A Novel E-coupon Scheme used Trapdoor Hash Function

Fuw-Yi Yang Wen-Jung Chao Cai-Ming Liao
Department of Computer Science and Information Engineering,
Chaoyang University of Technology

yangfy@cyut.edu.tw aoyama19@yahoo.com.tw maxman03211@hotmail.com

摘要

目前，大多數的電子票券系統通常使用公開金鑰演算法，達到系統的安全需求；然而，公開金鑰演算法的計算成本是相當大的，比較不適合應用於行動裝置。在 2000 年，有學者提出一些有後門赫序函數簽章方案，線上計算的部份僅需一次的整數乘法運算。為改善電子票券的計算效益，在本論文中，我們結合有後門的赫序函數，提出一個新的且更有效率的行動式電子票券系統，將更適合應用於行動式的環境之中。

關鍵字：電子票券、電子商務、行動商務、有後門赫序函數

Abstract

At present, most of the electronic coupon systems usually use public key algorithms to achieve system's security requirements. However, the public key algorithms do not suit for mobile devices, because these algorithms require expensive computational cost. Sine 2000, many cryptographic researchers have proposed some signature schemes used trapdoor hash functions; the on-line computation of signing only needs one operation of integer multiplication. In order to ameliorate the computational cost of electronic coupon, we propose one novel and efficient electronic coupon system with trapdoor hash functions. Thus this system will be more suitable for mobile environment and real-time application.

Key words: e-coupon, e-commerce, mobile commerce, trapdoor hash function

1. 緒論

發行票券可增進消費者購買的便利性，進而有效地增加銷售量，例如：當消費者瀏覽商店網址，店家會發行票券給消費者，消費者從網際網路獲得票券後，利用印表機列印出此票券，接著使用此票券換回合適的服務或者商品，此方法類似於傳統紙式票券；新的電子票券系統，消費者並不需要列印出電子票券，直接透過網路通訊向商店換取合適的服務及商品，因此，新的電子票券系統能夠提供消費時的便利性，進而增加店家的銷售量。

由於簡訊服務(SMS)、無線應用通訊協定(WAP)以及多媒體簡訊服務(MMS)的蓬勃發展與便利性，許多商業的應用以及服務的發展逐漸地以行動式環境為目標。設若電子票券系統能夠透過消費者的行動裝置接收電子票券，消費者接收與使用電子票券的方式，不只僅於網際網路，可透過簡訊服務(SMS)及藍芽技術傳送電子票券至其他消費者或店家，再由票券發佈者與電信業者確認此票券，完成整個交易；因此，電子票券系統所帶來的便利性，將可廣泛地應用於行動電子商務，例如：禮券、提升新產品促銷方式、廣告等；一個可行的電子票券系統必須考慮其安全性、效率及易管理等特性 [1]，保障消費者的權益以及實行的效益。

在 1999 年，Anand et al. [2] 設計一個植基於網際網路的電子票券發佈方案，此方案致力

於討論電子票券的內容、生命週期以及如何分配電子票券給消費者，而達到刺激消費者購買的慾望與增進產品銷售量。在 2006 年，Chang et al. [3] 提出一個可應用於行動式環境的電子票券系統，此系統結合單向赫序函數，將消費日期、票券使用期限附加在票券上，因此在 Chang et al. [3] 提出的系統中，於線上計算階段必須執行 $w+EXD$ 次的赫序運算($w+EXD$ 通常高達 32 位元，亦即需要 2^{32} 次運算數值)，對於消費者使用的行動式裝置效能而言，此計算量將是一大考驗；因此，在本篇論文中，我們將提出一個植基於有後門赫序函數的電子票券交易系統，解決電子票券之交易問題、安全性和處理效率；在線上計算的成本行動裝置負載，僅需計算一次的整數乘法運算，提升使用者行動裝置的執行效益。使其電子票券交易系統更適用於移動式的環境中，且廣泛的被使用者使用。

