Journal of e-Business
第七卷　第一期　2005 年 3 月（p.75~86）

# 一種隱藏式附加日期的電子現金付款機制

郭木興　謝東宏
朝陽科技大學資訊管理學系

**摘要**

隨著電子商務的盛行，電子付款系統在電子商務上的需求也越來越受到重視。在眾多的線上電子付款系統中，電子現金付款系統是最為消費者喜愛與注意的，原因是它像紙鈔現金一樣，是一種無具名且可自由轉移的電子支付工具。目前電子現金的實作系統多是根據 David Chaum 的「盲目數位簽章」（Blind Digital Signature）理論實作而成的。然而，Chaum 所提出的方法中並無附加日期資訊，因此可能會讓使用者有重複消費，以及商家無從了解銀行是否正確計息等問題。為此，Chang 等人提出一種在電子現金中附加日期資訊的方法來處理電子現金有效日期問題，然而他們的方法卻會產生日期資訊外曝的缺點。此一缺點將可能造成電子現金使用者的損失，例如，顧客向銀行提取電子現金時，此時若日期外曝的話，惡意人士若蓄意收集某銀行跟企業客戶電子現金提取交易的日期，而在企業客戶交易最頻繁的日期傳送大量封包使其交易產生延遲或中斷。另外，銀行體系也可能因本身之利益而利用電子現金日期資訊私下控制利息之高低，這也會影響到顧客的利益。所以，在本論文中我們進一步改善 Chang 等人的方法，提出一種將消費日期隱藏在電子現金中的方法，可決解日期外曝的缺點。

*關鍵字：電子商務、電子付款、電子現金、盲簽章*

---

# A Veiled Date-Attachment e-Cash Scheme

M. H. Kuo and D. H. Sei
Department of Information Management, Chaoyang University of Technology

Abstract

With the boom of electronic commerce（EC）, the needs of a safe and convenient electronic payment scheme have gained more and more respect by EC users. Many electronic payment schemes have been proposed up to date. Among them, electronic cash( e-cash )is one of the most popular schemes that support users on line payment. The implements of e-cash are always based on that of David Chaum blind digital signature theory. Unfortunately, Chaum method lacks date information. This will cause user double spends his e-cash, and the

merchant will be unable to check whether its e-cash is properly interested or not. Recently, Chang et al. proposed a flexible date-attachment scheme to solve the mentioned problems. However, Chang et al. method still has some drawbacks. One of them is the date information in e-cash that is easily explored to the public. Internet malicious users can use the date information to blockade the payment translation. It will cause both merchant and user serious loss. In this paper, we proposed a veiled date-attachment electronic cash scheme that effectively improves Chang et al. method drawbacks.

*Keywords: electronic commerce（EC）, electronic payment, e-cash, blind digital signature*

## 1. 緒論

由於電子商務的交易是一種全新的商業方式，交易主要是以電子化的形式進行，商家與顧客無法面對面的進行交易，所以顧客在網路上購買商品後，無法以傳統交易中現金的方式將貨款支付給商家，為了克服此種無法「一手交錢，一手交貨」的問題，目前 B2C 電子商務交易可行的付款方式可分為以下四種（薛夙珍，1997）：

(1) 貨到收款

消費者在商家的網站上看到中意的產品後，直接在該網站下單購買，俟商家送貨到府時，再一手交錢，一手交貨。這種付款方式可能會造成消費者虛購產品，或歹徒利用商家送貨為由進行一些非法行為。

(2) 郵政劃撥

消費者從網路上找到屬意的產品，記下產品的相關資料（如產品型號、商家的劃撥帳號），再到郵局以郵政劃撥的方式匯款給商家。而銷售方在收到劃撥金額後，再將產品寄出，所以它很像傳統的郵購。由於電子商務的主要優點是方便與迅速，所以這種付款方式並不符合電子商務的發展方向。

(3) 信用卡付款

消費者在網路上瀏覽電子商店所販售的產品內容或規格後，選定所要購買的產品，然後再以信用卡（登入消費者的信用卡號）作為交易的付款工具。雖然這種方式是目前 B2C 電子商務交易最普遍的付款方式，但是透過電話線或網際網路等公眾網路來進行不加密的資料傳輸，由於網際網路的安全設計並不嚴密，所以這種付款方式問題叢生。再者，由於每筆信用卡交易都須支付固定的手續費，所以對一些小額付款的交易是非常沒有效益的。

