以行動代理人為基礎之整合電子付款的行動拍賣機制*

曹偉駿*　　蘇雍超　　劉經緯
大葉大學 資訊管理學系
***E-mail: wjtsaur@mail.dyu.edu.tw**

摘要

與日俱增的消費者期望著能透過手持行動裝置享受行動商務的各樣式服務。在電子商務中，電子拍賣是越來越普及與重要的線上交易活動之一，此外，運用代理人技術以協助拍賣雖已蔚然成風，但行動拍賣機制卻鮮少探討行動代理人機密資訊的防護，而且目前的電子拍賣機制之研究亦少有探討到拍賣後的付款機制。因此，本研究使用低運算量之『植基於 ECC 的自我認證公開金鑰密碼系統』，以設計出以行動代理人為基礎之整合式行動電子拍賣機制。藉由本機制將可降低拍賣與付款過程中，手持裝置的運算量與網路通訊的傳輸量。而在安全性方面，本研究藉由代理鑑別金鑰隱藏議價者的私鑰，改善過去使用行動代理人議價的安全拍賣機制所造成的問題，使其滿足日益發展的行動商務環境之安全需求，並克服手持裝置硬體先天上的限制，進而促使行動商務更加蓬勃發展。

關鍵詞：行動商務、行動代理人、電子付款、電子拍賣、橢圓曲線密碼系統(ECC)、自我認證公開金鑰密碼系統。

1. 前言

隨著近年來行動通訊的快速發展，行動電話已經成為現代人的基本配件，且有越來越多的消費者，使用具上網功能的可攜式行動通訊設備，也因而帶動了整體行動上網技術的發展，再加上行動裝置本身所具有的行動性與便利性，行動商務勢必將是未來的趨勢。在電子商務中，電子拍賣 [1-3, 6]是日益普及與重要的線上交易活動之一，目前許多學者也針對電子拍賣的安全性提出相關機制加以解決，然而這些機制仍然難以實現議價者與拍賣者在線上競標的即時溝通協議，是故，就有一些可藉由行動代理人協商的電子拍賣機制 [4, 10, 11, 14, 15]的衍生。這些代理人雖然可以協助議價者在拍賣平台進行議價，但相對的卻必須面對到其他安全問題，像是代理人會攜帶議價者的私鑰進行交易，而此方式將造成私鑰被代理人平台所利用，或代理人拍賣機制的不夠有效率等問題存在。拍賣機制除了上述問題以外，目前鮮有將電子付款 [5, 7, 8, 12]整合至拍賣機制中，以致於整個拍賣流程不夠便捷，進而影響行動商務的發展。因此，整合電子拍賣與電子付款於一機制中也是相當重要的議題。有鑑於此，本研究將針對以上所存在之問題加以研究探討之。

本研究目的是設計一套以行動代理人為基礎之整合式行動電子拍賣機制。本研究將使用低運算量之橢圓曲線密碼系統(ECC)建構相關安全機制，以克服手持裝置有限的運算能力。此外，再結合行動代理人的特性，由行動代理人代替行動裝置使用者進行自動化的議價，以減少手持裝置的負擔。最後，整合安全電子付款於行動拍賣流程中，以達到安全又有效率的行動拍賣與付款的單一過程，如此可滿足行動商務環境的需求，以及克服手持裝置先天的硬體限制。

2. 以行動代理人為基礎之整合式行動電子拍賣機制

本機制『以行動代理人為基礎之整合式行動電子拍賣機制』之流程被描述於圖 1 之中。此機制包含九個主要階段，以下將介紹每個階段的詳細流程：

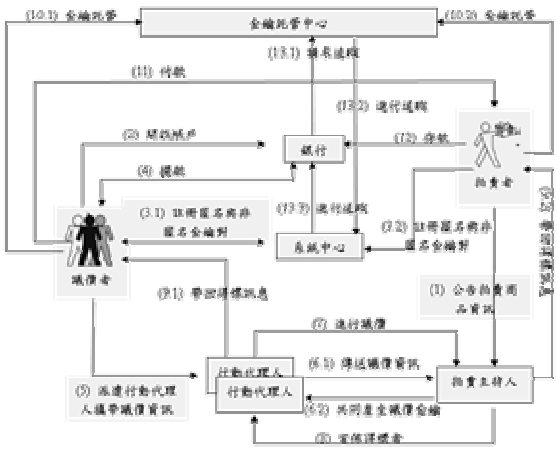

圖 1 以行動代理人為基礎之整合式行動電子拍賣流程

2.1 初始階段

*本研究接受國科會計畫案 NSC 93-2213-E-212-018, NSC-93-2622-E-212-005-CC3 資助，特此致謝。

在此階段中，系統中心會公佈如系統中心的公開金鑰，橢圓曲線方程式等資料。另外，拍賣者會向拍賣主持人公佈拍賣電子商品資訊，即圖 1 步驟 (1)。另外，欲參與拍賣之手持裝置使用者會向銀行要求開設一個帳戶，即圖 1 步驟 (2)。