2. 回顧有後門赫序函數技術

現今，電子簽章技術使用赫序函數進而增進系統的安全性已相當普遍，為了降低電子簽署訊息的時間，有學者 [4] 將電子簽署的處理過程區分為二個階段(離線計算階段及線上計算階段)。多型赫序函數 [5] 意指該赫序函數是有後門的，即為有後門的赫序函數，只要給予足夠的資訊，後門赫序函數金鑰的擁有者，便可找到其他的赫序碰撞資訊，藉由此方式找出相同的赫序值。此方法可應用於降低所有電子簽章技術的線上計算量，並且增加電子簽章技術的安全性 [4]，基於以上的考量，文獻 [6]、[7]、[8] 持續的改善有後門赫序函數的線上計算量。在結合有後門赫序函數的電子票券系統中，赫序操作和簽章簽署是在離線計算階段執行，即由消費者產生隨機訊息 m_1 及隨機亂數 r_1，計算赫序值 $TH_{HK}(m_1,r_1)$，接著傳送赫序值給票券簽署者簽署，因此，繁重的計算是可以事先在離線階段完成；在線上計算階段，消費者開始執行後門赫序函數操作，消費者計算並且決定簽署文件 m_2，接著使用後門赫序秘密金鑰尋找 r_2，使得 $TH_{HK}(m_1,r_1)=TH_{HK}(m_2,r_2)$，因此票券簽署者不需要再一次做簽署的動作。

3. 電子票券系統必要條件

電子票券系統必須滿足下列條件，達到安全及易處理之特性。

可識別：每張電子票券必須能夠辨別其擁有者，防止攻擊者假冒票券擁有者消費它。

不可偽造：只有電子票券簽署者能夠發行合法的電子票券，任何人都無法偽造。

不可否認：任何的票券擁有者消費電子票券，在完成交易後，無法否認這項交易。

使用期限：電子票券能設置使用期限。

易管理：電子票券系統能夠辨別電子票券是否重複使用。

獨立性：電子票券系統能在不同形式的平台上執行。

匿名性：任何人皆無法經由票券交易過程，而得知票券使用者個人資訊。

4. 我們的方案

我們將提出一個植基於有後門赫序函數的電子票券系統，假設公開金鑰加密系統已預先設置於電子票券系統中，每個實體擁有自己的公開金鑰、祕密金鑰和電子憑證。票券簽署者的角色如同公司總部，負責簽署、發佈及管理電子票券，當消費者使用電子票券時，由服務提供者提供商品或者合適的服務給消費者，此外，消費者可能於行動式裝置使用電子票券；因此，行動式裝置的低計算量及低通訊能力是必須考量的。在本系統中，我們利用有後門的赫序函數技術，降低線上階段的計算成本，此系統將電子簽署的處理過程以兩個部份分別為之，即為離線計算(註冊階段、發佈階段)與

線上計算(換回階段)。離線計算意指消費者收到票券的前置作業。線上計算意指消費者消費票券的計算過程，即使用備份資料產生換回資訊，電子票券系統將分為三個階段：註冊階段，發佈階段，以及換回階段。

