四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

歐盟 81；2004/10/29；No. EP 04105426.3

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明總體上涉及安全訊息傳遞邀請架構（secure messaging invitation architecture），其用於移動裝置，如蜂窩電話、靈巧電話、個人資料助理（PDA）、尋呼機、手持電腦、具備電話功能的膝上型電腦以及其他移動電子裝置，更具體來說，本發明涉及一種用於移動裝置的對等即時訊息傳遞解決方案。

【先前技術】

即時訊息傳遞（IM）是這樣一種業務，即，其在另一人（如朋友或同事）在線時通知用戶並允許他們相互即時地發送訊息，而沒有電子郵件解決方案中所固有的存儲-轉發延遲。通過即時訊息傳遞，每個用戶都創建一個他或她希望聯絡的其他用戶的列表（通常被稱爲"夥伴列表"）。即時訊息傳遞伺服器跟蹤保持其多個用戶中的每一個的在線狀態（通常稱爲現狀資訊），當用戶的夥伴列表中的某個人在線時，該業務通知該用戶並使得可以與另一用戶進行即時聯繫。

IM解決方案倍加迅速，並且不僅可以應用于陸線環境，而且可以應用於移動裝置（如蜂窩電話、靈巧電話、個人資料助理（PDA）、尋呼機、具備電話功能的膝上型電腦以及其他移動電子裝置）所使用的無線環境。無線環境爲IM解決方案提供了強大的潛能，這取決於用戶隨身攜帶

他們的移動裝置的時間。可運行 IM 解決方案的可用移動裝置數量非常巨大。

公知的是，在現有技術中，將 IM 用戶端的移植到移動裝置，以獲得對衆多可用 IM 業務中的一個 IM 業務的訪問。這些業務包括 AOL 的即時信使（AIM）、ICQ、Yahoo！以及微軟的 MSN 信使產品。這些產品具有由各 IM 伺服器支撐的數千萬用戶，而且這些社團有時相互連接，從而產生了更大的社團。然而，陸線和臺式 IM 解決方案缺乏經常處於移動狀態的用戶所希望和需要的，即，只有在他們可以與他們的移動裝置在一起時的良好 IM 功能。此外，移動裝置的小屏面和記憶體往往使在試圖使用 IM 過程中的人們得到失望的體驗。這些人被迫接受現有 IM 解決方案的差性能和體驗，因爲他們想要或需要聯繫到操作傳統臺式 IM 解決方案的陸線用戶並且沒有其他可選途徑。因此需要一種爲毋線移動電子裝置設計的更好且更完善的訊息傳遞解決方案（與 IM 相似，其使得能夠進行即時訊息傳遞），其可以利用移動裝置的“始終在線”特性的優點。

現有 IM 應用的另一問題是缺乏安全性。通過現有 IM 應用，很容易共用用戶的身份，這意味著用戶身份可能在未經允許的情況下被廣泛地散佈因而用戶可能接收到來自未知或不希望的源的訊息。這導致垃圾訊息、兜售資訊（spam）、病毒的滋生，以及其他安全性問題。而且難以核實或認證啓始訊息傳遞的邀請源，這可能導致冒名頂替和相關安全性問題。

另一通用無線訊息傳遞標準是北美、尤其是歐洲、中國以及印度廣泛使用的短信業務（SMS）。該業務也存在很多缺陷。首先，必須通過每個 SMS 用戶的 MS-ISDN 或電話號碼對他們執行定址。該電話號碼極容易散佈，因此不可能核實發送方的真實性。其次，不存在隱身（implied presence）或任何實際傳送資訊，因此資訊交換存在與其相關聯的許多風險。而且 SMS 沒有永久持續的對話概念，實際上沒有 SMS 裝置可以保持有關與另一方進行的 SMS 對話的長期狀態資訊。

【發明內容】

本申請描述了一種用於在移動裝置之間提供即時對等訊息傳遞的系統和方法。該系統和方法通過保持系統中的每個移動裝置用戶的基本地址標識的秘密性，提供了增強的安全性。公開了一種邀請架構，其使得可以交換個人識別號碼（PIN）而不必要求用戶直接訪問或提供他的或她的 PIN。訊息傳遞應用在通過現有通信應用將其關聯 PIN 提供給位於另一移動裝置上的訊息傳遞應用之前對該 PIN 進行加密。該邀請架構自動管理該加密過程、任何必要密鑰交換、對邀請和接受訊息的編輯以及對 PIN 的解密和存儲。

在一個方面中，本申請提供了一種在第一移動裝置與第二移動裝置之間安全地交換個人識別號碼的方法。在包括無線網路和耦合到該無線網路的擇路伺服器的系統中使用這些移動裝置。每個移動裝置都具有一個或更多個通信應

用並且每個移動裝置還具有訊息傳遞應用。第一移動裝置具有第一個人識別號碼，第二移動裝置具有第二個人識別號碼。該方法包括以下步驟：對第一個人識別號碼進行加密；通過所述通信應用中的一個從第一移動裝置向第二移動裝置發送加密第一個人識別號碼；以及對該加密第一個人識別號碼進行解密並把該第一個人識別號碼存儲在第二移動裝置上的記憶體中。該方法還包括以下步驟：對第二個人識別號碼進行加密；通過所述通信應用中的一個從第二移動裝置向第一移動裝置發送加密第二個人識別號碼；以及對該加密第二個人識別號碼進行解密並把該第二個人識別號碼存儲在第一移動裝置上的記憶體中。在進行了這種 PIN 交換之後，通過訊息傳遞應用在第一移動裝置與第二移動裝置之間交換對等訊息。每個對等訊息都含有一個個人識別號碼，並且所述擇路伺服器根據這些個人識別號碼對各對等訊息進行擇路。

在另一方面中，本申請提供了一種對等訊息傳遞系統。該系統包括多個移動裝置、無線網路以及耦合到該無線網路的擇路伺服器。每個移動裝置都具有一個或更多個通信應用，並且每個移動裝置都包括用於存儲第一個人識別號碼的記憶體。每個移動裝置還包括訊息傳遞應用，其中，該訊息傳遞應用包括加密元件、解密元件、聯繫人管理元件以及訊息傳遞元件。加密元件用於對第一個人識別號碼進行加密，並用於通過所述通信應用中的一個把經加密的第一個人識別號碼嵌入到向另一移動裝置發送的訊息中。

解密元件用於通過所述通信應用中的一個從該另一移動裝置接收到來的訊息並用於對加密的第二個人識別號碼進行擷取和解密，其中，該到來的訊息包括加密的第二個人識別號碼。聯繫人管理元件用於通過所述通信應用中的一個對與另一移動裝置的邀請和接受的交換進行自動管理。訊息傳遞元件用於發送和接收對等訊息，由此對等訊息各包括一個人識別號碼，並且其中擇路伺服器根據個人識別號碼對這些對等訊息進行擇路。

在又一方面中，本申請提供了一種用於在無線網路上與其他移動裝置進行對等訊息傳遞的移動裝置。該無線網路包括擇路伺服器。該移動裝置包括：通信子系統，用於與該無線網路進行無線通信；記憶體，用於存儲第一個人識別號碼；以及連接到該記憶體和通信子系統的處理器，用於控制該通信子系統的操作。該移動裝置還包括：通信應用，用於編輯訊息並將其發送給其他移動裝置；和訊息傳遞應用。該訊息傳遞應用包括加密元件、解密元件、聯繫人管理元件以及訊息傳遞元件。加密元件用於對第一個人識別號碼進行加密，並用於通過所述通信應用中的一個把經加密的第一個人識別號碼嵌入到向另一移動裝置發送的訊息中。解密元件用於通過所述通信應用中的一個從該另一移動裝置接收到來的訊息並用於對加密的第二個人識別號碼進行擷取和解密，其中，該到來的訊息包括加密的第二個人識別號碼。聯繫人管理元件用於通過所述通信應用中的一個對與另一移動裝置的邀請交換和接受進行自動管

理。訊息傳遞元件用於發送和接收對等訊息，由此對等訊息各包括一個人識別號碼，並且其中擇路伺服器根據個人識別號碼對這些對等訊息進行擇路。

根據以下詳細說明和示出了一個或更多個實施例的附圖，本領域的技術人員將清楚本申請的其他方面和特徵。

【實施方式】

現在參照附圖，第 1 圖是使得能夠進行即時對等訊息傳遞的系統 5 的框圖。系統 5 包括多個移動站 10，如第 1 圖所示的移動裝置 10A 和 10B，其可以是任何類型的無線移動電子通信裝置，例如蜂窩電話、靈巧電話、個人資料助理（PDA）、尋呼機、手持電腦、具備電話功能的膝上型電腦。已知的是，每個移動裝置 10 都可以配備各種應用，這些應用包括但是不限於使得能夠與其他移動裝置 10 進行通信的一種或更多種現有應用，如無線電話應用、電子郵件應用、短信業務（SMS）應用、多媒體訊息傳遞業務（MMS）應用、增強型訊息業務（EMS）應用以及其他具備因特網功能的訊息傳遞應用（這裏把其中每一種應用都稱爲“現有通信應用”）。此外，每個移動裝置 10 都配備有用於實現這裏所描述的對等訊息傳遞解決方案的應用（這裏稱爲“訊息傳遞應用”）。這裏所使用的術語“應用”應當單獨或組合地包括一個或更多個程式、常式、子常式、函數調用或其他類型的軟體或固件等。系統 5 還包括無線網路 15，無線網路 15 可以是任何無線通信網路或互連網路的組合，

