一個有效率的強指定驗證者簽章協定

Fuw-Yi Yang Cai-Ming Liao
Department of Computer Science and Information Engineering,
Chaoyang University of Technology
yangfy@cyut.edu.tw s9527645@cyut.edu.tw

摘要

強指定驗證方案能夠確保傳送者所傳送的資訊，除了指定接收者可以得知訊息的內容以及驗證，任何人都無法得知訊息內容。在 2007 年，Lee et al.提出結合訊息恢復機制的強指定驗證者簽章協定，使得原始的指定驗證者簽章協定，達到強化的特性，然而，在 Lee et al. 的協定中，並未達到較好的效率。在本論文中，我們將提出一個有效率的強指定驗證者簽章方案，在計算花費(僅需 33%)，通訊花費(僅需 50%)方面都是較輕量的，並且在安全性方面，我們將論證協定的安全性是建構於 CDH 假想之上。

關鍵詞： 指定驗證者、簽章、訊息恢復、CDH 假想

Abstract

Strong designated verifier signature scheme is able to ensure the transmitted information by sender. In addition to the contents of a message can be verified by the designated verifier, any third party can not know the content of the message. In 2007, Lee et al. proposed a strong designated verifier signature scheme with message recovery. This scheme makes the original designated verifier signature protocol to achieve strongness property. However, some improvements on the scheme are possible in the sense of communication and computation. In this paper, we will propose an efficient strong designated verifier signature scheme. The proposed scheme reduce the cost of computations and communications 50% (or more), as compared with that of the Lee et al.'s scheme. Furthermore, we prove the security based on the Computational Diffie-Hellman assumption.

Keywords: designated verifier, signature, message recovery, CDH assumption

1. 介紹

設若一個使用者想要傳送訊息給一個接收者，並且希望只有其接收者能夠驗證訊息的合法性以及得知其內容，對於這樣的需求，傳統簽章方案所產生的簽章，任何人都能對其簽章進行驗證，並無法滿足上述使用者之需求。在 1996 年，Jakobsson et al.提出指定驗證者簽章方案(M. Jakobsson, K. Sako, and R. Impagliazzo, 1996, [1])，與傳統簽章方案不同之處在於只有指定驗證者能夠驗證簽章的合法性，並且一個指定驗證者可藉由接收到的簽章，有效地模擬出另一個合法的簽章，因此，當指定驗證者想向第三者證明此簽章的真實來源時，第三者將難以確信此簽章的真實來源為傳送者或是接收者。

設若傳送端與接收端之間存在一個攻擊者，攻擊者在接收者收到簽章之前截取此簽章，則攻擊者有很高的機率可得知訊息的真實來源。對於這種型態的攻擊，我們可使用指定驗證者的公鑰，對每個簽章加密，使其問題獲得解決，然而，就計算花費而言是沒有效率的。因此，在 2003 年，Saeednia et al. 提出一

個新的強指定驗證者簽章方案(S. Saeednia, S. Kremer, O. Markowitch, 2003, [2])，不需利用任何的加密演算法，即使得第三者因無法得知指定驗證者的密鑰，而無法驗證其簽章；設若傳送者不希望第三者讀取訊息中的內容，作者進一步的提出 signcrypted 版本方案，利用對稱式加密系統將目標訊息加密成密文，使得第三者無法讀取訊息的內容，實際上，若採用此方案，在成本方面，必須設置二個版本供使用者選擇。

在[3, 4], Nyberg 與 Ruepple 提出訊息恢復機制的簽章方案，將一個目標訊息依附在簽章裡，當接收者收到簽章後，可將訊息恢復並驗證簽章的合法性。在 2007 年，Lee et al.提出一個結合訊息恢復機制的強指定驗證者簽章方案(Lee, J.S. and Chang, J.H., 2007, [5])，將指定驗證者簽章方案的特性，結合訊息恢復的機制，使其訊息隱藏在簽章中，因而只有指定驗證者能夠得知訊息的內容，並驗證其訊息之合法性，如此一來，只需使用一個版本，即可達到同樣的安全性以及特性，然而，在此協定的效率方面，並未達到較好的效率。在本論文中，我們將提出一個有效率的強指定驗證者簽章的方案，不但具備指定驗證者簽章方案的特性，並且在協定執行的效率方面，計算花費以及通訊花費分別僅需 Lee et al.方案的 33%與 50%；在安全性方面，我們將論證協定的安全性是建構於 CDH 假想 (Computational Diffie-Hellman Assumption)之上。

