改善的代理盲簽章協定

楊伏夷
朝陽科技大學資訊工程系
yangfy@cyut.edu.tw

梁菱仁
朝陽科技大學資訊工程系
s9827625@cyut.edu.tw

摘要

代理盲簽章結合了代理簽章及盲簽章的概念，適合應用在一些電子商務上，例如:電子投票、電子交易…等。在電子商務的環境中，經常需在短時間內處理一筆電子交易的紀錄；因此，通訊及計算成本顯得格外重要。在 2009 年，Oo 和 Thein 提出植基於離散對數問題的代理盲簽章，能在低通訊及低計算量的情況下完成代理盲簽章，並且達到代理盲簽章應俱備之安全需求；然而，我們發現這個協定無法提供代理盲簽章應俱備的完整性，並且會遭受到偽造簽章攻擊。在本篇文章，我們將回顧 Oo 和 Thein 的協定，並描述該協定之安全漏洞及攻擊方法，然後提出一個改善的代理盲簽章協定，此協定不僅保留原協定的低計算成本，在簽章長度也節省了 71%，並且提供簽章文件的完整性及防止偽造簽章攻擊，也能達到代理盲簽章應俱備的安全需求。

關鍵詞：代理盲簽章、完整性、偽造簽章攻擊。

1. 前言

近年來，網路發展迅速與普及化，電子商務漸漸的受到重視，許多現有的電子商務協定將簽章概念加入應用，傳統的數位簽章技術[1, 2]，簽署者使用自己的私密金鑰(Private Key)簽署電子文件，產生數位簽章，任何人可使用簽署者的公開金鑰(Public Key)驗證簽章的有效性，能提供文件簽署者的身份確認(真實性 Authenticity)、文件簽署者不可否認提供文件(不可否認性 Non-repudiation)及確保文件未曾被竄改(完整性 Integrity)；在電子商務的環境中，安全固然是很重要的議題，但是也不可忽略通訊時的計算成本，以電子交易為例，A 方為證券公司，B 方為一般的民眾，A 方一天可能有上萬筆的交易紀錄，隨著股價的變動，B 方可能隨時需要進行買賣，而 A 方需在短時間內處理這筆交易紀錄，若計算的時間過於冗長，則會影響到 B 方買賣的價格，因此簽章的計算成本也是在電子商務中需考慮到的一個因素。

在 1983 年，Chaum 提出盲簽章概念[3]，簽章請求者將文件盲化後交給簽章者，簽章者在不知道原始文件內容下進行簽章，而後請求者再將簽章後的文件解盲化，此協定可保護簽章請求者的身份(匿名性 Anonymity)及簽章者不可透過簽章來追蹤出請求者的身份(不可追蹤性 Untraceability)。在 1996 年，Mambo 等人提出代理簽章協定[4]，原始簽章者可將簽章能力轉移給代理簽章者，代理簽章者擁有原始簽章者授權之後，就能代表原始簽章者對外簽署文件，而驗證者可驗證原始簽章者及代理簽章者的身份。在 2002 年，Tan 等人整合代理簽章和盲簽章技術，成為代理盲簽章[5]，並表示一個完整的代理盲簽章應俱備可區分性、不可否認性、可驗證性、不可偽造及不可追蹤性。而後 Xue 和 Cao 指出 Tan 等人的協定不俱備匿名的特性，並提出一個新的協定[6]，解決 Tan 等人協定的問題。但是，Li 等人也發現 Xue 和 Cao 的協定無法提供不可偽造性及不可連結性[7]。在 2007 年，Li 和 Wang 提出了使用自我認證公開金鑰的代理盲簽章協定[8]，能抵擋公鑰替換攻擊，並且與 Tan 等人的協定進行效能比較。公鑰替換攻擊是替換原用戶公開金鑰的一種攻擊方法，由於許多協定使用到公開金鑰基礎建設(Public Key Infrastructure, PKI)，因此大多數的公開金鑰都會存放至基礎建設中，倘若攻擊者替換了某用戶的公開金鑰，極可能導致他人使用錯誤的公開金鑰來進行加密，使得原用戶無法解開此加密訊息。在 2008 年，Yang 和 Yu 提出有效的代理盲簽章協定[9]，是基於離散對數問題上，並指出他們的協定在計算量上比 Li 和 Wang 的協定更有效率。在 2009 年，Oo 和 Thein 提出植基於離散對數問題的代理盲簽章協定[10]，並表示他們的協定不僅滿足代理盲簽章所需俱備之安全需求，也比其他協定更有效及低計算量。

