有關 Song 和 Cui 的電子投票機制匿名性之探討
On the Anonymity of Song and Cui's Electronic Voting Scheme

謝濱燦
德明財經科技大學
Bin-Can Xie
Takming University of Science and Technology
Email: bintsan@mail.takming.edu.tw

羅子惟
德明財經科技大學
Zi-Wei Luo
Takming University of Science and Technology
Email: dowdow1201@gmail.com

摘　要

近來 F. Song 和 Z. Cui 提出了一個新的電子投票機制，它是採用 RSA 數位簽章和 ElGamal 盲簽章來建構，雖然這已滿足了電子投票系統八個特性中的七個，但卻未達到匿名性的要求，因此本篇論文主要是回顧 F. Song 和 Z. Cui 所提出的電子投票機制，針對其方法進行安全性分析，最後我們指出其所提出的電子投票機制是不具匿名性的。

關鍵詞：電子投票、RSA、ElGamal、盲簽章。

Abstract

Recently, F. Song and Z. Cui proposed a new e-voting scheme in which the RSA and ElGamal signature schemes are employed. It possessed several security properties of a secure e-voting scheme but the anonymity. In this paper, we first review F. song and Z. Cui's e-voting scheme and give the security analysis. Finally, we pointed out that it does not have the anonymity with their election voting scheme.

Keywords：Election Voting、RSA、ElGamal、Blind Signature。

一、緒論

歷史上剛開始有投票行為時，即是使用球來當作選票(Ballot)，這個詞也就是來自於義大利語的球(Ball)，候選人有其專屬的容器，當所有選民將球放入心儀的容器後，就能統計總數，也就會產生選舉結果。從前的選票除了球以外也有黏土或鐵片等特殊的方式，隨著時代的持續之進化，紙本選票也就逐漸應用在選舉上[3][3] 。

電子投票發展至今，大致能分成兩大類，分別是E-voting(Electronic-voting)、I-voting(Internet-voting)。以E-voting來說，選民必須要親自到投票所投下神聖的一票，而這方式是利用投票所內之電腦設備，以觸控式螢幕或是用按鍵的方式來進行投票的行為，當投票時間終止後，即可利用投票機來統計總得票數。而I-voting則是選民必須利用網際網路來來進行投票的行為，其又可分為在投票所內和在任何地方。而它的投票流程如下：

(1) 選民要先在投票委員會幫自己認證。
(2) 選民填好選票之內容後，將選票放入一個內部信封。
(3) 這個內部信封之後被放入另一個填好選民資料的信封。
(4) 這個信封會被寄到選民的當地投票站，接著選民之資格就會被驗證，假使選民是符合資格，那外部信封就會被打開，而匿名之內部信封則被放進票箱內。

現今的選舉投票方式，普遍來說，以紙本選票的投票方式最為盛行，但傳統的投票不僅必須要消耗可觀的金錢，人力的投入也不在話下，當然計票結果的公佈亦是相當之緩慢。有鑑於此，安全電子投票系統的設計如火如荼的發展中。一般而言，一個可靠的電子投票系統必須滿足以下八個特性：合法性、完整性、匿名性、不可重複性、公平性、可證實性、強固性和可行性。一個完善的系統不僅要能夠大幅提高比現今的傳統投票方式更為準確的計票結果，又必須要大大縮短原本冗長的計票時間。不過在一些較為重要或不允許出錯的場合中，大部份民眾對於電子投票系統仍然是抱持著存疑之立場。

二、文獻回顧

以下分成五小節來回顧，第一節是回顧 RSA，第二節是回顧 RSA 之盲簽，第三節是回顧 ElGamal，第四節是回顧 ElGamal 盲簽，第五節是回顧 F. Song, Z. Cui 模型。

2.1. RSA

在 1977 年 5 月由 Ronald Rivest, Adi Shamir, Leonard Adleman 所共同提出[2]。RSA 是一種非對稱式密碼系統，它利用公開鑰匙作為加密，只有使用正確的私密鑰匙才能夠解密，所以解密者如果不去洩露私密鑰匙，其餘有心人士就算擁有公開鑰匙，也是很難去推演出私密鑰匙的。而它

的安全性建立在分解二個大質數上的數學問題，它是一種觀念簡單，但安全性卻相當高的一種公開金鑰密碼系統。

RSA 加密解密過程

UserA 將明文 m 加密成密文 c 傳給 UserB，UserB 則將密文 c 解密為明文 m [4][5]。

(1) UserB先挑2個大質數 p 和 q ，接著計算出 $n = p*q$ 。

(2) UserB算出 $\phi(n) = (p-1)*(q-1)$ ，找出一個正整數，使 e 滿足和 $\phi(n)$ 互質。

(3) UserB將 (n, e) 公開，也就是公開金鑰。

(4) UserA將明文 m 加密為密文 $c = m^e \pmod n$ 。

(5) UserB計算出 e 在 $\bmod \phi(n)$ 下之乘法反元素，也就是 $e*d \equiv 1 \pmod{\phi(n)}$ 。

這時 D 為私密鑰匙。UserB 將密文 c 透過解密的式子 $m \equiv c^d \pmod n$ 還原為明文 m 。

RSA 數位簽章過程

(1) UserB利用私密金鑰 d 將明文 m 簽名為 $s \equiv m^d \pmod n$ 。

(2) UserB將 s 傳回給UserA，UserA利用公開鑰匙 (n, e) ，計算 $s^e \bmod n$ 和 n ，比較兩者，若是相同，則為合法簽章，反之，即為不合法。

2.2. RSA 盲簽

在1982年由David Chaum所提出的第一個盲簽章，而他是利用RSA演算法。如果滿足下列兩項條件才能稱的上是盲簽章：

(1) 簽名者對所簽的文件一定要是無法得知其內容的。

(2) 簽名者無法從日後公佈之數位簽章和文件找出兩者之關聯性。

RSA 盲簽章過程

UserA想將明文 m 給UserB簽名，但又不想讓UserB知道明文 m 之內容。

(1) UserA 任選一個整數 k ，使 k 滿足 $\gcd(k, n) = 1$ ，接著計算 $t \equiv k^e * m \pmod n$ ，最後將 t 送給UserB。

(2) UserB 把 t 簽名成 $\tilde{s} \equiv t^d \pmod n$ ，將 $\tilde{s}$ 傳回給 UserA。

(3) UserA 計算 $s = \tilde{s} * k^{-1} \pmod n$ 即得 UserB 對 m 的數位簽章 $s \equiv m^d \pmod n$ 。

2.3. ElGaml

在1985年由T. ElGamal提出。其安全性是基於解離散對數之困難度[6]。

ElGamal加密解密

UserA將明文 m 加密成密文 c 傳給UserB，UserB則將密文 c 解密為明文 m [7]。

(1) UserB必須先選擇一個大質數 p ，並取得 g 的order為 g 的生成子(generator)。

(2) UserB再任意挑選 $x < p-1$ ，x 即私密金鑰。

(3) UserB計算公開金鑰 $y = g^x \bmod p$ ，這時 (y, g, p) 就是公開金鑰。

(4) UserA選擇每次不同的亂數 $0 \le k \le p-1$ ，並計算 $c_1 = g^k \bmod p$ ， $c_2 = y^k * m \bmod p$ ，這時 (c_1, c_2) 即是密文 c 。

(5) UserB利用自己的私密金鑰和數學式 $(m = c_2 c_1^{-x} \bmod p)$ 解密得到明文 m 。

ElGamal數位簽章

$h(\bullet)$ = 雜湊函數

(1) UserB任意挑選一整數 k ，並滿足 k 和 $\phi(p)$ 互質。

(2) UserB 計算 $r = g^k \bmod p$ 以及簽章 $s^* = k^{-1}(h(m) - g*r) \bmod \phi(p)$ 。

(3) UserB將數位簽章 $s = (m, r, s^*)$ 傳給UserA。

(4) UserA收到數位簽 s ，接著利用UserB的公開金鑰 (y, g, p) 計算 $v_1 = y^r * r^{S^*} \bmod p$ 和 $v_2 = g^{h(m)} \bmod p$ ，比較兩者，若是相同，則為合法簽章，反之，即為不合法。

2.4. ElGamal盲簽章過程

p = 大質數； g = order 為 g 的生成子(generator)； UserB 私密金鑰 x ； UserB 公開金鑰 $y = g^x \bmod p$

(1) UserA 任意挑個 h 並計算 $\beta = g^h \bmod p$ 和 $m' = m^h \bmod (p-1)$

(2) UserA 傳 (β, m') 給 UserB

(3) UserB 任意挑個 k 並計算 $\gamma = \beta^k \bmod p$ 和 $s = x\gamma + m'k \bmod (p-1)$

(4) UserB 傳 (γ, s) 給 UserA

(5) UserA 驗證 $g^s = \gamma^m y^\gamma \bmod p$ 如果成立的話，簽名即是合法。

2.5. F. Song, Z. Cui模型

F. Song, Z. Cui模型[1]是由六個階段組成，首先第一階段為產生金鑰，VoterB先產生金鑰，第二階段為確認身分，CenterA確認VoterB的身分，第三階段為將票盲化，CenterA將票盲化後，傳給VoterB，第四階段為投票階段，第五階段為計票階段。

產生金鑰

(1) 任意選擇兩個大質數 p 和 q

(2) 計算 $n = p*q$

(3) 計算 $\phi = (p-1)*(q-1)$

(4) 挑選 e (滿足 $1 < e < \phi$ 且和 ϕ 互質)

(5) 計算 $e*x \equiv 1 (\mathrm{mod}\ \phi)$

因此 VoterB 的公開金鑰 $y = (e, n, ID)$;私密金鑰＝x。

確認身分

VoterB 向 CenterA 申請投票資格之數位簽章，CenterA 確認 VoterB 身分後，發給 VoterB 包含 VoterB 的公開金鑰和 CenterA 簽過之數位簽章。

將票盲化

(1) CenterA 產生任意數 e

(2) 利用 VoterB 公鑰 y 計算 $\beta = \alpha^{h} \bmod p$

(3) 計算 $m' = m^{e} \bmod (p-1)$

(4) 利用DrawerD公鑰計算 $\beta_D = \alpha^{h} \bmod p_D$

(5) 將 m' 置入XML文件檔，以下為XML格式

```
<Signature>
<SignedInfo>
<CanonicalizationMethod/>
  <SignatureMethod/>
        <Reference(URI=?)>
              <Transforms/>
              <DigestMethod/>
              <DigestValue/>
              </Reference>
  </SignedInfo>
  <SignatureValue/>
<KeyInfo/>
<Object/>
</Signature>
```

(6) CenterA傳XML文件檔給VoterB

投票階段

VoterB將公鑰y和投票內容利用XML文件檔傳至CenterA。

計票階段

(1) 驗證票的有效性

(2) 驗證票是否有被串改

(3) 驗證簽章

如果皆符合，則計算票。

監票

多個監票員，以確保有至少有一個監票工作時間，和每一張選票將被正確計算。

三、分析

普遍來說，一個可靠的電子投票系統必須滿足以下八個特性：

(1) 合法性(Legitimacy)：只有同時具備投票之資格和經過合法之認證的選民，才能夠參與投票。

(2) 完整性(Completeness)：在整個選舉之過程中，選票不可以被更改其內容、刪除和複製，也必須能夠證實選票計算正確。

(3) 匿名性(Anonymity)：除了選民自己，任何人都不能透過任何之方法聯想選票之內容，亦或是得知投票者身分。

(4) 不可重複性(Non-repeatability)：任何合法的選民都只能一人一票，決不允許有重複投票之情況發生。

(5) 公平性(Impartiality)：在投票階段結束之前，不能公開任何有關當前得票數之資訊，以免影響選民之決定。

(6) 可證實性(Verifiability)：任何人都能檢驗最後的投票結果是否正確，以證實這是合法且有效的。

(7) 強固性(Robustness)：就算遭遇任何惡意之攻擊，皆不能中斷系統的運行，以避免影響投票之進行。

(8) 可行性(Feasibility)：安裝和配置皆可接受的金錢與時間，而且選民不需要額外之技能和裝備。

匿名性分析

(1) 驗證票的正確性 $\alpha^{s} = \gamma^{m} y^{\gamma} \bmod p$

(2) 驗證票是誰投的，如果 $s_v^{e} = m_v$ 成立，則這張票即是 A 投的。

$$m = (m_v, \mathrm{RSA}(m_v))$$

$$s_v = m_v^{d} \bmod n$$

$$m = (m_v, s_v)$$

四、評論

一個完善的電子投票系統能夠大幅提高比現今的傳統投票方式更為準確的計票結果，又可以大大縮短原本冗長的計票時間。不過在一些較為

重要或不允許出錯的場合中，大部份民眾對於電子投票系統仍然是抱持著反對之立場。因此建立出一個可以提升大眾信心的電子投票系統是很重要的。最近 F. Song, Z. Cui 提出一個電子投票系統，而本論文即是提出 F. Song, Z. Cui 電子投票系統是不具匿名性的。雖然這系統符合了以上分析的七個特性，但卻未達到匿名性的要求，因為在驗證階段就能透過 $s_v^e = m_v$ 的成立，而得知票是誰投的，所以是不具匿名性的。

參考文獻

[1] F. Song, Z. Cui, "Electronic Voting Scheme About ElGamal Blind-signatures Based on XML," *Procedia Engineering*, 2012, 29, pp. 2721–2725.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *communication of the ACM*, where 1978, vo1. 21, No. 2.

[3] 王淳, "NCKU 電子投票系統之安全性分析," *碩士論文*

[4] 楊宗偉, "密碼學的發展與應用," *碩士論文*

[5] 陳嘉耀, "高效RSA 密碼系統解密方法及實作," *碩士論文*

[6] 陳震寰, "基於RSA與ElGamal簽署之新盲簽章," *碩士論文*

[7] 賴滄本, "基於離散對數難題之新盲簽章," *碩士論文*