其包括但是不限於 Mobiltex™、DataTAC™、AMPS、TDMA、CDMA、GSM/GPRS、PCS、EDGE、UMTS 或 CDPD。已知的是，無線網路 15 包括多個基站，這些基站執行射頻（RF）協定以支援與移動裝置 10A 和 10B 進行資料和話音交換。擇路伺服器 20 耦合到無線網路 15。擇路伺服器 20 可以是能夠對資料分組進行擇路的任何類型的擇路設備，其包括但不限於 TCP/IP 路由器（如美國加利福尼亞州聖何塞市的 Cisco Systems, Inc.銷售的 TCP/IP 路由器）或網路位址轉換伺服器（NAT）。

系統 5 的每個移動裝置 10 都被指配並存儲有唯一的個人識別號碼（PIN）。在製造移動裝置 10 時或者通過其用戶身份識別模組（SIM）可以指配用於各移動裝置 10 的 PIN 並將其存儲在其中。將每個 PIN 映射到無線網路 15 上的對應移動裝置 10 的網路位址，該網路位址使得可以將資料擇路到移動裝置 10。擇路伺服器 20 包括一個或更多個用於根據該映射對由移動裝置 10 發送的訊息進行擇路的路由表。在一個示例性實施例中，該 PIN 實際上可以是網路位址本身，在另一示例性實施例中，該 PIN 可以是移動裝置 10 的電話號碼或移動裝置 10 的唯一 ID（如移動用戶 ISDN（MSISDN）），而網路位址可以是 IP 地址等。應當明白，這裏使用的術語“個人識別號碼”或“PIN”不應僅限於數位識別字，而應當被廣泛地理解，並可以包括可用於使得能夠進行對等訊息傳遞的字母識別字、二進位識別字或其他識別字。

爲了便於對兩個移動裝置 10 之間的對等訊息傳遞會話的建立和維護進行描述，參照第 1 圖所示的移動裝置 10A 和 10B。然而，應當理解，相同的描述適用於任何兩個移動裝置 10 之間的對等訊息傳遞會話。當移動裝置 10A 的用戶想要與另一移動裝置 10（如移動裝置 10B）建立對等訊息傳遞會話時，移動裝置 10A 使用移動裝置 10A 和移動裝置 10B 所共有的一個或更多個現有通信應用創建一邀請並將其發送給移動裝置 10B。優選地，使用在移動裝置 10A 的顯示器上爲用戶顯示的合適的功能表和/或對話方塊，通過對等訊息傳遞應用幫助並實現對該邀請的創建和發送。例如，在一個實施例中，用戶通過選擇與訊息傳遞應用相關聯的對話方塊或功能表中的邀請選項來啓始邀請。可以提示用戶提供用於通過現有通信應用對邀請進行擇路的地址資訊。例如，用戶可以提供與移動裝置 10B 相關聯的郵件位址。然後，訊息傳遞應用使得創建一電子郵件並通過電子郵件應用將其發送給移動裝置 10B。

每種情況下的邀請都由適合於特定現有通信應用的訊息（如電子郵件、SMS、EMS 或 MMS 訊息或無線電話呼叫）組成，其包括某種形式的請求，該請求涉及移動裝置 10B 的用戶是否想要接受該邀請並通過移動裝置 10B 和將該訊息標識爲邀請的指示符來建立與移動裝置 10A 的對等訊息傳遞會話，以進行對等訊息傳遞。該指示符可以包括使得移動裝置 10B 上的訊息傳遞應用能夠把訊息識別爲邀請的附件、嵌入文本或其他資料元素。將該訊息傳遞應用

設計成監視“收件箱”或注意接收與一個或更多個現有通信有關的訊息。具體來說，該訊息傳遞應用對到來訊息進行監視以確定這些訊息是否含有表示該訊息是對等訊息傳遞邀請的指示符。

當接收到這種邀請時，移動裝置 10B 上的訊息傳遞應用調用接受過程或常式。具體來說，該訊息傳遞應用通知移動裝置 10B 的用戶已接收到邀請並徵求來自用戶的針對是否應當接受邀請的輸入。該通知可以包括對移動裝置 10A 的用戶進行標識的資訊，如可從該邀請獲得的郵件地址或其他這種資訊。在一個實施例中，可以按對話方塊、功能表、彈出視窗或其他圖形用戶介面（GUI）的形式通過訊息傳遞應用把該通知呈現給移動裝置 10B 的用戶。在一個實施例中，通知視窗或介面可以包括可選按鈕或其他圖形輸入特徵，以允許移動裝置 10B 的用戶指示是否接受邀請。

如果移動裝置 10B 的用戶例如通過選擇 GUI 上的“接受”按鈕指示他或她接受該邀請因而希望建立對等訊息傳遞會話，那麼移動裝置 10B 上的訊息傳遞應用通過合適的現有通信應用使接受通信被發送給始發移動裝置 10A。例如，在一個實施例中，訊息傳遞應用使得創建一接受電子郵件並通過電子郵件應用發送它。將移動裝置 10A 上的訊息傳遞應用設計成識別對接受訊息（如接受電子郵件）的接收。

移動裝置 10A 和 10B 除了使用現有通信應用交換邀請和接受以外，或者與此相結合地，還交換 PIN。在一個實施

例中，與接受訊息一起發送移動裝置 10B 的 PIN。在一個實施例中，可以要麼與邀請訊息一起要麼在接收接受訊息之後與隨後的確認訊息一起發送移動裝置 10A 的 PIN。

根據本申請，儘管需要在移動裝置之間交換 PIN，但是保持了 PIN 的保密性和機密性。如果通過在不安全通道上發送用戶 PIN 而使得另一用戶普遍地可以獲得該用戶 PIN，那麼該另一用戶很容易與大範圍的用戶一起共用該 PIN 或者對於未授權接受方來說很容易截獲訊息並獲得該 PIN。大部分現有通信應用（如電子郵件）都使用不安全的信道。結果，移動裝置可能接收到來自獲得了該移動裝置的 PIN 的不希望的源的訊息。因此，在本申請所公開的多個實施例中按加密形式交換 PIN。

可以將加密 PIN 直接嵌入通過現有通信應用發送的訊息內或者可以將其附加到訊息中。例如，通過電子郵件應用，可以將加密 PIN 附加爲二進位文件。應當理解，附加有二進位文件的電子郵件可能在經過防火牆和垃圾郵件篩檢程式時會碰到問題。因此，在另一實施例中，將加密 PIN 直接嵌入電子郵件主體內。在該實施例中，電子郵件的閱讀者所看到的加密 PIN 是不可理解的文本符號序列，但是將訊息傳遞應用設計成對加密 PIN 進行擷取和解密。以下給出了涉及加密 PIN 的交換和相關密鑰管理以及密鑰交換操作的其他細節。

如將會理解的，一旦完成了上述步驟，移動裝置 10A 將具有移動裝置 10B 的 PIN，並且移動裝置 10B 將具有移

動裝置 10A 的 PIN。現在，如果移動裝置 10A 或 10B 希望向另一方發送對等訊息，那麼它使用對等訊息傳遞應用準備對等訊息，該對等訊息除待發送訊息資訊外，優選地在訊息頭中還包括接受方移動裝置 10（根據情況可以是 10A 或 10B）的 PIN。然後通過無線網路 15 由移動裝置 10 向擇路伺服器 20 發送該對等訊息。擇路伺服器 20 從該對等訊息獲得所述 PIN 並使用它以通過存儲於其中的擇路表確定接受方移動裝置 10（根據情況可以是 10A 或 10B）的網路位址，並使用確定的網路位址通過無線網路 15 將訊息發送給接受方移動裝置 10（根據情況可以是 10A 或 10B）。一旦接收到，就可以把該對等訊息（具體來說，包含在其中的訊息資訊）顯示給接受方移動裝置 10（根據情況可以是 10A 或 10B）的用戶。

下面參照第 5 圖，其示出了移動裝置 10 的示例實施例的框圖。在該示例實施例中，移動裝置 10 是具有資料並且可能還有話音通信能力的雙向移動通信裝置 10。在一示例實施例中，裝置 10 具有與因特網上的其他電腦系統進行通信的能力。根據裝置 10 提供的功能，在各種實施例中，該裝置可以是資料通信裝置、針對資料和話音通信設計的多模通信裝置、移動電話、具備無線通信能力的 PDA、或帶有無線數據機的電腦系統以及其他裝置。

裝置 10 包括通信子系統 111，通信子系統 111 包括接收機 112、發送機 114 及關聯元件，如一個或更多個（優選地，內嵌或內部的）天線單元 116 和 118，以及處理模組（如數