在本篇文章，我們首先回顧 Oo 和 Thein 的代理盲簽章協定，並在安全分析指出他們的協定無法提供代理盲簽章應俱備的完整性，以及會遭受到偽造簽章攻擊；並提出改善的代理盲簽章協定，保留原協定的低通訊及低計算成本，並且能提供完整性、不可偽造性以及代理

盲簽章所需俱備的安全需求。

2. 回顧 Oo 和 Thein 協定[10]

Oo 和 Thein 提出一個以離散對數問題為基礎的代理盲簽章協定，此協定可分為四個階段：1.代理授權階段、2.代理盲簽章產生階段、3.簽章取出階段、4.簽章驗證階段。協定中的參與者包括：原始簽章者、代理簽章者、簽章請求者和驗證者。

系統參數：

p,q：系統產生兩個大質數，滿足 $q \mid p-1$，且 p 為往後計算的共同模數

g：g 是 Z_p^* 的元素，其序為 q

x_o, y_o：原始簽章者的私密金鑰及公開金鑰，並且 $y_o = g^{x_o} \bmod p$

x_p, y_p：代理簽章者的私密金鑰及公開金鑰，並且 $y_p = g^{x_p} \bmod p$

s_{pr}, y_{pr}：代理簽章的私密金鑰及公開金鑰，並且 $y_{pr} = g^{s_{pr}} \bmod p$

m_w：委託代理簽章的證書，包含原始簽章者及代理簽章者的身份資訊、代理權限、代理期限等資訊

$h(\cdot)$：安全的單向無碰撞雜湊函數

2.1 代理授權階段

當原始簽章者欲授權簽署能力給代理簽章者時，需執行下列步驟：

(1) 原始簽章者先選擇亂數 $k_o \in Z_q^*$，並產生授權簽體 S_o，計算如下：

$$R_o = g^{k_o} \bmod p$$

$$S_o = x_o + k_o \cdot h(m_w \| R_o) \bmod q$$

原始簽章者將授權訊息 (R_o, S_o, m_w) 傳給代理簽章者，m_w 為授權委託書。

(2) 代理簽章者收到授權訊息 (R_o, S_o, m_w) 後，驗證授權簽體 S_o 是否合法：

$$g^{S_o} \stackrel{?}{=} y_o \cdot R_o^{h(m_w \| R_o)} \bmod p$$

若等式成立，代理簽章者接受原始簽章者之授權委託，透過有效的授權訊息，代理簽章者產生代理簽章私密金鑰 S_{pr}，而相對應的代理簽章公開金鑰為 y_{pr}，計算如下：

$$s_{pr} = S_o + x_p \bmod q$$

$$y_{pr} = g^{s_{pr}} = y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)} \bmod p$$

2.2 代理盲簽章產生階段

(1) 代理簽章者隨機選擇亂數 $k \in Z_q^*$，並計算參數 r：

$$r = g^k \bmod p$$

將代理授權階段時收到的 R_o 連同 r 傳給簽章請求者。

(2) 簽章請求者收到訊息後，選擇隨機亂數 $u, v \in Z_q^*$，並計算出 r^*, e^*，將其訊息 e^* 盲化後，得到盲訊息 e，如下所示：

$$r^* = r \cdot g^u (y_o \cdot y_p)^{-v} \bmod p$$

$$e^* = h(r^* \| m)$$

$$e = e^* - v \bmod q$$

而後簽章請求者將盲訊息 e 傳給代理簽章者。

(3) 當代理簽章者接收到盲訊息 e 後，利用原始簽章者與代理簽章者所共同授權的代理簽章私密金鑰 s_{pr}，對盲訊息 e 簽章，產生簽章後的盲訊息 S^*：

$$S^* = k + e \cdot s_{pr} \bmod q$$

代理簽章者回傳盲簽章訊息 S^* 給簽章請求者。

2.3 簽章取出階段

當簽章請求者收到盲簽章訊息 S^* 後，對盲簽章訊息進行解盲化，計算如下：

$$S = g^{S^* + u} \cdot R_o^{-v \cdot h(m_w \| R_o)} \bmod p$$

最後簽章請求者取得完整的代理盲簽章文件即為 (m, m_w, S, e^*, R_o)。

2.4 簽章驗證階段

驗證者收到簽章請求者公開的簽章文件 (m, m_w, S, e^*, R_o)，可透過下面驗證式檢查代理盲簽章是否合法：

$$y_{pr} = y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)} \bmod p$$

$$e^* \stackrel{?}{=} h(S \cdot y_{pr}^{-e^*} \bmod p \,\|\, m)$$

設若正確，代表簽章文件是由合法的原始簽章者與代理簽章者所簽發之文件。

3. 分析簽章完整性及偽造簽章攻擊

本章節指出 Oo 和 Thein 提出的協定中，若攻擊者攔截到簽章訊息，便可竄改簽章文件的內容，而驗證者收到簽章後，仍然能夠驗證成功而無法察覺出簽章已遭受竄改，因此無法提供簽章的完整性；另外，攻擊者能在不知道代理簽章私密金鑰的情況下，偽造出一個有效的代理盲簽章，而驗證者無法察覺出此簽章是由攻擊者所偽造的文件，因此無法達到不可偽造的特性，攻擊方法如下所述：

