

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：

1. 美國 2004 年 3 月 16 日 10/801,470

☐ 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】

本發明涉及一種將安全認證邏輯集成到移動電話的技術。

【先前技術】

密碼是一種能阻止未授權用戶訪問電腦系統的普遍應用的安全措施，它也能在訪問時對授權用戶進行認證。然而，未授權用戶已經能使用各種方法查明授權用戶密碼。

一旦未授權用戶已經獲得授權用戶的密碼，這個未授權用戶能像授權用戶一樣以相同方式訪問電腦系統。大多時候，未授權用戶帶著惡意目的訪問電腦系統。通常，直到顯著破壞或者混亂已經發生的時候，未授權用戶的活動才會被察覺。

要求授權用戶在規則時間間隔內改變他們的密碼，至少在某些程度上能減少未授權用戶的活動。然而，這些規則間隔時間的周期經常是幾個星期或者幾個月。在這個時間周期內，未授權用戶能引起顯著破壞或者混亂。即使用戶每天改變密碼，仍然不能有效持續地禁止未授權用戶做出顯著的破壞或者混亂。

因此，一些電腦系統使用隨時間變化隨機產生的密碼提供給每一授權用戶。這種電腦系統的管理者給每位元授權用戶提供一種裝置。這種裝置包括一個在相對短的時間間隔（比如每一分鐘）內產生編碼的偽隨機號碼生成器。此電腦系統也能在一個給定時間內確定該偽隨機號碼。當授權用戶試圖訪問電腦系統時，授權用戶使用由該裝置產生並顯示的編碼作為密碼。

前述提供了在短時間內有效的快速變化密碼。相應地，即使未授權用戶確實獲得密碼，這個密碼在一個非常短的時間期間有效。這顯著地減少了未授權用戶所能做出的破壞。

衆所周知的缺點之一與爲授權用戶提供這樣的裝置有關。有了網路全球化送達，在許多情況下這種裝置不得不經過郵務專遞公司或者郵件遞送給用戶。這會使授權用戶的初始訪問延遲幾天。另外，當用郵件送達裝置時，未授權用戶可能會截住該裝置。

通過本發明一些特徵與這樣系統的比較，普通和傳統方法的進一步局限性和缺點將對本領域的普通技術人員來說是顯而易見的，當然這些特徵會在本申請的其餘部分結合附圖敘述。

【發明內容】

這裏展示的是將安全認證邏輯集成到移動通信裝置的系統和方法。

在一實施例中，展示了一種提供密碼的方法。這種方法包括接收一個記錄，其中所述記錄包括與一個移動終端有關的電話號碼；以及傳送資訊到所述移動終端，所述密碼爲資訊的函數。

在另一實施例中，展示了一種移動終端，其包括收發器、偽隨機號碼生成器、控制器和輸出。所述收發器從遠端通信裝置接收一個種子（seed）。所述偽隨機號碼生成器基於所述種子在規則時間間隔內產生偽隨機號碼。所述控制器將所述種子提供到所述偽隨機號碼生成器。所述輸出基於所述偽隨機號碼在規則時間間隔內提供密碼。

在另一實施例中，展示了包括一種包括第一節點和第二節點的通信系統。所述第一節點接收一個種子。第二節點通過分頁通道 (paging channel)，傳送所述種子到預定移動終端的偽隨機號碼生成器。