(4) 線上電子付款

由於傳統的付款方式在電子商務之運作上會產生以上諸多問題，因此必須有一

些利用網路付款的機制來解決這些問題，這也就是所謂的「電子付款」系統。廣義而言，電子付款就是消費者在網路上購買商品或服務後，以線上方式進行買賣雙方的金融轉換，它是電子商務交易中不可或缺的一部份。根據美國 Cyber Cash 公司對 819 位網路交易者的一項線上調查顯示，其中 98%（相當 804 位）的受訪者希望能透過網路進行付款，理由是網路付款甚為方便（薛夙珍，1997）。此項調查結果顯示，網路使用者上網購物的意願逐漸增強，而網路付款的方便性是吸引使用者進行網路購物的一大主因。

至於電子付款的型式分類上，國內學者郭木興認為，電子付款系統可概略分為三大類（郭木興，2003），分別介紹如下：

(1) 現金式電子付款系統

現金式電子付款系統有時候又稱作代幣式電子付款系統，交易的進行是經由電子貨幣的即時交換所產生。此類付款系統最有名的就是電子現金。

(2) 預付式電子付款系統

此類付款系統包括電子錢包、智慧卡。就付款的時間而言，它是屬於一種「預付的方式」，也就是說，使用者須要預先儲存一筆金額來換取付款系統的使用權；而就使用的對象而言，此種付款系統是任何人皆可使用，可自由轉換，且不會留下交易個體的交易紀錄。然而，使用者則須自行承擔付款系統遺失、盜用及錯誤的風險。

(3) 後付式電子付款系統

後付式電子付款系統的運作方式是消費者在購買前，商家先連繫銀行，在確認客戶消費的信用能力後，再進行交易。這類的電子付款系統包括有電子支票、加密信用卡、第三者擔保等。相對於代幣式付款系統，後付式電子付款系統的付款時間則是一種「延後付款」或「信用付款」的方式，使用者在消費後，並未立即支出金額，而是等到一段期間後，發行機構才向客戶進行清算。

上述的諸多電子付款系統中，就以電子現金最受到各方的喜愛與重視，歸納其原因主要有下（郭木興，2003）：

(1) 使用時具有匿名性

電子現金只有在向金融機構申購時會留下開戶記錄，但在使用電子現金時是獨立的，與銀行帳戶沒有直接的關連，因此無法由電子現金的使用追蹤到消費者的身份，對於消費者的隱私權與帳戶的安全性有較佳的保障。

(2) 方便的交易媒介

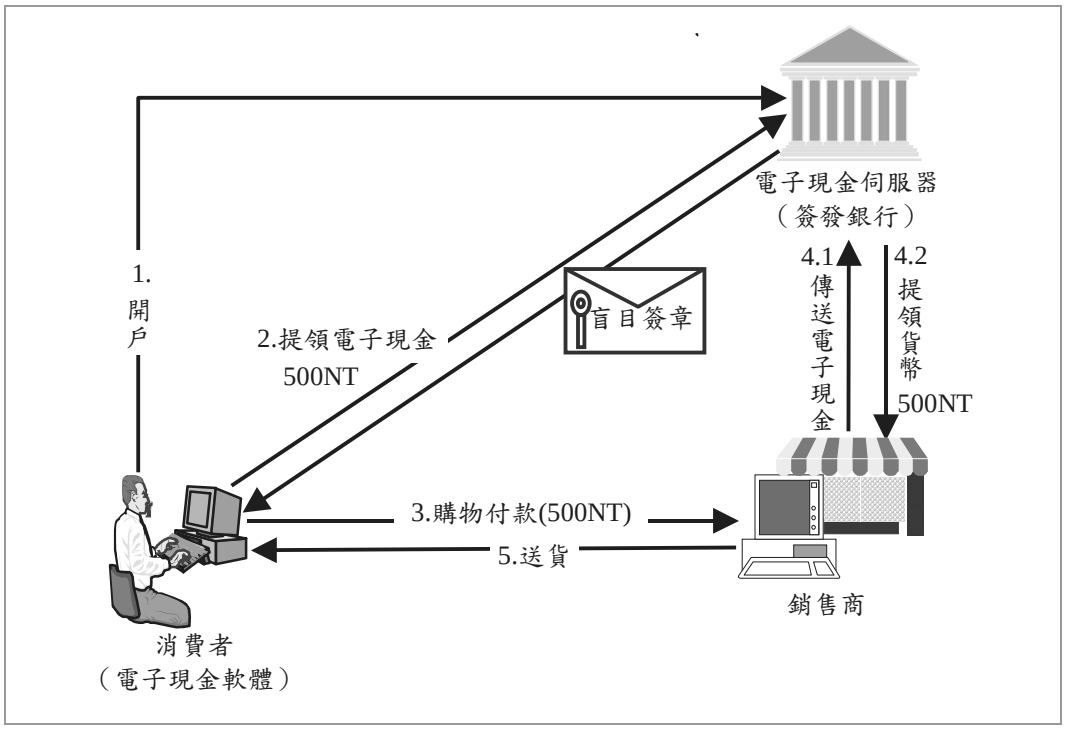
電子現金具有紙鈔現金的貨幣價值，又具有電子媒體交換迅速的功能，是電子商務中一種非常方便的交易媒介。電子現金未來若相關發行機構與清算機制發展成熟的話，可以視為網路上的一種法定貨幣，具有一般現金即時兌現的性質，廠商將很樂意收到這種付款。

