可訊息回復之免憑證簽章機制之研究

Certificateless Signatures with Message Recovery

左瑞麟
National Chengchi University, Taiwan, ROC
raylin@cs.nccu.edu.tw

詹省三
National Chengchi University, Taiwan, ROC
g9718@cs.nccu.edu.tw

陳淵順
National Chengchi University, Taiwan, ROC
g9736@cs.nccu.edu.tw

陳力瑋
National Chengchi University, Taiwan, ROC
g9726@cs.nccu.edu.tw

摘要(Abstract)

在傳統的簽章機制中，我們需要一個具有公信力的第三方 (Trusted Third Party,TTP) 來核發數位憑證，以驗證公開金鑰確實屬於簽章者所擁有，為了減少 TTP 的負擔，於是就有學者提出了免憑證簽章 (Certificateless Signature) 機制。另一方面，具有訊息回復 (Message Recovery) 功能的數位簽章是指原始訊息不需要與簽章一起傳送給接收者以簡化訊息及簽章在傳送時的長度。本論文中我們提出了一個具有訊息回復功能的免憑證簽章機制，和一般簽章方式相比，我們的方法不僅具有免憑證簽章的優點，訊息回復功能也減少了訊息和簽章的總長度，提昇了訊息的傳送效率 (Communication Cost)，在效能方面也表現的不錯，因此非常適用於以頻寬為主要考量的公司組織以及對短訊息作簽章的應用，本研究也是第一個提出具有訊息回復功能之免憑證簽章方法。

In traditional digital signature systems, a trusted third party (TTP) is required in order to issue a digital certificate. The certificate is to assure that the public key actually belongs to the person of the signature. The management of certificates including revocation, storage and distribution is considered to be costly. ID-based signatures do not need a certificate but has the key escrow problem. In 2003, the concept of certificateless signature scheme was introduced. It successfully removed the necessity of certificates and the key escrow problem. On the other hand, a digital signature with message recovery is a signature that the message itself is not required to be transmitted together with the signature. It has the advantage of small data size of communication. In this paper, a certificateless signature with message recovery is proposed. It inherits both the advantages of certificateless signatures and signatures providing message recovery. The performance of our scheme is compared with other schemes which shows that our scheme is quite efficient. We emphasize that this is the first work that proposing the certificateless signatures with message recovery.

關鍵詞： 雙線性配對(Bilinear Paring)、免憑證簽章(Certificateless Signature)、訊息回復(Message Recovery)

一、緒論

在現今的電子化社會裡，數位簽章一直都扮演極為重要的角色，而我們主要是利用它的訊息完整性來達到防止接收到的訊息被更改以及利用其可驗證性來檢驗使用者是否合法。在傳統的簽章機制中，為了驗證公開金鑰確實屬於簽章者所擁有，我們需要一個具有公信力的 TTP 來核發數位憑證，藉由驗證此數位憑證來驗證使用者的公開金鑰。但憑證的註銷 (Certificate Revocation) 等等的問題會造成 TTP 過多的負擔。另外，對簽名的驗證者來說，憑證的驗證也增加了許多的計算成本(Computation Cost)。

在 1984 年的時候，Shamir[7]提出了第一個基於身份認證的簽章方法 (ID-based Signature)，ID-based signature 的優點是允許簽名者以個人訊息來當作他的公開金鑰，例如 email address、姓名、電話號碼等，如此接收者就不需要透過憑證去驗證公開金鑰的合法性，也大幅地減少了 TTP 的計算量與記憶體空間，在這裡我們稱 TTP 為 PKG (Private Key Generator) ，然而，由於所有簽名者的私密金鑰皆是由 PKG 所生成，所以 ID-based signature 可能會有金鑰託管（Key escrow）的問題，這會導致 PKG 的權限過大，PKG 可假冒簽名者對任意訊息做簽名，因此簽名者也可以否認之前所簽過的訊息，這並不符合數位簽章中的不可否認性。