➢ 系統所使用之參數如下：

1. CA、AM、A_k、U_i、MA_i、$KEA1$、$KEA2$、B：分別代表系統中心、拍賣主持人、拍賣者k、使用者i、使用者i的代理人、金鑰託管中心一、金鑰託管中心二與銀行。
2. Z：代表系統角色，$Z \in \{CA, AM, A_k, U_i, KEA2, KEA1, B\}$。
3. I_Z：角色Z的身份。
4. PS_Z：角色Z的匿名身份。
5. p：有限場的大小，而其長度為160 bits的大質數。
6. 位於 F_p 上的橢圓曲線 E：橢圓曲線方程式 $y^2 = x^3 + ax + b$，其中 $a,\ b \in F_p$ 且滿足 $4a^3+27b^2 \neq 0 \pmod p$。另外，其所有的點$(x, y)$位於橢圓曲線 E 而形成$E(F_p)$的集合，且包含一無窮遠點O，其中$x, y \in F_p$。
7. G：即序為n之橢圓曲線上的生成點，而n為長度160 bits的大質數。
8. s_Z：角色Z的私鑰，其中 $s_Z \in [2,\ n-2]$。
9. P_Z：角色 Z 的公鑰，其中系統中心的公鑰為 $P_{CA} = s_{CA} \cdot G$ （“ · ”表示一個數值乘上一個橢圓曲線上的點)。
10. $SK_{a,b}$：兩方通訊過程中共同使用的交談金鑰，可用來加、解密傳輸訊息。
11. $E_{SK_{a,b}}(M)$：使用 a 與 b 共同產生的交談金鑰，對訊息 M 加密，其密文為 CPT。
12. $h()$：單向雜湊函數(One-way hash function)，其輸出為一固定長度值 j，$j \in [2,\ q-2]$，而其長度為 160 bits。
13. w_Z：角色 Z 的公鑰證明(Witness)。
14. x_P：P 點的 x 軸座標。
15. y_P：P 點的 y 軸座標。
16. ||：訊息的連結符號。
17. N：使用者要求代理人 MA_i 議價的限制，其中包含商品的描述、最高容忍價格、每次出價的價差與出價最終時間等。
18. W：使用者授權給代理人 MA_i 的委任書，而此委任書內容包含代理人名稱、使用者匿名身份 I_{PS_i}、使用者匿名公鑰 P_{PS_i} 與指派時間等。
19. M：由拍賣主持人 AM 發給得標者的得標訊息，其訊息包含得標合約與時間郵戳，另外，得標合約則記載著得標商品名稱、得標價格與拍賣者身份等資訊。
20. $bid_{i,j}$：授權代理人MA_i在第j回合出價的價格。
21. c：電子現金。
22. ACC_Z：角色 Z 的帳戶號碼。
23. BB：拍賣電子公佈欄，由拍賣主持人 AM 所維護，參與競標的行動代理人可將議價資訊公佈於此電子公佈欄中。

➢ 系統所使用之資料庫與廢止清單如下：

C-DB：儲存所提領還沒有花費的電子現金的資料庫。PSD-DB：儲存使用者秘密金鑰 $\{(s_{U_i}, P_{U_i}), (s_{PS_i}, P_{PS_i})\}$ 及秘密資訊的資料庫。U-DB：儲存使用者身份以及銀行帳戶號碼的資料庫。W-DB：儲存提款(Withdrawal Transcripts)的資料庫。D-DB：儲存存款(Deposit Transcripts)的資料庫。P-DB：儲存尚未存款電子現金的付款資料庫。U-BL：記錄廢止的匿名公開金鑰。C-WL：記錄合法的電子現金。B-BL：記錄廢止的銀行公開金鑰。