3.1 無法提供簽章的完整性

攻擊者在攔截到有效的簽章文件 (m, m_w, S, e^*, R_o) 之後，便可竄改簽章中的 S 及 R_o；首先，攻擊者先選擇隨機亂數 $R_o' \in Z_p^*$，接著計算出 $y_{pr}' = y_o \cdot y_p \cdot R_o'^{h(m_w \| R_o')}$，並且找出相對應的 S'，使得 $S' \cdot y_{pr}'^{-e^*} = S \cdot y_{pr}^{-e^*} \bmod p$ 等式成立，經過竄改的簽章文件為 (m, m_w, S', e^*, R_o')，此文件透過驗證式仍然能通過驗證，因此無法提供簽章所需俱備的完整性。

3.2 無法抵擋偽造簽章攻擊

攻擊者在取得簽章請求者公開的簽章文件 (m, m_w, S, e^*, R_o)，便可以透過下面的計算式，偽造一個有效的代理盲簽章文件，而驗證者收到偽造的簽章文件，無法察覺出此簽章是由攻擊者所偽造的，並且透過驗證式仍然相信此簽章是原始簽章者與代理簽章者所簽署之文件；首先攻擊者先選擇隨機亂數 $R' \in Z_p^*$ 及 $m \in \{0,1\}^*$，接著做以下的計算：

$$e^* = h(R' \| m)$$

$$y_{pr} = y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)} \bmod p$$

$$S' = R' \Big/ y_{pr}^{-e^*} \bmod p$$

偽造出來的簽章為 (m, m_w, S', e^*, R_o)，驗證者將此簽章透過以下驗證式仍然能夠驗證通過，因此可證明文獻[10]的協定是無法達到不可偽造的特性。

$$e^* \stackrel{?}{=} h(S' \cdot y_{pr}^{-e^*} \bmod p \,\|\, m)$$

4. 改善的協定

在此章節，我們結合 Schnorr 簽章[11]與部份盲簽章[12]技術，提出改善的代理盲簽章協定，本協定同時俱備盲簽章與代理簽章的安全需求，在下一章節逐一討論之。此協定可分為四個階段：1. 代理授權階段、2. 代理盲簽章產生階段、3. 簽章取出階段、4. 簽章驗證階段。協定中的參與者包括：原始簽章者、代理簽章者、簽章請求者和驗證者。

4.1 代理授權階段

(1) 原始簽章者先選擇亂數 $k_o \in Z_q^*$，並使用自己的私密金鑰 x_o 對授權內容簽章，產生授權簽體 S_o，計算如下：

$$r_o = g^{k_o} \bmod p$$

$$h = h(m_w \| r_o \| y_o \| y_p)$$

$$S_o = k_o - h \cdot x_o \bmod q$$

原始簽章者將授權訊息 (m_w, S_o, h) 傳給代理簽章者，m_w 為授權委託書。

(2) 代理簽章者收到授權訊息 (m_w, S_o, h) 後，驗證 h 是否合法：

$$h \stackrel{?}{=} h(m_w \| g^{S_o} \cdot y_o^h \bmod p \,\|\, y_o \| y_p)$$

若等式成立，代理簽章者接受原始簽章者之授權委託，並計算代理簽章私密金鑰 s_{pr}，而相對應的代理簽章公開金鑰為 y_{pr}：

$$s_{pr} = h \cdot x_p \bmod q$$

$$y_{pr} = g^{s_{pr}} = y_p^h \bmod p$$

4.2 代理盲簽章產生階段

(1) 首先代理簽章者隨機選擇亂數 $k \in Z_q^*$，並計算參數 $r = g^k \bmod p$，將 r, h, S_o 傳給簽章請求者。

(2) 簽章請求者收到訊息後，會產生兩個隨機亂數 $u, v \in Z_q^*$，計算參數 r^*, e^*，將訊息 e^* 盲化後，得到盲訊息 e，如下所示：

