相互認證電子支票系統之改善

楊伏夷
朝陽科技大學資訊工程系
yangfy@cyut.edu.tw

黃建誌
朝陽科技大學資訊工程系
s9927625@cyut.edu.tw

摘要

近年來，在電子商務的應用上，電子支票是很重要的一部分，它能提供付款時間及付款金額的便利。在本篇文章中，回顧 Chang 等人利用盲簽章和 RSA 加密技術去結合線上的電子支票，但是經由我們的分析，Chang 等人的協定無法提供相互認證。因此，本篇文章提出一個新的方法來改善 Chang 等人協定的弱點。

關鍵詞：電子商務、電子支票、盲簽章、RSA 、相互認證。

Abstract

Recently, the electronic check (E-check) is an important application on electronic commerce. It can provide convenience on the time of payment and the amount of payment. In this paper, we review Chang et al.'s protocol, which is the on-line e-check using blind signature and RSA encryption. Unfortunately, their scheme can't provide with the mutual authentication. Therefore, this paper proposes a novel method to improve the weaknesses of Chang et al.'s scheme.

Keywords: E-Commerce, E-check, blind signature, RSA, mutual authentication

1. 前言

隨著資訊科技與網路技術的蓬勃成長，電子商務的應用越來越普遍於現實生活中。在最近幾年內，電子商務[1]技術結合網路可以應用在不同的系統上。例如在電子付費系統中，應用的層面包含了線上信用卡付費[7]、 電子現金[6]、電子支票[2]等。線上信用卡付費具有便利與省時，大部分線上信用卡付費運用在旅行、購物等用途，但由於信用卡金額的限制，以致於消費者無法支付龐大金額的交易。電子現金具有匿名與低成本的特性，適合用於小額付款的電子商務上，但由於電子現金不包含個人的資訊，因此任何一人只要撿到遺失的電子現金情況下，仍然可以使用電子現金。

近年來，在電子商務的應用上，電子支票是很重要的一部分，它能透過網路遠端交易，提供付款時間及付款金額的便利，是個典型的電子付費系統。在典型電子付費系統中包含著三個參與者，可信賴的銀行、付款人以及收款人。假如付款人想要使用電子支票系統，首先，付款人必須先向銀行註冊，接著銀行發行電子支票給付款人，付款人透過網路方式使用電子支票進行線上交易。

數位簽章[11,12,13,14]技術在文件交換、電子商務等各方面的用途日益增加，需求也愈來愈迫切。數位簽章技術分成兩種：RSA [8]和 ElGamal，RSA 是建立在解因式分解的數學難題上來保障簽章的安全性；ElGamal 則是基於解離散對數的困難來保障其安全性。基於這兩種方法，許多密碼學者衍生出不同種類的數位簽章技術，例如盲簽章[9,10]、代理簽章等；在本篇文章中，加入盲簽章的技術，利用盲簽章不可追蹤的特性，防止簽章者日後發現盲簽章訊息，因而察覺出簽章請求者的身份。

在 1989 年，Chaum 提出一個有效率離線電子支票協定[4]。在 Chaum 協定裡，無法從交易過程中決定買方電子支票的金額以及立即驗證賣方的身份。在 2005 年，Chen 提出一個有效率線上電子支票協定[5]，改善了上述協定的弱點。在 2009 年，Chang 等人指出 Chen 的協定並不能有效提供重要電子支票系統，因此提出一個線上電子支票相互認證協定[3]，有效改善上述協定的弱點，並提供付款人和收款人雙方交易的相互認證。本篇指出在 Chang 等人協定裡，並不能有效提供相互認證，付款人可以自行偽造出盲簽章通過收款人的驗證和銀行的驗證，因此本篇提出一個新的方法有效改善上述協定的弱點。

本篇文章架構如下。首先，第二節先回顧 Chang 和 Lee 等人的協定，第三節提出 Chang 和 Lee 等人的協定未必提供相互認證，第四節描述本篇提出的協定，第五節描述本協定的安全分析，最後是結論。