2.2 註冊階段

凡是想要參加競標的參與者，必須在拍賣會開始之前，先向系統中心註冊競標者的匿名公鑰，以便取得對該拍賣物品的競標權、競標之匿名身分(pseudonym)、合法金鑰對與匿名金鑰對，即圖 1 步驟 (3.1)。其機制如下。

➢ 使用者 U_i 隨選一個亂數 $x_i, x_{PS_i} \in [2,\ n-2]$，且計算 $Z_i = h(x_i \| I_i) \cdot G$ 與 $Z_{PS_{U_i}} = h(x_{PS_{U_i}} \| I_{PS_{U_i}}) \cdot G$，並將自己的身分 I_{U_i}、$I_{PS_{U_i}}$、Z_i 與 $Z_{PS_{U_i}}$ 傳送給 CA。

➢ CA 選擇一個亂數 k_i, l_i，且計算使用者 U_i 的公鑰為 $P_{U_i} = Z_i + (k_i - h(I_{U_i})) \cdot G = (x_{P_{U_i}}, y_{P_{U_i}})$ 與公鑰證明 $w_{U_i} = k_i + s_{CA} \cdot (x_{P_{U_i}} + h(I_{U_i})) \pmod n$，而使用者 U_i 的匿名公鑰為 $P_{PS_{U_i}} = Z_{PS_{U_i}} + (l_i - h(I_{PS_{U_i}})) \cdot G = (x_{P_{PSU_i}}, y_{P_{PSU_i}})$ 與匿名公鑰證明 $w_{PS_{U_i}} = l_i + s_{CA} \cdot (x_{P_{PS_{U_i}}} + h(I_{PS_{U_i}})) \pmod n$，並儲存$\{P_{U_i}, w_{U_i}, I_{U_i}, P_{PS_{U_i}}, w_{PS_{U_i}}, I_{PS_{U_i}}\}$於 PSD-DB 中，之後，再傳送$\{P_{U_i}, w_{U_i}, P_{PS_{U_i}}, w_{PS_{U_i}}\}$給使用者 U_i。

➢ 使用者 U_i 計算自己的私鑰與匿名私鑰 $s_{U_i} = w_{U_i} + h(x_i \| I_{U_i}) \pmod n$ 與 $s_{PS_{U_i}} = w_{PS_{U_i}} + h(x_i \| I_{PS_{U_i}}) \pmod n$，並驗證公鑰的有效性是否成立：$s_{U_i} \cdot G = P_{U_i} + h(I_{U_i}) \cdot G + [(x_{P_{U_i}} + h(I_{U_i})) \bmod n] \cdot P_{CA}$ 與 $s_{PS_{U_i}} \cdot GP_{PS_{U_i}} + h(I_{PS_{U_i}}) \cdot G + [(x_{P_{PSU_i}} + h(I_{PS_{U_i}})) \bmod n] \cdot P_{CA}$，若驗證成功，則使用者 U_i 的公鑰對與匿名公鑰對分別是 (s_{U_i}, P_{U_i})，$(s_{PS_{U_i}}, P_{PS_{U_i}})$。

拍賣者產生金鑰對的方法與使用者方式相同，因此，可獲得 (s_{A_k}, P_{A_k})，$(s_{PS_{A_k}}, P_{PS_{A_k}})$，即圖 1 之步驟 (3.2)。此外，銀行、拍賣主持人與金鑰託管單位產生金鑰對的方法與上述註冊方式相同，但無

須註冊匿名金鑰對，因此，分別可獲得 (s_B, P_B)、(s_{AM}, P_{AM})、(s_{KEA1}, P_{KEA1}) 與 (s_{KEA2}, P_{KEA2})。

2.3 提款階段

當使用者要從事電子交易前，可透過手持裝置向銀行提領電子現金，並儲存在適用於手持裝置的智慧卡(smart card)中，即圖 1 步驟 (4)。手持裝置使用者執行以下步驟向銀行提領電子現金：