(3) 可以離線作業

電子現金系統分為線上付費機制（on-line）和離線付費機制（off-line）兩種。在線上付費機制中，商家在收到消費者所傳送的電子現金後，即利用線上驗證方法向簽發銀行驗證此電子現金的真偽及是否有重複使用。而在離線付費機制中，商家是可以不連線而獨立驗證消費者的電子現金是否為合法，若商家認定電子現金為合法，則完成網路交易的動作。目前大部分的電子現金系統具有離線驗證的功能，可以在離線的狀況下進行付款。

電子現金在英文上有許多不同的名稱，如 e-money, electronic money, network money, digital currency , electronic currency, digital cash , electronic cash, e-cash, cyber cash 等（Nicholls, 1998）。在國內我們一般稱它叫做電子現金（Digital Cash）或電子錢（Digital Money）。國際清算銀行（Bank for International Settlement, BIS）在其所提出之「電子貨幣之發展對中央銀行之影響」報告中，將電子貨幣定位為：「以電子形式儲存於由消費者持有的電子設備中，以現行貨幣單位計算之貨幣價值」（European Central Bank, 1998）。而 European Central Bank 則將電子貨幣定義為：「將貨幣價值以電子方式儲存於某種技術裝置上，可以用來支付發行者以外對象的付款工具，而且交易過程不必然牽涉到銀行的帳戶」（http://knight.fcu.edu.tw/~d8655601/電子貨幣之前言及介紹.htm）。

本論文主要是依據電子現金付款系統的精神，消費者要能使用電子現金付款，首先要在發行電子現金的銀行開設帳號及在此帳號內存入足夠的金錢來支持他的任何採購，而此銀行多半是由傳統的銀行來負責線上的作業。消費者在使用電子現金時，他首先用其電腦上的數位簽章技術，對所要提領的金額做加密處理，再將處理後的資料（票據：為一隨機亂碼）傳送給電子現金發行銀行。而銀行在收到此消費者（其顧客）的資料後，則會利用顧客的數位簽章將資料解密，並自顧客帳戶中提領此筆金錢。接著，銀行使用其私密金鑰對所要求金額的票據予以數位簽章，並將該票據送回給顧客做為電子現金，如此顧客便可使用電子現金在網路上消費了。使用電子現金付款時，顧客利用網路將電子現金傳送給商家。商家在收到消費者所傳送的電子現金後，即利用線上驗證方法向簽發銀行驗證此電子現金的真偽及是否有重複使用，商家為了交易的時效性，需要在生效日期當天立即交付給銀行進行存款。整個電子現金付款系統的付款流程如圖 1 所示。




▲ 圖 1　電子現金的付款流程

從上述的電子現金的使用流程中我們可以知道，在網路上所使用的電子現金事實上是一連串的數位訊息所組成，例如 e-cash 是由美國 Digicash 公司根據電子現金之父 David Chaum 於 1982 所提出的「盲目數位簽章」（Blind Digital Signature）理論實作而成的系統（Chaum, 1983; Chaum, et al., 1990; Hwang, et al., 2001）。這種數位訊息中並沒有消費日期記錄，如此可能會讓使用者有重複消費的行為；同時對於一些關心利息的商家也無從了解銀行是否正確的計息。為了解決這些問題，一些研究即提出在電子現金訊息中加上附加日期資訊，並以資料庫來記錄電子現金的使用，此附加日期會包含一個使用日期的資訊，存入至電子現金中，利用此附加日期便可準確地計算銀行應支付的利息，同時此日期代表電子現金移轉的生效日期，所以附加日期代表一個特殊之訊息，可使數位現金的實用性大大提昇（Abe and Fujisaki, 1996; Fan and Lei, 1998; Fan, et al., 2000; Chang and Lai, 2003）。

