基於模糊簽章的電子投票系統之安全性分析及其改良方案

Security Analysis and Improvement of E-voting System based on Oblivious Signatures

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

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

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

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

中文摘要：

近期電子投票系統時常被廣泛討論，此系統在實作上應用了密碼學中的加解密及數位簽章的機制來達成其所需的安全性。在數位簽章方面，以往的研究多是基於數位盲簽章的技術來建構出一個安全的電子投票系統。針對盲簽章的問題，而又衍生出更多不同的方法。C. Song 等學者首先利用了模糊簽章(Oblivious Signature)的概念來建構電子投票系統。與利用盲簽章技術實作比較，利用模糊簽章技術實作是比較實用的，同時也符合一般大型選舉的要求。但我們發現 C. Song 等學者的方法中還有可以改善的部分，於是我們針對這個可以改善的部分提出改良的方案，以加強利用模糊簽章技術實作電子投票系統的安全性。

Abstract：

E-voting systems have been widely investigated during these years. To achieve the security requirement, most of the e-voting systems utilize cryptographic technologies such as the encryption/decryption schemes and digital signature schemes. In the utilization of digital signatures, blind signatures and their extensions are widely used in the literature. In 2008, C. Song et al. firstly introduced their e-voting systems based on the utilization of oblivious signatures. However, we found that there are some security flaws or problems of C. Song et al.'s idea. In this paper, we will first point out these security flaws and then introduce our improved schemes. We hope that our research will be beneficial for the investigation of e-voting systems.

關鍵詞(key word)：盲簽章(blind signature)、電子

投票(e-voting)、模糊簽章(oblivious signature)

一、緒論

隨著網際網路的快速發展，電子投票系統常常被學者們廣泛地討論及研究，慢慢地逐漸成為熱門的議題之一。電子投票系統就是一個模擬現實生活中公民投票過程的線上系統，其應考慮的安全性以及性質也必須符合現實中投票的實況。簡單來說，就是把現實生活中的公民投票電子化及線上化，以節省時間及大量的人力、物力，並讓公民能更簡單輕鬆的投票。

2005 年 8 月，愛沙尼亞國家正式實施一個完整的電子投票系統[12]，這是第一個全面採用電子投票系統的國家。針對應考慮到的安全性，他們設計出一套完善的系統，利用 ID-card 來儲存個人相關機密資料而後經由一連串的機制完成線上投票程序。從這個例子來看，電子投票系統在未來是可行的，當然相關的安全性必須要嚴密的探討。

在最近這幾年關於電子投票系統的研究中，很多都是以盲簽章(blind signature) [1]為基礎來建構，進而對於盲簽章的安全性來做探討以及加以改進。盲簽章的概念最早是由學者 D. Chaum [1]於 1982 年所提出，隨後並引起相當多的相關研究[3][4][11]。在盲簽章的協定中，通常有使用者、簽章者及驗證者三個角色，其運作過程大致如下：使用者將要簽章的訊息用盲因子（亂數）盲化後，送交給簽章者進行簽名。由於簽章者收到的是盲化過的訊息，所以無從得知訊息的實際內容，簽章者只是盲目地進行簽名的動作，然後將盲簽章送回給使用者。使用者收到盲簽章後，使用盲因子從中取出真正的簽章。而驗證者可以使用簽章者的公鑰(public key)驗證簽章的正確性。在電子投票的應用中，利用盲簽章的特性，使得簽章者無法得知投票者是將票投給哪位候選人，以達到隱密性的特性。之後更有學者提出將盲簽章結合代理簽章(proxy signature) [5]的新方法，提出了基於離散對數問題的代理盲簽章方法並應用在電子投票系統上[10]。代理盲簽章有幾點安全性質：分辨能力(Distinguish-ability)、不可否認性(Non-repudiation)、可驗證性(Verifiability)、不可偽造性(Unforgeability)、不可連結性(Unlinkability)。結合兩種簽名的優點改善盲簽名的缺點。