1. U_i 與 B 共同產生交談金鑰 $SK_{B,PS_{U_i}}$，以便在傳輸資料時供加/解密用。
2. U_i 選擇 c 並計算 $c' = h(x_{P_{PS_{U_i}}} \| c)$，將 $E_{SK_{B,PS_{U_i}}}(c', c)$ 傳給 B。
3. B 收到並解密後，隨機選取一個數 $u_B \in [2, n-2]$，並計算 $R_B^{'} = u_B \cdot G$，將 $R_B^{'}$ 傳給 Ui。
4. U_i 收到後隨機選取兩個數 a 與 b 並計算 $R_B = a \cdot R_B^{'} + b \cdot G = (x_{R_B}, y_{R_B})$, $F = h(x_{R_B} \| c \| x_{P_{PS_i}})$,與 $F^{'} = F / a$，並將 F'傳給 B。
5. B 收到 F'後，計算 $S_B^{'} = s_B \cdot F^{'} + u_B \pmod n$，並將 $S_B^{'}$ 傳給 U_i。然後 B 儲存 $I_{U_i}, c^{'}, S_B^{'}$ 在 W-DB 資料庫中，並從使用者帳戶中扣款。
6. U_i 收到 $S_B^{'}$ 後計算 $S_B = a \cdot S_B^{'} + b \pmod n$，$\sigma_B = (R_{U_B} \| S_B)$，並驗證 $S_B \cdot G = h(x_{R_B} \| c \| x_{P_{PS_{U_i}}}) \cdot V_B + R_B$，驗證式成立後，則儲存電子現金 $(c, \sigma_B, P_{PS_{U_i}})$ 在適用於手持裝置的智慧卡之 C-DB 資料庫中。

2.4 拍賣階段

在此階段中，手持裝置使用者會將所要競標的電子商品與拍賣需求資訊，經由行動代理人 MA_i 攜帶至拍賣網站平台，即圖 1 步驟 (5)與步驟 (6.1)，其資訊將用 Lin 等人的機制加以保護之。之後，MA_i 會與 AM 共同產生議價金鑰，即圖 1 步驟 (6.2)。MA_i 並藉此議價金鑰自動地提供每回合的議價資訊，直至拍賣過程結束，即圖 1 步驟 (7)。其流程如下：

➢ 拍賣設定

手持裝置使用者 U_i：

1. U_i 建立拍賣商品的需求限制，以侷限拍賣主持人的權限，並計算 $d = h(N)$，$D = d \cdot G = (x_D, y_D)$ 與 $f = h(W \| x_D \| TS)$
2. U_i 使用匿名私鑰計算 $r = d - f \cdot s_{PS_{U_i}} \pmod n$，並將需求資訊 (f, r, W, TS) 透過行動代理人 MA_i 攜帶至拍賣主持人 AM。
3. 當 AM 接收 MA_i 所攜帶的拍賣需求資訊 (f, r, W, TS) 後，將從 W 中取得 U_i 的匿名身份 I_{PS_i} 與匿名公鑰 P_{PS_i}，之後計算 $V_{PS_{U_i}} = P_{PS_{U_i}} + h(I_{PS_{U_i}}) \cdot G + [(x_{P_{PS_{U_i}}} + h(I_{PS_{U_i}})) \bmod n] \cdot P_{CA}$
4. AM 開始進行驗證 MA_i 的拍賣需求資訊 (f, r, W, TS) 是否為合法使用者 U_i 所要求，其作法如下。AM 首先檢查時間郵戳，以防止重送與偽冒攻擊，之後，計算 $D' = r \cdot G + f \cdot V_{PS_{U_i}} = (x_{D'}, y_{D'})$，以驗證 $h(W \| x_{D'} \| TS) = f$ 是否成立，若成立，則 (f, r, W, TS) 則是合法的拍賣需求資訊，反之，AM 將拒絕 MA_i 的拍賣需求。
5. AM 選擇一隨機亂數 $t \in [2, n-2]$，並計算 $E_i = t_i \cdot G$.
6. AM 透過 t_i 與 r，共同產生 MA_i 的議價金鑰 $Y_{U_i} = t_i + r + f \cdot s_{AM} \pmod n$，因此，在競標的過程中 MA_i 可藉由此議價金鑰出價。
7. AM 宣告新加入的競標者，並將其公開資訊 (f, D, W, TS, E_i) 公佈於 AM 所管理之拍賣電子佈告欄 BB。

➢ 代理人競標

MA_i 必須依照以下的出價步驟來參與拍賣的每個回合：

1. 首先，隨機選取一整數 $q_{i,j} \in [2, n-2]$，並選取適當的價格 $bid_{i,j}$ 作為第 j 回合的出價，之後，使用 Y_{U_i} 計算議價資訊的數位簽章：$Q_{i,j} = q_{i,j} \cdot G = (x_{Q_{i,j}}, y_{Q_{i,j}})$，$\lambda_{i,j} = h(x_{Q_{i,j}} \| bid_{i,j})$ 與 $\upsilon_{i,j} = q_{i,j} + \lambda_{i,j} \cdot Y_{U_i} \pmod n$
2. 公佈此回合的議價資訊 $\{bid_{i,j}, \lambda_{i,j}, \nu_{i,j}\}$ 於議價資訊電子公佈欄。