雖然在電子現金訊息中加上日期資訊可以防止重複消費的行為，並可做為計息的依據，然而這種方法卻存在日期外曝的疑慮，它可能導致下列的缺點：

(1) 惡意人士蓄意收集某銀行跟企業客戶電子現金提取交易的日期，而在企業客戶交易最頻繁的日期蓄意傳送大量封包使其交易產生延遲或中斷。

(2) 防止銀行惡意控制利息高低之行為或刻意、無意走漏日期而遭人蓄意攻擊。

在本論文中，我們將提出一種新的加入日期資訊的電子現金付款機制來改善過去日期附加方法上的缺點。全文共分五節，除本節外，第二節探討過去學者在電子現金附加日期研究上的優缺點，第三節主要在描述我們所提出的新方法，而在第四節中則針對我們所提出的方法進行安全分析，最後在第五節做總結說明。

## 2. 文獻探討

在探討電子現金附加日期資訊的研究方面。Fan 等人認為 Chaum 所提出的電子現金無附加日期（Fan, et al., 2000），這樣會讓使用者有重複消費的行為，另外關心利息的商家也無從了解銀行是否正確的計息，所以 Fan 等人提出一種在電子現金訊息中加上截止日期資訊的技術來改善 Chaum 方法的缺點。接著 Chang 等人提出了幾個發生在 Fan 等人方法上的缺點，例如 Y2K、顧客與商家串謀等，進一步改善了 Fan 等人方法的缺點，使得附加日期更具彈性（Chang and Lai, 2003）。Chang 等人的方法如下：

(1) 初始階段

銀行選取四個大質數 $p$ 、 $q$ 、 $p^*$ 及 $q^*$ ，計算 $n = p \cdot q$ 、 $n^* = p^* \cdot q^*$ 、 $\phi(n) = (p-1)(q-1)$ 及 $\phi(n^*) = (p^*-1)(q^*-1)$ ，接著銀行選擇兩個整數 $e$ 和 $e^*$ 且找出兩整數 $d$ 與 $d^*$ 來分別滿足 $e \cdot d \equiv 1 \bmod \phi(n)$ 及 $e^* \cdot d^* = 1 \bmod \phi(n^*)$ 。此階段為產生 RSA 的金鑰，而 $(e, n)$ 和 $(e^*, n^*)$ 為公開金鑰，$(d, p, q)$ 和 $(d^*, p^*, q^*)$ 為私密金鑰，並公佈兩個雜湊函數 $H(\cdot)$ 和 $G(\cdot)$ 。

(2) 提款及解盲因子階段

顧客在 $Z_n^*$ 選取一個盲因子 $r_1$ ，計算 $\alpha = r_1^e H(m) \bmod n$ ，將 $\alpha$ 傳給銀行。銀行便對 $\alpha$ 進行簽章，計算 $t_1 = \alpha^d \bmod n$ ，再將 $t_1$ 傳送給顧客並且從顧客帳戶中扣除 $w$ 元。當顧客接收到 $t_1$ 之後，解盲因子，計算 $s = r_1^{-1} t_1 \ H(m)^d \bmod n$ ，$s$ 為銀行對 $H(m)$ 所作的電子簽章。顧客再從 $Z_{n^*}^*$ 中隨機選出另一個盲因子 $r_2$ ，計算 $\beta = r_2^{e^*} G(s) \bmod n^*$ 並將 $\beta$ 傳送給銀行，銀行計算 $t_2 = b^{d^*} \bmod n^*$ ，並傳回 $t_2$ 給顧客，顧客解盲因子計算 $\delta = r_2^{-1} t_2 \bmod n^* = (G(s))^{d^*} \bmod n^*$ ，而 $\delta$ 就是銀行對 $G(s)$ 的簽章。

(3) 附加日期階段

當顧客消費時，傳送 $\delta$ 、 $s$ 和日期 $(a, b, c)$（例如為西元 2004 年 4 月 23 日，則 $a$ = 2004、$b$ = 4、$c$ = 23）經由匿名通道傳給銀行，銀行檢查 $\delta^{e^*} = G(s) \bmod n^*$ 是否相等，若相等，銀行則對 $G(s \| a \| b \| c)$ 作簽章 $s' = (G(s \| a \| b \| c))^{d^*} \bmod n^*$ ，‖為連結符號，並傳送 $s'$ 給顧客。顧客可

使用銀行之公開金鑰 $e^*$，檢查 $G(s \| a \| b \| c) = s'^{e^*} \bmod n^*$ 是否滿足，若滿足，則確定該訊息 $G(s \| a \| b \| c)$ 已由銀行所簽署。