2. 回顧 Lee et al.的協定

設p, q為二個強質數且q整除(p-1)，g是由Z_p^*乘法群挑選其序為q，m為目標訊息其值對應到Z_q加法群。假設A與B分別代表使用者以及指定驗證者，使用者A的密鑰與公鑰分別為x與X，其中x由Z_q^*產生且$X = g^x \bmod p$；指定驗證者B的密鑰與公鑰分別為y與 Y，其中y由Z_q^*產生且$Y = g^y \bmod p$。設$H(\cdot)$為一個無碰撞的單向雜湊函數且輸出值對應到Z_q^*, ||代表字串連結運算符號。

設若使用者 A 想要傳送一個簽章訊息給指定的驗證者 B，並且結合訊息恢復的機制。其通訊過程如下:

簽章產生階段. A分別由Z_q^*與Z_q隨機各選擇一個亂數k_1以及k_2，計算$t = g^{k_1} \bmod p$、$c = m \cdot Y^{k_2} \bmod p$、$r = H(m, g^{k_2} \bmod p)$以及$s = k_1^{-1}(xr - k_2) \bmod q$，接著傳送簽章$(t, c, r, s)$給$B$。

訊息恢復與驗證階段. 當B收到簽章訊息(t, c, r, s)後，計算$m = c(t^s X^{-r}) \bmod p$並驗證$r \stackrel{?}{=} H(m, t^{-s} X^r)$；若相等，則視為合法訊息。

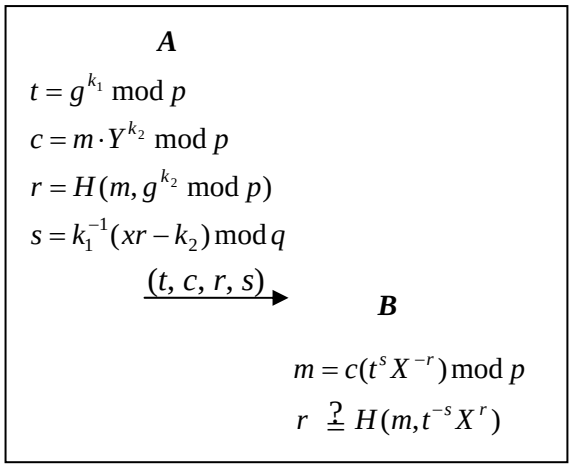

Fig. 1

副本模擬. B收到簽章(t, c, r, s)後，分別由Z_q^*與Z_q隨機選擇亂數w_1以及w_2，接著模擬副本簽章如下：

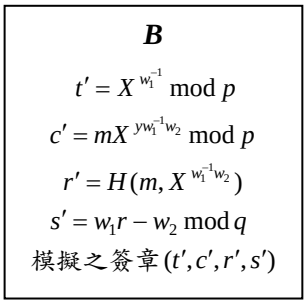

Fig. 2

設若 B 提供密鑰給第三者 C，C 將可驗證

模擬的合法簽章，然而 C 知道 B 可以輕易地模擬一個合法的簽章，因此 C 將無法確信此簽章的真實簽章者為接收者還是傳送者。

3. 我們的協定

我們提出一個有效率的強指定驗證者簽章方案，當使用者 A 想傳送簽章(r, MAC)給指定的驗證者 B，我們的協定不但能夠達到指定驗證者方案所需的特性，在協定執行時，所需的計算量以及通訊花費都是較輕量的，並且協定的安全性是建構於 CDH 假想之上。為了方便比較，我們協定中所使用的參數，除了隨機亂數之外其餘的系統參數皆與第二章節相同。

簽章產生階段. A由Z_q隨機選擇亂數t，計算 $r = (m\|t)\cdot Y^{x\cdot MAC} \bmod p$ 以及 $MAC = H(m\|t)$，接著傳送(r, MAC)給B.

