Cryptanalysis of a DLP based Proxy Blind Signature Scheme with Low-Computation

楊伏夷
朝陽科技大學資訊工程系
副教授
yangfy@cyut.edu.tw

劉鎮瑋
朝陽科技大學資訊工程系
研究生
s9727628@cyut.edu.tw

摘要

代理盲簽章方案結合代理簽章與盲簽章的特性，原始簽章者可授權能力給代理簽章者來對外簽署文件，而這類的技術通常都使用在電子投票或電子現金系統上。在 2009 年，Oo 和 Thein 提出一個植基於解離散對數問題的代理盲簽章方案，不僅滿足代理簽章與盲簽章的安全需求，並且與先前幾位密碼學者所提出的方案相較之下，此協定擁有較低的運算量。然而，我們發現 Oo 和 Thein 方案依然沒有達到不可偽造以及不可連結特性。以下的內容中，我們將回顧 Oo 和 Thein 的協定，並描述該方案之安全漏洞與攻擊方法。

關鍵詞：密碼分析、代理盲簽章、偽造攻擊、可連結性。

1. 緒論

在 1982 年，David Chaum[1]首先提出盲簽章技術的概念，簽章者在無法得知原始文件資訊為何的情況下執行簽章，此方案提供使用者保有匿名與不可連結的特性，因而廣泛應用在電子投票或電子現金系統之上。在 1996 年，Mambo 等人[2]提出一個代理簽章的方案，原始簽章者可將簽章能力授權給代理簽章者，代理簽章者獲得原始簽章者的授權後，即可代表原始簽章者來對外簽署文件。在 2000 年，Lin 和 Jan[3]將盲簽章和代理簽章融合在一起，創造出新的代理盲簽章技術。在 2002 年，Tan 等人[4]提出一個結合數位簽章的代理盲簽章方案，並表示一個強固的代理盲簽章應具有可區分性、不可否認、可驗證性、不可偽造與不可連結性之安全需求。隨後，Xue 和 Cao[5]指出 Tan 等人提議的方案不具有匿名性，代理簽章者可藉由公開的簽章資訊找到盲簽章請求者為誰；Xue 和 Cao 因此提出一個新的代理盲簽章方案，解決 Tan 等人協定上的缺失。很不幸的，Li 等人[6]顯示 Xue 和 Cao 提議的方案並沒有達到不可偽造性和不可連結性。近年來，Yang 和 Yu[7]提出一個有效率的代理盲簽名方案植基於解離散對數的問題上，解決先前幾位密碼學者協定中易遭受偽造攻擊與可連結性的安全漏洞。在 2009 年，Oo 和 Thein[8]提出一個植基於解離散對數問題的代理盲簽章，不僅滿足代理盲簽章方案的安全特性，此協定也比先前幾位密碼學者所發表之代理盲簽章方案更具有效率與低運算量。

在本篇文章，我們將指出 Oo 和 Thein 方案仍然存在一些安全漏洞，在以下的內容中，我們將回顧 Oo 和 Thein 提出的代理盲簽章方案，並且透過分析來證明 Oo 和 Thein 方案並沒有達到不可偽造以及不可連結特性，最後將結論本篇文章。

2. 回顧 Oo 和 Thein 方案

Oo 和 Thein 提出一個植基於解離散對數問題的代理盲簽章方案。此系統運作可分為五個階段：1.系統設置階段、2.代理委任階段、3.盲簽章產生階段、4.簽章取出階段、5.驗證階段。協定中的參與者包括：原始簽章者(O)、代理簽章者(P)、簽章請求者(A)和驗證者(V)。

2.1 系統初始階段

- 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，且為有限群 GF(p)的原根。
- x_o, y_o：原始簽章者產生之私密和公開金鑰，且 $y_o = g^{x_o} \bmod p$ 。
- x_p, y_p：代理簽章者產生之私密和公開金鑰，且 $y_p = g^{x_p} \bmod p$ 。
- m_w：包含原始簽章者與代理簽章者的身份資訊、委任授權限制與有效的委任執行期間。
- $h(\cdot)$：單向無碰撞雜湊函數。