➢ 驗證競標資訊

當 MA_i 在議價資訊電子公佈欄公佈其議價資訊後，任一的其他的議價者皆可合法地驗證此議價資訊，首先，驗證者必須在拍賣電子布告欄，取出屬於 MA_i 的公開參數，並計算

$V_{AM} = P_{AM} + h(I_{AM}) \cdot G + [(x_{P_{AM}} + h(I_{AM})) \bmod n] \cdot P_{CA}$

$V_{PS_{U_i}} = P_{PS_{U_i}} + h(I_{PS_{U_i}}) \cdot G + [(x_{P_{PS_{U_i}}} + h(I_{PS_{U_i}})) \bmod n] \cdot P_{CA}$

$V_{PS_{U_i}, AM} = Y_{U_i} \cdot G = [(t_i + r + f \cdot s_{AM}) \bmod n] \cdot B$

$= E_i + D - f(V_{PS_{U_i}} + \cdot V_{AM})$

$Q_{i,j}^{'} = \upsilon_{i,j} \cdot G - \lambda_{i,j} \cdot V_{PS_{U_i}, AM}$ ，以驗證 $\lambda_{i,j} = h(x_{Q_{i,j}}' \| bid_{i,j})$，若此驗證式成立，則代表此議價資訊的確是由 MA_i 所提供。

2.5 宣佈階段

當最高的競標價格已經不再變動時，拍賣主持人會公告得標者資訊於得標電子公佈欄，即圖 1 步驟 (8)。讓參與競價者驗證競標過程的合法性，最後拍賣主持人會將唯一的得標合約 $M=(Cont \| TS)$ 使用鑑別加密，並藉由手持裝置使用者的行動代理人 MA_i 帶回至行動裝置使用者 U_i，即圖 1 步驟 (9.1)。之後，拍賣主持人也會將此 M 鑑別加密後傳送給拍賣者 A_k，即圖 1 步驟 (9.2)。其流程如下：

1. *AM* 公佈得標者資訊 $\{I_{PS_i}, bid_{i,\max}, Y_{U_i}\}$ 於得標電子公佈欄。另外，任一的驗證者皆可使用 Y_{U_i} 驗證
   $Y_{U_i} \cdot G = [(t_i + r + f \cdot s_{AM}) \bmod n] \cdot B = E_i + D - f(V_{PS_{U_i}} + V_{AM})$
2. *AM* 隨機選擇兩個整數 $\alpha, \beta \in [2, n-2]$，並按照以下步驟進行鑑別加密：
   $V_{PS_{U_i}} = P_{PS_{U_i}} + h(I_{PS_{U_i}}) \cdot G + [(x_{P_{PS_{U_i}}} + h(I_{PS_{U_i}})) \bmod n] \cdot P_{CA}$
   $T = \alpha \cdot G = (x_T, y_T)$，$\varepsilon = M \oplus h(x_T)$，
   $\theta = \alpha + h(\varepsilon) \cdot s_{AM} + Y_{U_i} \pmod n$，
   $C_1 = \beta \cdot G$，$H = \beta \cdot V_{PS_{U_i}} = (x_H, y_H)$，
   $C_2 = \varepsilon \oplus h(x_H)$
   AM 要求 MA_i 攜帶此鑑別加密訊息 $\{C_1, C_2, \theta\}$ 送回給行動裝置使用者。
3. 當 U_i 接收到 MA_i 帶回的訊息時，U_i 按照以下計算還原回契約 M：
   $H' = s_{PS_{U_i}} \cdot C_1 = (x_{H'}, y_{H'})$，$\varepsilon = C_2 \oplus h(x_{H'})$，
   $V_{AM} = P_{AM} + h(I_{AM}) \cdot G + [(x_{P_{AM}} + h(I_{AM})) \bmod n] \cdot P_{CA}$
   $V_{PS_{U_i},AM} = Y_{U_i} \cdot G = E_i + D - f(V_{PS_{U_i}} + V_{AM})$，
   $T' = \theta \cdot G - h(\varepsilon) \cdot V_{AM} - V_{PS_{U_i},AM} = (x_{T'}, y_{T'})$，
   $M = \varepsilon \oplus h(x_{T'})$
   另外，U_i 必須檢查此鑑別加密訊息是否包含有效的冗餘，若此冗餘為有效的，則此鑑別加密訊息 $\{C_1, C_2, \theta\}$ 也將是有效的訊息。