另一方面，L. Chen[2]於 1994 年提出了模糊簽章(oblivious signature)的概念，而由 R. Tso 等學者於 2008 年將模糊簽章的模型及安全性明確的定義了出來[7]。2008 年 12 月，C. Song 等學者提出了基於模糊簽章[6]的技術來實作電子投票系統。在這篇文章中提出了投票者有可能傳送一些使簽章者無法簽章的訊息來影響干擾整個投票。所以 C. Song 等學者提出了一個新的電子投票方法，它可以確保已簽章的選票中所留的訊息確實是 L 個候選人的其中一個。

基於模糊簽章來實作電子投票系統是很好的想法，但我們發現，在 C. Song 等學者的實作中可能會產生幾個問題。首先，任何人都有可能在開票前就可以先得知投票者將選票投給了誰，而失去了投票者應有的隱私性。另外，在開票階段時需投票者的參與(傳送之前加密用的密鑰)，因此降低了實用性並增加了投票者的負擔。因此，本研究將針對這些問題加以改善並分析其安全性，讓基於模糊簽章的電子投票系統更加完善。

關於本篇文章的章節：第二章介紹與本文章主題相關的技術。第三章介紹 C. Song 等學者所提出的方法以及需改善的問題所在。第四章詳細介紹我們改善的完整方法。第五章簡述安全性的分析。第六章針對我們的方法做一個結論。

二、相關技術

我們所提出的方法用到了兩個相關的技

術：模糊簽章[2]、C.P. Schnorr 認證方法[8]。我們將在這一章介紹這兩個相關的技術。

1. 模糊簽章：

模糊簽章是電子簽章的一種類型，是由 L. Chen[2]在 1994 年所提出的。完整的模糊簽章包括了三個成員：一個簽章者(a signer S)，一個接受者(a recipient R)及一個認證者(a verifier V)。模糊簽章的特性就是接受者可以在 L 個訊息中選擇一個訊息給簽章者簽名，而簽章者不知道 L 個簽章中何者為接受者所需要的，只能確定接受者所選的訊息確實在 L 個訊息中的其中一個。因此，使用這個方法可以保障使用者的隱私而又能保護簽名者不會簽到任何他不願意簽署的文件(註：盲簽章不具保護簽名者的功能)。

2008 年，R. Tso 等學者[7]認為先前的方法沒有很清楚的顯現出模糊簽章的正規化的概念，而且方法的架構對於通訊和計算方面缺乏效率，因此 R. Tso 等學者發表了一篇 1-out-of-n oblivious signatures 來改善這些問題，與先前的方法相比較更有效率。

2. Schnorr Identification：

Schnorr Identification Scheme[8]是 1991 年由 C.P. Schnorr 所發表的一個基於離散對數問題的認證方法。這個方法需要一個可信賴的機構，Trusted Authority (TA)， 來選擇系統所需要的參數，其參數如下：p，q 是很大的質數其中 $q \mid p-1$，$q \geq 2^{140}, p \geq 2^{512}$，$\alpha \in_R Z_p^*$ 序(order)為 q。*TA* 的簽章及驗證演算法分別為 $Sign_{TA}$，Ver_{TA}。這個驗證方法的流程如下所示：

(1) *A* 選擇一個祕密的值 $a \in_R Z_p^*$，計算相對應的公鑰 $v = \alpha^{-a} (\bmod p)$，接著傳送 (ID, v) 給 *TA*，其中 *ID* 為 *A* 的認證字串訊息。

(2) *TA* 驗證 *A* 的身份後，對 (ID, v) 簽章 $s = Sign_{TA}(v)$，接著回傳 $C(A) = (v, s)$ 給 *A*。

(3) *A* 挑選一個亂數 $k \in_R Z_p^*$，接著計算 $\gamma = \alpha^k (\bmod p)$ 然後傳送 $(C(A), \gamma)$ 給驗證者 *B*。

(4) *B* 藉由驗證 *TA* 的簽章來驗證 $C(A)$ 確實由 *TA* 簽署。驗證成功之後 *B* 傳送一個亂數 $r(1 \leq r \leq 2^t)$ 給 *A*，t 為一秘密參數。