為了解決金鑰託管的問題，在2003年的時候，Al-Riyami等學者[1]提出了免憑證簽章的概念，它同時具有傳統簽章與ID-based signature的優點，既可解決金鑰控管的問題，也可保有ID-based signature免憑證的特點，其主要的差異在於簽名者的私密金鑰並不是完全由PKG所生成，所以PKG無法得知簽名者的私密金鑰。

在1993年的時候，Nyberg等學者[6]提出了第一個具有訊息回復之數位簽章，此方法是基於離散對數問題(Discrete Logarithm Problem)，自此以後，關於這方面的研究也如雨後春筍般的出現，直到2005年的時候，Zhang等學者[10]提出了第一個具有訊息回復之ID-based signature，基於Zhang等學者以及Barreto等學者[3]的概念，在2007年的時候，Tso等學者[8]提出了更有效率的方法，而我們的方法則是基於Tso等學者的概念下去做延伸。

具有訊息回復功能的數位簽章是指原始訊息不需要與簽章一起傳送給接收者，且接收者可在驗證階段利用一些公開參數與簽章去回復原始的訊息，這類型的簽章其目的是為了簡化簽章在傳送時的長度，因此非常適用於以頻寬為主要考量的公司組織以及對短訊息作簽章的應用。

本研究擷取免憑證簽名系統及訊息回復功能數位簽章的優點，提出免憑證簽章結合訊息回復的概念。本研究是第一個提出此概念的文章，另外，提案方式在效能方面也有不錯的表現。

關於本篇文章的章節，在接下來第二部份我們會介紹一些相關的背景知識，第三部份則是我們提出的方法，第四部份我們會針對一些安全性問題去做分析，第五部份則是效能分析與比較，最後一部分則是我們對本研究的結論。

二、相關背景知識

1. 雙線性配對 (Bilinear Pairing)

G_1 為一加法群 (Additive Group)，序(Order)為 q，G_2 為一乘法群 (Multiplicative Group)，序也為 q。P 是 G_1 的生成元(Generator)，則一個雙線性配對表示為 e：$G_1 \times G_1 \to G_2$，具有以下三種性質[4,9]:

(1) 雙線性(Bilinear)：P, Q$\in G_1$ 及 a,b$\in Z_q^*$，

e(aP,bQ)=e(P,Q)^{ab}。

(2) 非退化性(Non-degenerate)：P, Q$\in G_1$，滿足 e(P,Q)$\neq$1。

(3) 可計算性(Computable)：P, Q$\in G_1$，存在一有效率的演算法可計算 e(P,Q)。

在密碼學的研究領域，為符合系統安全的需求，通常會有許多計算難問題的假設，以下是對本研究相關的難問題做定義[2,5]：

(1) 橢圓曲線離散對數問題(ECDLP)
橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem,ECDLP)，在有限體 F_p 之下，給定橢圓曲線 E 上的兩個相異點 P 和 Q，要求得整數 k 並滿足 Q=kP 是很困難的。

(2) 雙線性 Diffie-Hellman 問題(BDHP)
雙線性 Diffie-Hellman 問題(Bilinear Diffie-Hellman Problem,BDHP)，a,b,c$\in Z_q^*$ 為未知數，給定 P,aP,bP,cP$\in G_1$，要求得 $e(P,Q)^{abc} \in G_2$ 是非常難解的。

2. 基本架構(Scheme Model)

本研究中，關於我們提出的免憑證簽章大致可以定義成七個階段，如下所述：

(1) Setup
此階段 PKG 會生成一對金鑰，且會公開一些系統參數。

(2) Partial-Private-Key-Extract
此階段 PKG 會根據使用者的身份識別 ID 生成部份的私密金鑰與公開金鑰並將部份私密金鑰傳送給使用者。