訊息恢復與驗證階段. 當 B收到簽章訊息(r, MAC)，計算$(m\|t) = r \cdot X^{-y\cdot MAC} \bmod p$，並驗證 $H(m\|t) \stackrel{?}{=} MAC$;若相等，則視為合法訊息。

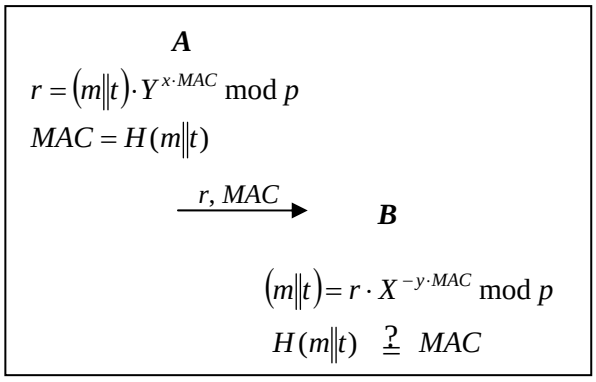

Fig. 3

副本模擬. B收到(r, MAC)後，由Z_q隨機選擇一個亂數t'，接著計算副本簽章(r', MAC') 如下：

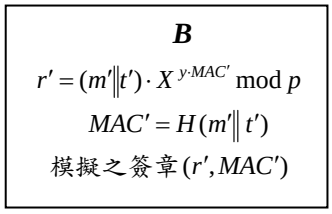

Fig. 4

4. 協定分析

我們將在這個章節針對協定的安全性以及效率進行分析。

4.1 安全性分析

論證定理 1 的證明是建立在CDH假想之上，接下來我們將簡短地描述CDH假想，更進一步的詳情，請參考[6, 7]。假設G 是一個乘法群且其序為大質數q，$g \in G$並可產生乘法群G，其CDH問題如下：由G隨機地選擇二個亂數X與Y，找到$Z = g^{xy} \in G$，其中 $x = \log_g^X$及$y = \log_g^Y$。CDH假想意味著CDH問題是難以解決的難題，也就是解決CDH問題的機率是可被忽略的。

定理 1. 設想接收者 B 如實地執行 Fig. 3 的協定。設若一個攻擊者有不可忽略的機率能夠去假冒傳送者，那就表示 CDH 問題是可以在多項式時間內被解決。

證明. 設想g可產生群$G \subset Z_p^*$。我們由乘法群G隨機挑選二個元素X與Y。提供X與Y，我們的目標是解決CDH問題，即找到$Z = g^{xy} \in G$。設傳送者A的公鑰為X，接收者B由群組$\{1, 2, \ldots, q\text{-}1\}$選擇一個密鑰$y'$並計算公鑰$Y' = Y^{y'} \bmod p$。公開$A$與$B$的公鑰$X$以及$Y'$。

設若此攻擊者成功地假冒傳送者A，當接收者B收到(r, MAC)，接收者B計算出$m\|t = r \cdot X^{-y'\cdot MAC} \bmod p$值，來獲得目標訊息$m$與隨機亂數$t$，並驗證$MAC$ 是否等同於$H(m\|t)$。由於$H(\cdot)$為一個無碰撞的單向雜湊函數，而且公鑰X及Y'是公開的資訊，故攻擊者成功地假冒傳送者A可以簡約成解開CDH問題，細節如下：

由協定的結構$r = (m\|t) \cdot Y'^{x\cdot MAC} \bmod p$，其中$x = \log_g^X$，我們可得知攻擊者無法計算出$x$值，因為攻擊者必須面臨解離散對數難題；因此，提供二個隨機亂數X與Y，計算CDH問題就如同$(Y)^x = (r \cdot (m\|t)^{-1})^{1/y'\cdot 1/MAC} \bmod p$。若攻擊者能夠成功地計算出$(r, MAC)$，接收者$B$可以利用其密鑰及接收的訊息計算$Z = (Y)^x = g^{xy} \bmod p$，如此