我們首先描繪電子票券系統雛型於圖 1，說明參數符號於 4.1，描述系統協定於 4.2。

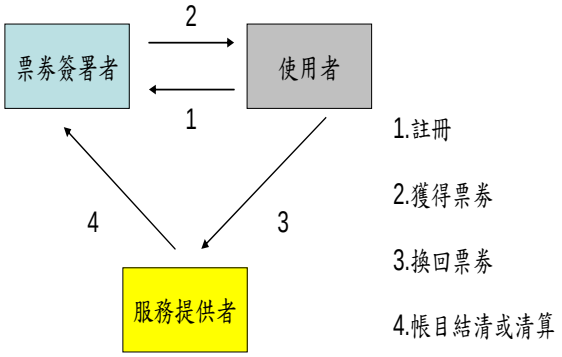

圖 1 電子票券系統雛型

4.1 參數符號

我們將系統參數劃分為三個部份；參數之定義如下：

公開參數及計算函式描述：

$Cert_A$ ：實體 A 之電子憑證。

S_b ：服務提供者 ID。

EXD ：電子票券使用期限。

NOW ：交易日期。

$H(\cdot)$：赫序函數。

||：位元串接運算符號。

消費者參數：

C ：消費者。

RI ：消費者的個人資訊。

CID ：票券簽署者分配給消費者的假名。

r_1、m_1：二個隨機產生之亂數(離線計算階段備用之資料)。

x：為秘密之 Trapdoor key，例如：$TK = x$。

HK：為公開之 Trapdoor Hash key，例如：$HK = (g, n, y)$。

票券簽署者參數：

ISU ：電子票券簽署者。

SN ：電子票券之編號。

RT ：電子票券換回表(Redeemed Table)。

$Enc(\cdot)$，$Dec(\cdot)$：ISU 之公開金鑰加解密演算法。

P, Q, p, q, t ：皆為大質數，並且 P 及 Q 為相同之編碼長度，且 $P = 2p \cdot t + 1$，$Q = 2 \cdot q + 1$。

k, l：依安全等級而定之參數，$k = 80$，$l = 160$。

n：為二安全質數相乘之乘積，$n = P \cdot Q$。

g ：$g \in Z_n^*$ 其序為 p， p 之編碼長度為 l，即 $|p| = l$。

4.2 電子票券系統

設若消費者欲申請電子票券，消費者必須傳送個人私密資訊給票券簽署者進行註冊，註冊完成時，票券簽署者發佈一個假名給消費者。之後於發佈階段，票券簽署者產生票券序號，並且利用簽署者唯一的密鑰簽署此電子票券。消費者可利用此票券換回合適的服務及商品。設若電子票券系統參數設置：$P = 2p \cdot t + 1$，$Q = 2q + 1$，其中 (P, Q, p, q, t) 皆為大質數，$|P| = |Q| = 512$，$|p| = 160$，$n = P \cdot Q$，$g \in Z_n^*$ 其序為 p， g 之產生過程詳細如文獻[6]、[7]、[9]，令 $x \in Z_p^*$、$y = g^x \bmod n$，有後門赫序函數公開金鑰為 (g, n, y)，私密金鑰為 x。系統執行程序分為下列三個階段：

使用者註冊階段

在此階段中，C_i 向 ISU 註冊並獲取假名，所有訊息皆在秘密通訊管道傳送。詳細程序，如以下步驟，通訊資料以圖2表示之。

1. 首先，C_i 傳送個人資訊 RI_i 及電子憑證 $Cert_i$ 給 ISU 。
2. ISU 在收到訊息後，確認 $Cert_i$ 是否正確；若正確，ISU 接著產生 C_i 之假名 CID_i，將 CID_i 傳送給 C_i ，並儲存 $(CID_i, RI_i, Cert_i)$ 至註冊表(Registration table)中。
3. 當 C_i 收到註冊完成資訊時，儲存 CID_i 到智慧卡或SIM (Subscriber Identity Module)卡裡。