- $\|$:位元串接運算符號。

2.2 代理委任階段

(1) 原始簽章者從 Z_q^* 選取一個隨機亂數 k_o，並產生授權簽體 s_o，計算如下：

$$R_o = g^{k_o} \bmod p,$$
$$s_o = x_o + k_o \cdot h(m_w \| R_o) \bmod q.$$

原始簽章者經由安全通道傳送 (R_o, s_o) 與委託書 m_w 給代理簽章者。

(2) 代理簽章者在收到授權訊息 (R_o, s_o) 與委託書 m_w 後，檢查簽體 s_o 是否合法：

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

若通過上述驗證式，代理簽章者接受代理工作並計算代理簽章秘密金鑰 s_{pr}：

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

2.3 盲簽章產生階段

(1) 原始簽章者從 Z_q^* 選取一個隨機亂數 k，計算混淆參數 r：

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

然後傳送 (R_o, r) 與委託書 m_w 給簽章請求者。

(2) 簽章請求者收到代理簽章者傳送過來的訊息 (R_o, r, m_w) 後，隨機選取兩個盲因子 $u, v \in_R Z_q^*$，並將欲傳送給代理簽章者簽章之原始文件 m 盲化，產生盲訊息 e，計算如下：

$$r^* = r \cdot g^u (y_o \cdot y_p)^{-v} \bmod p,$$
$$e^* = h(r^* \| m) \bmod q,$$
$$e = e^* - v \bmod q.$$

若 $r^* = 0$，則簽章請求者重新選擇新的盲因子 (u, v)。反之，傳送盲訊息 e 給代理簽章者。

(3) 當收到盲訊息 e 後，代理簽章者使用經由原始簽章者授權的代理簽章秘密金鑰 s_{pr}，產生盲簽章 s^*：

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

並回傳簽章後的訊息 s^* 給簽章請求者。

2.4 簽章取出階段

簽章請求者收到簽章訊息後，對盲簽章 s^* 進行解盲化，得到經過代理簽章者授權的簽體 s：

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

最後，完整的代理盲簽章合法文件即為 (m, m_w, s, e^*, R_o)。

2.5 簽章驗證階段

驗證者收到簽章請求者公開的合法簽章文件 (m, m_w, s, e^*, R_o)，驗證者可利用原始簽章者和代理簽章者的公開金鑰 (y_o, y_p) 等資訊，檢查代理盲簽章是否合法，以下 $y_{pr} = y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)} \bmod p$，驗證方法如下：

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

若上述驗證成功，則表示簽章文件是經由合法的原始簽章者與代理簽章者所簽發之文件。圖一表示整個代理盲簽章之流程。

3. 安全性分析

本章節將指出 Oo 和 Thein 提出的方案存在安全漏洞，並且針對協定的漏洞提出了三個攻擊方法，如下所述：

3.1 偽造簽章攻擊一

簽章請求者可在不經由代理簽章者授權的情況下，自行偽造代理簽章，將原本合法簽章取代後，依然能通過驗證式 $\hat{e} \stackrel{?}{=} (h(\hat{s} \cdot y_{pr}^{-\hat{e}} \bmod p \| m)) \bmod q$，使得驗證者以為此簽章是由合法的原始簽章者與代理簽章者簽署之授權簽體。

步驟一：簽章驗證階段

當簽章請求者收到代理簽章者傳來的訊息 (R_o, r, m_w) 之後，簽章請求者將自行產生偽造代理簽章，如下所示：

$$X = g^x \bmod p,$$
$$\hat{e} = h(X \| m),$$
$$\hat{s} = [(y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)})^{\hat{e}} \cdot X] \bmod p.$$

產生簽章訊息 $(m, m_w, \hat{s}, \hat{e}, R_o)$ 即為一個經過偽造授權資訊的簽體，並公開此資訊給驗證者驗證。

步驟二：簽章驗證階段

當驗證者想驗證此代理盲簽章是否正確，即可使用公開的偽造簽章資訊 $(m, m_w, \hat{s}, \hat{e}, R_o)$，

透過驗證式 $\hat{e} \stackrel{?}{=} (h(\hat{s} \cdot y_{pr}^{-\hat{e}} \bmod p \,\|\, m)) \bmod q$ 確認是否合法，此時可以發現經過偽造的簽體 $\hat{s}$，仍能通過驗證式的認證，並且完整的簽章資訊 (m, m_w, s, e^*, R_o) 包含有委任書 m_w，因此驗證者會以為此簽章是經過代理簽章者所簽署的合法簽章。