根據本發明，提供了一種用於提供密碼的方法，所述方法包括：

接收記錄，其中所述記錄包括標識移動終端的識別字；以及
傳送資訊到所述移動終端，所述密碼為資訊的函數。

作為進一步的改進，所述識別字包括電話號碼。

作為進一步的改進，所述識別字包括 MAC 地址。

作為進一步的改進，所述資訊包括一個種子。

作為進一步的改進，所述種子為時間的函數。

作為進一步的改進，傳送所述資訊到所述移動終端包括：

設置呼出電話到所述移動終端。

作為進一步的改進，所述方法進一步包括：

生成基於所述資訊的隨時間變化的密碼；

接收訪問請求和提供的密碼；

根據所述提供的密碼是否與所述隨時間變化的密碼匹配
選擇性地對訪問進行授權。

根據本發明，提供一種移動終端，所述移動終端包括：

用於接收種子的收發器；

根據所述種子在規則時間間隔內生成偽隨機號碼的偽隨

機號碼生成器；

用於將所述種子提供給所述偽隨機號碼生成器的控制器；

在規則時間間隔內根據所述偽隨機號碼提供密碼的輸出。

作為進一步的改進，所述輸出包括螢幕。

作為進一步的改進，所述輸出包括介面埠。

作為進一步的改進，所述密碼是所述偽隨機號碼。

作為進一步的改進，所述移動終端進一步包括：

用於儲存可由所述控制器執行的多個指令的記憶體，所述多個指令用於：

接收命令和種子；以及在接收所述命令之後將所述種子載入所述偽隨機號碼生成器。

作為進一步的改進，所述多個指令還用於接收同步時間，並且其中在接收所述命令之後把種子載入所述偽隨機號碼生成器進一步包括在所述同步時間將所述種子載入所述偽隨機號碼生成器。

作為進一步的改進，通過分頁通道接收所述命令和種子。

作為進一步的改進，所述分頁通道是安全分頁通道。

作為進一步的改進，在電話請求期間接收所述命令和種子。

根據本發明，一種通信系統包括：

用於接收種子的第一節點；和

通過分頁通道將所述種子和將所述種子載入偽隨機號碼生成器的命令傳送到預定移動終端的第二節點。

作為進一步的改進，所述第一節點接收一個同步時間，而其中所述第二節點通過所述分頁通道傳送所述同步時間到所述移動終端。

作為進一步的改進，所述第一節點包括移動交換中心。

作為進一步的改進，所述第二節點包括基本收發器站。

作為進一步的改進，所述第二節點接收一個來自所述移動終端的肯定回應。

作為進一步的改進，所述第一節點接收所述來自源的種子並且傳送所述肯定回應到所述源。

作為進一步的改進，在所述第一節點和第二節點之間的所述通信通道使用公共密鑰加密技術。

從以下敘述和附圖中，本發明的以上和其他優點、新穎的特徵以及其中圖示實施例的詳述將會得到更充分的理解。

【實施方式】

現在參見附圖 1，其示出了根據本發明的一個實施例的示例性的通信系統的框圖，該通信系統用於配置移動終端以提供隨時間變化的隨機密碼。該系統包括電腦網路 100 和無線電話網路 150。

該通信系統包括通過電腦網路 100 可被客戶終端 115 訪問的伺服器 105。電腦網路 100 可包括各種通信媒介的任一組合，比

如，但不局限於：因特網、公共交換電話網絡、局域網（LAN）、和廣域網（WAN）。

伺服器 105 可以提供到儲存敏感資訊或者類似資訊的資料庫的訪問，或者允許個體進行各種處理。相應地，控制到伺服器 105 的訪問是很重要的。因此，伺服器 105 需要來自客戶終端 115 的密碼，此密碼在客戶終端 115 上驗證用戶的身份。

然而，未授權用戶已經知道使用各種措施獲得一個授權用戶的密碼。利用此密碼，未授權用戶經常帶著惡意的目的進行訪問伺服器 105。

爲了減少這種情況，伺服器 105 使用隨時間變化的偽隨機密碼。偽隨機號碼生成演算法在相對短的時間間隔（比如每一分鐘甚至更少）內根據期望的密碼安全所需的間隔（granularity）生成隨時間變化的偽隨機密碼。相應地，即使未授權用戶成功獲得授權用戶的密碼，此密碼僅僅在短時間間隔的剩餘部分內有效。

偽隨機號碼生成演算法可用許多方法中的一種在伺服器 105 上實現。例如，特定用途積體電路（ASIC）也可包含於不斷運行偽隨機號碼生成演算法的伺服器 105 中。可供選擇地，偽隨機號碼生成演算法可作為套裝軟體含於伺服器 105 中。

授權用戶從移動終端 120 接收隨時間變化的偽隨機密碼。實施偽隨機號碼生成演算法的邏輯集成到移動終端 120。此邏輯可以是 ASIC，也可是在移動終端 120 中的 ASIC，或是運行在移動終端 120 中的軟體程式的一部分。移動終端 120 在它的顯示幕上

顯示當前的隨時間變化的偽隨機密碼。因此，當授權用戶試圖經由客戶終端 115 訪問伺服器 105 時，授權用戶提供由移動終端 120 顯示的隨時間變化的偽隨機密碼。然後，伺服器 105 把由授權用戶提供的隨時間變化的偽隨機密碼和由伺服器 105 上的偽隨機號碼生成演算法產生的偽隨機號碼相比較。如果二者嚴格匹配，伺服器 105 允許訪問。