拍賣者 A_k 可收到同樣的訊息 M，以作為付款階段驗證之付款者是否為合法的得標者。

2.6 金鑰託管階段

此階段使用 Pedersen [9]提出之可驗證式秘密分享機制(Verifiable Secret Sharing, VSS) ，即當競標者付款前，必須將其部份秘密金鑰以及將拍賣者共同產生的交談金鑰託管至金鑰託管中心一(*KEA1*)與金鑰託管中二(*KEA2*)中，即圖 1 步驟 (10.1)與(10.2)。其詳細流程請參照 Pedersen 的機制 [9]。

2.7 付款階段

得標之手持裝置使用者經拍賣者確認後，會要求手持裝置使用者付款，手持裝置使用者就把從銀行提領的電子現金，傳送給拍賣者作付款的動作，即圖 1 步驟 (11)。此階段的所有傳輸資料將經由交談金鑰 $SK_{PS_{A_k},PS_{U_i}}$ 加密。其步驟如下：

1. 手持裝置使用者 U_i 與拍賣者 A_k 共同產生交談金鑰 $SK_{PS_{A_k},PS_{U_i}}$，以便在傳輸資料時供加/解密用，並託管此交談金鑰。
2. A_k 傳送加密後的電子商品 $E_{GK}(goods)$ 給 U_i，其中 *GK* 為加密電子商品的秘密金鑰，並只有 A_k 才擁有。
3. U_i 隨機選取一個數 $e_{U_i} \in [2, n-2]$ 並計算
   $R_{U_i} = e_{U_i} \cdot G = (x_{R_{U_i}}, y_{R_{U_i}})$
   $S_{U_i} = s_{PS_{U_i}} \cdot h(x_{R_{U_i}} \| c \| I_{PS_{A_k}} \| x_{P_{PS_{U_i}}} \| h(M)) + k_{U_i} \pmod n$
   $\sigma_{U_i} = (R_{U_i} \| S_{U_i})$
   將 $E_{SK_{PS_{A_k},PS_{U_i}}}(c, P_{PS_{U_i}}, \sigma_B, \sigma_{U_i})$ 傳送給 A_k
4. A_k 收到加密訊息，將解密還原出 $c, P_{PS_{U_i}}, \sigma_B, \sigma_{U_i}$ 後檢驗：
   假如 $P_{PS_{U_i}} \in$ U-BL，則拒絕電子現金 c；
   假如 $P_B \in$ B-BL 且 $h(x_{P_{PS_{U_i}}} \| c) \notin$ C-WL，則拒絕電子現金 c
5. 若上述的檢驗都沒問題，則驗證下面等式是否成立：
   $V_B = P_B + h(I_B) \cdot G + [(x_{P_B} + h(I_B)) \bmod n] \cdot P_{CA}$
   驗證 $S_B \cdot G = h(x_{R_B} \| c \| x_{P_{PS_{U_i}}}) \cdot V_B + R_B$
   $V_{PS_{U_i}} = P_{PS_{U_i}} + h(I_{PS_{U_i}}) \cdot G + [(x_{P_{PS_{U_i}}} + h(I_{PS_{U_i}})) \bmod n] \cdot P_{CA}$
   驗證 $S_{U_i} \cdot G = h(x_{R_{U_i}} \| c \| I_{PS_{A_k}} \| x_{P_{PS_{U_i}}} \| h(M)) \cdot V_{PS_{U_i}} + R_{U_i}$
   若等式都驗證成立的話，A_k 將 $(c, P_{PS_{U_i}}, M, \sigma_{U_i}, \sigma_B)$ 儲存在 P-DB 資料庫中，接受使用者的付款。
6. A_k 傳送電子商品之解密金鑰 $E_{SK_{PS_{A_k},PS_{U_i}}}(GK)$ 給 U_i

U_i 可透過 *GK* 解開 $E_{GK}(goods)$，以獲得電子商品。

2.8 存款階段

在此階段，拍賣者 A_k 會將收到的電子現金存入銀行的先前申請的帳戶中。首先，拍賣者將收到之電子現金傳送給銀行進行存款的動作，假如電子現金是合法的，銀行則將錢存入拍賣者的帳戶中，即圖 1 步驟 (12)。其步驟如下：