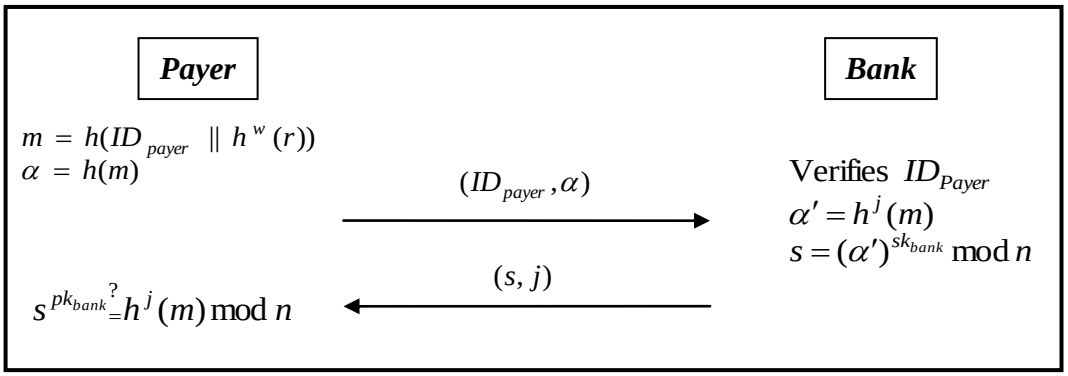

圖 1. 線上電子支票相互認證協定註冊階段

2. 回顧 Chang 和 Lee 等人的協定

在本章節，我們先回顧Chang和Lee等人的線上電子支票相互認證協定，註冊階段與付費階段。如圖1和圖2。接著說明本協定的參數設置，以及詳細敘述註冊階段和付費階段。

本協定的參數設置：

p, q:兩個隨機大質數。

n:一個合成數，滿足 $n=p\cdot q$。

w:電子支票最大面額值。

j:電子支票簿可使用次數。

a:交易的面額。

$h(\cdot)$:單向雜湊函數。

T:時戳。

$\|$:訊息串接符號。

$\oplus$:互斥或閘運算符號。

$\stackrel{?}{=}$:判斷符號。

ck:付款人和銀行之間的密鑰。

$E_x(\cdot)$:對稱加密。

$\stackrel{?}{\leq}$:判斷小於等於符號。

i:電子支票簿已使用次數。

2.1 註冊階段：

首先，客戶先向銀行申請電子支票簿，申請流程描述如下。

(1)付款人隨機選擇一個安全整數 r，並且計算 m,α，計算式如下：

$m = h(ID_{payer} \| h^w(r)),\ \alpha = h(m)$

付款人把身份 ID_{payer} 及保護的訊息 α 傳送給銀行。

(2)銀行接收到付款人身份和訊息後，首先確認付款人身份 ID_{payer}，並且計算 α', s，計算式如下：

$\alpha' = h^j(m)$，$s = (\alpha')^{sk_{bank}} \bmod n$ 銀行傳送簽章 s 及電子支票簿可使用次數 j 回傳給付款人。

(3)付款人接收到簽章和電子支票簿可使用次數後，付款人使用銀行公開金鑰驗證簽章 $s^{pk_{bank}} \stackrel{?}{=} h^j(m)$ 是否正確。設若正確，則付款人存入 m,s,j 到電子支票簿。

2.2 付費階段：

買家使用電子支票跟賣家購買商品，交易流程描述如下。

(1)首先，付款人隨機選擇兩個整數 R 和 b，並計算 k，計算式如下：

$k = R^{pk_{payee}} \cdot b \bmod n'$

付款人把訊息 k 傳送給收款人。

(2)收款人接收到訊息後，收款人對訊息作盲化，並計算 k'，計算式如下：

$k' = (k)^{sk_{payee}} = R \cdot b^{sk_{payee}} \bmod n'$

收款人把盲簽章 k' 回傳給付款人。

(3)付款人接收到盲簽章後，付款人將盲簽章作解盲化取得訊息，並計算 M, C_1, C_2，計算式如下：

$M = k' \cdot R^{-1} = b^{sk_{payee}} \bmod n'$

$C_1 = h^{w-a}(r) \oplus M$

$C_2 = E_{ck}(i \| T)$

付款人利用收款人的公開金鑰對訊息作驗證 $b \stackrel{?}{=} M^{pk_{payee}} \bmod n'$ 是否正確。設若正確，付款人將 $ID_{payer}, ID_{payee}, a, b, j, s, C_1, C_2, T$ 傳送給收款人，否則終止交易。