(5) *A* 則傳送 $y = (k + ar) \bmod q$ 給 *B*。

(6) *B* 去驗證 $\gamma \equiv \alpha^v v^r \bmod p$，如果等式成立則接受 *A* 的身份證明。

Schnorr Identification Scheme 不管是在計算量或是訊息量來看，其優點是速度快且有效率。

3. 電子投票系統的安全性需求及考量：

電子投票系統的安全性跟現實中投票系統幾本上需求及考量是一樣的，其中包含：

(1) 投票資格(Eligibility)：只有具有投票資格者才能進行投票。

(2) 不可重複性(Non-reusability)：一個有資格投票的投票者只能投票一次。

(3) 合理性(Soundness)：沒有人可以改變其他人的選票。

(4) 完整性(Completeness)：每個投票者都可以確認自己的選票有被計數。

(5) 認證性(Verifiability)：沒有人可以竄改投票後的結果。

(6) 公平性(Fairness)：沒有人可以得知任何與投票內容相關的資訊，直到最後公開時才能得知。

(7) 隱私性(Privacy)：沒有人可以確定誰投給誰，每個人對於自己所投的票都有隱私性，除非自己告訴別人，否則其他人應無法得知。

以上是一般投票系統應符合的幾點考量。

三、相關研究

這一章節我們將簡單介紹一下 C. Song 等學者所提出的方法[6]以及我們認為可以改進的部分。

首先，他們定義了四個角色：

(1) Trusted Center(*TC*)：用來驗證投票者的資格。

(2) Certification Authority(*CA*)：確認投票者的資格，並負責對選票簽章，負責所有的投票相關事項。

(3) Voting Center(*VC*)：負責收集所有選票，計算票數，並公布選舉的結果。

(4) Voter(*V*)：具有投票資格的投票者。

此外，定義了一個公佈欄可以公佈相關資訊。在[6]的方法裡，*TC* 公佈所有取得認證的投票者的 pseudo-name 在公佈欄上，*CA* 公佈它的公鑰，*VC* 則公佈選票以及投票最後的結果。沒有任何一個機構能消除在公佈欄上的任何資訊。

他們的方法總共有五個步驟：Preparation phase, Registration phase, Voting phase, Ballot casting phase, Tally phase。以下是每個步驟詳細的流程：

1. Preparation phase：

這個步驟首先定義參數，p，q 是很大的質數其中 $q|p-1$，$q \geq 2^{140}, p \geq 2^{512}$，$\alpha \in_R Z_p^*$ 序為 q，g, h 兩個元件屬於 Z_p^* 與 α 有相同序。$H:\{0,1\}^* \to Z_q^*$，$f:\{0,1\}^* \to Z_q^*$ 這兩個為 one way hash functions。

CA 選擇一個亂數 $x \in_R Z_q^*$，計算出投票系統的公鑰 $y = g^x \bmod p$ 然後公告給投票者。*CA* 也將 L 個候選人的列表公佈 $\{CAN_1, CAN_2, ..., CAN_L\}$。所有參與者在此階段公佈他們的公鑰在公佈欄上。

2. Registration phase：

想加入投票系統的投票者必須先向 *TC* 註冊，具有投票資格的人才能參與投票。

首先投票者 *V* 選擇 $a \in_R Z_p^*$，計算相對應的公鑰 $v = \alpha^{-a} (\bmod p)$，然後 *V* 將(*ID*,*v*)傳送給 *TC*，其中 *ID* 為 *V* 的認證字串，*v* 為 *V* 的 pseudo-name。

TC 收到訊息後驗證 *V* 的身份及投票資格，如果 *V* 具有投票資格則 *TC* 對 *v* 簽章 $s = Sign_{TC}(v)$，然後回傳認證 $C(V) = (v, s)$ 給 *V*。*TC* 將所有獲得認證的投票者的 pseudo-name 公佈到公佈欄上。