位信號處理器（DSP）120）。在某些實施例中，通信子系統包括本機振蕩器（LO）113，在某些實施例中，通信子系統111和微處理器138共用一振蕩器。通信領域的技術人員應當理解，通信子系統111的具體設計將取決於裝置10將運行於其中的通信網路。

把由天線116通過無線網路15接收的信號輸入給接收機112，該接收機112可以執行諸如信號放大、下變頻、濾波、通道選擇等的通用接收機功能，在某些實施例中，可以執行模數轉換。按類似方式，通過DSP 120對待發送信號進行例如包括調製和編碼的處理，並將其輸入給發送機114以進行數模轉換、上變頻、濾波、放大，並通過天線118在無線網路15上進行發送。

裝置10包括用於控制該裝置的整體操作的微處理器138。微處理器138與通信子系統111相交互，還與其他裝置子系統相交互，這些裝置子系統例如有圖形子系統144、快閃記憶體124、隨機存取記憶體（RAM）126、用戶身份識別模組（SIM）156、輔助輸入/輸出（I/O）子系統128、序列埠130、鍵盤或小鍵盤132、揚聲器134、麥克風136、短程通信子系統140以及通常被設計的任何其他子系統成142。圖形子系統144與顯示器122相交互並將圖形或文本呈現在顯示器122上。

在一個示例實施例中，在諸如快閃記憶體124或類似存儲單元的持久性記憶體中存儲有微處理器138所使用的作業系統軟體154和各種軟體應用158。本領域的技術人員應

當理解，可以將作業系統 154、軟體應用 158 以及它們的多個部分臨時載入到易失性記憶體如 RAM 126 中。可以設想，也可以將接收的通信信號存儲到 RAM 126。

微處理器 138 除了具有其作業系統功能以外，優選地，還使得能夠在該裝置上執行軟體應用 158。在製造過程中，可以在裝置 10 上安裝預定的一組通信應用 162。該通信應用 162 可以包括資料通信應用和/或話音通信應用。典型的資料通信應用可以包括用於允許用戶接收、閱讀、編輯以及發送文本型訊息的電子訊息傳遞模組。例如，該電子訊息傳遞模組可以包括電子郵件應用、SMS 應用、MMS 應用和/或 EMS 應用。還可以通過網路 15、輔助 I/O 子系統 128、序列埠 130、短程通信子系統 140 或任何其他合適的子系統 142 把其他軟體應用 158 和/或通信應用 162 載入到裝置 10 上，並由用戶將其安裝在 RAM 126 或非易失性記憶體中以由微處理器 138 來執行。應用安裝的這種靈活性增加了裝置 10 的功能性，並且可以提供增強的裝置上功能、通信相關功能或這兩者。

在資料通信模式中，將由通信子系統 111 來處理諸如文本訊息或網頁下載的接收信號並將其輸入給微處理器 138，優選地，微處理器 138 進一步處理接收信號以通過圖形子系統 144 將其輸出給顯示器 122，或者另選地輸出給輔助 I/O 裝置 128。裝置 10 的用戶還可以使用鍵盤 132 結合顯示器 122（可能還有輔助 I/O 裝置 128）在軟體應用 158 或通信應用 162 內編輯資料項目（例如，電子郵件訊息）。

然後可以通過通信子系統 111 在通信網路上發送這種編輯項。

通常在希望其可以與用戶的臺式電腦（未示出）同步的個人資料助理（PDA）型通信裝置中實現第 5 圖所示的序列埠 130，但是這是個可選裝置元件。這種埠 130 使得用戶可以通過外部裝置或軟體應用設置個人偏好（preference），並且其通過提供經由無線通信網路以外的到裝置 10 的資訊或軟體下載，將擴展該裝置的能力。

短程通信子系統 140 是可以提供裝置 10 與不同系統或裝置（其不必是類似的裝置）之間的通信的其他元件。例如，子系統 140 可以包括紅外裝置和相關電路和元件或 Bluetooth™ 通信模組，以提供與具備類似功能的系統和裝置之間的通信。裝置 10 可以是手持裝置。

裝置 10 還包括訊息傳遞應用 160。訊息傳遞應用 160 包括監視元件、邀請元件以及接受元件，可以把它們一起稱爲聯繫人管理元件。該聯繫人管理元件的作用是建立聯繫人或“夥伴”關係，即，根據對新聯繫人的邀請和接受的發送或接收更新和維護聯繫人資訊。訊息傳遞應用 160 還包括用於使用該聯繫人資訊執行對等訊息傳遞的訊息傳遞元件。

把與移動裝置 10 相關聯的 PIN 存儲在記憶體中。例如，可以將其存儲在 SIM 156、RAM 126、固件或其他裝置中。存儲在裝置 10 上的記憶體中的還有與訊息傳遞應用 160 相關聯地使用的聯繫人資訊。該聯繫人資訊含有聯繫人名稱

和相關 PIN。

訊息傳遞應用 160 的邀請元件編輯邀請並將其發送給預期的聯繫人。裝置 10 的用戶指示訊息傳遞應用 160 向另一裝置發送邀請。該用戶可以提供用於到達其他裝置的位址，如電子郵件位址。邀請元件通過所述多個通信應用 162 中的一個生成並發送邀請訊息，如電子郵件申請。

訊息傳遞應用 160 的監視元件監視對來自另一移動裝置 10 的邀請訊息的接收。例如，監視元件可以監視電子郵件應用的收件箱以評估任何接收訊息是否是訊息傳遞邀請。訊息傳遞邀請可以包括用於表示其爲訊息傳遞邀請的預定義文本、代碼或某些其他資料要素。如果監視元件識別出邀請，那麼它可以通知用戶並提示用戶接受或拒絕該邀請。例如，監視元件可以顯示對話方塊或彈出視窗，其示出了與邀請發送方有關的資訊並爲用戶提供了選項，如“接受”和“拒絕”按鈕。如果用戶表示接受該邀請，那麼觸發接受元件。

接受元件通過所述多個通信應用 162 中的一個（如電子郵件應用）自動生成並發送接受訊息。

訊息傳遞應用 160 包括用於執行加密、解密以及相關密鑰管理功能以交互 PIN 的元件。可以將這些元件設置爲邀請和接受元件的一部分或設置爲與其相交互的獨立元件。這些元件對以下功能進行管理：對駐留 PIN 的加密、對任何所需密鑰值或會話密鑰的生成或計算、通過所述多個通信應用 162 中的一個把加密 PIN 附加或嵌入到發送訊息

中、以及對通過所述多個通信應用 162 中的一個從其他移動裝置 10 接收的加密 PIN 的解密。以下給出了與在邀請架構環境中的加密、解密以及密鑰交換有關的其他細節。

再次參照第 1 圖。在一個實施例中，使用多個現有通信應用在多重通信路徑上發送如上所述的邀請可以增強對等訊息傳遞中的安全性。如將理解的，每個通信路徑都將確認邀請發送方的不同位址標識，因此有助於確認邀請的真實性。例如，移動裝置 10A 的用戶通過使用電子郵件應用和 SMS 應用發送如上所述的邀請可以希望與移動裝置 10B 的用戶建立對等訊息傳遞會話。在此情況下，當移動裝置 10B 接收到該邀請訊息時，移動裝置 10B 的“收件箱”等將顯示來自移動裝置 10A 的兩條訊息，即，電子郵件邀請和 SMS 邀請。當這些訊息到達時，移動裝置 10B 的用戶可能正在使用移動裝置 10B 的任何應用（如日曆應用、地址簿應用、瀏覽器應用或電話應用）進行工作，或者當前根本不在使用移動裝置 10B（儘管它是打開的）。按與移動裝置 10B 接收的任何其他訊息相同的方式（例如，通過發出嘟嘟聲和/或振動）向用戶通知邀請訊息的到達。當移動裝置 10B 的用戶打開這兩條訊息中的任何一條時，將調用對等訊息傳遞應用以處理該訊息。通過爲每條邀請訊息配備任何形式的特殊指示符（用於指示這是對等訊息傳遞會話的邀請）並通過對該對等應用進行編程以針對這種指示符監視所有到來訊息，可以實現對該對等訊息傳遞應用的自動調用。此外，每個邀請訊息在對等訊息傳遞應用中被創

建時都包括被發送的邀請訊息（在不同路徑上）的數量的表示。在使用多個路徑的情況下，如在本示例中，對等訊息傳遞應用接著針對其他邀請訊息掃描“收件箱”等。例如，如果首先打開電子郵件邀請訊息，則對等訊息傳遞應用將針對 SMS 邀請訊息掃描“收件箱”等。如上所述，可以通過設置於其中的特殊指示符識別邀請訊息。在發現其他邀請訊息之前，本實施例中的對等訊息傳遞應用不會爲移動裝置 10B 的用戶提供接受邀請的能力。一旦發現其他邀請訊息，移動裝置 10 的用戶就可以如上所述地接受邀請、拒絕邀請或推遲對接受或拒絕的決定。