$$r^* = r^u \cdot g^v \bmod p$$

$$e^* = h(r^* \| m)$$

$$e = e^* / u \bmod q$$

計算之後，簽章請求者將盲化後的訊息 e，傳給代理簽章者。

(3) 代理簽章者收到盲訊息 e 後，利用原始簽章者與代理簽章者所共同授權的代理簽章私密金鑰 s_{pr}，對盲訊息 e 進行簽章，產生簽章後的盲訊息 S^*，計算方式如下：

$$S^* = k - e \cdot s_{pr} \bmod q$$

再將簽章後的盲訊息 S^* 傳給簽章請求者。

4.3 簽章取出階段

當簽章請求者收到盲簽章訊息 S^* 後，對盲簽章訊息進行解盲化，產生完整的代理盲簽章：

$$S = u \cdot S^* + v \bmod q$$

簽章請求者取得完整的代理盲簽章文件即為 (m, m_w, S, e^*, S_o, h)。

4.4 簽章驗證階段

驗證者在收到簽章請求者公開的簽章文件 (m, m_w, S, e^*, S_o, h)，透過驗證式檢查簽章是否合法，驗證方法如下：

$$h \stackrel{?}{=} h(m_w \| g^{S_o} \cdot y_o^h \bmod p \| y_o \| y_p)$$

$$e^* \stackrel{?}{=} h(g^S \cdot y_p^{h \cdot e^*} \bmod p \| m)$$

設若正確，驗證者相信此簽章文件為原始簽章者與代理簽章者所簽發之文件。

5. 安全分析

此章節分析我們提出改善的協定能透過驗證式驗證簽章的有效性(可驗證性 Verifiability)；任何人能從簽章中的授權書 m_w 區分簽章的特性(可區別性 Distinguishability)以及原始簽章者與代理簽章者的身份(可識別性 Identifiability)；除了代理簽章者外，第三者無法產生簽章(不可偽造性 Unforgeability)；原始簽章者及代理簽章者皆不可否認簽過此文件(不可否認性 Non-repudiation)；代理簽章者無法從簽章文件中找到簽章請求者的身份(不可追蹤性 Untraceability)。

(1) 可驗證性：驗證者可透過驗證式 $e^* \stackrel{?}{=} h(g^S \cdot y_p^{h \cdot e^*} \bmod p \| m)$ 來驗證簽章的合法性，不僅能確認文件是否正確，也能驗證簽章者的身份。

(2) 可區別性：完整的代理盲簽章文件為 (m, m_w, S, e^*, S_o, h)，任何人能從委託書 m_w 知道原始簽章者和代理簽章者的相關授權訊息以及身份，因此可從完整的盲簽章文件 (m, m_w, S, e^*, S_o, h) 中，區分代理盲簽章與一般簽章的不同。

(3) 可識別性：完整的代理盲簽章文件 (m, m_w, S, e^*, S_o, h) 中，附有授權書 m_w，此授權書包含原始簽章者和代理簽章者的身份資訊，驗證者能透過完整的簽章資訊，確認相對應的原始簽章者和代理簽章者的身份。

(4) 不可偽造性：若攻擊者想偽造一個合法的代理簽章者對訊息 m 進行簽章，必須計算代理簽章私密金鑰 s_{pr}，但是攻擊者在沒有原始簽章者和代理簽章者的私密金鑰 (x_o, x_p) 的情況下，是無法計算出代理簽章私密金鑰 s_{pr}，因此想要偽造簽章是很困難的。

(5) 不可否認性：在簽章驗證階段，驗證者會使用原始簽章者公開金鑰 y_o 驗證 h，接著使用代理簽章者公開金鑰 y_p 驗證簽章 e，設若正確，表示此簽章是由原始簽章者授權給代理簽章者所簽署之文件，因此簽章者無法否認在訊息 m 上簽署過。

(6) 不可追蹤性：從產生代理盲簽章文件 (m, m_w, S, e^*, S_o, h) 期間，代理簽章者可得知每次簽章的部份資訊 (m_w, S_o, h, r, e, S^*)，若代理簽章者想透過部份資訊來查出簽章接收者的身份是很難的；因為接收者在傳送訊息給代理簽章者執行簽章前，會先選擇兩個盲因子 u, v 來盲化訊息，等到代理簽章者回傳簽署的盲訊息後，在對盲訊息進行解盲化的動作。因此，代理簽章者在不知道盲因子的情況下，無法透過部份資訊來找出簽章文件與簽章接收者的關聯性。