1. A_k 將電子現金 $(c, P_{PS_{U_i}}, \sigma_B)$ 傳送給銀行 B。
2. B 收到電子現金 $(c, P_{PS_{U_i}}, \sigma_B)$ 後，驗證下式 $S_B \cdot G = h(x_{R_B} \| c \| x_{P_{PS_{U_i}}}) \cdot V_B + R_B$，若等式成

立後，接著檢驗 c 不是已經存款過了，搜尋 D-DB 資料庫中，假如找到 $(c, P_{PS_{U_i}}, \sigma_B)$，則代表是重複存款。$B$ 在 D-DB 資料庫中找出相對應的 σ_B，並將其回傳給 A_k，並可要求 CA 協同找出重複存款或重複花費的使用者；如沒找到，則 B 傳給 A_k 一個有關電子現金 c 是合法的回應 $E_{SK_{A_k,B}}(succ)$。

3. A_k 再將 $E_{SK_{A_k,B}}(I_{PS_{A_k}}, ACC_{A_k}, \sigma_{U_i}, h(M))$ 傳給 B。
4. B 解密後再驗證下列等式是否成立。

$$S_{U_i} \cdot G = h(x_{R_{U_i}} \| c \| I_{PS_{A_k}} \| x_{P_{PS_{U_i}}} \| h(M)) \cdot V_{PS_{U_i}} + R_{U_i}$$

若成立後，銀行儲存 $(c, P_{PS_{U_i}}, I_{A_i}, \sigma_U, \sigma_B)$ 在 D-DB 資料庫中。

2.9 追蹤階段

若整個交易行為雙重花費、雙重存款、拍賣者哄抬價格、得標者降低價格或不承認此筆拍賣交易時，本機制可透過銀行、系統中心與金鑰託管中心的合作，以追蹤出濫用電子現金的使用者身份，即圖 1 步驟 (13.1~13.3)。其追蹤步驟如下：

➢ 使用者身份追蹤

1. 銀行 B_j 將 $(c, P_{PS_{U_i}}, \sigma_U, \sigma_B)$ 送給 CA。
2. CA 可利用 $P_{PS_{U_i}}$ 比對 PSD-DB 中找出 U_i 的真實身份 I_{U_i}，並告知 B 以便找出是誰超支花費。

➢ 違約交易追蹤

交易雙方若在付款階段企圖毀約降低價格、哄抬價格或不承認此筆拍賣交易時，任一方皆可要求拍賣主持人進行追蹤。首先，拍賣主持人持 CPT' 向 CA 申請解密，其還原流程請參照 Pedersen 的機制 [9]，進而追查是否拍賣者或得標者是否違約的情形發生，若有則將違約的一方記錄於 U-BL。

3. 安全性與功能分析

表一 電子英式拍賣功能之比較

	Yi 與 Siew 的機制 [15]	本機制
Anonymity		∨
No framing	∨	∨
Non-repudiation	∨	∨
Fairness	∨	∨
Public verifiability		∨
Efficiency of bidding		∨
One-time registration	∨	∨
Easy revocation	∨	∨
Attaining integrity and authenticity	∨	∨
Preventing the confidential information from leaking out	∨	∨
Ensuring mobile agent's security	∨	∨

從表一可得知，本機制可達到全部 11 項安全需求，Yi 與 Siew 的機制 [15]無法達到匿名性、公開驗證性、有效率的議價與使用有效率的密碼系統等需求。有鑑於此，本機制除了安全性考量還兼顧效率，因此更適用於行動電子英式拍賣的環境中。

表二 各種無線付款方法的比較

項目		Hu et al. scheme [5]	本機制
Security & Privacy	Cheating Possible	No	No
	Multiple Spending	No	No
	Stealing in Transit	No	No
	Anonymity	Yes	Yes
	User Tracing	No	Yes
	Message Recovery	No	Yes
System Flexibility	Cost Less Session Key	Yes	Yes
	Suitable for Mobile Telephones	Yes	Yes
	Vendor Specific	No	No
	Payment Mobility	Yes	Yes
	Auto Debiting of Unused Coins	Yes	No