(4) 消費及存款階段

顧客傳送 $(s', m, s, (a, b, c))$ 給商家為消費付款用，商家藉由檢查是否滿足 $s^e = H(m) \bmod n$ 和 $(s')^{e^*} = G(s \| a \| b \| c) \bmod n^*$ 來驗證電子現金的正確性，若滿足，則電子現金為正確，商家便回存該筆電子現金給銀行，銀行驗證 $s^e = H(m) \bmod n$ 和 $(s')^{e^*} = G(s \| a \| b \| c) \bmod n^*$，再確定是否為重複消費，若無，則將電子現金轉換為實體現金存入商家之帳戶。

從上述 Chang 等人所提出的四個階段中，我們可以看出在附加日期階段中，其日期資訊是任何人都可以得知的，這包含銀行本身。日期外曝的缺點是，它有可能讓顧客受到損失或傷害，例如，顧客向銀行提取電子現金時，此時若日期外曝的話，惡意人士若蓄意收集某銀行跟企業客戶電子現金提取交易的日期，而在企業客戶交易最頻繁的日期傳送大量封包使其交易產生延遲或中斷，如此將造成顧客損失。另外，銀行體系也可能因本身之利益而利用電子現金日期資訊私下控制利息之高低，這也會影響到顧客的利益。因此，我們在下一節中提出了隱藏式附加日期的觀念來解決 Chang 等人所提方法會讓日期外曝的缺失。

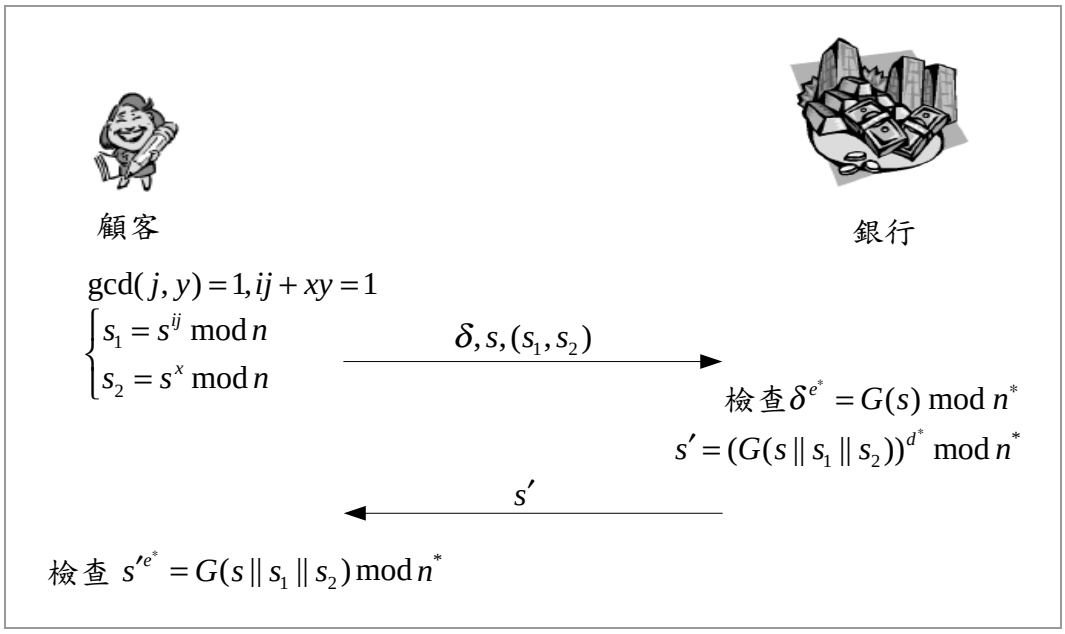
## 3. 隱藏式附加日期的電子現金付款機制

我們在此節中提出新的方法來改善 Chang 等人所提方法中會使日期外曝的缺點，我們的步驟分為四個階段：(1)初始階段、(2)提款及解盲因子階段、(3)隱密式附加日期階段及(4)消費及存款階段。其中初始階段、提款與解盲因子階段與 Chang 等人的方法相同，而隱密式附加日期階段及消費存款階段，如下所述：