下面參照第 4 圖，其示出了用於通知用戶訊息傳遞邀請接收的圖形用戶介面 200 的示例實施例。圖形用戶介面 200 包括覆蓋或層疊在收件箱顯示幕面 202 的頂部上的彈出對話方塊 204。第 4 圖所示的彈出對話方塊 204 顯示了發送方的名稱、時間、日期並確認在發送邀請時使用了多個路徑（其提供了關於源的某些真實性）。彈出對話方塊 204 還向用戶呈現 3 個可選按鈕，它們對應於接受邀請、拒絕邀請以及延遲決定接受還是拒絕邀請的選項。

再次參照第 1 圖和 5。如上所述，在本申請所述的邀請架構中，使用所述多個現有通信應用中的一個秘密地交換移動裝置 10 的相應 PIN。發送移動裝置在使用該通信應用發送其 PIN 之前對它進行加密。在接收移動裝置處，對接收加密 PIN 進行解密。通過合適的密鑰管理，把對未加密 PIN 的訪問限制於相應兩個移動裝置上的訊息傳遞應用。

存在許多可以用於本申請範圍內的各種實施例的加密和密鑰管理技術。而且，可以結合密鑰值一起使用以把 PIN 轉換成加密 PIN 的具體變換或功能可以包括寬範圍的密碼變換或功能。本領域的技術人員將理解，寬範圍的這種功能是公知的，並且可以針對處理能力和與具體應用或系統相關聯的任何時間約束選擇這種功能。

在一個實施例中，訊息傳遞應用 160 使用對稱加密。對稱加密是這樣一種密碼技術：其中，在密鑰對中，在計算上很容易根據一個密鑰確定另一密鑰。在大部分對稱加密方案中，密鑰是相同的。對稱加密依賴於密鑰的秘密性。因此，通常安全地分發密鑰對，並且不在不安全通道上分發。在一個實施例中，移動裝置 10A 的用戶使用相對安全的通道（如話音通道）向移動裝置 10B 的用戶提供密鑰值或種子值，根據該密鑰值或種子值可以導出密鑰。例如，第一用戶可以向第二用戶提供第二用戶在被提示時輸入到移動裝置 10B 中的口令或密碼，。可以結合演算法使用該口令或密碼作爲種子值以計算出用於加密或解密通信的密鑰。

在另一實施例中，訊息傳遞應用 160 使用公鑰加密術。公鑰加密術是這樣一種具有加密變換和解密變換的密碼技術，其中，根據加密變換在計算上確定解密變換是不可行的。換句話說，該加密功能是提供輸出密文的陷阱門（trap-door）單向功能。即使知道該密文和加密密鑰，也無法確定解密密鑰因而無法獲得未加密內容。

公鑰加密術通過使每個移動裝置10生成公鑰-私鑰對來起作用。各裝置共用其公鑰但是保護其私鑰的秘密性。其他裝置可以使用第一裝置的公鑰對針對該第一裝置的訊息進行加密，只有第一裝置能夠對該訊息進行解密，這是因爲只有第一裝置具有對應的私鑰。

在這裏所描述的訊息傳遞系統的環境下，訊息傳遞應用160包括用於對密鑰對生成和密鑰交換進行管理的元件。可以根據隨機種子值（例如，時間和日期或其他僞隨機種子）生成密鑰對。通過所述多個通信應用 162 中的一個把各移動裝置 10 的公鑰傳送給其他移動裝置 10。例如，可以將公鑰值嵌入或附加到從一個移動裝置 10A 發送給其他移動裝置 10B 的電子郵件中。在某些實施例中，啓始移動裝置 10A 上的訊息傳遞應用 160 將其公鑰 K_a 嵌入或附加到向接收移動裝置 10B 發送的邀請訊息中。接收移動裝置 10 接著將其公鑰 K_b 嵌入或附加到向啓始移動裝置 10A 發送的接受訊息中。在一個實施例中，由訊息傳遞應用 160 用以實現邀請和接受過程的通信應用 162 是電子郵件應用。在這種實施例中，可以將公鑰附加到電子郵件作爲二進位文件。另選地，可以把它們嵌入電子郵件文本的主體中。本領域的技術人員應當熟悉把公鑰資料附加或嵌入到現有通信應用訊息中的可能性範圍。

下面參照第 6 圖，其按流程圖形式示出了一種用於在移動訊息傳遞系統中安全地交換 PIN 的方法 300。第 6 圖所示的方法 300 涉及使用公鑰加密方案的實施例。

方法 300 始於步驟 302，其中通過第一裝置 10A（第 1 圖）的訊息傳遞應用 160（第 5 圖）生成第一公鑰-私鑰對 E_A、D_A。可以由裝置 10A 爲裝置 10A 所發送的每個邀請生成密鑰對，或者可以只生成一次密鑰對，或者只周期性地生成密鑰對，並且可以將其用於一個以上的邀請訊息傳遞過程。

在步驟 310 中，第二裝置 10B 生成第二公鑰-私鑰對 E_B、D_B。與步驟 302 相同，可以針對每個接收邀請重新執行步驟 310，或者計算一次（或周期性地計算），並將其用於一個以上的邀請訊息傳遞過程。應當理解，可以把裝置 10 所生成的公鑰-私鑰對 E、D 用於啓始裝置對邀請的發送過程或用於接收裝置對邀請的回應過程。在某些實施例中，離線生成密鑰對並在製造或配置時將其存儲在裝置 10 中。

裝置 10A 的用戶通過向訊息傳遞應用 160 提供邀請命令觸發邀請過程。可以由用戶從功能表選擇該邀請命令。可以要求用戶提供該邀請的期望接收方的地址或其他的聯繫人資訊。邀請命令調用訊息傳遞應用 160 的邀請元件，該邀請元件在步驟 304 中編輯邀請訊息。通過所述多個通信應用 162 中的一個，如電子郵件應用，編輯該訊息。訊息傳遞應用 160 確保所編輯的訊息包括一指示符，該指示符用於告訴接收移動裝置 10B 上的訊息傳遞應用 160 該訊息是邀請的事實。

在步驟 306 中，訊息傳遞應用 160 把第一公鑰 E_A 附加

或嵌入到所編輯的邀請訊息中。在一個實施例中，該訊息是電子郵件訊息，並將第一公鑰 E_A 插入該電子郵件訊息的文本主體中以使得該訊息能夠通過防火牆和垃圾郵件篩檢程式。

在步驟 308 中，通信應用把邀請訊息發送給接收移動裝置 10B。在接收移動裝置 10B 處，該訊息出現在通信應用的“收件箱”中。在接收到該邀請訊息時或者一旦用戶打開該邀請訊息，訊息傳遞應用 160 的監視元件將其識別爲邀請。因此，在步驟 312 中，觸發訊息傳遞應用 160。

在步驟 314 中，訊息傳遞應用 160 詢問用戶以確定用戶希望接受邀請還是拒絕該邀請。如果用戶拒絕該邀請，那麼方法 300 結束。如果用戶接受該邀請，那麼在步驟 316 中訊息傳遞應用 160 從邀請訊息擷取出第一公鑰 E_A。在步驟 318 中，訊息傳遞應用 160 接著根據預定加密變換或功能使用擷取的第一公鑰 E_A 對第二移動裝置 10B 的 PIN(即，PIN_B）進行加密。在步驟 320 中訊息傳遞應用 160 接著通過所述多個通信應用 162 中的一個（如電子郵件應用）編輯用於發送的接受訊息。該接受訊息包括加密 PIN_B 和第二公鑰 E_B。可以將加密 PIN_B 和第二公鑰 E_B 嵌入或附加到接受訊息中。然後在步驟 322 中把該接受訊息發送給第一移動裝置 10A。

第一移動裝置 10A 上的訊息傳遞應用 160 在接收該接受訊息時或在用戶打開該接受訊息時識別出該訊息，並在步驟 324 中從該接受訊息擷取出第二公鑰 E_B。在步驟 326

中，訊息傳遞應用 160 根據預定加密變換或功能對啓始移動裝置 10A 的 PIN（即，PIN_A）進行加密。在步驟 328 中訊息傳遞應用 160 接著通過所述多個通信應用 162 中的一個（如電子郵件應用）編輯用於發送的確認訊息。該確認訊息包括加密 PIN_A，可以將加密 PIN_A 嵌入或附加到確認訊息中。然後在步驟 330 中把該確認訊息發送給第二移動裝置 10B。

如步驟 332 和 334 所示，各移動裝置 10 分別使用其私鑰 D_A、D_B 對其所接收的加密 PIN 進行解密。然後裝置 10 與其他裝置 10 的用戶的聯繫人資訊相關聯地存儲該解密 PIN。因此，其他裝置 10 的用戶現在是訊息傳遞應用 160 所使用的“夥伴列表”或聯繫人列表的一部分。現在，使用訊息傳遞應用來編輯包括其他用戶的 PIN（用於進行擇路）的訊息，可以從一個用戶直接向另一用戶發送訊息。

