t_2^{-2}+\bar{c}_2t_2^2)(t_3^{-2}+\bar{c}_3t_3^2))) \bmod p_1q_1\end{aligned}$$

然而，因為 $x^2 \neq 0$ 而且由 $r_1r_2=r_3$ 知

$$\bar{a}_1(t_1^{-2}+\bar{c}_1t_1^2)+\bar{a}_2(t_2^{-2}+\bar{c}_2t_2^2)-\bar{a}_3(t_3^{-2}+\bar{c}_3t_3^2)=0$$

，所以得到 $0 \equiv x^2 \cdot 0 \bmod p_1q_1$。因此，攻擊者根本無法從 $0 \equiv x^2 \cdot 0 \bmod p_1q_1$ 中求出秘密金匙 x。

6. 結論

本論文除了指出李等[1]所提出的植基於因數分解與離散對數雙重難題的公平盲簽章易受 Pollard-Schnorr 演算法攻擊外，並提出一個修正的方法，使其不但可避免 Pollard-Schnorr 攻擊，而且保有原來雙重難題簽章演算法的特性。

參考文獻

[1] 李志豪,林秀峰,陳志瀅," 植基於分解因數和離散對數雙重難題之公平盲簽章",第十二屆全國資訊安全會議, pp163-170, 2002.

[2] D. Chaum, "Blind signature systems," proceedings of Crypto'83, p.153, 1984.

[3] J. Camenisch, J. M. Piveteau, and M. Stadler, "An efficient fair payment system," 3rd ACM Conference on computer Communications Security, pp.88-94, 1996.

[4] H.Y. Chien, J.K. Jan and Y.M. Tseng, "RSA-based partially blind signature with low computation", Parall- el and Distributed Systems, 2001. ICPADS 2001. Proceedings.

Eighth International Conference on , pp. 385 –389,2001.

[5] C.I. Fan and C.L. Lei, “A multi-recastable ticket scheme for electronic elections,” Advances in Cryptolog- y-ASIACRYPT’96, LNCS 1163, Springer-Verlag, pp. 116-124, 1996.

[6] C.I. Fan and C.L. Lei, “User efficient blind signatures” Electronics Letters, Vol. 34, No. 6, pp.544-546, 1998.

[7] C.I. Fan and C.L. Lei, “Low computation partially blind signatures for electronic cash” IEICE TRANS. F- UNDAMENTALS, Vol. E81-A, No. 5 May 1998.

[8] C.I. Fan, C.L. Lei and Y.P. Chiu, “Comments on improved user efficient blind signature, ” Proceeding Conference on Information Security, Tainan. ROC, pp. 51-53, May 2001.

[9] J. He and T. Kiesler, “Enhancing the security of original EIGamal’s signature scheme,” IEE Proc. Comput, Digit. Tech, 141, (4), pp.249-252, 1994.

[10] K. Ireland and M. Rosen, A Classical Introduction to Moden Number Theory. 2nd ed. New York: Spring-V-erlag, 1992.

[11] N.Y. Lee and T. Hwang, “On the security of Fair blind signature scheme using oblivious transfer,”Elsevier, computer communications 22, 287-290, 1999.

[12] C.H. Lee, H.F. Lin and C.Y.Chen,”An Improved Shao’s Signature Scheme Based on Factoring and Discrete Logarithms,” WCE 2001, Proceedings, Taipei ROC, Oct 2001.

[13] K. Nyberg, “New digital signature scheme based on discrete logarithm (comment)”, Electron. Lett., 30, (6), pp.481, 1994.

[14] J. M. Pollard,and C. P. Schnorr,: ‘An efficient solution of the congruence $x^2 + ky^2 = m(\mathrm{mod}\ \ n)$’, IEEE Transactions on Information Theory, Vol. 33, No.5, pp.702-709, 1987

[15] K.H. Rosen, Elementary Number Theory and It’s Applications, 2nd td . Addision Wesle, 1988.

[16] S.von Solms, D. Naccache, “On blind signature and perfect crime,” computer security, 11, 1992.

[17] M. Stadler, J.M. Piveteau and J. Camenisch, “Fair blind signatures,” Advances in Cryptology Eurocypt’95, pp.209-219, 1996

[18] Z. Shao, “Improved user efficient blind signatures,” Electronics Letters, Vol. 36, No. 16, pp.1372-1374, 2000.