(3) 隱密式附加日期階段

本階段運作流程如圖 2 所示。首先，顧客選取一個大質數 $j$、一個日期 $y_1$（例如為西元 2004 年 4 月 23 日，則 $y_1$ =200414123）及一亂數 $y_2$，令 $y = y_1 \| y_2$，滿足 $\gcd(j, y) = 1$，並經由歐幾里延伸定理（Extended Euclidean Algorithm）（Alfred, et. al., 1996），得到兩個唯一的整數 $i$ 和 $x$ 來滿足 $i \cdot j + x \cdot y = 1$。顧客計算 $s_1$ 及 $s_2$：

$$\begin{cases} s_1 = s^{ij} \bmod n \\ s_2 = s^x \bmod n \end{cases} \tag{1}$$




▲ 圖 2　隱藏式附加日期階段

並透過匿名通道傳送 $\delta$ 、$s$ 和 $(s_1, s_2)$ 給銀行，當銀行收到後，用其公開金鑰 $e^*$ 檢查是否滿足 $\delta^{e^*} = G(s) \bmod n^*$ ；若相等，銀行對 $s$ 和 $(s_1, s_2)$ 作簽章，$s' = (G(s \| s_1 \| s_2))^{d^*} \bmod n^*$ ，最後將 $s'$ 傳回給顧客。顧客收到 $s'$ 後，檢查是否滿足 $(s')^{e^*} = G(s \| s_1 \| s_2) \bmod n^*$ ；若相等，則顧客其電子現金已附加日期。值得注意的，顧客需在同一日內完成消費，如此才不致於造成計息的問題。

(4) 消費及存款階段

本階段運作流程如圖 3 所示。顧客傳 $(s', m, s, (s_1, s_2), y)$ 給商家，將所提取之電子現金付作為消費付款用，商家藉由檢查是否滿足下列等式，驗證電子現金的正確性：

$$(s_1 \cdot s_2^y)^e = H(m) \bmod n \tag{2}$$

$$(s')^{e^*} = G(s \| s_1 \| s_2) \bmod n^* \tag{3}$$

而 $y$ 中包含了日期 $y_1$ 及亂數 $y_2$ ，商家可從 $y$ 中的前六碼攫取出日期。最後，商家回傳 $(s', m, s, (s_1, s_2), y)$ 給銀行，銀行先驗證等式(2)及(3)是否滿足，再從 $y$

中攫取出日期，檢查該筆電子現金無重複消費，若其合法，則將電子現金存入商家之帳戶中。

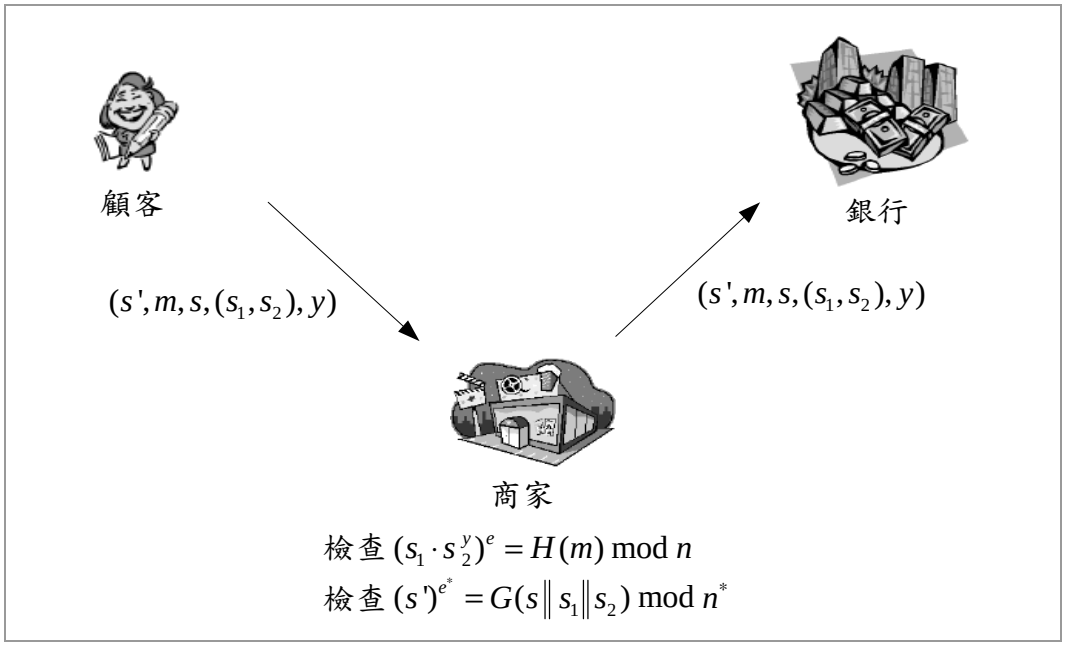



圖 3　消費及存款階段

等式(2)的正確性，可經由等式(1)，將等式(2)寫成

$$\begin{aligned}(s_1 \cdot s_2^{y})^{e} &= (s^{ij} \cdot s^{xy})^{e} \bmod n \\ &= (s^{ij+xy})^{e} \bmod n \\ &= (s)^{e} \bmod n \\ &= (H(m))^{de} \bmod n \\ &= H(m) \bmod n\end{aligned}$$