爲了使伺服器 105 上的偽隨機號碼生成演算法在相同時間上提供和移動終端 120 一樣的偽隨機號碼，偽隨機號碼生成演算法是相同的和同步的。

偽隨機號碼生成演算法要求一種叫“種子 (seed)”的輸入以產生偽隨機號碼。該種子可由一外部源提供給偽隨機號碼生成演算法。偽隨機號碼生成演算法從種子產生第一偽隨機號碼，然後從第一偽隨機號碼產生第二偽隨機號碼，以此類推，等等。

正如所看到的，由偽隨機號碼生成演算法產生的偽隨機號碼的序列依靠種子。另外，不同種子對於相同偽隨機號碼生成演算法導致不同偽隨機號碼序列。實際上，相同偽隨機號碼生成演算法通過爲每一用戶提供不同的種子，可以爲任何數量的用戶提供不同的隨時間變化的偽隨機密碼。爲了保證給每一用戶的偽隨機號碼序列的唯一性，所產生的偽隨機號碼的大小也起到一個顯著的作用。

當在客戶終端 115 上的用戶初次註冊 (register) 以訪問伺服器 105 時，該註冊記錄 (registration) 可包括電話號碼或是任何其

他與此用戶的移動終端 120 有關的識別號碼。伺服器 105 可為此用戶選擇一個種子。作為一種附加安全措施，伺服器 105 可基於記錄時間選擇種子。然後，伺服器 105 可使用終端 125 訪問移動電話網絡 130。終端 125 使用移動電話網絡 130 將種子傳送到移動終端 120。終端 125 直接或經由一個公共交換電話網絡訪問移動電話網絡 130。

例如，在一實施例中，終端 125 建立到移動終端 120 的電話。當電話建立時，終端 125 可通過移動電話網絡 130 傳送代表種子的音頻信號。移動終端 120 可相應地在一個預定時間內把種子載入偽隨機號碼生成器，以與伺服器 105 同步。考慮到從伺服器 105 到移動終端 120 通信的路徑延遲時間，預定時間最接近傳送時間（比如在下一分鐘間隔）更為合適。

在另一實施例中，終端 125 可使移動電話網絡 130 傳送指示種子到移動終端 120 的控制信號。移動終端 120 可相應地在一個預設時間內把種子載入偽隨機號碼生成器，以與伺服器 105 同步。

移動電話網絡 130 可包括各種無線遠端通信網路，比如，但是不局限於全球移動通信系統（GSM）、或者個人通信服務（PCS）網路、碼分多路訪問（CDMA）網路、IEEE 802.11 無線區域網路、藍牙網路，等等。

現在參見附圖 2，示出了一種全球移動通信系統（GSM）公共陸地移動網路（PLMN）210 系統。其中，PMLN 210 由多個區域 212 組成，每一區域都具有有一個節點，該節點即通常所說的移

動轉換中心 (MSC) 214 和集成訪問者位置寄存器 (VLR) 216。MSC/VLR 區域 212 依次包括多個位置區域 (LA) 218，其被定義為一個給定 MSC/VLR 區域 212 的一部分，在此部分中移動終端 120 不必向 MSC/VLR 區域 212 發送控制 LA 218 的更新的位置資訊而可自由地移動。每一位置區域 212 被分成許多單元 222。移動終端 120 是物理設備，比如，移動用戶使用的汽車電話或者其他攜帶型電話，以與移動分區網路 210、相互之間及與所述網路外的用戶通信（無線或者有線）。

MSC 214 至少與一個基站控制器 (BSC) 223 通信，該 BSC 223 輪流與至少一個基收發器站 (BTS) 224 聯繫。BTS 是一個包括物理設備的節點，為了簡便起見表示為一個無線電通信塔，此塔提供無線電覆蓋到其負責的單元 222 的地理部分。應理解到 BSC 223 可以與幾個基收發器站 224 相連，並且可作為一個獨立節點或者與 MSC 214 相結合進行實施。在任一情況下，BSC 223 和 BTS 224 元件作為一個整體通常可看成為一個基站系統 (BSS) 225。至少一個 MSC 214 與公共交換電話網絡 (PSTN) 連接。