3. Voting phase：

在這個階段中，假設投票者想得到 *CA* 對於訊息 $CAN_j \in \{CAN_1, CAN_2..., CAN_j\}$ 所簽的模糊簽章。

步驟 1：

V 由 *L* 個候選人中選擇心中所屬的候選人，假設選擇了第 j 個候選人 CAN_j，然後他計算出 $c = g^r h^j \bmod p$，$r \in Z_q^*$ 為 *V* 所選的一個亂數。接著將 $(c, C(V))$ 傳送給 *CA*，*CA* 利用 Schnorr identification 方法認證 *V* 的身份，假如是具資格的投票者，則 CA 選擇一亂數 $k_i \in_R Z_q^* (1 \leq i \leq L)$，$K_i = g^{k_i} \bmod p$，$\hat{e}_i = H(CAN_i, K_i c/(gh)^i \bmod p)$，$\hat{s}_i = k_i - x\hat{e}_i \bmod q$，接著傳送 $(\hat{e}_i, \hat{s}_i)$ $(1 \leq i \leq L)$ 給投票者 *V*，並將 $C(V)$存進資料庫。

步驟 2：

V 計算 $\delta_i = g^{(r-i)} h^{(j-i)} \bmod p (1 \leq i \leq L)$，如果 $\hat{e}_i = (CAN_i, g^{\hat{s}_i} y^{\hat{e}_i} \delta_i \bmod p)$，則 *V* 得到了模糊簽章。接著 *V* 計算 $e = \hat{e}_j$，$s = r - j + \hat{s}_j \bmod q$，則 CAN_j 的簽章為 $\sigma = (e, s)$。

4. Ballot casting phase：

投票階段將持續到投票截止。

步驟 1：

V 計算 $CAN' = f(CAN_j, \beta)$，f 為一個使用亂數金鑰 β 的 secure bit-commitment 方法。然後 V 將 (σ, CAN') 傳送給 VC。

步驟 2：

VC 收到 V 傳送的資料後，檢查 σ 是否存在資料庫內，如果沒有則 VC 將 σ 存進資料庫中並且將 (t, σ, CAN') 公佈到公佈欄上，t 為一序列數字；如果 σ 存在於資料庫中，則將訊息丟棄。

5. Tally phase：

當投票截止後即進入計票階段。

步驟 1：

V 檢查他的選票是否在名單內，如果沒有則重新傳送 (σ, CAN') 給 VC。

步驟 2：

V 將金鑰 β 和序列數 t 經由匿名通道傳送給 VC。

步驟 3：

VC 將 $CAN' = f(CAN_j, \beta)$ 解開得到 CAN_j，然後 VC 檢查在選票 CAN_j 上 CA 的簽章，只有在 $e = H(CAN_j, g^s y^e \bmod p)$ 成立時 VC 才能確定是合法簽章。VC 將 $(t, \sigma, CAN', CAN_j, \beta)$ 公佈到公佈欄上。

步驟 4：

VC 開始計票並將投票結果公佈。

以上就是 C. Song 等學者於[6]中所提出完整的方法，但我們經過仔細研讀後，發現其方法有兩點可以改進的地方，如下所述：

1. 投票者的負擔：

這個方法在最後 Tally phase 時，投票中心 VC 還是需要投票者 V 透過匿名通道傳送金鑰 β，如此 VC 才能夠解出 V 所投的候選人結果。本來投票者 V 投完票後，只需要等待開票結果就好，但是因為這道程序，使得投票者在投票結束後還必須多做一件事情（在開票時），否則自己的票將無法被正確的計數。這無形中增加了投票者的負擔。

2. 可預測性：

在 Voting phase 中，任何一張有效的投票都會得到 CA 對訊息 $CAN_j \in \{CAN_1, CAN_2, ..., CAN_j\}$ 所簽的模糊簽章 $\sigma = (e, s)$。然後在 Ballot casting phase 中，投票者會將 σ 傳送給 VC。但為保障投票的公正性，此簽章 σ 的正確性應在 Tally phase，也就是記票階段才可被驗證。簽章的正確性是透過計算 e 是否等於 $H(CAN_j, g^s y^e \bmod p)$ 的值來驗證。然而，任何攻擊者其實在開票之前，就可事先知道每張有效票的投票的結果。因為 g, y, p 是公開的，而 e, s 攻擊者可以經由 Ballot casting phase 的步驟 2 擷取獲得 $\sigma = (e, s)$，所以驗證方程式只剩下 CAN_j 無法得知，但是因為候選人是有限個，因此攻擊者可以透過暴力攻擊法一個一個代入測試得知選票是投給哪位候選人，進而取得投票最後的結果，達到投票結果的可預測性。