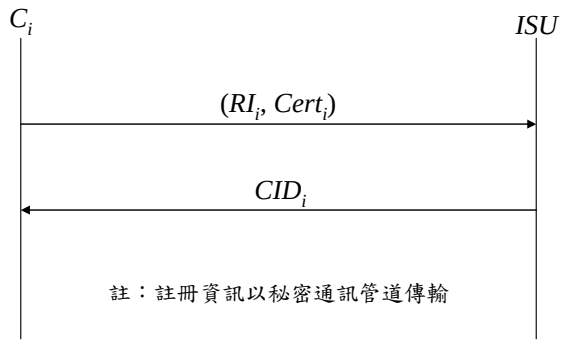

圖 2 消費者註冊階段

電子票券發佈階段

當 C_i 欲向 *ISU* 發出申請電子票券之資訊時，C_i 必須選取 $x \in_R \{0,1\}^l$，計算 $y = g^x \bmod n$，並且隨機產生訊息 $m_1 \in_R \{0,1\}^l$、隨機亂數 $r_1 \in \{0,1\}^{2l+k}$，計算赫序值 $A = g^{r_1} y^{m_1} \bmod n$，接著將 (m_1, r_1) 儲存備用，以便爾後在換回階段計算赫序碰撞值，之後使用公鑰對赫序值及使用者假名加密過後，傳送申請需求的訊息給 *ISU*，當 *ISU* 接收到傳送資訊時，利用本身的密鑰解密，獲取其假名與未簽署的電子票券，並確認消費者的身份；若為合法消費者，*ISU* 將交易票券使用期限、序號、與未簽署的電子票券進行簽署，接著，傳送電子票券 (SN, s, EXD) 給 C_i 並儲存 (A, CID_i) 於資料庫中；C_i 驗證簽章若為正確，則為合法的電子票券，在此階段，所有訊息皆在公開通訊管道傳送。詳細程序，如以下步驟，通訊資料以圖3表示之。

1. 首先，C_i 產生隨機亂數 $r_1 \in_R \{0,1\}^{2l+k}$ 及訊息 $m_1 \in_R \{0,1\}^l$，計算 $A = TH_{HK}(m_1, r_1) = g^{r_1} y^{m_1} \bmod n$ 及 $D = Enc(A \| CID_i \| y)$，接著傳送 D 給 *ISU*。
2. *ISU* 接收到 D 後，解密 $(A \| CID_i \| y) = Dec(D)$；若正確，產生電子票券唯一的序號 SN，並且利用本身的密鑰對 $(A \| SN \| EXD \| y)$ 簽署 $s = Sign_{SK}(A \| SN \| EXD \| y)$，接著傳送 (SN, s, EXD) 給 C_i。
3. 當 C_i 接收到 (SN, s, EXD) 後，驗證 $(A \| SN \| EXD \| y) \stackrel{?}{=} Ver_{PK}(s)$；若相等，表示 C_i 獲得 (SN, s, EXD) 為合法的電子票券。
4. 此時 C_i 確定獲得完整之電子票券 (SN, s, EXD)。

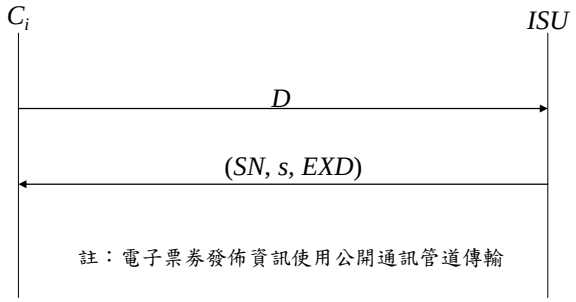

圖 3 電子票券發佈階段

電子票券換回階段

當 C_i 欲向服務提供商 S_b 換回電子票券上的服務或商品，首先，C_i 必須計算並且決定簽署之文件 m_2，文件 m_2 資訊為票券使用期限、消費日期及服務提供者 *ID*，此時 C_i 先由儲存資料庫中取出備用之資料 m_1 及 r_1，接著利用後門金鑰 *TK* 執行後門赫序操作，由此求取赫序碰撞值，此線上計算僅僅只需執行一次的整數乘法運算，即由 (m_1, m_2, r_1) 找出 r_2，並且傳送 r_2、電子票券及相關資訊給 S_b，接著 S_b 利用赫序函數之公開金鑰 $HK = (g, n, y)$，求取 (m_2, r_2) 的赫序值，使得 $g^{r_2} y^{m_2} = g^{r_1} y^{m_1} \bmod n$，即；$g^{r_1 + x \cdot m_1} = g^{r_2 + x \cdot m_2} \bmod n$；經由 S_b 與 *ISU* 確認為合法，並且電子票券之序號是未登錄於 *RT* 中，S_b 即提供電子票券上的服務或商品給 C_i，在此階段，所有訊息皆在公開通訊管道傳送。詳細程序，如以下步驟，通訊資料以圖4表示之。