(3) Set-Secret-Value
此階段使用者會隨機選取一秘密參數。

(4) Set-Private-Key
此階段使用者會利用秘密參數做一些運算，得到的結果為使用者的私密金鑰。

(5) Set-Public-Key
此階段使用者會利用秘密參數做一些運算，得到的結果為使用者的公開金鑰。

(6) Sign
此階段使用者會利用私密金鑰與公開的系統參數去對訊息做簽章。

(7) Verify
此階段使用者可透過一決定型的演算法去驗證簽章的合法性。

3. 安全性定義(Security Definition)

由於 PKG 不再是公正的 TTP，再加上簽名者持有自己生成的私密金鑰，所以免憑證簽章的安全性通常會分兩種情況討論，如下所述：

- Type I 攻擊者
  此種情況是假設 PKG 是公正的 TTP，攻擊者無法從 PKG 那裡得到 PKG 所生成的部份私密金鑰，但攻擊者會嘗試偽造簽名者的私密金鑰去做攻擊，此種攻擊者我們歸為 Type I 攻擊者。
- Type II 攻擊者
  此種情況是假設在 PKG 不是公正的 TTP 且 PKG 不可替換簽名者生成的金鑰下，攻擊者可輕易地從 PKG 那裡得到 PKG 所生成的部份私密金鑰，但無法得到與簽名者相對應的私密金鑰，基於這種假設的攻擊者我們歸為 Type II 攻擊者。

若免憑證簽章系統可以抵擋此兩種攻擊者的攻擊，則我們可以說此系統是安全的。

4. 符號標記

本研究中我們會使用到一些符號，其定義如下：

- $a\|b$：a 字串與 b 字串結合的連續字串。
- $\oplus$：二進位系統中的 X-OR 運算。
- $[x]_{10}$：x 的十進位表示法且 $x\in\{0,1\}^*$。
- $[y]_2$：y 的二進位表示法且 $y\in Z$。
- ${}_{l_1}|\beta|$：從 β 左側開始算起的 l_1 位元(最高有效 l_1 位元)。
- $|\beta|_{l_2}$：從 β 右側開始算起的 l_2 位元(最低有效 l_2 位元)。

三、可訊息回復之免憑證簽章方法

在此章節我們將會提出可訊息回復之免憑證簽章的方法，關於訊息回復在我們的方法中我們分兩點討論，第一點就是訊息長度有限制，但可以回復完整的訊息，例如，$m\in\{0,1\}^{l_1}$ 即 m 的長度限制為 l_1，第二點則是訊息長度不限制，但只能回復部份的訊息，以下我們會個別提到。

I. 限制訊息長度之免憑證簽章

我們需要七個步驟來達到本系統設計的方法及目的，其分述如下：

[Setup]

首先 PKG 隨機選取一亂數 $s\in Z_q^*$ 為 PKG 的私密金鑰，接著計算 P_{pub}=sP 為 PKG 的公開金鑰。最後 PKG 公開系統參數給使用者：

$<G_1, G_2, q, e, P, P_{pub}, \mu, H_1, H_2, F_1, F_2, l_1, l_2>$

且系統參數的定義分別如下：

- G_1, G_2 皆為相同序 q 的循環群，且 $|q|=l_1+l_2$
- e：$G_1\times G_1\to G_2$
- μ =e(P,P)
- $H_1:\{0,1\}^*\to G_1$，輸入為 $\{0,1\}^*$ 的字串，輸出為 G_1 中的元素的單向雜湊函數 (one way hash function)
- $H_2:\{0,1\}^*\to Z_q^*$，輸入為 $\{0,1\}^*$ 的字串，輸出為 Z_q^* 中的元素的單向雜湊函數
- $F_1:\{0,1\}^{l_1}\to\{0,1\}^{l_2}$，輸入為 $\{0,1\}^{l_1}$ 的字串，輸出為 $\{0,1\}^{l_2}$ 的字串的單向雜湊函數
- $F_2:\{0,1\}^{l_2}\to\{0,1\}^{l_1}$，輸入為 $\{0,1\}^{l_2}$ 的字串，輸出為 $\{0,1\}^{l_1}$ 的字串的單向雜湊函數