PLMN 服務區域或者無線網路 210 包括一個本地位置寄存器 (HLR) 226，該寄存器是一個維持所有用戶資訊的資料庫，比如，用戶簡檔、當前位置資訊、國際移動用戶身份 (IMSI) 號碼、和其他管理資訊。HLR 226 可與一個給定的 MSC 214 共同設置，與 MSC 214 結合在一起，或者可為多個 MSC 214 服務，後者在附圖 2 中進行闡釋。

VLR 216 是一個包含關於所有當前位於 MSC/VLR 區域 212 內的移動終端 120 的資訊的資料庫。如果移動終端 120 漫遊到一個新的 MSC/VLR 區域 212 內，與 MSC 214 連接的 VLR 216 將請求來自 HLR 資料庫 226 的關於那個移動終端 120 的資料(同時通知 HLR 226 關於移動終端 120 的當前位置)。相應地，如果移動終端 120 的用戶然後想打一個電話，本地 VLR 216 將不必再次詢問 HLR 226 而帶有必要的身份資訊。以前述方式，VLR 和 HLR 資料庫 216 和 226 分別包括與給定移動終端 120 相聯繫的不同用戶資訊。

在一實施例中，終端 125 可直接或是經由 PSTN 通過 GSM PLMN210 與移動終端 120 建立一個電話通話。在建立電話通話後，終端 125 傳送音頻信號到移動終端 120，從而使移動終端 120 把一個特定種子載入偽隨機號碼生成器。可供選擇地，終端 125 可經由一個基站 224 使一個 MSC214 傳送控制信號到移動終端 120，從而使移動終端 120 把一個特定種子載入偽隨機號碼生成器。這些是把所述種子載入移動終端 120 中的偽隨機號碼生成邏輯的許多可能技術中的少數技術。

在一個已建立的通話期間的種子的傳輸通過建立預定的通信協定實現，該協定用於在終端 125 和移動終端 120 之間進行安全通信。這樣的預定協定可包括指示種子隨後將被傳輸到的移動終端 120 的任意控制信號的傳送。在接收前述任意控制信號後，移動終端 120 準備接收種子並把種子載入偽隨機號碼生成器。在終

由偽隨機號碼生成器 325 產生的偽隨機號碼得到。例如，在隨機號碼較長的情況下，控制器 305 可以截取偽隨機號碼的一部分或者執行其他類型的數學操作以減少它的長度。

所述隨時間變化的偽隨機密碼以及用戶認證，可通過各種方式提供。在一個實施例中，隨時間變化的偽隨機密碼可被輸出到介面埠 321。介面埠 321 連接到諸如客戶終端 115 的電腦。把介面埠 321 連接到客戶終端 115 可使隨時間變化的偽隨機密碼顯示在一個與客戶終端 115 有關的螢幕上。在另一實施例中，隨時間變化的偽隨機碼可連續地顯示在螢幕 320 上。在另一實施例中，用戶可在螢幕 320 提供的圖形用戶介面的輔助下使用小型鍵盤 310 請求當前時間變化的偽隨機密碼。

偽隨機號碼生成器 325 可包括諸如一個電路，比如產生偽隨機號碼的線性反饋移位寄存器（LFSR）。可供選擇地，偽隨機號碼生成器可由一個處理器執行一組指令來實施，其中該組指令促成了偽擬隨機號碼生成演算法的執行。

另外，偽隨機號碼生成器 325 和控制器 305 之間可有不同地集成級。例如，控制器 305 和偽隨機號碼生成器 325 可以是分離的積體電路，該電路可在插板級別焊接在一起。可供選擇地，控制器 305 和偽隨機號碼生成器 325 可以集成在一個積體電路中。

正如以上所提到的，用於偽隨機號碼生成器 325 的種子是由移動電話網絡 130 提供的。移動終端 120 經由收發器 315 接收來自移動電話網絡 130 的無線電信號。可以執行各種解調、信號處

服器 105。移動終端 120 等待同步時間 (425)。在同步時間，移動終端 120 和伺服器 105 把種子載入它們各自的偽隨機號碼生成器 (430)。

在種子被載入偽隨機號碼生成器之後，移動終端 120 螢幕可顯示一個隨時間變化的偽隨機密碼。在客戶終端 115 上的一個授權用戶通過提供顯示在移動終端 120 螢幕上的隨時間變化的偽隨機密碼 (信號 435) 建立一個客戶服務連接。伺服器 105 把從客戶終端 115 接收到的密碼與在伺服器 105 上的一個偽隨機號碼生成器進行比較 (440)。如果上述相一致，伺服器允許訪問 (信號 445) 客戶終端 115。