1. C_i 欲向服務提供商 S_b 換回電子票券中的服務及商品時，使用 m_1，r_1 及密鑰 x 計算 $m_2 = (EXD \| NOW \| S_b)$，計算 $TH_{TK}(m_2) = r_2 = (m_1 - m_2) \cdot x + r_1$，接著傳送 $(S_b, EXD, SN, NOW, r_2, y, s)$ 給 S_b。
2. 當 S_b 收到 $(S_b, EXD, SN, NOW, r_2, y, s)$ 後，計算 $m_2 = (EXD \| NOW \| S_b)$ 並使用 *ISU* 的公鑰驗證

$(g^{m_2} y^{r_2} \bmod n \| SN \| EXD \| y) \stackrel{?}{=} Ver_{PK}(s)$；若為相等，$S_b$ 轉傳 $(S_b, EXD, SN, NOW, r_2, y, s)$ 給 *ISU* 。

3.由 *RT* 確認 *SN* 是否已存在；若無，則進行同上 S_b 之驗證；驗證結果若為合法交易，*ISU* 在收到此交易資訊 $(S_b, EXD, SN, NOW, r_2, y, s)$ 時，*ISU* 回覆 S_b 此電子票券為合法的。

4.當 S_b 收到的回覆為合法，S_b 依據電子票券上聲明的項目，提供合適的服務或商品給 C_i，並保存此電子票券，以便日後與 *ISU* 核對交易金額。

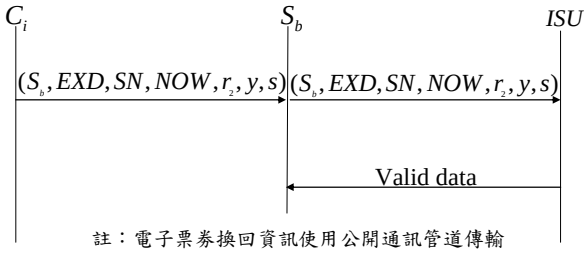

圖 4 電子票券換回階段

5. 討論安全性及實用性

我們將分析電子票券系統的安全性及效率。安全需求將說明於5.1；執行效率討論將說明於5.2。

5.1 安全性討論

我們提出的電子票券系統可滿足以下的安全特性：

5.1.1 可驗證性：

電子票券可提供任何的實體驗證，任何實體消費者、店家、*ISU* ，只需利用 *ISU* 的公鑰，即可驗證其電子票券的合法性。

5.1.2 預防偽造攻擊：

每一個合法的電子票券皆由 *ISU* 的密鑰簽署並發佈，若攻擊者欲偽造一個合法的電子票券，必須取得 *ISU* 的密鑰，但是我們知道此密鑰是唯有 *ISU* 知道的秘密資訊。

5.1.3 預防竄改：

此系統可預防二種種類的更改攻擊。

(1)電子票券是經由 *ISU* 的密鑰簽署，若攻擊者欲竄改電子票券的內容，將因無法取得 *ISU* 的密鑰，而無法竄改電子票券之內容。

(2)使用資料 m_1 及 r_1 為 C_i 個人的私密資訊，因此，任何人皆無法在多項式時間內取得其值進行攻擊。

5.1.4 預防重複贖回：

在每一次交易中，*ISU* 以 *SN* 為搜索鍵值，確認 *SN* 是否已存在 *RT* 之中；若有，*ISU* 將能立即發現此電子票券為非法的，因此，惡意的使用者無法重覆使用電子票券。

5.1.5 匿名性：

在電子票券換回階段，通訊資訊與驗證資訊皆無可以確認消費者的身份資訊，因此，任何人皆無法經由傳送的訊息確認票券消費者的個人資訊(例如：消費者的身份資訊)。

5.1.6 不可否認特性：

在電子票券發佈階段，C_i 將申請票券請求訊息(赫序值及消費者假名)加密後，傳送給 *ISU* 進行確認，若為合法使用者，*ISU* 儲存赫序值 *A* 及消費者假名 CID_i 於資料庫；設若惡意的消費者想在爾後交易成功時提出否認，*ISU* 將可由資料庫提出證據。

5.2 效率分析

根據Geoffrey在1999年 [10] 所提出的文獻，在6805處理器的環境中，SHA執行一次赫序函數操作需要67244個週期；然而，在Chang et al.所提出的電子票券系統，*w* 為服務提供者編號上限值，*EXD* 為電子票券使用期限；設若 *w* 值為1000，*w* 就需10位元的長度；*EXD* 值依年、月、日編碼(例如20091231為2009年12月31日)為，需32位元的長度。此系統於線上計算階段需要執行 $(w+EXD)$ 次的赫序運算，因此，於線上計算階段就需要執行 $(w+EXD)\cdot 67244$ 個週期；其計算量對於行動式裝置效能而言將是一大考驗，在我們提出的電子票券系統中，

我們結合有後門赫序函數，降低系統的線上計算量(即使用者行動裝置的計算負擔)。於線上計算僅需執行一次的整數乘法運算，約需160^2個週期，比起Chang et al.於線上計算所需要計算的$(w+EXD)\cdot 67244$個週期，將降低許多線上計算量，設若clock為5MHz，則每週期耗時0.2 μs，我們的協定線上計算耗時5.12 ms，Chang et al. 的線上計算平均耗時$0.2\ \mu s\cdot 2^{31}\cdot 67244 = 28881078$ seconds $= 334.27$天。

	Chang et al. 的協定	我們的 協定
線上計算 （週期）	$(w+EXD)\cdot 67244$ (平均$2^{31}\cdot 67244$個)	160^2
離線計算	$2(w+EXD)$ 次赫序運算 + 2 次指數運算	3 次指 數運算
換回通 訊量	4768 bit	5184 bit

圖 5 效能分析表

6. 結論

在本篇論文中，我們提出一個植基於有後門赫序函數的電子票券系統，在我們的系統中，電子票券可彈性且安全地應用於電子商務的環境之中，消費者並不會在票券交易過程，洩漏本身的個人資訊，並且，電子票券可被每個實體驗證去防止偽造攻擊。在線上計算的成本行動裝置負載，僅需執行一次的整數乘法運算，提升使用者行動裝置的執行效益。使其電子票券交易系統更適用於行動式的環境中，且廣泛的被使用者使用。

參考文獻

[1] K. Matsuyama and K. Fujimura, "Distributed Digital-Ticket Management for Rights Trading System," ***Proceedings of the 1st ACM conference on Electronic commerce***, pp. 110-118, 1999.

[2] R. Anand, M. Kumar, and A. Jhingran, "Distributing E-Coupon on the Internet", ***Proceedings of the 9th Annual Conference of the Internet Society*** (INET'99), 1999.

[3] C.-C. Chang, C.-C. Wu, and I.-C. Lin, "A Secure E-coupon System for Mobile Users," ***IJCSNS International Journal of Computer Science and Network Security***, Vol. 6, No. 1, January, pp. 273-280, 2006.

[4] A. Shamir and Y. Tauman, "Improved online / offline signature schemes," ***Advances in Cryptology-CRYPTO'01***, LNCS 2139, pp. 355-367, 2001.

[5] H. Krawczyk and T. Rabin, "Chameleon signatures," ***Symposium on Network and Distributed Systems Security*** (NDSS'00), pp. 143-154, 2000.

[6] F. Y. Yang, S. H. Chiu, and C. M. Liao, "Trapdoor Hash Functions with Efficient Online Computations," ***The Proceedings of Multimedia and Networking Systems Conference 2006*** (MNSC 2006), Kaohsiung Cuty, Taiwan, Session G1, 2006.

[7] F. Y. Yang, "Efficient trapdoor hash function for digital signatures," ***Chaoyang Journal***, Vol. 12, pp. 351-357, 2007.

[8] F. Y. Yang, "Improvement on a trapdoor hash Function,"***International Journal of Network Security***, Vol. 8, pp. 317-321, 2009.

[9] T. Okamoto, M. Tada and A. Miyaji, "Efficient 'on the fly' signature schemes based on integer factoring," ***Proceedings of the 2nd International Conference on Cryptology in India, INDOCRYPT'01***, LNCS 2247, pp. 275-286, 2001.

[10] K. Geoffrey, "Performance Analysis of AES candidates on the 6805 CPU core," ***Second AES Candidate Conference*** (AES2),1999.