在表二中，我們以安全性與隱私權以及系統彈性等類別，與 Hu 等人的機制 [5] 作一比較。其比較的類別乃採 Sandirigama 等人 [12]所提出的，是故，其項目可作為本研究評估的標準。安全性方面，本研究同樣地可以達到相同的安全等級，亦即提供匿名性與預防表二中所列的三項攻擊手法的功能。最後在系統彈性方面，雖然本機制在部分需求方面沒辦法達到，但本研究主要是提供較高效率與安全的付款程序，有鑑於此，本研究之付款機制將可有效率地克服行動裝置的限制，使得行動消費者更能安心且便捷地進行消費。

4. 結論

本研究以低運算量之『植基於 ECC 的自我認

證公開金鑰密碼系統』設計一套以行動代理人為基礎之整合式行動電子拍賣機制，使其安全且有效率地應用於行動商務環境。本機制除了採取低運算量的密碼系統，另外結合行動代理人的特性，由行動代理人代替行動裝置使用者進行自動化的議價，以減少手持裝置的負擔，克服了手持裝置有限運算能力的缺點；在安全性方面，本機制藉由代理鑑別金鑰隱藏議價者的私鑰，改善過去行動代理人議價機制所存在私鑰外洩的問題。因此，本機制不但改善了 Yi 與 Siew 機制之效率不彰的架構，也兼具高安全性。此外，本機制在電子付款方面，可追蹤出濫用電子現金的使用者身份與否認交易之證據回復的功能，以防止雙重花費、雙重存款等惡意交易行為，及追查拍賣者哄抬價格、得標者降低價格或不承認此筆拍賣交易等證據。有鑑於此，本機制將電子付款整合至拍賣機制中，可促使拍賣流程更佳便捷與完整，相信能為更多使用者所接受，進而促進行動商務的蓬勃發展。

參考文獻

[1] T.S. Chen, “An English Auction Scheme in The online transaction environment,” *Computers & Security*, Vol. 23, No. 5, pp. 389–399, 2004.

[2] C.C. Chang and Y.F. Chang, “Efficient anonymous auction protocols with freewheeling bids,“ *Computers & Security*, Vol. 22 No. 8, pp. 728–734, 2003.

[3] eBay, http://www.ebay.com.

[4] M. Gini, A. Jaiswal and Y. Kim, “Design and implementation of a secure multi-agent marketplace,“ *Electronic Commerce Research and Applications*, Vol. 3, No. 4, pp. 355–368, 2004.

[5] Z.Y. Hu, Y.W. Liu, X. Hu and J.H. Li, “Anonymous micropayments authentication (AMA) in mobile data network,” *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 2004.

[6] M.N. Huhns and J.M. Vidal, “Online auctions,” *IEEE Internet Computing*, Vol. 3, No. 3, pp. 103–105, 1999.

[7] M.A. Kim, H.K. Lee, S.W. Kim, W.H. Lee, and E.K. Kang, “Implementation of anonymity-based e-payment system for m-commerce,” *IEEE 2002 International Conference on Communication, Circuits and Systems and West Sino Expositions*, 2002.

[8] S. Kim and H. Oh, “An atomic micropayment system for a mobile computing environment,” *IEICE Transactions Information & Systems*, Vol.84, No. 6, 2001.

[9] T.P.Pedersen, “Distributed provers with applications to undeniable signature,” *Advances in Cryptology–EUROCRYPT’91*, LNCS, Vol. 547, pp. 221-238, 1991.

[10] T. Sandholm and Q. Huai, “Nomad: mobile agent system for an internet-based auction house,” *IEEE Internet Computing*, Vol. 4, No. 2, pp. 80–86, 2000.

[11] D.H. Shih, S.Y. Huang and D.C. Yen, “A new reverse auction agent system for m-commerce using mobile agents,” *Computer Standards & Interfaces*, Vol. 27, No. 4, pp. 383–395, 2005.

[12] M. Sandirigama, A. Shimizu and M.T. Noda, “Simple and secure coin (SAS-Coin)—a practical micropayment system,” IEICE Transactions Fundamentals, Vol.83, No.12, 2000.

[13] W.J.Tsaur, “Several security schemes constructed using ecc-based self-certified key cryptosystems,” *Applied Mathematics and Computation*, Available online 2004.

[14] M. Yokoo and K. Suzuki, “Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions,” *In Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems, 2002.*

[15] X. Yi and C. K. Siew, “Secure agent-mediated online auction framework,” *International Journal of Information Technology*, Vol. 7, No. 1, pp. 1–13, 2001.