在又一實施例中，訊息傳遞應用 160 使用 Diffie-Hellman 密鑰協定建立在兩個移動裝置 10 之間共用的秘密密鑰。該協定需要兩個參數 p 和 g，其中 p 是質數，g 是小於 p 的數，它們具有這樣的性質：對於在 1 與 p-1 之間（包括 1 和 p-1）的每個數 n，存在 g 的 k 次冪使得 $n=g^k \bmod p$。在本申請的對等訊息傳遞系統中的訊息傳遞應用 160 的環境下，第一訊息傳遞應用生成私有值 a 和公有值 $g^a \bmod p$，其中 a 爲從 1 到 p-2 選擇的整數。第二訊息傳遞應用生成其自己的私有值 b 和公有值 $g^b \bmod p$，其中 b 爲從 1 到 p-2 選擇的整數。如上結合第 5 圖所述，訊息傳遞應用交換公有值，然後根

據關係式 $k=g^{ba}=(g^a)^b \bmod p$ 計算出共用會話密鑰 k。

在又一實施例中，本申請的邀請架構包括口令型認證過程。從第一移動裝置向第二移動裝置發送的邀請包括一問題。呈現給第二移動裝置的用戶的 GUI 對話方塊包括該問題的顯示並爲用戶提供了選擇或提交答案的機會。與從第二裝置向第一裝置發送的接受訊息一起發送該問題。第一裝置對包含在接受訊息中的答案與存儲在第一移動裝置處的正確答案進行比較以驗證第二移動裝置用戶的身份。第一移動裝置的用戶可以通過另選通信應用（如通過話音呼叫）爲第二移動裝置的用戶提供正確答案。口令型認證過程提供了用於確保在正確的多方之間建立訊息傳遞關係的增強的安全性。

再次參照第 1 圖。根據本申請的另一方面，各移動裝置 10 的對等訊息傳遞應用包括聯繫人資料庫，該聯繫人資料庫存儲另一移動裝置 10 的每個用戶的姓名和/或其他識別資訊以及對應的 PIN，移動裝置 10 的用戶通過對等訊息傳遞應用與該另一移動裝置 10 的用戶通信或者可能希望進行通信。因此該聯繫人資料庫類似于作爲 IM 應用的一部分的“夥伴列表”。每當用戶與另一用戶建立對等訊息傳遞會話時，就可以將用戶和 PIN 資訊添加並存儲到該聯繫人資料庫中。用戶也可以從聯繫人資料庫有選擇地刪除條目。第 2 圖是移動裝置 10 的顯示器的一部分的圖，其示出了作爲對等訊息傳遞應用的一部分的示例性聯繫人資料庫屏面 25 並顯示了存儲在該聯繫人資料庫中的聯繫人的列表 30。

如在第 2 圖中看到的，聯繫人資料庫屏面 25 還提供了列表 30 所列出的每個聯繫人的狀態資訊 35，該狀態資訊 35 涉及特定聯繫人參與對等訊息傳遞會話的可能的可聯繫性，這被稱爲“隱性可聯繫性”。以下對該可聯繫性資訊進行更詳細的討論。

根據本申請的再一方面，每個移動裝置 10（爲清楚起見，稱爲“第一移動裝置 10”）周期性地（例如每 10 分鐘，以使資料流程量最小化）使用在第一移動裝置 10（爲清楚起見，稱爲“其他移動裝置 10”）的聯繫人資料庫中列出的多個用戶中的每一個的存儲 PIN 通過無線網路 15 和擇路伺服器 20 向這些用戶中的每一個的移動裝置 10 發送與其有關的可聯繫性資訊。在一個具體實施例中，如果任何其他移動裝置 10 關機或在覆蓋範圍之外，則擇路伺服器 20 把預留給這種其他移動裝置 10 的多個可聯繫性資訊訊息排成佇列，並且一旦該其他移動裝置 10 打開或回到覆蓋範圍內就傳送這些可聯繫性資訊訊息。根據第一移動裝置 10 的當前操作狀態得出該可聯繫性資訊（其隨時間變化）。可聯繫性資訊旨在提供對第一移動裝置 10 的用戶活動的表示，以爲聯繫人資料庫中的其他移動裝置 10 的各個用戶提供這樣的估計，即，第一移動裝置 10 的用戶有多大可能讀到並回復發送給第一移動裝置 10 的用戶的對等訊息。因而，由於系統 5 中的所有移動裝置 10（除非如下所述地被禁用了）都把它們的可聯繫性資訊發送給它們的所有聯繫人，因此應當理解，系統 5 中的每個移動裝置 10 都具有其聯繫人資

料庫中的其他用戶中的每一個的可聯繫性資訊。結果，任何移動裝置 10 的用戶都可以查詢在移動裝置 10 的聯繫人資料庫中列出的任何聯繫人的可聯繫性資訊，以得到關於特定聯繫人是否可能接收到對等訊息並對其作出反應的意見，該資訊可能影響關於到底發送對等訊息與否的決定。

可聯繫性資訊可以由通用狀態指示符組成，如：“可聯繫”，例如表示移動裝置 10 開機並在無線網路 15 的範圍內並且不在使用可能阻止對等訊息被收到的應用（如正在通過電話應用進行電話呼叫）；或“不可聯繫”，例如表示移動裝置 10 關機或在無線網路 15 的範圍以外。此外，可聯繫性資訊可以涉及移動裝置 10 的特定狀態或正在發生的事件，如由置於移動裝置 10 中的日曆應用的條目所指示的不理睬來電呼叫、用戶將移動裝置 10 關機、第一移動裝置 10 正在進行當前電話呼叫、第一移動裝置 10 的用戶正在開會，或者移動裝置 10 的用戶當前正在使用對等訊息傳遞應用。如將理解的，可以將可聯繫性資訊關聯到移動裝置 10 的每個動作和/或在移動裝置 10 內可提供的每條資訊，並可以從中得到該可聯繫性資訊，並且以上列出的具體示例僅爲示例性的而非限制性的。此外，根據與移動裝置 10 的特定狀態和/或在其上發生的事件有關的資訊，通用狀態指示符可以包括可聯繫性的多個級或程度。在這種情況下，可以按表示各種可聯繫性級或程度的標度報告可聯繫性資訊，如“可聯繫-1 級”、“可聯繫-2 級”等。此外，如果移動裝置 10 的給定用戶不希望如此密切地跟蹤他們的可聯

繫性，他們可以選擇性地防止他們的移動裝置 10 發送可聯繫性資訊。

第 3 圖是移動裝置 10 的顯示器的一部分的圖，其示出了構成對等訊息傳遞應用的一部分的示例性狀態屏面 40。狀態屏面40是對等訊息傳遞應用的主屏面並爲移動裝置10的用戶提供了與對等訊息傳遞應用有關的整體狀態資訊。具體來說，狀態屏面 40 提供了有關各種組的資訊，這些組包括當前對話組 45、阻止通信人組 50 以及挂起（pending）對話組 55。當前對話組 45 列出並提供了與所有對等訊息傳遞會話（也被稱爲對話，移動裝置 10 正在參與該對話）有關的資訊。當前對話是指：移動裝置 10 已向另一移動裝置 10 發送如上所述的邀請並接著接收到如上所述的接受訊息；或者另一移動裝置 10 已向移動裝置 10 發送如上所述的邀請並且移動裝置 10 以如上所述的接受訊息作爲回應。阻止通信人組 50 提供了其他移動裝置 10 的這種用戶的列表，即，移動裝置 10 的用戶不再希望接收到來自這些用戶的對等訊息，他們的訊息將被阻止並且不會顯示給用戶。優選地，由移動裝置 10 向各阻止通信人發送“不可聯繫的”可聯繫性資訊。另選地，通過從聯繫人資料庫中刪除這樣的用戶，即，移動裝置 10 的用戶不再希望接收到來自其他移動裝置 10 的這些用戶的對等訊息，可以阻止來自這種其他用戶的對等訊息並且不把它們顯示給用戶；在此情況下，可以將對等訊息傳遞應用調節成阻止來自聯繫人資料庫所未列出的任何用戶的訊息。挂起對話組 55 提供了與

移動裝置 10 的所有當前挂起對話有關的資訊。挂起對話是指：移動裝置 10 已向另一移動裝置 10 發送如上所述的邀請並且尚未接收到回應；或者另一移動裝置 10 已向移動裝置 10 發送如上所述的邀請並且移動裝置 10 尚未回應。

可以選擇性地擴展當前對話組 45、阻止通信人組 50 以及挂起對話組 55，其中顯示附加資訊，或者縮略附加資訊，或者不顯示附加資訊。第 3 圖按擴展形式示出了當前對話組 45、阻止通信人組 50 以及挂起對話組 55 中的每一個。通過輸入裝置（如多個鍵和/或旋轉指輪（thumbwheel），其作爲移動裝置 10 的一部分而被包括進來）向移動裝置 10 提供輸入，用戶可以在擴展和縮略狀態之間選擇性地切換。在擴展狀態下，當前對話組 45 爲每個當前對話列出：（1）與其他移動裝置 10 相關聯的用戶；（2）與其他移動裝置 10 有關的可聯繫性資訊；以及（3）最近發送或接收的訊息的日期和/或時間。由於對等訊息傳遞會話可以在很長時段（例如，數周或數月）內保持打開和活動狀態，因此資料項目（3）提供了針對哪個對話是最活動和最新的快速參考。在擴展狀態下，挂起對話組 55 爲每個挂起對話列出：（1）與其他移動裝置 10 相關聯的用戶；和（2）與其他移動裝置 10 有關的可聯繫性資訊。如在第 3 圖中看到的，優選地，將表示可聯繫性資訊的圖示 60 置於當前對話組 45 和挂起對話組 55 中的每個條目的旁邊，以便於用戶參考。