將推翻CDH假想，由此反證協定的安全性等同於CDH問題。

定理 2. 我們的協定是指定驗證者簽章協定。

證明. 我們將論證指定驗證者所模擬的簽章副本，對於任何的第三者是難以去確信真實來源為指定驗證者或者簽章者。由*A*產生的簽章與*B*模擬的簽章副本如下:

$$\sigma=(r,MAC):\begin{cases}t\in_R Z_q\\ r=(m\|t)\cdot Y^{x\cdot MAC} \bmod p\\ MAC=H(m\|t)\end{cases}$$

以及

$$\sigma'=(r',MAC'):\begin{cases}t'\in_R Z_q\\ r'=(m\|t')\cdot Y^{x\cdot MAC'} \bmod p\\ MAC'=H(m\|t')\end{cases}$$

假設在所有*A*的合法簽章中，$(\bar{r},\overline{MAC})$是一個隨機選擇給*B*的簽章，則*A*所能產生的簽章與*B*所能模擬的副本簽章，其機率如下:

$$\Pr_{\sigma}\left[(r,MAC)=(\bar{r},\overline{MAC})\right]=\Pr_{t\in Z_q}\left[\begin{array}{l}r=(m\|t)\cdot Y^{x\cdot MAC} \bmod p=\bar{r}\\ MAC=H(m\|t)=\overline{MAC}\end{array}\right]=\frac{1}{q}$$

以及

$$\Pr_{\sigma'}\left[(r,MAC)=(\bar{r},\overline{MAC})\right]=\Pr_{t'\in Z_q}\left[\begin{array}{l}r=(m\|t')\cdot Y^{x\cdot MAC} \bmod p=\bar{r}\\ MAC=H(m\|t')=\overline{MAC}\end{array}\right]=\frac{1}{q}$$

由上面二個結果可知，*B*將難以模擬出與A相同之簽章。

4.2 效率分析

在效能分析的部份，我們針對計算花費以及通訊花費做比較。設 p 和 q 分別為 1024 位元與 160 位元的大質數，雜湊函數 $H(\cdot)$的輸出位元為 160 位元。由於指數運算成本極大於雜湊函數運算，因此我們將其雜湊函數的運算量忽略不計。

表 1

協定	Lee et al 的協定		我們的協定	
	A	*B*	*A*	*B*
通訊花費（位元數）	2368		1184	
指數運算花費	3	3	1	1

由上表 1.可知，我們的協定之所以能夠降低計算花費以及通訊花費，是因為使用者與驗證者只需使用密鑰分別作簽章以及解密，即可達到保護訊息的目的；在通訊花費方面，只須傳送(*r, MAC*)給 *B*，即可達到簽章以及訊息隱藏的功能，因此，我們提出的協定是具有較好的效率。

5. 結論

我們提出的協定，具有指定驗證者簽章所要求的特性，在安全性以及效率方面，我們的協定是建構於計算 Diffie-Hellman 問題上，並且擁有更好的效率，使得指定驗證者簽章方案，能夠實際地被執行。

6. 參考文獻

[1]. M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," ***Advances in Cryptology - EUROCRYPT '96***, LNCS 1070, pp. 143-154, 1996.

[2]. S. Saeednia, S. Kremer, O. Markowitch, "An efficient strong designated verifier signature scheme," ***ICISC'03***, LNCS 2971, pp. 40-54, 2003.

[3]. K. Nyberg, R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," ***Proc. of the First ACM Conference on Computer and Communication Security***, Vol. 1, pp. 58-61, 1993.

[4]. K. Nyberg, R. A. Rueppel, "Message recover for signature schemes based on the discrete logarithm problem," ***Advances in Cryptology - EUROCRYPT'94***, LNCS 950, pp. 182-193, 1994.

[5]. J.S. Lee and J.H. Chang, "Strong Designated Verifier Signature Scheme with Message Recovery," ***Advanced Communication Technology***, Vol. 1, pp. 801-803, 2007.
[6]. V. Shoup, "On formal models for secure key exchange," ***IBM Research Report RZ 3120 Version 4***, 1999.
[7]. W. Diffie and M. E. Hellman, "New directions in cryptography," ***IEEE Transactions on Information Theory***, Vol. 22, pp. 644-654, 1976.