(4)收款人收到 $ID_{payer}, ID_{payee}, a, b, j, s, C_1, C_2, T$ 後，收款人使用銀行的公開金鑰驗證簽章

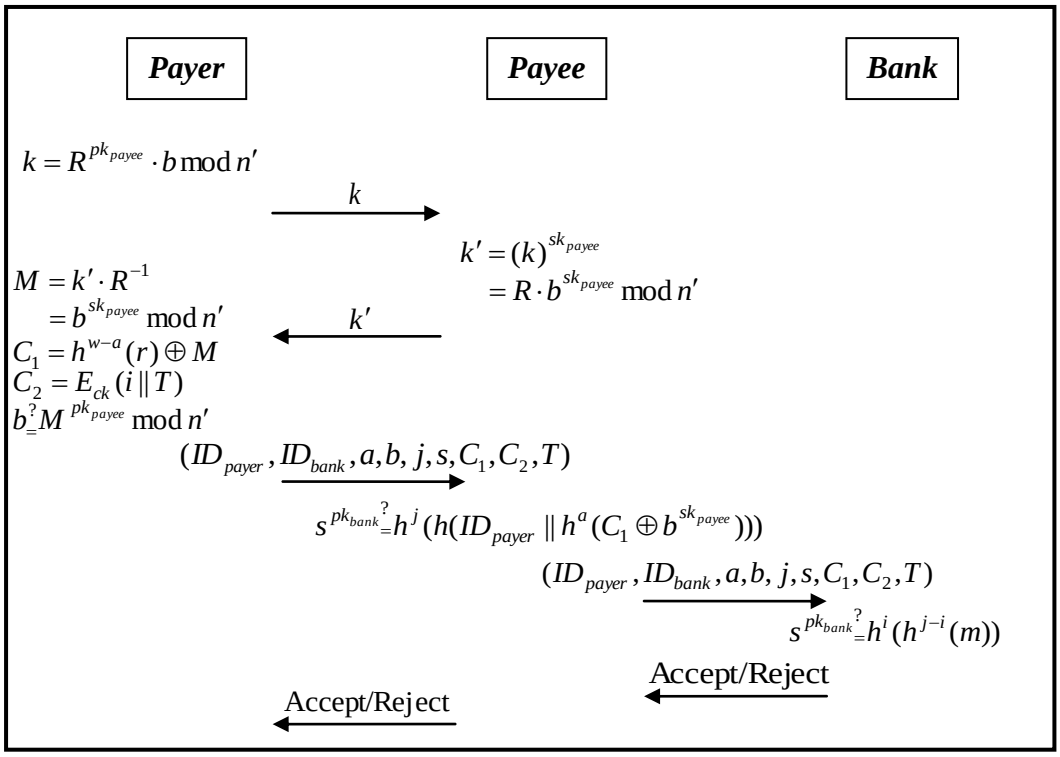

圖 2. 線上電子支票相互認證協定付費階段

$s^{pk_{bank}} \stackrel{?}{=} h^j(h(ID_{payer} \| h^a(C_1 \oplus b^{sk_{payee}})))$ 是否正確。設若正確，收款人把 ID_{payer},ID_{payee},a,b,j,s,C_1,C_2,T 傳送給銀行有效防止重複消費，否則拒絕電子支票。

(5)銀行收到 ID_{payer},ID_{payee},a,b,j,s,C_1,C_2,T 後，確認電子支票是否重複存在銀行資料庫。設若失敗，銀行執行下一個步驟，否則拒絕電子支票。

(6)銀行確認電子支票交易面額 a 是否有超過付款人的存款。設若失敗，銀行執行下一個步驟，否則拒絕電子支票。

(7)銀行確認時戳 $(T' - T) \stackrel{?}{\leq} \Delta T$ 是否在傳送時間範圍內。設若正確，銀行有效防止重複攻擊並執行下一個步驟。否則拒絕電子支票。

(8)銀行確認簽章 $s^{pk_{bank}} \stackrel{?}{=} h^i(h^{j-i}(m))$ 是否正確。設若正確，銀行更新付款人電子支票簿的紀錄，並且傳送 Accept 訊息給收款人。否則 Reject 訊息給收款人。

(9)設收款人正確收到 Accept 訊息後，收款人傳送 Accept 訊息給付款人。否則收款人傳送 Reject 訊息給付款人。

3. 未必提供相互認證

本章節提出 Chang 和 Lee 等人的協定不能提供相互認證。付費階段之前，付款人經由盲簽技術取得收款人對亂數 b 的盲簽章 $k' = R \cdot b^{sk_{payee}} \bmod n'$，即 $M = b^{sk_{payee}} \bmod n'$。在付費過程中，將 $C_1 = h^{w-a}(r) \oplus M$ 和 b 等資訊傳遞給收款人，收款人使用私密金鑰 sk_{payee} 來還原 $h^{w-a}(r) = C_1 \oplus b^{sk_{payee}}$，藉此達到收款人和付款人相互認證。但付款人仍然可以自己偽造出訊息 $M' = b'^{sk_{payee}} \bmod n'$，執行方法如下：付款人任選 $M' \in_R Z_{n'}$，計算 $b' = M'^{pk_{payee}} \bmod n'$，故可得 $M' = b'^{sk_p} \bmod n'$，因此，付款人和收款人未必經過相互認證才可完成交易。

4. 我們的協定

經由第三節弱點分析，我們指出 Chang 和 Lee 等人的協定並不能有效達成雙方認證。因此，本章節提出一個新的相互認證電子支票系統之改善協定，有效達成雙方相互認證。如圖 3 和圖 4。本協定分成兩個階段: 註冊階段和付費階段，註冊階段如圖 1，接著詳細敘述各階段的流程。

4.1 註冊階段：

首先，客戶先向銀行申請註冊電子支票簿，註冊流程描述如下。

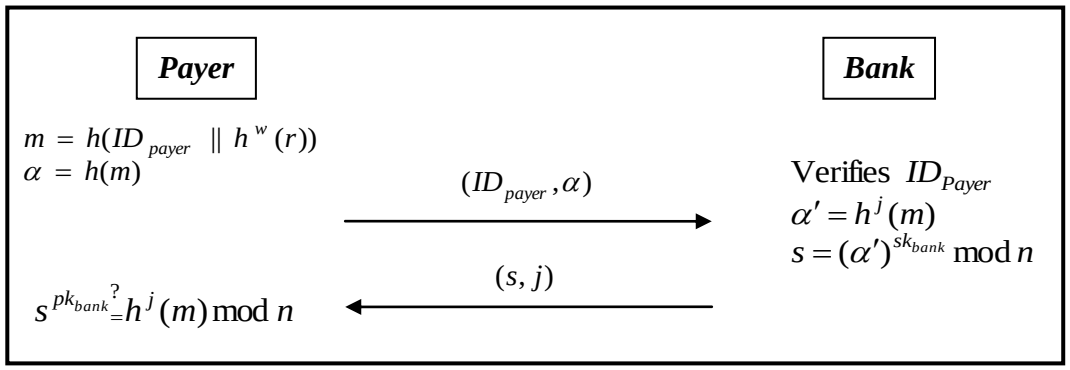

圖 3.相互認證電子支票系統之改善註冊階段

(1)付款人隨機選擇一個安全整數 r，並且計算 m,α，計算式如下：

$m = h(ID_{payer} \| h^w(r)),\ \alpha = h(m)$

付款人把身份 ID_{payer} 及保護的訊息 α 傳送給銀行。

(2)銀行接收到付款人身份和訊息後，首先確認付款人身份 ID_{payer}，並且計算 α', s，計算式如下：

$\alpha' = h^j(m)$ ， $s = (\alpha')^{sk_{bank}} \bmod n$

銀行傳送簽章 s 及電子支票簿可使用次數 j 回傳給付款人。

(3)付款人接收到簽章和電子支票簿可使用次數後，付款人使用銀行公開金鑰驗證簽章 $s^{pk_{bank}} \stackrel{?}{=} h^j(m)$ 是否正確。設若正確，則付款人存入 m, s, j 到電子支票簿。

4.2 付費階段：

買家使用電子支票跟賣家購買商品，交易流程描述如下。

(1)首先，付款人隨機選擇一個整數 R 和亂數 v，並且計算訊息 k，計算式如下：

$v \in_R Z^*_{n'}, v = h(ID_{payer}, ID_{payee}, Date)$

$k = R^{pk_{payee}} \cdot v \bmod n'$

付款人把訊息 k 傳送給收款人。

(2)收款人收到訊息後，收款人對訊息作盲化，並計算盲簽章 k'，計算式如下：

$k' = k^{sk_{payee}} = R \cdot v^{sk_{payee}} \bmod n'$ 收款人把盲簽章 k' 回傳給付款人。

(3)付款人接收到盲簽章後，付款人將盲簽章作解盲化取得訊息，並計算 u, C_1, C_2，計算式如下：

$u = k' \cdot R^{-1} = v^{sk_{payee}} \bmod n'$

$C_1 = h^{w-a}(r) \oplus u$

$C_2 = E_{ck}(i \| T)$

付款人利用收款人的公開金鑰對訊息作驗證 $v \stackrel{?}{=} u^{pk_{payee}} \bmod n'$ 是否正確。設若正確，付款人將 $ID_{payer}, ID_{payee}, a, b, j, s, C_1, C_2, T$ 傳送給收款人，否則終止交易。

(4)收款人收到 $ID_{payer}, ID_{payee}, a, v, j, s, C_1, C_2, T$ 後，收款人使用銀行的公開金鑰驗證簽章 $s^{pk_{bank}} \stackrel{?}{=} h^j(h(ID_{payer} \| h^a(C_1 \oplus v^{sk_{payee}}))$ 是否正確。設若正確，收款人把 $ID_{payer}, ID_{payee}, a, v, j, s, C_1, C_2, T$ 傳送給銀行能有效防止重複消費，否則拒絕電子支票。

(5)銀行收到 $ID_{payer}, ID_{payee}, a, v, j, s, C_1, C_2, T$ 後，確認電子支票是否重複存在銀行資料庫。設若失敗，銀行執行下一個步驟，否則拒絕電子支票。

(6)銀行確認電子支票面額 a 是否有超過付款人的存款。設若失敗，銀行執行下一個步驟，否則拒絕電子支票。

(7)銀行確認時戳 $(T' - T) \stackrel{?}{\leq} \Delta T$ 是否在傳送時間範圍內。設若正確，銀行能有效防止重複攻擊並執行下一個步驟。否則拒絕電子支票。

(8)銀行確認電子支票 $s^{pk_{bank}} \stackrel{?}{=} h^i(h^{j-i}(m))$ 是否正確。設若正確，銀行更新付款人電子支票簿的紀錄，並且傳送 Accept 訊息給收款人。否則 Reject 訊息給收款人。

(9)設收款人正確收到 Accept 訊息後，收款人傳送 Accept 訊息給付款人。否則收款人傳送 Reject 訊息給付款人。

5. 安全性分析

在本章節，我們討論提出的方法可以抵擋以下攻擊：5.1 重送攻擊(Replay attack)、5.2 電子支票簿遺失(Electronic check book loss)、5.3 提供相互認證(Provide mutual authentication)、5.4 冒充攻擊(Impersonating attack)、5.5 重複消費(Double spending)。

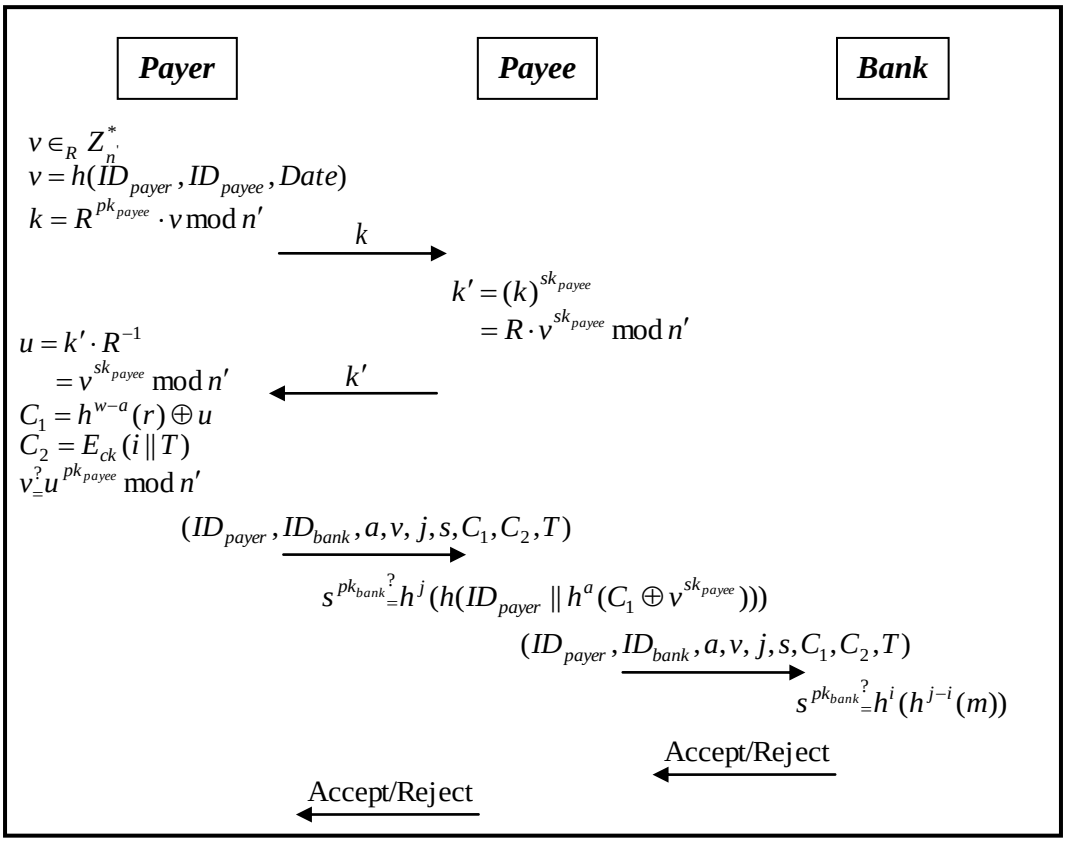

圖 4.相互認證電子支票系統之改善付費階段

5.1 重送攻擊

若攻擊者想要重覆傳送訊息 ID_{payer},ID_{payee},a,v,j,s,C_1,C_2,T 去欺騙銀行，首先訊息必須通過 $(T'-T) \stackrel{?}{\leq} \Delta T$ 驗證才能傳送，但是攻擊者在不知道 T 的情況下，是無法重覆傳送訊息。若攻擊者產生一個新的 T_a 並且將訊息透過 $(T'-T_a) \stackrel{?}{\leq} \Delta T$ 作驗證，是不能驗證成功的，因為先前的訊息 T 和重送的訊息 T_a 是不相同的，因此本篇協定可以抵擋重送攻擊。

5.2 電子支票簿遺失

假設攻擊者偷取到遺失的電子支票簿，則攻擊者假裝付款人使用電子支票簿，交易過程如下：首先攻擊者選擇一個整數 R^*並且計算

$v^* \in_R Z_{n'}^*$

$v^* = h(ID_{payer}, ID_{payee}, Date)$

$k^* = (R^*)^{pk_{payee}} \cdot v^* \bmod n'$

傳送 k^* 給收款人；收款人收到 k^* 並計算

$(k')^* = (k^*)^{sk_{payee}} = R^* \cdot (v^*)^{sk_{payee}} \bmod n'$

回傳 $(k')^*$ 給攻擊者；攻擊者選擇一個亂數 r^* 並計算

$u^* = (k')^* \cdot (R^*)^{-1} = (v^*)^{sk_{payee}} \bmod n'$

$C_1^* = h^{w-a}(r^*) \oplus u^*$

$C_2 = E_{ck}(i \| T)$

攻擊者傳送訊息 $ID_{payer}, ID_{bank}, a, v^*, j, s, C_1^*, C_2, T$ 給收款人，收款人收到訊息後，收款人驗證 $S^{pk_{bank}} \stackrel{?}{=} h^j(h(ID_{payer} \| h^a(C_1^* \oplus (v^*)^{sk_{payee}})))$ 是不可能的，因為攻擊者無法從 C_1 破解單向雜湊函數 $h(\cdot)$ 獲得安全密鑰 r，因此本協定可以抵擋攻擊。

5.3 提供相互認證

付款人在付費階段之前經由盲簽技術，偽造出收款人對亂數 v 產生的盲簽章 $k' = k^{sk_{payee}} = R \cdot v^{sk_{payee}} \bmod n'$，接著付款人計算 $u = v^{sk_{payee}} \bmod n'$，驗證 $v \stackrel{?}{=} u^{pk_{payee}} \bmod n'$ 是不能達到相互認證，因為亂數 v 是由產生 $Z_{n'}^*$ 出來的，並且保護著 $h(ID_{payer}, ID_{payee}, Date)$，因此本協定可以提供雙方相互認證。

5.4 冒充攻擊

假設攻擊者想要冒充付款人使用電子支票，首先攻擊者必須知道盲簽章k'，接著計算出 C_1 和 C_2，透過驗證 $s^{pk_{bank}} \stackrel{?}{=} h^j(h(ID_{payer} \| h^a(C_1 \oplus v^{sk_{payee}})$ 冒充付款人是不可能的，因為攻擊者在不知道安全金鑰 ck 的情況下是無法對 C_2 做解密動作。即使攻擊者攔截到 ck，並且對 C_2 做解密動作，但攻擊者必須破解亂數 v 單向雜湊函數 $h(\cdot)$ 才有可能。

5.5 重複消費

若攻擊者對收款人重覆使用電子支票 ID_{payer},ID_{payee},a,v,j,s,C_1,C_2,T，收款人要求銀行從資料庫中檢查是否有重複使用。因此本協定可以抵擋重複消費攻擊。

6. 結論

在本研究中，我們發現協定[3]在一般情況下，未必能提供相互認證，付款人可以自己製造出訊息來通過收款人的相互認證。因此，本篇協定提出一個新的方法對協定[3]弱點作出改善，並達成雙方交易之間的相互認證。

致謝

作者感謝審稿委員們寶貴的評論與建議。本研究承蒙教育部補助技專校院建立特色典範計畫支持部分經費，謹此致謝，計畫編號：台技(一)字第 0990045921n 號。

參考文獻

[1] Quaddus, M. and Achjari, D., "A model for electronic commerce success," ***Telecommunications Policy***, Vol. 29, Issues. 2-3, pp. 127-152, 2005.

[2] Yu, H. C., His, K. H. and Kuo, P. J., "Electronic payment systems an analysis and comparision of types," ***Technol soc***, pp. 331-47, 2002.

[3] Chang, C. C., Chang, S. C. and Lee, J. S., "An on-line electronic check system with mutual authentication," ***Computers& Electrical Engineering***, Vol. 35 , Issue. 5, pp. 757-763, 2009.

[4] Chaum, D., den Boer, B., Van Heyst, E, Mjolsnes, S. and Steenbeenk, A., "Efficient offline electronic check," ***Proceedings of advances in Enrocrypt'89***, Vol. 434, pp. 294-301, 1989.

[5] Chaen, W. K., "Efficient on-line electronic checks," ***Applied Mathematics and Computation***, Vol. 162, Issue. 3, pp. 1259-63, 2005.

[6] Chaum, D., Fiat, A. and Naor, M., "Untraceable electronic cash," ***Proceedings of advances in Crypto '88, California***, Vol. 403, pp. 227-33, 1990.

[7] Hwang, J. J., Yeh, T. C. and Li, J. B.,"Securing on line credit card payments without disclosing privacy information," ***Computer Standard & Interfaces***, Vol. 25, Issue. 2, pp. 119-129, 2003.

[8] Rivest, R. L., Shamir, A. and Adleman, L. A., "method for obtaining digital signatures and public key cryptosystems," ***Commun ACM***, pp. 120-6, 1978.

[9] Chaum, D., "Blind signature systems," ***Proceedings of advances in Crypto'83***, pp . 153, 1983.

[10] Chaum, D., "Blinding for unanticipated signatures," ***Proceedings of advances in Eurocrypt'87***, pp. 227-33, 1987.

[11] Diffie, W. and Hellman, M., "New directions in cryptography," ***IEEE Trans Inform Theory***, pp. 644-54, 1976.

[12] Rabin, M. O., "Digital signatures andpublic-key functions as intractable as factorization," ***MIT Laboratory for Computer Science***, Technical Report, MIT. /LCS. /TR212, 1979.

[13] Rivest, R. L., Shamir, A. and Adleman, L. A., "method for obtaining digital signatures and public key cryptosystems," ***Commun ACM***, pp. 120-6, 1978.

[14] Schnorr. C. P., "Efficient identification and signatures for smart cards," ***Proceedings of advances in Crypto'89***, Vol. 435, pp. 239-52, 1990.