[Partial-Private-Key-Extract]

PKG 會根據簽名者 A 的身份識別 ID_A 計算 $Q_A=H_1(ID_A)$ 為簽名者 A 的部份公開金鑰。接著 PKG 會計算 $D_A=sQ_A$ 為簽名者 A 的部份私密金鑰，並將部份私密金鑰傳送給簽名者 A。

[Set-Secret-Value]

簽名者 A 隨機選取一亂數 $X_A\in Z_q^*$。

[Set-Private-Key]

簽名者 A 計算 $S_A=X_AQ_A$ 為自己的私密金鑰。

[Set-Public-Key]

簽名者 A 計算 $pk_A = X_A P$ 為自己的公開金鑰。

[Sign]

針對一欲簽名的訊息 $m \in \{0,1\}^{l_1}$，簽名者 A 會執行以下步驟來對 m 做簽名：

(1) 計算 $\beta = F_1(m) \| (F_2(F_1(m)) \oplus m)$，接著定義 $\alpha = [\beta]_{10}$。

(2) 隨機挑選一亂數 $r \in Z_q^*$，接著計算 $V = H_2(\mu^r) + \alpha$。

(3) 計算 $U = rP + V(D_A + S_A)$。

最後得到對 m 的簽名為 $\sigma = (U, V)$。

[Verify]

針對簽名 σ，使用者可依以下步驟驗證 σ 是否合法：

(1) 使用者根據簽名 $\sigma = (U, V)$ 及公開的參數可計算出：

$$\alpha = V - H_2\left(e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}\right)$$

。

(2) 接著可推算出 $\beta = [\alpha]_2$。

(3) 回復訊息 $m' = F_2\left(_{l_2}|\beta|\right) \oplus |\beta|_{l_1}$。

(4) 若 $_{l_2}|\beta| = F_1(m')$ 則表示此簽章 σ 為合法簽章。

此方法的正確性可被證明如下：

因為 $\alpha = V - H_2\left(e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}\right)$

$$= H_2(\mu^r) + \alpha - H_2\left(e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}\right)$$

所以我們只需證 $\mu^r = e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}$ 的等式是否成立即可：

$$e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}$$

$$= e(rP + V(D_A + S_A), P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}$$

$$= e(rP, P) \cdot e(D_A + S_A, P)^V \cdot e\left(Q_A, X_A P + P_{pub}\right)^{-v}$$

$$= e(P,P)^r \cdot e(D_A, P)^V \cdot e(S_A, P)^V \cdot e(Q_A, X_A P)^{-V} \cdot e(Q_A, sP)^{-V}$$

$$= e(P,P)^r \cdot e(D_A, P)^V \cdot e(S_A, P)^V \cdot e(X_A Q_A, P)^{-V} \cdot e(sQ_A, P)^{-V}$$

$$= e(P,P)^r \cdot e(D_A, P)^V \cdot e(S_A, P)^V \cdot e(S_A, P)^{-V} \cdot e(D_A, P)^{-V} = e(P,P)^r = \mu^r$$

若 σ 是合法的簽名，則 $[\beta]_{10} = \alpha$ 且 $\beta = F_1(m) \| (F_2(F_1(m)) \oplus m) = \beta = [\alpha]_2$。

因此，我們可以得到：

$$F_2\left(_{l_2}|\beta|\right) \oplus |\beta|_{l_1}$$

$$= F_2(F_1(m)) \oplus (F_2(F_1(m)) \oplus m)$$

$$= m$$

最後，若 $_{l_2}|\beta| = F_1(m)$，則即可驗證訊息的正確性。

II. 不限制訊息長度之免憑證簽章

針對長訊息，簽名的步驟與方法大致上跟前面所提的一樣，因此這裡我們只針對有修改的部份做討論：

[Setup]