在隱密式附加日期階段中，任何人及銀行都無法從 $\delta$ 、 $s$ 和 $(s_1, s_2)$ 中，得知有關日期相關資訊，因為顧客的消費日期直到消費階段才曝露在外，因此可避免日期外曝的缺點。另外一方面，顧客也無法在隱藏式附加日期階段後，擅自修改日期。在消費及存款階段中，商店及銀行也無法在接受電子現金後私自竄改原有之日期。

## 4. 安全分析

本節所作的安全分析主要是以電子現金的使用特性，再加上本論文所提出的隱藏式附加日期方法為依據來進行安全分析。和 Chang 等人方法相同的，在初始階段、提取及解盲因子階段，我們使用 Chaum 的盲簽章來達到不可追蹤匿名之安全性，其安全性在於解兩質數相乘的因式分解之困難度。在盲簽章的過程中，分別有 $r_1$ 和 $r_2$ 盲因子，使銀行無法的知道其簽署的內容。接著，我們分別發動多個可能的攻擊來分析本文所提方法的安全性。

- **攻擊一**：在隱密式附加日期階段中，惡意攻擊者或銀行欲知道顧客所附加的日期。

  **分　析**：當惡意攻擊者由匿名通道上攔截到 $\delta$ 、$s$ 和 $(s_1, s_2)$ 後，雖然惡意攻擊者知道等式 $s_1 = s^{ij} \bmod n$ 和 $s_2 = s^x \bmod n$ ，但 $i$ 、$j$ 及 $x$ 為顧客所產生，且為私密值，惡意攻擊者並無法確實得知其附加日期為何。相同的，當銀行收到 $\delta$ 、$s$ 和 $(s_1, s_2)$ 後，在不知 $i$ 、$j$ 及 $x$ 的情況下，仍無法取得日期。另外一方面，惡意攻擊者或銀行試圖猜測日期為 $y_1'$ ，但 $y$ 不僅包含日期，也包含一亂數，因此，惡意攻擊者或銀行無法經由是否滿足 $s = s_1 \cdot s_2^{y_1'} \bmod n$ 或 $\delta^{e^*} = G(s_1 \cdot s_2^{y_1'}) \bmod n^*$ ，來驗證其猜測日期是否正確。

- **攻擊二**：在隱密式附加日期階段中，惡意攻擊者或銀行欲更改顧客所附加的日期。

  **分　析**：當惡意攻擊者由匿名通道上攔截到 $\delta$ 、$s$ 和 $(s_1, s_2)$ 後，將任意改成 $(s_1', s_2')$ 。當銀行收到 $\delta$ 、$s$ 和 $(s_1', s_2')$ 後，檢查是否滿足 $\delta^{e^*} = G(s) \bmod n^*$ ，其結果將會相等，銀行對 $s$ 和 $(s_1', s_2')$ 作簽章，$s' = (G(s \| s_1' \| s_2'))^{d^*} \bmod n^*$，最後將 $s'$ 傳回給顧客。顧客收到 $s'$ 後，檢查是否滿足 $(s')^{e^*} = G(s \| s_1 \| s_2) \bmod n^*$；而結果並不會相等。因此，顧客得知其附加的日期並不成功。然而要偽造 $s' = (G(s \| s_1 \| s_2))^{d^*} \bmod n^*$ ，相當於要破解 RSA 的簽章之困難度。

- **攻擊三**：在消費及存款階段中，商家欲更改顧客所附加的日期。

  **分　析**：商家收到 $(s', m, s, (s_1, s_2), y)$ ，欲竄改日期為 $y_1'$ 。因為商家可從 $y$ 中分別得到日期 $y_1$ 及亂數 $y_2$ ，在將 $y' = y_1' \| y_2$ 取代原本的 $y = y_1 \| y_2$ ，並傳送 $(s', m, s, (s_1, s_2), y')$ 給銀行。但當銀行驗證 $(s_1 \cdot s_2^y)^e = H(m) \bmod n$ 時，則無法通過。另外一方面，商家產生 $i' \cdot j' + x' \cdot y' = 1$ ，其中 $y'$ 包含了其欲更改的日期，並分別計算 $s_1' = s^{i'j'} \bmod n$ 和 $s_2' = s^{x'} \bmod n$ ，並將 $(s', m, s, (s_1', s_2'), y')$ 傳送給銀行。雖然銀行驗證 $(s_1 \cdot s_2^y)^e = H(m) \bmod n$