6. 效能比較

在本章節我們將探討提出來的協定與其他

作者的協定，在代理授權階段、代理盲簽章產生階段及簽章驗證階段，所需使用的計算成本進行比較，一般情況下，模指數運算的計算量遠大於單向雜湊函數及模乘法運算，因此我們僅分析各協定所需的模指數運算次數，以及簽章的位元長度進行比較，顯示於表 1；從表 1 可以看出在驗證簽章部份，雖然我們的協定比原協定多出兩次的模指數運算，但是在簽署文件部份比原協定少了兩次的模指數運算，考慮到簽署文件，可能在行動裝置上進行，而驗證簽章則是在一般的硬體設施上進行，因此較適合用於行動簽章文件的場合，例如行動購物、行動投票等；此外，假設單向雜湊函數 $H(\cdot)$ 輸出 160 位元的雜湊字串，模 p 的位元長度 1024 位元，模 q 的位元長度 160 位元，Yang 的協定，簽章 σ 的位元長度為 2208 位元；Oo 和 Thein 的協定，簽章 σ 的位元長度為 2208 位元；相較於我們的協定，簽章 σ 的位元長度為 640 位元，比原協定節省了 71%。由此可知，在模指數運算相同的情況下，改善的協定能在通訊時，提供更低的傳輸資訊量。

7. 結論

在本篇文章中，我們回顧 Oo 和 Thein 提出基植於離散對數問題的代理盲簽章協定，在計算量上比其他協定更加有效。然而在安全性方面，經過上述的分析後，我們發現 Oo 和 Thein 的協定沒有達到一個完善的代理盲簽章所該俱備的完整性與不可偽造的特性，攻擊者不需要使用到代理簽章私密金鑰的情況下，仍可偽造一個有效的代理盲簽章訊息欺騙驗證者。

因此，我們提出一個改善的代理盲簽章協定，與 Oo 和 Thein 提出的協定比較，不僅保留原協定的低計算量，且簽章的位元長度節省了 71%，在安全性方面，能夠提供代理盲簽章的完整性，也能達到不可偽造性和完善的代理盲簽章所應俱備的安全需求，並且更適用於需要行動簽章的環境。

參考文獻

[1] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms," ***IEEE Trans. Inform. Theory***, IT-31, (4), pp. 469-472, 1985.

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

[3] Chaum, D., "Blind signature for untraceable payments," ***Advances in Cryptology, proceeding of CRYPTO'82***, Springer-Verlag, New York, pp. 199-203, 1983.

[4] Mambo, M., Usuda, K. and Okamoto, E., "Proxy signatures: Delegation of the power to sign messages," ***IEICE Transaction on Fundamentals***, Vol. E79-A, No. 9, pp. 1338-1354, 1996.

[5] Tan, Z. W., Liu, Z. J., and Tang, C. M., "A proxy blind signature scheme based on DLP," ***Journal of Software***, Vol. 14, No. 11, pp. 1931-1935, 2003.

[6] Xue, Q. S. and Cao, Z. F., "A new proxy blind signature scheme with warrant," ***IEEE Conference on Cybernetics and Intelligent Systems, Singapore***, Vol. 2, pp. 1386-1391, 2004.

[7] Li, J. G., Zhang, Y. C. and Yang, S. T., "Cryptanalysis of new proxy blind signature scheme with warrant," ***International Conference of Computational Methods in Sciences and Engineering (ICCMSE 2005)***, accepted, Athens, Greece, 2005.

[8] Li, J. G. and Wang, S. H., "New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key," ***International Journal of Network Security***, Vol. 4, No. 2, pp. 193–200, 2007.

[9] Yang, X. and Yu, Z. P., "Efficient Proxy Blind Signature Scheme based on DLP," ***International Conference on Embedded Software and Systems (ICESS2008)***.

表 1. 計算需求量與簽章長度

	Tan [5]	Li [8]	Yang [9]	Oo [10]	Our
代理授權	4	3	3	3	3
簽署文件	7	5	5	5	3
驗證簽章	3	3	2	2	4
簽章的位元長度	1344	1344	2208	2208	640

[10] Oo, A. N. and Thein, N., "DLP based Proxy Blind Signature Scheme with Low-Computation," ***Fifth International Joint Conference on INC, IMS and IDC***, pp. 285-288, 2009.

[11] Schnorr, C. P., "Efficient signature generation for smart cards," ***Journal of Cryptology***, Vol. 4, pp. 161-174, 1991.

[12] Yang, F. Y. and Jan, J. K., "A Secure Scheme for Restrictive Partially Blind Signatures," ***The Sixth International Conference on Information Integration and Web-based Applications & Services IIWAS 2004***, Jakarta Indonesia, pp. 541-548, 2004.