在這個步驟我們只修改了 F_1，新的定義如下：

- $F_1 : \{0,1\}^* \to \{0,1\}^{l_2}$

[Sign]

此階段針對一欲簽名的訊息 $m \in \{0,1\}^*$，簽名者 A 會執行以下步驟來對 m 做簽名：

(1) 計算 $\beta = F_1(m) \| (F_2(F_1(m)) \oplus m)$，接著定義 $\alpha = [\beta]_{l0}$。

(2) 將訊息 m 劃分為 $m_2 \| m_1$ 且 $m_1 \in \{0,1\}^{l_1}$。

(3) 隨機挑選一亂數 $r \in Z_q^*$，接著計算 $V = H_2(\mu^r) + \alpha$。

(4) 計算 $U = rP + V(D_A + S_A)$。

最後我們將 m 的簽名 $\sigma = (U,V)$ 及部份訊息 m_2 送給驗證者。

[Verify]

針對簽名 σ，使用者可依以下步驟驗證 σ 是否合法：

(1) 使用者根據簽名 $\sigma = (U,V)$ 及公開的參數可計算出：

$$\alpha = V - H_2\left(e(U,P) \cdot e\left(Q_A, pk_A + P_{pub}\right)^{-v}\right)$$

。

(1) 接著可推算出 $\beta = [\alpha]_2$。

(2) 回復部份訊息 $m_1' = F_2\left(_{l_2}|\beta|\right) \oplus |\beta|_{l_1}$。

(3) 若 $_{l_2}|\beta| = F_1(m_2 \| m_1')$ 則表示此簽章 σ 為合法簽章。

(4) 若簽章 σ 為合法簽章，我們可以回復訊息 $m = m_2 \| m_1'$。

關於此改良方法的正確性，其證明與前面所述差不多，故這裡就不多做介紹。

四、安全性分析

因為上一章節中所提到的兩種簽名方法很類似，所以在此章節我們只針對有限制訊息長度之免憑證簽章做安全性分析，且我們會分兩種攻擊者來做個別討論，如下所述：

- Type I 攻擊者

因為 PKG 是公正的 TTP，所以攻擊者 F 沒有辦法從 PKG 那得知簽名者 A 的 D_A，雖然攻擊者 F 知道 P_{pub}，但基於 ECDLP 也無法推算出 s，因此攻擊者 F 沒有辦法去計算出簽名者 A 的 D_A，即使攻擊者 F 嘗試隨機選取一隨機亂數 s' 來計算出 D_A'，且隨機選取一亂數 X_A' 來偽造簽名者 A 的 S_A' 與 pk_A'，則攻擊者 F 可以利用偽造的金鑰來得到 U'，最後得到的簽章為 $\sigma' = (U',V)$，但在驗證階段，驗證者利用 σ' 與一些公開參數算出的 α'，並不能推算出正確的 β 值，所以驗證者進行驗證時，利用 α' 推算出的 β' 去做驗證 $_{l_2}|\beta'| = F_1(m)$ 是不會成立的，因此本研究所提出的免憑證簽章具有不可偽造性，所以我們認為這個方法是安全的。

- Type II 攻擊者

因為 PKG 不是公正的 TTP，所以攻擊者 F 可以輕易地得知簽名者 A 的 D_A，但沒辦法得知簽名者 A 相對映的 S_A，雖然攻擊者 F 知道 pk_A，但基於 ECDLP 也無法推算出 X_A，因此攻擊者 F 沒有辦法去計算出簽名者 A 的 S_A，簽名時與 Type I 攻擊者遇到的問題一樣，即使攻擊者 F 偽造出簽名者 A 的 S'_A 與 pk'_A，但由於不知道真正的 S_A，所以利用最後得到的簽章 $\sigma' = (U', V)$ 去做 $_{l_2}|\beta'| = F_1(m)$ 的驗證也是不會成立的，因此基於 Type II 攻擊者的假設下，本研究所提出的免憑證簽章也是具有不可偽造性的，所以我們認為這個方法是安全的。

五、效能分析

根據表 1，由於 ZSM[10]與 Tso[8]的方法皆是 ID-based signature，所以都會有金鑰控管的問題，然而，我們提出的方法是基於 Certificateless 的概念，所以我們不會有此問題。效能運算方面，1Exp 代表一次的指數運算，1EC 代表一次的橢圓曲線運算，1e 代表一次的雙線性配對運算，所以由表 1 我們可以發現我們的方法在簽章跟驗證階段的效能運算都不會太差，甚至還要更好，但我們最主要的優勢就是沒有金鑰控管的問題。

表 1、效能分析與比較

	Key escrow	Sign	Verify
Scheme1*	N	1Exp+2EC	1e+1Exp
Scheme2	N	1Exp+2EC	1e+1Exp
ZSM[10]1*	Y	1Exp+2EC	2e+1Exp+1EC
ZSM[10]2	Y	1Exp+2EC	2e+1Exp+1EC
Tso[8]1*	Y	1Exp+1EC	1e+1Exp+1EC
Tso[8]2	Y	1Exp+1EC	1e+1Exp+1EC

註：*為有限制訊息長度之簽章方法

六、結論

本研究為第一個利用免憑證簽章的概念去實現訊息回復的功能，我們的方法不只在效能上有不錯的表現，而且也沒有金鑰控管的問題，同時又能簡化簽章和訊息在傳送時的總長度，因此我們的方法非常適用於以頻寬為主要考量的行動網路服務以及需要大量對短訊息做簽章的相關應用，未來我們希望可以再降低其運算量以及增加其安全性，使這些優點更適合應用在行動通訊網路上。

七、參考文獻

[1] S. Al-Riyami, K. Paterson, “Certificateless public key cryptography”, Advances in Cryptology-Asiacrypt’03, Springer-Verlag, LNCS 2894, 2003, pp.452-473.

[2] F. Bao, R. Deng, and H. Zhu, “Variations of Diffie-Hellman Problem,” In Proceedings of ICICS 2003, LNCS 2836, Springer-Verlag, 2003, pp. 301-312.

[3] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. Quisquater, “Efficient and provably-secure identity-based signatures and signcryption from bilinear maps”, Advances in cryptology –ASIACRYPT’05, Lecture Notes in Computer Science 3778, pp.515–532, 2005.

[4] D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, 2001, pp. 516-534.

[5] IEEE Standard Specifications for Public-Key Cryptography, IEEE 1363-2000, 2000.

[6] K. Nyberg and R. A. Tuepple, “A new signature scheme based on the DSA giving message recovery”, Proceedings of the 1st ACM conference on communication and Computer security, pp.58–61, 1993

[7] A. Shamir, “Identity-based cryptosystems and signature schemes”, Advances in cryptology –CRYPTO’84, Lecture Notes in Computer Science 0196, pp.47–53, 1984.

[8] R. Tso, C. Gu, T. Okamoto, and E. Okamoto, “Efficient ID-based digital signatures with message recovery”, in Proceedings of the 6th International Conference on Cryptology and Network Security (CANS2007), Springer, Lecture Notes in Computer Science, Vol. 4856, pp. 47-59, 2007.

[9] F. Zhang, and K. Kim, “Efficient ID-based Blind Signature and Proxy Signature from Bilinear Pairings,” The 8th Australasian Conference on Information Security and Privacy, 2003, pp. 312-323.

[10] F. Zhang, W. Susilo, and Y. Mu, “ Identity-based partial message recovery signatures (or How to shorten ID-based signatures) ”, FC’05, Lecture Notes in Computer Science 3570, pp.45–56, 2005.