3. 以上兩點是我們的方法所要改進的部份。

四、我們的改進方法

我們針對第三章所列出的問題提出了改進的方法，以下將詳細介紹我們所提出的方法。

我們的方法與 C. Song 等學者提出的方法一樣有五個步驟：Preparation phase, Registration phase, Voting phase, Ballot casting phase, Tally phase。

1. Preparation phase：

這一階段與 C. Song 等學者提出的相同，唯一不同的地方就是 *CA* 另外多選擇一個亂數 $x_{VC} \in_R Z_q^*$ 作為私鑰，其對應的公鑰為 $y_{VC} = g^{x_{VC}} \bmod p$， 並將此公鑰一併公開。

2. Registration phase：

與 C. Song 等學者提出的步驟相同。

3. Voting phase

與 C. Song 等學者提出的步驟相同。最後 *CA* 將投票者 *V* 的認證 C(*V*)存進資料庫中，而投票者 *V* 得到了對於 CAN_j 的簽章 $\sigma = (e, s)$。

4. Ballot casting phase：

在這個階段中，共有兩個步驟來完成投票者 *V* 將選票送至 *VC*。

步驟 1：

投票者 *V* 將 $(\sigma \| CAN_j)$ 利用先前 *CA* 所公開的金鑰 y_{VC} 透過非對稱式公開金鑰加密系統加密得到一密文 C_V。此步驟取代了 C. Song 等學者所提出的方法利用 bit-commitment 方法來加密，使得投票者 *V* 無需再傳送 key β 至 *VC*，減少了投票者 *V* 的負擔。

步驟 2：

V 將(C(*V*), C_V)傳送至 *VC*，就算攻擊者攔截到此訊息也無法得知 σ 而事先得知投票結果。*VC* 檢查 C(*V*)是否已存在資料庫中，如果沒有則將 C(*V*)存入，並且將 $(t, C(V), C_V)$ 公佈到公佈欄上，*t* 為一序列數字； 如果 C(*V*)已存在資料庫中，則將訊息丟棄。投票者 *V* 檢查他的選票是否有在列表上，如果沒有則再次傳送(C(*V*), C_V)給 *VC*。

5. Tally phase：

當投票時間結束，*VC* 準備開始計票。

步驟 1：

CA 將解密用私鑰 x_{VC} 傳給 *VC*。

步驟 2：

VC 利用 x_{VC} 將密文 C_V 解開得到 $(\sigma \| CAN_j)$，然後 *VC* 檢查 *CA* 對於選票 CAN_j 上的簽章，只有 在 $e = H(CAN_j, g^s y^e \bmod p)$ 成立 *VC* 才能確定是合法簽章。*VC* 將 $(t, C(V), C_V, CAN_j, y_{VC})$ 公佈於公佈欄上，以便讓所有人可以驗證。

步驟 3：

VC 計算候選人的得票數並且將結果公佈。

五、安全性分析

針對第二章第三點的電子投票系統的安全性分析與考量，以下對於我們改進的方法做分析。

投票資格(Eligibility)：在投票開始之前，投票者必須透過 TC 申請註冊，只有合法的投票者才能得到認證，具有投票資格。

不可重複性(Non-reusability)：當投票者 *V* 想得到 *CA* 的簽章必須經過 *V* 提供的身份驗證才能得到。所有的 C(*V*)都會被儲存於資料庫中，如果投票者 *V* 想投兩次以上則必須再次傳送 C(*V*)給 *VC*，而 *VC* 會檢查資料庫中是否存在相同的 C(*V*)，如果有則丟棄。因此避免重複一直投票的情況。

合理性(Soundness)：因為所有選票都是公開在公佈欄上，如果 *CA* 的簽章不是合法的簽章，則選票會被認為是無效的選票，也不會公佈在公佈欄上，因此就不會被記數。