3.2 偽造簽章攻擊二

對於盲簽章 (m, m_w, s, e^*, R_o) 而言，基本上必須驗證方程式 $e^* \stackrel{?}{=} (h(s \cdot y_{pr}^{-e^*} \bmod p \,\|\, m) \bmod q$ 及 $y_{pr} = y_o \cdot y_p \cdot R_o^{h(m_w \| R_o)} \bmod p$ 是否皆成立。在傳統的簽章方案中，y_o 和 y_p 或許會有附帶的公開金鑰憑證來證明其真偽，但代理簽章公開金鑰 y_{pr} 未必有憑證，因此當 y_{pr} 沒有憑證時，就會產生了以下的安全漏洞。

(1) 將 m_w 改成 m_w'，並得到 $y_{pr}' = y_o \cdot y_p \cdot R_o^{h(m_w' \| R_o)} \bmod p$。

(2) 由方程式 $s \cdot y_{pr}^{-e^*} = s' \cdot y_{pr}'^{-e^*} \bmod p$，可計算出 s'。

(3) 可得到偽造簽章資訊 (m, m_w', s', e^*, R_o)。

由於 m_w 為授權內容，若攻擊者是一個合法的代理簽章者，即可自由的變更授權內容，例如：代理簽章授權日期、代理權限等。經過偽造的簽章資訊 (m, m_w', s', e^*, R_o)，任何驗證者可透過驗證式 $e^* \stackrel{?}{=} (h(s' \cdot y_{pr}'^{-e^*} \bmod p \,\|\, m) \bmod q$ 確認它是合法的代理盲簽章。

3.3. 不具不可連結特性

由於代理簽章者在每次通訊過程中都會記錄簽章請求者的每一筆資訊 (e_1, s_1^*, k_1, r_1)，$(e_2, s_2^*, k_2, r_2)\cdots$，並將其資訊儲存至驗證資料庫中，因此代理簽章者可由驗證資料庫中任意選擇一組資訊來進行確認，假設找到一組資訊 (e_1, s_1^*, k_1, r_1)，且計算可能之盲因子 $v = e^* - e_1 \bmod q$，接著利用公開的合法簽章資訊 (m, m_w, s, e^*, R_o) 來計算出 $r^* = s \cdot y_{pr}^{-e^*} \bmod p$，並使用上述計算出之參數以及原始簽章者和代理簽章者的公開金鑰產生另一盲因子 $g^u = r^* \cdot r_1^{-1} (y_o \cdot y_p)^v \bmod p$，最後代理簽章者可將計算之結果，並且以驗證式 $s \stackrel{?}{=} g^{s^*} \cdot g^u \cdot R_o^{-v \cdot h(m_w \| R_o)} \bmod p$ 來驗證所計算出之資訊，若通過上述驗證，則表示找到盲訊息與簽章請求者之間的關聯性，反之，則確認下一組資訊 (e_2, s_2^*, k_2, r_2)，直到通過上述驗證式為止。

4. 結論

在本篇文章，我們回顧 Oo 和 Thein 所提議的植基於解離散對數問題的代理盲簽章方案。雖然 Oo 和 Thein 的協定確實比先前幾位密碼學者所發表之代理盲簽章方案更有效率。但很不幸的，透過上述的安全性分析，我們將指出 Oo 和 Thein 協定依然沒有達到一個完善的代理盲簽章所該具備的不可偽造與不可連結之安全需求。

參考文獻

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

[2] 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.

[3] Lin, W. D. and Jan, J. K., "A security personal learning tools using a proxy blind signature scheme," ***International Conference on Chinese Language Computing***, pp. 273-277, 2000.

[4] 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.

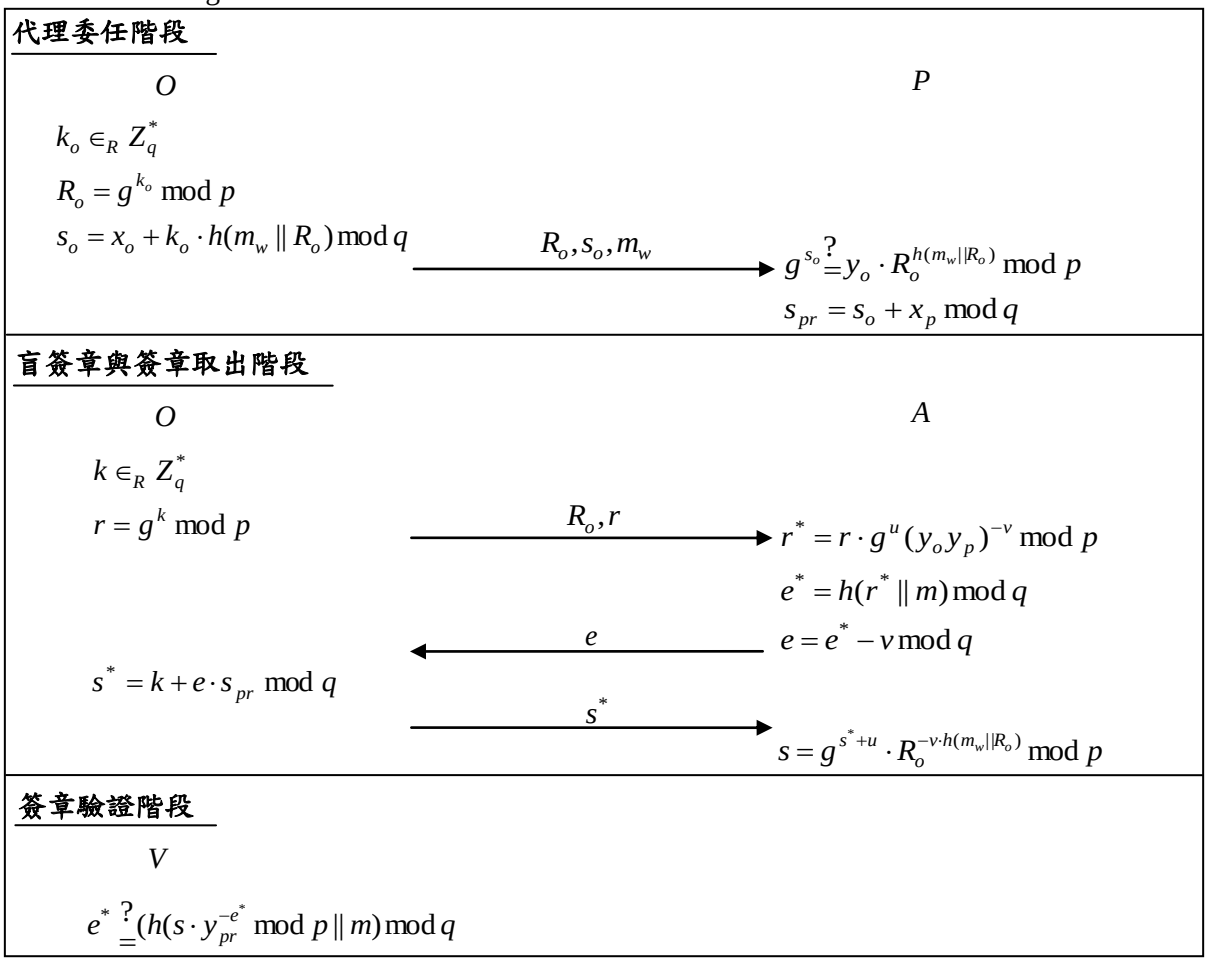
[5] Xue, Q. S. and Cao, Z. F. "A new proxy blind signature scheme with warrant," ***IEEE Conference on Cybernetics and Intelligent Systems***, Singapore, Vol. 2, pp.1386-1391, 2004.

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

[7] Yang, X. and Yu, Z. "An Efficient Proxy Blind Signature Scheme Based on DLP," ***International Conference on Embedded***

***Software and Systems* (*ICESS 2008*)**, pp.163-166, 2008.

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



圖一 Oo 和 Thein 代理盲簽章方案之通訊流程