會通過，但驗證 $(s')^{e^*} = G(s \| s_1 \| s_2) \bmod n^*$ 則無法通過。

- **攻擊四**：在消費及存款階段中，顧客與商家欲共謀更改附加的日期。

  **分　析**：和分析攻擊三相同的，不論顧客、商家或共謀，都無法竄改日期，因為在隱密式附加日期階段中，銀行所產生的 $s'$ 已包含了原本的附加日期。因此，任何人都無法在隱密式附加日期階段後，更改其附加的日期。

## 5. 結論

由於電子商務的交易是一種全新的商業方式，交易主要是以電子化的形式進行，商家與顧客無法面對面的進行交易，所以顧客在網路上購買商品後，無法以傳統交易中現金的方式將貨款支付給商家，為了克服此種無法「一手交錢，一手交貨」的問題，線上電子付款的機制於焉產生。在眾多的線上電子付款系統中，電子現金付款系統是最為消費者喜愛與注意的，原因是它像紙鈔現金一樣，是一種無具名且可自由轉移的電子支付工具。

電子現金的安全性重點主要是建立在其匿名性消費與電子現金不被偽造上。目前電子現金的實作系統多是根據電子現金之父 David Chaum 於 1982 所提出的「盲目數位簽章」（Blind Digital Signature）理論實作而成的。然而，Fan 等人認為 Chaum 所提出的電子現金理論中無附加日期，這樣可能會讓使用者有重複消費的行為，以及使得關心利息的商家無從了解銀行是否正確計息等問題，於是他們提出在電子現金中加入日期資訊的方法來改善 Chaum 方法的缺點。接著 Chang 等人發現了幾個發生在 Fan 等人方法上的缺點，例如 Y2K、顧客與商家串謀等問題，進而提出改善的方法，使得附加日期更具彈性。然而，在 Chang 等人的方法中卻存在著日期外曝的疑慮，有關 Chang 等人方法的缺點我們已在本文第二節中詳加說明。

為了解決日期外曝的問題，我們提出一種在電子現金中隱藏附加日期的方法，此方法除了保有先前 Chang 等人方法的彈性日期外，也強化了顧客在消費時的不可追蹤性。在這個付款機制中，當消費者向銀行提取電子現金時之日期不會走漏，同時消費者在網路上向商店消費付款時，商家只可得知其日期但無法得知消費者是誰也無法偽造電子現金。

## 參考文獻

[1] 薛夙珍（1997），《電子商務付款系統之研究》，博士論文，國立交通大學資訊管理研究所。

[2] 郭木興（2003），《電子商務-觀念,策略與案例實作》，台北：學貫行銷出版。

[3] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone（1996）, *Handbook of*

*Applied Cryptography*, CRC Press.

[4] C. C. Chang and Y. P. Lai（2003）,“A flexible date-attachment scheme on e-cash”, *Computers & security*, vol.22, no.2, 160-166.

[5] C. I. Fan and C. L. Lei（1998）,“Low-computation partially blind signature for electronic cash”, *IEICE Transactions on Fundamentals of Electronics*, vol.E81-A, 940-949.

[6] C. I. Fan, W. K. Chen, and Y. S. Yeh（2000）,“Date attachable electronic cash”, *Computer Communications*, vol.23, 425-428.

[7] D. Chaum（1983）,“Blind signature for untraceable payment”, *Advances in Crytology'83*, 199-203.

[8] D. Chaum, A. Fiat, and M. Naor（1990）,“Untraceable electronic cash”, *Advances in Cryptology-CRYPTO'88*, 319-327.

[9] European Central Bank（1998）,“Report on electronic money”, http://www.ecb.int/home/html/lingua.en.html.

[10] M. Abe and E. Fujisaki（1996）,“How to date blind signature”, *Advanced in Cryptology-ASIACRYPT'96*, 244-251.

[11] M. S. Hwang, I. C. Lie, and L.-. Li（2001）,“A simple micro-payment scheme”, *International Journal Systems and Software*, vol.55, no.3, 221-229.

[12] Paul Nicholls（1998）,“Survey: Nine Out of Ten Want to Pay Bills On Internet”, http://www.internetnews.com/ec-news/article/0-1087-430561-00.html.

[13] “The Impact of Digital Money on the Current Financial Market and the conduct of Stabilization Policy”, http://knight.fcu.edu.tw/~d8655601/電子貨幣之前言及介紹.htm.