完整性(Completeness)：投票結束後，*VC* 將 $(t, C(V), C_V, CAN_j, y_{VC})$ 公佈以利於所有人都可以驗證最後的結果，避免選票記數錯誤。

認證性(Verifiability)：由於最後的選票以及證明的訊息都伴隨著投票者 *V* 的資訊，所有選票都可

以被驗證，最後的投票結果也可以被驗證，達到可驗證性。

公平性(Fairness)：任何參與者都無法在投票結束開始計票之前得知任何有關投票者的選票的訊息。

隱私性(Privacy)：當選票利用 y_{VC} 加密傳送後，由於離散對數問題，任何人都無法解密得到訊息在投票結束之前，除了 *CA*。在我們的方法中，我們假設 *TC*，*CA* 及 *VC* 皆是獨立可信任的機構，但皆隸屬於中央選舉委員會，所以私鑰的傳送可以在 offline 中執行，例如，將私鑰存在 CD 並密封，開票時再將 CD 送至 *VC*。另外，因為皆為可信任的機構，所以我們假設三者之間沒有任何不法的密謀。實務上可利用立法及政策上的執行來達到。另外，技術上可利用秘密分享機制(Secret Sharing Schemes)[9]來增加密謀的困難度。如此，我們提出的電子投票系統具有隱私性。

六、結論

在這篇文章中，我們針對 C. Song 等學者所提出的方法，提出可以改進的部分，然後利用新的方法加以改善，減少投票者的負擔，也解決攻擊者可事先得知投票結果的問題，使得基於模糊簽章的電子投票系統更加完善。雖然使用公開金鑰加密方法來改善 C. Song 等學者的方法可能造成在系統成本方面會比 C. Song 等學者的方法來的多，但是以成本換取使用者的便利相信應該是等價的交易。未來的工作可更深入的探討其安全性、可行性以及針對可能的攻擊類型加以討論並提供更全面的描述，此外也必須去分析計算系統的成本，使得基於模糊簽章的電子投票系統更加嚴謹。

七、參考文獻

[1] D. Chaum. *Blind signatures for Untraceable Payments*. Advances in Cryptology-Crypto'82. Plenum Press, 1983, pp:199-203.

[2] L. Chen. *Oblivious signatures*. IN: Gollmann, D.(ed.) ESORICS 1994.LNCS 875. Springer. Heidelber, 1994, pp:161-172.

[3] J. Kim, K. Kim, and C. Lee. *An Efficient and Provably Secure Threshold Blind Signature*, ICICS2001, LNCS 2288, 2001, pp318-327, springer-verlag, Berlin Heidelberg.

[4] X. Lin, R. Lu, H. Zhu, P. Ho and X. Sherman. *Provably Secure Self-certified Partially Blind Signature Scheme from Bilinear Pairings*, ICC2008, 2008, pp 1530-1535.

[5] M. Mambo, K. Usuda, and E. Okamot. *Proxy signature: delegation of the power to sign messages*. IEICE Trans. Fundamentals, Vol. E79-A, NO.9, 1996, pp 1338-1353.

[6] C. Song, X. Yin, Y. Liu. *A Practical Electronic Voting Protocol Based upon Oblivious Signature Scheme*. CIS.2008, IEEE, 2008, pp. 381-384

[7] R. Tso, T. Okamoto and E. Okamoto. *1-out-of-n oblivious signatures*. In Proceedings of the 4th Information Security Practice and Experience Conference (ISPEC2008), Springer, Lecture Notes in Computer Science, Vol. 4991, 2008, pp:45-55.

[8] C.P. Schnorr . *Efficient signature generation for smart cards*. Journal of Cryptology, 1991,4(3). pp: 161- 174.

[9] A. Shamir. *How to Share a Secret*. Communications of ACM, vol.22, no.11, 1979, pp.612-613.

[10] S. Wang, H. Fan, G. Cui. *A proxy blind signature schemes based DLP and applying in e-voting*. ICEC '05, ACM, 2005, pp. 641-645.

[11] B-Y. Wang, F. Yang, Y-F. Hu. *Online Voting Scheme Based on Blind Digital Signature*. MINIMICRO SYSTEM, 2002(3), pp:588-591.

[12] http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf