針對 Hu-Li 代理環簽章的取消匿名性之評論

Remarks on the Revocable Anonymity of Hu-Li's Proxy Ring Signature

Kuan-Chieh Liao
Assistant Professor,
Department of Accounting and Information Systems,
Asia University
lkc@asia.edu.tw

Tzu-Chung Chen
Master Student,
Department of Accounting and Information Systems,
Asia University
ctcmikechen@gmail.com

摘要

Hu 與 Li 兩位學者於 2007 年提出了一個具備取消匿名性(Revocable Anonymity)的代理環簽章(Proxy Ring Signature)方法。該方法提供了原始簽章者(Original Signer)將其簽章能力授權給一群代理簽章者(Proxy Signers)。如此一來，代理簽章者中的任一成員即有能力代理原始簽章者進行文件簽署動作。此外，原始簽章者還能於事後取消代理環簽章的匿名性以便得知真實簽章者的身分，以防止代理簽章者仗勢著匿名性而濫用其簽章的權力。然而，在本論文中，我們將指出 Hu-Li 之代理環簽章方法無法做到其所宣稱的取消匿名特性。換言之，一個惡意的代理環簽章者仍然可以簽署一份合法的環簽章並成功的避開原始簽章者的追查。

關鍵詞：密碼學、代理環簽章、匿名性

1. 前言

環簽章(Ring Signature)的想法最早是在 2001 年由 Rivest, Shamir 及 Tauman 等三位學者所提出[9]。其部份概念與群體簽章(Group Signature)相似，可以讓簽章驗證者相信簽署文的確是出自群體中的某位成員。然而最大的差異在群體簽章於產生群組金鑰(Group Key)的過程必須透過群組管理者(Group Manager)或是其他群組成員的協助才能順利完成。主要目的是讓群組管理者可於事後追查出群組簽章的真正簽章者，以防止惡意的群組成員濫用其簽章能力。除此之外，群組簽章中的群組成員通常需要事先設定好，反觀環簽章則提供簽章者自由選擇群組成員的彈性空間。

總結上述介紹可得知，環簽章不但可以讓驗證者相信簽署的訊息的確是由群體中的某個成員所簽署，而且還能同時保障該成員的身份的匿名性。自從 Rivest 等學者提出了環簽章的概念，相關研究亦陸續地被提出[3], [5], [8], [10]，更突顯了該議題的重要性與研究價值。

另一方面，代理簽章(Proxy Signature)的概念首先於 1996 年由 Mambo, Usuda, 及 Okamoto 等三位學者所提出[7]。它提供了原始簽章者(Original Signer)將其簽章能力授權給代理簽章者(Proxy Signer)，並讓代理簽章者代理他來簽署文件。在代理簽章的概論提出之後，亦有許多學者紛紛嘗試將代理簽章與其他種類簽章做結合[6], [11], [12]。其中，代理環簽章(Proxy Ring Signature)的一些方法[1], [13]亦在近年來相繼被提出。其應用環境如下：公司老闆可以將其簽章的能力授權給公司中特定的一群代理簽章者，這群代理簽章者中的任一成員即可代表老闆簽署文件，除了證明該文件的確出自於代理簽章者之手，並且同時享有匿名的特性。然而，這也使得惡意代理簽章者有機可乘，能藉由身分無法被追蹤的匿名優勢進而濫用其代理簽章的權力。有鑑於此，Hu 與 Li 兩位學者於 2007 年提出了一個具備取消匿名性(Revocable Anonymity)的代理環簽章方法[4]。即原始簽章者有能力可以在事後揭露代理環簽章者的身份。如此一來，公司老闆便能放心的將其簽章能力授權下放，因為他可以隨時將代理環簽章的匿名特性取消，找出真正的代理簽章者，以防止可能之權力濫用狀況發生。

由上述分析不難看出，取消匿名性在代理環簽章法中扮演了關鍵的重要角色，亦直接地決定了一個代理環簽章的實用價值。然而，在本論文中我們將指出 Hu-Li 代理環簽章方法並無法做到其所宣稱的取消匿名特性。也就是說

一個惡意的代理簽章者仍然有辦法製造一個合法的代理環簽章並成功地躲開原始簽章者的追查。接下來我們將於第二章中簡單介紹Hu-Li代理環簽章方法,而該方法在取消匿名性的瑕疵也將於第三中進行詳細說明，並於第四章做總結。

2. Hu-Li 代理環簽章方法回顧

在此章節，我們將回顧 Hu-Li 代理環簽章方法。首先將介紹相關的系統參數之定義，請參考表 1 之說明。

表 1. 系統參數說明

p, q	兩個大質數，其中 $q\|p-1$
g	$g \in Z^*_p$, 其序(order)為q
x_o	x_o為原始簽章者A_o的秘密金鑰
x_i	x_i為代理簽章者U_i的密鑰，其中 $1 \le i \le n$.
$y_o = g^{x_o} \bmod p$	y_o為原始簽章者A_o的公鑰
$y_i = g^{x_i} \bmod p$	y_i 為代理簽章者U_i的公鑰，其中 $1 \le i \le n$.
$H(\cdot), H'(\cdot)$	單向雜湊函數

Hu-Li 代理環簽章方法共包含四個階段，分別為代理金鑰產生階段、簽章階段、驗證階段、以及取消匿名階段，以下將依序說明之。

2.1 代理金鑰產生階段

原始簽章者A_o首先選擇亂數$k_o \in_R Z_q$，並替每一個代理人群組成員U_i選擇一亂數$k_i \in_R Z_q$, 並計算

$$\bar{s}_i = x_o g^{k_i} + k_i + x_o g^{k_o} + k_o,$$
$$\bar{r}_i = g^{k_i},$$
$$\bar{r} = g^{k_o}.$$

接下來A_o保留參數k_i，並將$(\bar{s}_i, \bar{r}_i, \bar{r})$等參數秘密地傳送給$U_i$. 當$U_i$收到訊息後，將驗證下列方程式

$$g^{\bar{s}_i} = y_o^{g^{k_i}} g^{k_i} y_o^{g^{k_o}} g^{k_o} = y_o^{\bar{r}_i} \bar{r}_i y_o^{\bar{r}} \bar{r}.$$

若成立，便計算代理秘密金鑰如下列方程式

$$s_i = x_i + \bar{s}_i.$$

2.2 簽章階段

不失一般性，假設代理簽章者U_i欲簽署一訊息m，而環簽章群組成員(Ring members)為$B = (U_1, U_2, \ldots, U_n)$，其簽章步驟如下：

1. 選擇一亂數$d \in_R Z_q$，並計算
   $$h = H(m),$$
   $$\sigma_i = h^{s_i - d},$$
   $$A = \sigma_i^{\frac{1}{i}}.$$
2. 選擇一亂數$w_i \in_R Z_q$，並計算
   $$a_i = g^{w_i},$$
   $$b_i = h^{w_i}.$$
3. 對於所有$j \ne i$選取亂數$z_j, c_j, r_j \in_R Z_q$, 並計算
   $$a_j = g^{z_j} y_j^{c_j} y_o^{c_j} r_j^{c_j} (\bar{r} y_o^{\bar{r}})^{c_j},$$
   $$\sigma_j = A^j,$$
   $$b_j = h^{z_j} \sigma_j^{c_j}.$$
4. 計算
   $$V = g^{g^{-d}}, \quad (1)$$
   $$c = H'(m, a_N, b_N, V), \quad (2)$$
   其中$a_N = (a_1, \ldots, a_n)$, $b_N = (b_1, \ldots, b_n)$.
5. 計算
   $$c_i = c - \sum_{j \ne i} c_j, \text{ 及} \quad (3)$$
   $$z_i = w_i - c_i s_i + c_i d.$$
6. 計算
   $$r_i = y_o^{(\bar{r}_i - 1)} \bar{r}_i g^{-d}.$$

   所產出之代理環簽章
   $\sigma = (m, A, z_N, c_N, r_N, V)$,
   其中$z_N = (z_1, \ldots, z_n)$, $c_N = (c_1, \ldots, c_n)$, $r_N = (r_1, \ldots, r_n)$.

2.3 驗證階段

假設接收者收到之代理環簽章為$\sigma = (m, A, z_N, c_N, r_N, V)$，其簽章之驗證步驟如下：

1. 計算 $h = H(m)$.
2. 計算
   $$\sigma_i = A^i,$$
   $$a_i = g^{z_i} y_i^{c_i} y_o^{c_i} r_i^{c_i} (\bar{r} y_o^{\bar{r}})^{c_i}, \text{ 及}$$
   $b_i = h^{z_i} \sigma_i^{c_i}$, 其中 $1 \le i \le n$.
3. 驗證下列方程式是否成立

$$H'(m,a_N,b_N,V)=\sum_{i\in B}c_i \quad (4)$$

若成立，則認同σ為合法之環簽章。

2.4 取消匿名階段

若原始簽章者欲揭露真實簽章者的身分，可計算下列方程式

$$g^{r_i}=V^{y_o^{(\bar{r}_i-1)}\bar{r}_i} \quad (5)$$

，其中$1\le i\le n$。若等式成立，則代理人U_i即為真實的簽章者。

3. 針對取消匿名性之評論

我們發現在Hu-Li代理環簽章方法[4] 並無法做到其所宣稱的取消匿名特性。也就是說，代理人可以在不被原始簽章者得知身分的情況下做出合法的環簽章。因此，代理人可能的簽章權利濫用狀況依然存在。以下將說明如何產生一個合法的環簽章並且成功地避開原始簽章者的追查。

假設一個惡意的代理簽章者在原簽章階段的第四步驟改成計算

$c=H'(m,a_N,b_N,V)$, 其中V為代理簽章者所選的一個亂數，a_N = (a_1, …, a_n), b_N = (b_1, …, b_n).

其餘步驟皆維持不變。如此一來，在簽章驗證階段，驗證用之方程式(4)依然會成立，該驗證式之推導如下：

$$\begin{aligned}&H'(m,a_n,b_n,V)\\&=c\\&=c_i+\sum_{j\neq i}c_j\\&=\sum_{i\in B}c_i.\end{aligned}$$

由此可知，即使將簽章過程中之參數$V\neq g^{g^{-d}}$而是改為選擇一個亂數取代之，依然可以成功通過驗證步驟被證實為一合法代理環簽章。但是在取消匿名階段，也由於$V\neq g^{g^{-d}}$原始簽章者為了要要得知真實簽章者的身份所計算之方程式(5)也將因此不會成立，該驗證式之說明如下：

$$\begin{aligned}&g^{r_i}\\&=g^{y_o^{(\bar{r}_i-1)}\bar{r}_i g^{-d}},\\&=(g^{g^{-d}})^{y_o^{(\bar{r}_i-1)}\bar{r}_i},\\&\neq V^{y_o^{(\bar{r}_i-1)}\bar{r}_i}.\end{aligned}$$

由上述分析可得知，原始簽章者將無從查證此環簽章是由哪一位代理人所簽出。也就是說，Hu-Li 代理環簽章方法將無法做到其所宣稱之取消匿名功能。

4. 結論

在本篇論文中，我們分析了 Hu-Li 代理環簽章方法，並詳細地描述一個惡意的代理簽章者如何簽署一合法代理環簽章並成功地躲避原始簽章者的追查，因此，證實了 Hu-Li 代理環簽章方法無法做到其所宣稱的取消匿名性之功能。

參考文獻

[1] Awasthi, A. K., Lal, S., “ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings,” ***Cryptology ePrint Archive***, Report 2004/184, available at http://eprint.iacr.org, 2004.

[2] Bender, A., Katz, J., Morselli, R., “Ring signatures: stronger definitions, and constructions without random oracles,” ***In S.Halevi and T. Rabin, editors, Theory of Cryptography ł TCC 2006***, Lecture Notes in Computer Science, Springer-Verlag, Vol. 38762, pp. 60–79, 2006.

[3] Bresson, E., Stern, J., Szydlo, M., “Threshold ring signatures and applications to ad-hoc groups,” ***In Moti Yung, editor, Advances in Cryptology-CRYPTO 2002***, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2442, pp. 465–480, 2002.

[4] Hu, C., Li, D., “A New Type of Proxy Ring Signature Scheme with Revocable Anonymity,” ***Eighth ACIS International Conference***, Vol. 1, pp. 866-868, 2007.

[5] Komano, Y., Ohta, K., Shimbo, A., Kawamura, S., “Toward the fair anonymous signatures: Deniable ring signatures,” ***In D.Pointcheval, editor, CT-RSA’06***, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3860, pp. 174–191, 2006.

[6] Lin, W. D., Jan, J. K., “A security personal learning tools using a proxy blind signature scheme,” ***Proceedings of International Conference on Chinese Language Computing***, Illinois, USA, pp. 273–277, July 2000.

[7] Mambo, M., Usuda, K., Okamoto, E. "Proxy signature: Delegation of the power to sign messages," ***IEICE Trans. Fundamentals***, Vol. E79-A, No. 9, pp. 1338–1353, September, 1996.

[8] Naor, M., "Deniable ring authentication," ***In CRYPTO 2002***, pp. 481–498, 2002.

[9] Rivest, R. L., Shamir, A., Tauman Y., "How to leak a secret," ***Advances in Cryptology-Asiacrypt 2001***, LNCS 2248, pp. 552–565, Springer-Verlag, 2001.

[10] Bender, A., Katz, J., Morselli, R., "Ring signatures: stronger definitions, and constructions without random oracles," ***In S.Halevi and T. Rabin, editors, Theory of Cryptography, TCC 2006***, Lecture Notes in Computer Science, Springer-Verlag, Vol. 38762, pp. 60–79, 2006.

[11] Yi, L., Bai, G., Xiao, G., "Proxy multi-signature scheme: A new type of proxy signature scheme," ***Electronics Letters***, Vol. 36, pp. 527–528, 2000.

[12] Zhang, K., "Threshold proxy signature schemes," ***1997 Information Security Workshop***, pp. 191-197, September, 1997.

[13] Zhang, F., Naini, R. S., Lin, C. Y., "New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings," ***Cryptology ePrint Archive***, available at: http://eprint.iacr.org/2003/, 2003.