儘管上述說明提到可以把 PIN、密鑰或其他資料要素嵌

入或附加到由所述多個通信應用中的一個發送的訊息中，但是應當理解，這裏使用的術語“嵌入”或“附加”旨在被寬泛地解釋成包括附加、嵌入或與訊息一起傳送或發送這種資料要素。

【圖式簡單說明】

下面參照附圖僅通過示例對多個實施例進行描述，附圖中：

第 1 圖是提供移動裝置間的即時對等訊息傳遞的系統的框圖；

第 2 圖是移動裝置顯示器的一部分的圖，其示出了作爲對等訊息傳遞應用的一部分的示例性聯繫人資料庫屏面；

第 3 圖是移動裝置顯示器的一部分的圖，其示出了構成對等訊息傳遞應用的一部分的示例性狀態屏面；

第 4 圖示出了用於通知用戶接收訊息傳遞邀請的圖形用戶介面的示例實施例；

第 5 圖按框圖形式示出了設計成提供對等訊息傳遞的移動裝置；以及

第 6 圖按流程圖形式示出了一種用於在移動訊息傳遞系統中安全地交換個人識別號碼的方法。

在所有圖中，使用相似的標號標示相似的要素和特徵。

【元件符號說明】

5　系統

10、10A、10B　移動裝置

15　無線網路

20　擇路伺服器

25　聯繫人資料庫屏面

30　聯繫人的列表

35 各聯繫人的狀態資訊

40 狀態屏面

45 當前對話組

50 阻止通信人組

55 挂起對話組

60 表示可聯繫性資訊的圖示

111 通訊子系統

113 LO 本機振蕩器

116、118 天線

120 DSP 數位信號處理器

126 RAM 隨機存取記憶體

156 SIM 身份識別模組

200 圖形用戶介面

202 收件箱顯示幕面

204 對話方塊

300 在移動訊息傳遞系統中安全地交換 PIN 的方法

五、中文發明摘要：

安全對等訊息傳遞邀請架構。提供了一種用於在無線系統中的多個移動裝置（10）之間提供即時對等訊息傳遞的系統和方法。公開了一種邀請架構，其使得可以交換個人識別號碼（PIN）而不必要求用戶直接訪問或提供他的或她的 PIN。訊息傳遞應用（160）在通過現有通信應用（162）將其關聯 PIN 提供給位於另一移動裝置（10）上的訊息傳遞應用（160）之前對該 PIN 進行加密。該邀請架構自動管理該加密過程、任何必要密鑰交換、對邀請和接受訊息的編輯以及對 PIN 的解密和存儲。

六、英文發明摘要：

A system and methods providing immediate peer-to-peer messaging between mobile devices (10) in a wireless system. An invitation architecture is disclosed which enables the exchange of personal identification numbers (PINs) without requiring a user to directly access or provide his or her PIN. A messaging application (160) encrypts its associated PIN before providing it to a messaging application (160) on another mobile device (10) through an existing communication application (162). The invitation architecture automatically manages the encryption, any requisite key exchanges, the composition of invitation and acceptance messages, and the decryption and storage of PINS.

七、指定代表圖：

(一)本案指定代表圖為：第（ 5 ）圖。

(二)本代表圖之元件符號簡單說明：

10　移動裝置

111　通訊子系統

113　LO 本機振蕩器

116、118　天線

120　DSP 數位信號處理器

126　RAM 隨機存取記憶體

156　SIM 身份識別模組

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

I328383

97年10月20日修正替換頁

公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號： 094135399

※ 申請日期： 94 年 10 月 11 日　　※IPC 分類：H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

安全點對點傳訊邀請架構

Secure Peer-To-Peer Messaging Invitation Architecture

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

動態研究有限公司

Research in Motion Limited

代表人：（中文/英文）賴瑞・康利　Larry CONLEE

住居所或營業所地址：（中文/英文）

加拿大安大略 N2L 3W8 滑鐵盧菲利普街 295 號

295 Phillip Street, Waterloo, Ontario, N2L 3W8, Canada

國　籍：（中文/英文） 加拿大　CA

三、發明人：（共 3 人）

1. 姓　名：（中文/英文） 格哈德・迪特里希・克拉森
Gerhard Dietrich KLASSEN

國　籍：（中文/英文） 加拿大　CA

2. 姓　名：（中文/英文） 沙莫爾・法梅 Samer FAHMY

國　籍：（中文/英文） 加拿大　CA

3. 姓　名：（中文/英文） 大衛・亞克 David YACH

國　籍：（中文/英文） 加拿大　CA

99年1月29日修正替換頁

第 094135399 號專利申請案
中文申請專利範圍替換本(99 年 1 月)

十、申請專利範圍：

1. 一種由一系統中的一移動裝置實施的方法，該系統包括該移動裝置、一無線網路以及與該無線網路耦合的一擇路伺服器，其中該移動裝置具有一使用者介面、一個或多個通信應用、一訊息傳遞應用以及一第一個人識別號碼，該方法包含：

經由該或該等通信應用的一個通信應用接收一邀請，該邀請包括一問題；

顯示包括該問題之該邀請；

經由該使用者介面接收回應該問題的一答案；

利用該答案產生一密鑰；

利用該密鑰加密該第一個人識別號碼；

傳輸該已加密的第一個人識別號碼以回應該已接收的邀請；

接收一已加密的第二個人識別號碼，以回應該已傳輸的第一個人識別號碼；以及

解密該已加密的第二個人識別號碼，

藉此，該移動裝置利用該訊息傳遞應用來傳送及接收點對點訊息，且其中各已傳輸之點對點訊息包含該第二個人識別號碼，各已接收之點對點訊息包含該第一個人識別號碼，且點對點訊息由該擇路伺服器根據該個人識別號碼進行擇路。

2. 如申請專利範圍第1項所述的方法，其中傳輸該已加密的第一個人識別號碼之步驟包含傳輸一接受訊息，該接

受訊息包含該已加密的第一個人識別號碼。

3. 如申請專利範圍第1項所述的方法，其中接收該已加密的第二個人識別號碼之步驟更包含接收一確認訊息，且其中該確認訊息包含被該密鑰加密的該第二個人識別號碼。

4. 如申請專利範圍第1項所述的方法，其中該通信應用的該一個通信應用包含一電子郵件應用。

5. 如申請專利範圍第1項所述的方法，其中該接收的步驟包括自一第一移動裝置接收該邀請，該傳輸的步驟包括傳輸該已加密的第一個人識別號碼至該第一移動裝置，接收該已加密的第二個人識別號碼之步驟包含從該第一移動裝置接收該已加密的第二個人識別號碼。

6. 一種由一系統中的一移動裝置實施的方法，該系統包括該移動裝置、一無線網路以及與該無線網路耦合的一擇路伺服器，其中該移動裝置具有一個或多個通信應用、一訊息傳遞應用以及一第一個人識別號碼，該方法包含：

經由該或該等通信應用的一個通信應用傳送一邀請，該邀請包括一問題，且該問題具有一答案；

利用該答案產生一密鑰；

利用該密鑰加密該第一個人識別號碼；

接收一已加密的第二個人識別號碼，以回應該邀請；

解密該已加密的第二個人識別號碼；以及

傳輸該已加密的第一個人識別號碼以回應該已加密的

第二個人識別號碼的接收，

藉此，該第一移動裝置利用該訊息傳遞應用傳送及接收點對點訊息，且其中各已傳輸之點對點訊息包含該第二個人識別號碼，各已接收之點對點訊息包含該第一個人識別號碼，各已接收之點對點訊息包含該第一個人識別號碼，且各點對點訊息由該擇路伺服器根據該個人識別號碼進行擇路。

7. 一種用於一點對點訊息傳遞系統之移動裝置，該系統包含該移動裝置、一無線網路以及與該無線網路耦合的一擇路伺服器，該移動裝置包含：

一第一記憶體，用以儲存一第一個人識別號碼；

一個或多個通信應用；

一第一加密元件，其配置以對該第一個人識別號碼進行加密，及利用一密鑰對一已加密的第二個人識別號碼進行解密；

一第一聯繫人管理元件，其配置以

經由該一個或該等通信應用的一個通信應用接收一邀請，該邀請包括一問題；

顯示包含該問題的該邀請；

利用一使用者介面接收一答案以回應該問題；

傳輸該已加密的第一個人識別號碼以回應該邀請；以及

接收該已加密的該第二個人識別號碼以回應該已加密的第一個人識別號碼之傳輸；以及

一第一訊息傳遞應用，用以傳送及接收點對點訊息，

從而，各已傳輸之點對點訊息包括該第二個人識別號碼，各已接收之點對點訊息包括該第一個人識別號碼，且其中該點對點訊息由該擇路伺服器根據該個人識別號碼進行擇路；

其中該第一加密元件係配置以利用該答案產生該密鑰。

8. 如申請專利範圍第7項所述的移動裝置，其中該第一聯繫人管理元件是配置以傳送一接受訊息以回應該邀請，且該接受訊息包含該已加密的第二個人識別號碼。

9. 如申請專利範圍第7項所述的移動裝置，其中該第一聯繫人管理元件是配置以接收一確認訊息，且其中該確認訊息包含該已加密的第二個人識別號碼。

10. 如申請專利範圍第7項所述的移動裝置，其中該通信應用的該一個通信應用包含一電子郵件應用。

11. 一種點對點訊息傳遞系統，其包含如申請專利範圍第7項所述的該移動裝置及另一移動裝置，該另一移動裝置包含：

一第二記憶體，用以儲存該第二個人識別號碼；

一個或多個通信應用；

一第二加密元件，其配置以對該第二個人識別號碼進行加密，及利用該密鑰對該已加密的第一個人識別號碼進行解密；

一第二聯繫人管理元件，其配置以

利用該或該等通信應用的該一個通信應用傳送該邀請

至該移動裝置；

從該移動裝置接收一接受，其顯示成功輸入該答案；

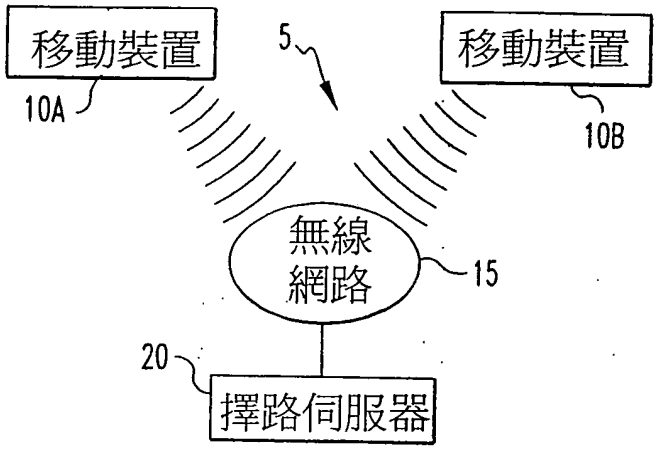
從該移動裝置接收該已加密的第一個人識別號碼；以及

傳輸該已加密的第二個人識別號碼至該移動裝置；以及

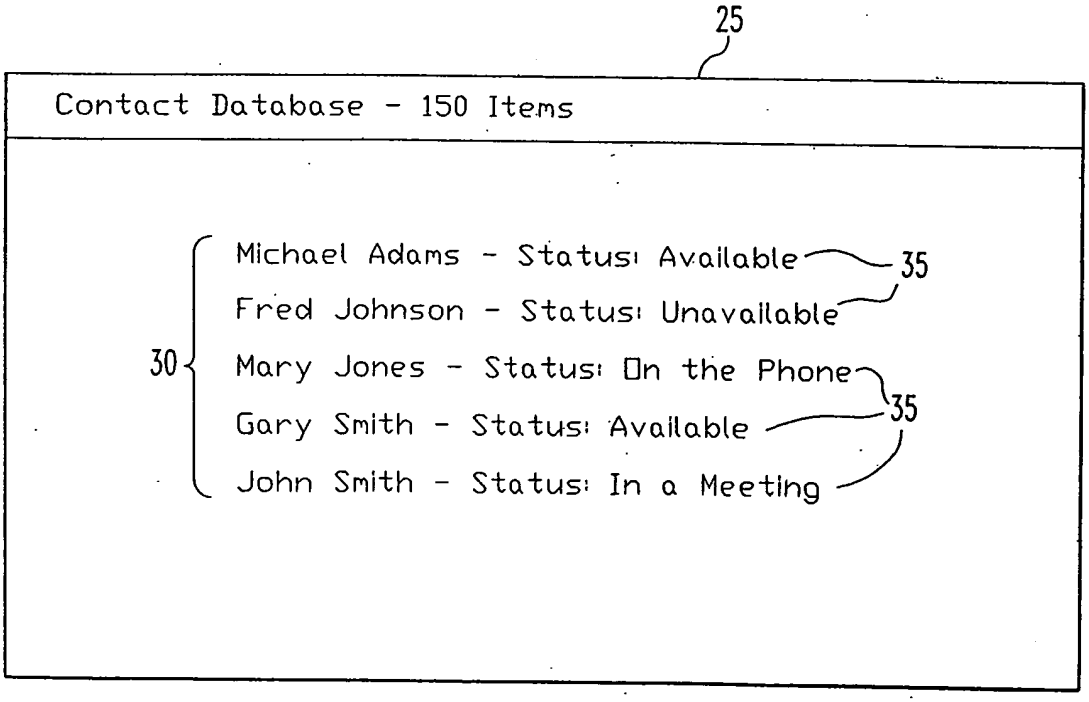
一第二訊息傳遞應用，用以傳送及接收點對點訊息；

其中該第二加密元件係配置以利用該答案產生該密鑰。

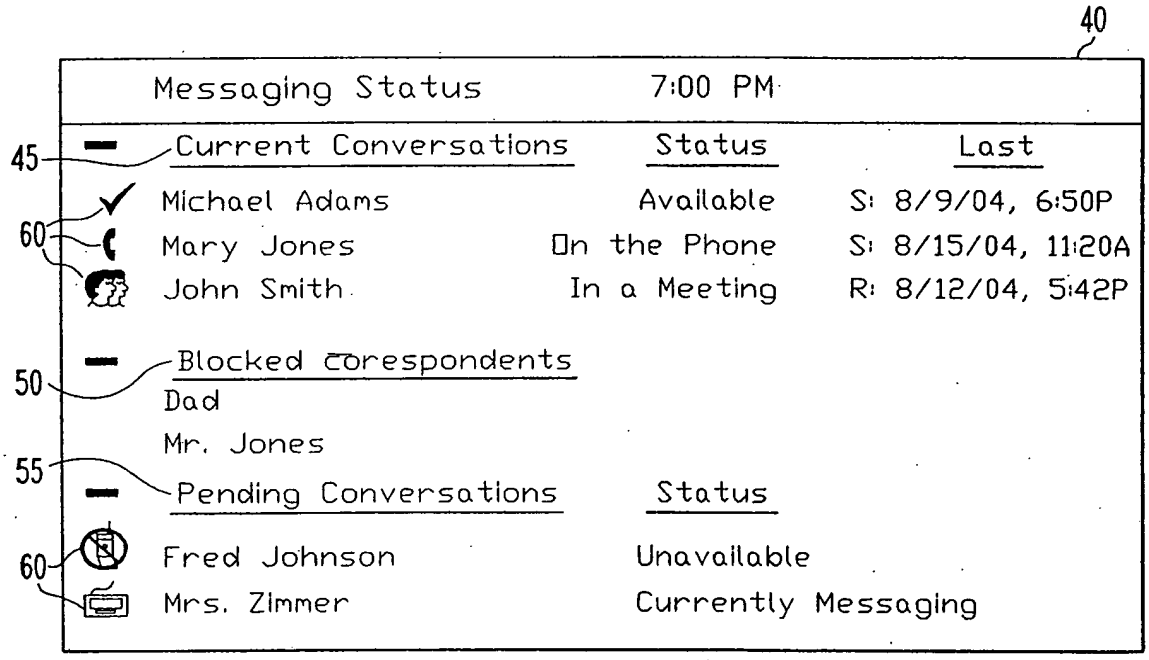
十一、圖式：　　1/5



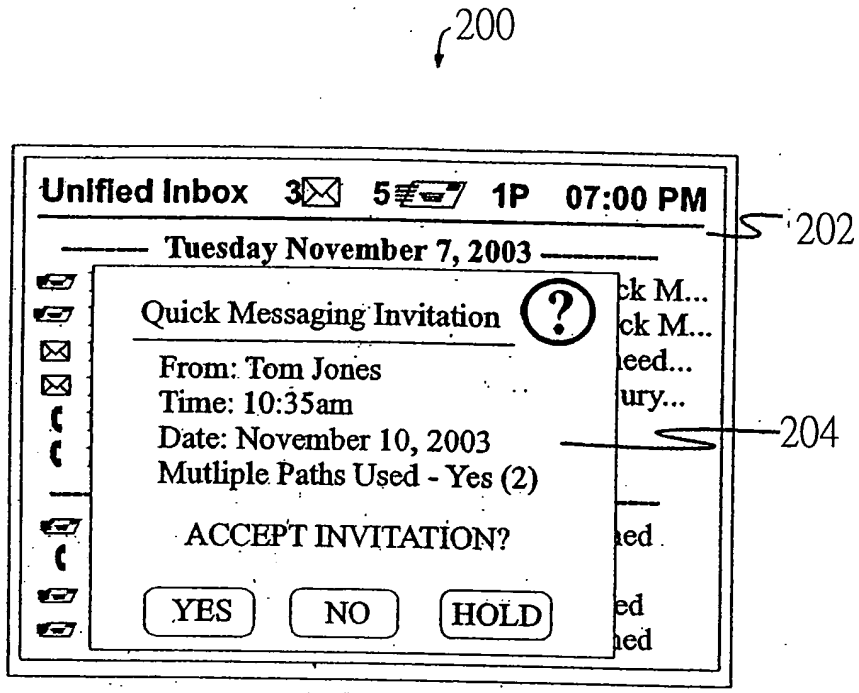
第 1 圖



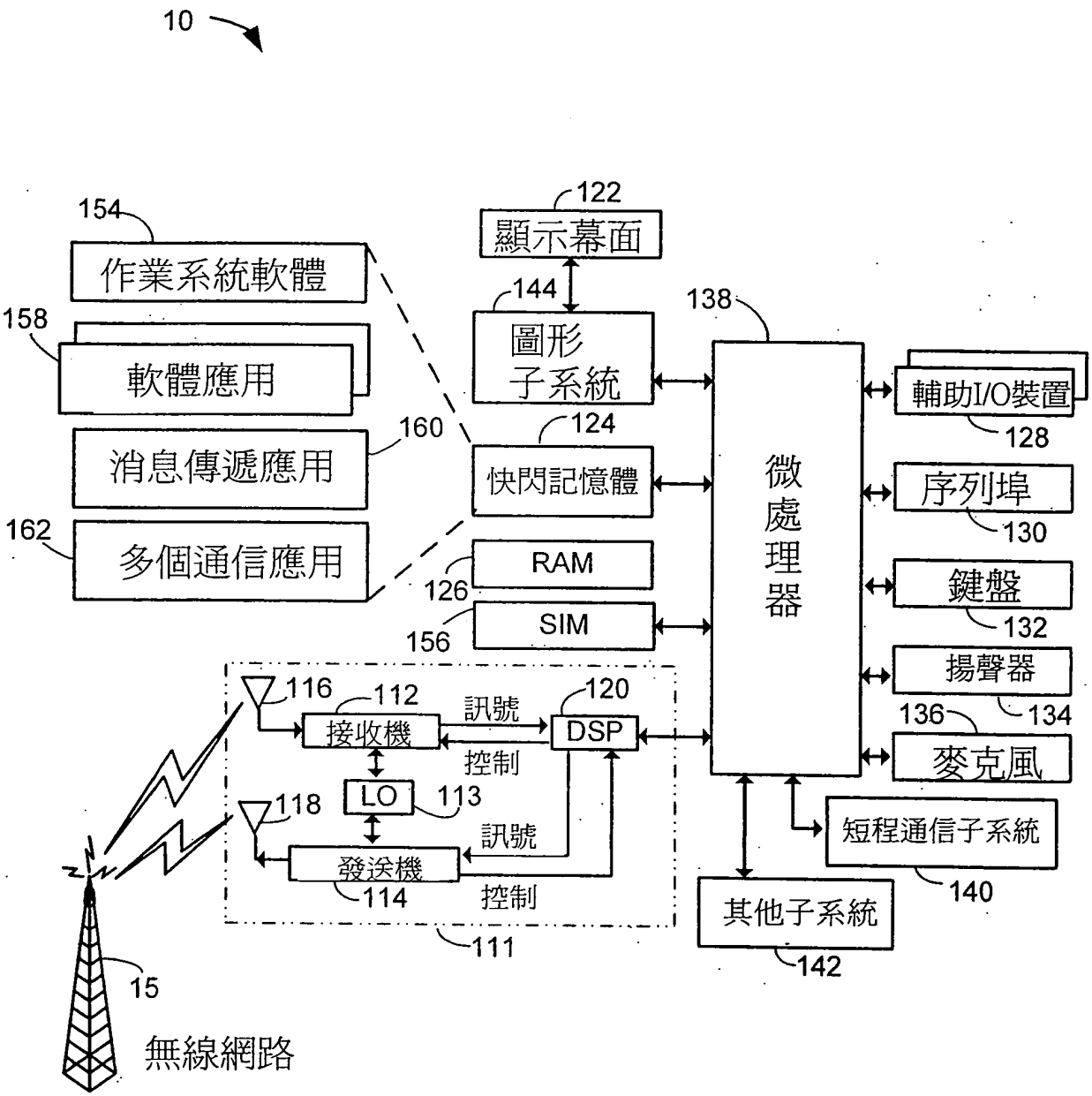
第 2 圖


40
Messaging Status
7:00 PM
45
Current Conversations
Status
Last
60
Michael Adams
Available
S: 8/9/04, 6:50P
Mary Jones
On the Phone
S: 8/15/04, 11:20A
John Smith
In a Meeting
R: 8/12/04, 5:42P
50
Blocked Corespondents
Dad
Mr. Jones
55
Pending Conversations
Status
60
Fred Johnson
Unavailable
Mrs. Zimmer
Currently Messaging

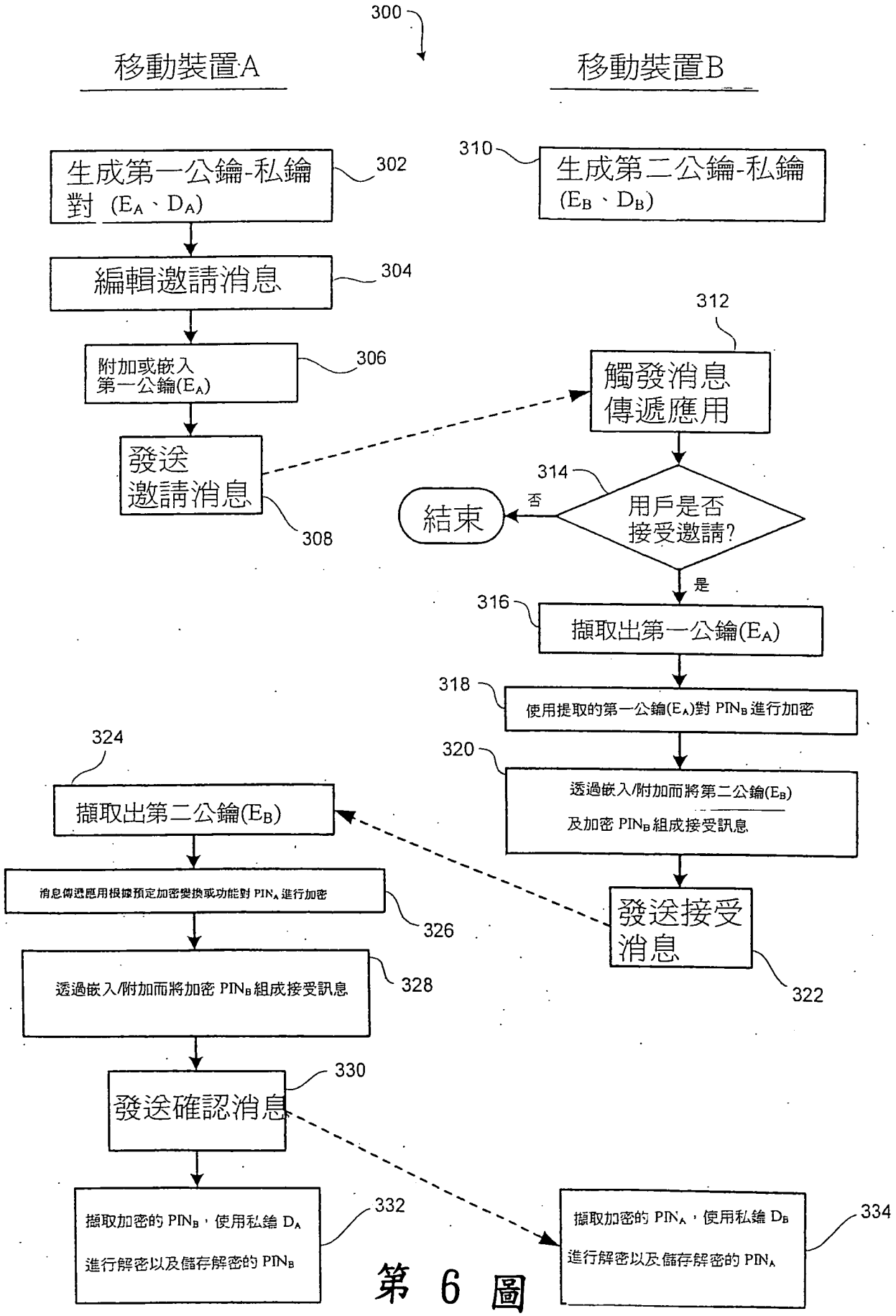
第 3 圖


200
Unified Inbox 3 5 1P 07:00 PM
202
Tuesday November 7, 2003
Quick Messaging Invitation
From: Tom Jones
Time: 10:35am
Date: November 10, 2003
204
Mutliple Paths Used - Yes (2)
ACCEPT INVITATION?
YES
NO
HOLD

第 4 圖



第 5 圖



第 6 圖