現在參見附圖 5，示出了根據本發明一個實施例的一個給一個偽隨機號碼生成器提供一個種子和時間的信號流程框圖。在初始註冊 (信號 505) 期間，用戶提供與他們移動終端有關的電話號碼。作為回應，伺服器 105 為用戶分配一個種子並且確定一個同步時間。

伺服器 105 通過終端 125 請求一個到註冊期間所提供電話號碼的呼出電話通話 (信號 510)。移動電話網絡 130 的基礎結構識別和定位與電話號碼有關的移動終端 120。一個最接近移動終端 120 的 MSC 214 使用一個分頁通道對移動終端 120 調頁。

在接收上述頁後，移動終端 120 提醒用戶回復此通話。在用戶回復後，在伺服器 105/終端 125 和移動終端 120 之間建立起一個電話通話。伺服器 105/終端 125 傳送指示一個在指定時間 (信號

530) 內載入隨後的種子的命令 (信號 525) 的音頻信號。

移動終端 120 等待 (535) 所提供的同步時間 535 並把種子載入 (540) 偽隨機號碼生成器。在那裏，伺服器 105 同樣地把種子載入 (540) 偽隨機號碼生成器。

在種子被載入偽隨機號碼生成器之後，移動終端 120 螢幕會顯示一個隨時間變化的偽隨機密碼。一個在客戶終端 115 上的授權用戶通過提供顯示在移動終端 120 螢幕上的隨時間變化的偽隨機密碼 (信號 545) 建立一個客戶服務連接。伺服器 105 把從客戶終端 115 接收的密碼和在伺服器 105 上的一個偽隨機號碼生成器進行比較 (550)。如果前述相一致，伺服器允許訪問 (信號 555) 客戶終端 115。

儘管已參考本發明的某些實施例對本發明進行了描述，熟悉本技術領域的人員應該理解，可在不脫離本發明的範圍內做出各種變化和等效替換。另外，可在不脫離本發明的範圍內，可做許多修改以將本發明的教授適用到特定情況或材料。因此，本發明不局限於所公開的特定實施例，而是將會包括落在附加權利要求範圍內的所有實施例。

【圖式簡單說明】

圖 1 是根據本發明的一個實施例的通信系統的框圖，該通訊系統用於配置移動終端以提供隨時間變化的隨機密碼；

圖 2 是根據本發明的一個實施例的能使用移動通信公共陸地移動

五、中文發明摘要：

在此所展示的是用於將安全認證邏輯集成到移動電話的系統和方法。接收一個記錄，其中所述記錄包括標識移動終端的識別字。資訊被傳送到所述移動終端，其中密碼是所述資訊的函數。

六、英文發明摘要：

Present herein are systems and methods for integrating secure identification logic into cell phones. A registration is received, wherein said registration includes an identifier identifying a mobile terminal. Information is transmitted to the mobile terminal, wherein a password is a function of the information.

十、申請專利範圍：

1、一種提供密碼的方法，所述方法包括：

接收一個記錄，其中所述記錄包括標識移動終端的識別字；以及
傳送資訊到所述移動終端，所述密碼為所述資訊的函數。

2、如申請專利範圍第 1 項所述的方法，其中所述識別字包括電話號碼。

3、如申請專利範圍第 1 項所述的方法，其中所述識別字包括 MAC 位址。

4、如申請專利範圍第 1 項所述的方法，其中所述資訊包括種子。

5、如申請專利範圍第 4 項所述的方法，其中所述種子是時間的函數。

6、一種移動終端，包括：

用於接收種子的收發器；

用於在規則時間間隔內根據所述種子產生偽隨機號碼的偽隨機號碼生成器；

把所述種子提供給所述偽隨機號碼生成器的控制器；以及
在規則時間間隔內根據所述偽隨機號碼提供密碼的輸出。

7、如申請專利範圍第 6 項所述的移動終端，其中所述輸出包括螢幕。

8、如申請專利範圍第 6 項所述的移動終端，其中所述輸出包括介面埠。

9、一種通信系統，包括：

用於接收種子的第一節點；

用於通過分頁通道將所述種子和將所述種子載入偽隨機號碼生成器的命令傳送到預定移動終端的第二節點。

10、如申請專利範圍第9項所述的通信系統，其中所述第一節點接收同步時間，所述第二節點通過所述分頁通道傳送所述同步時間到所述移動終端。

I268084

十一、圖示：

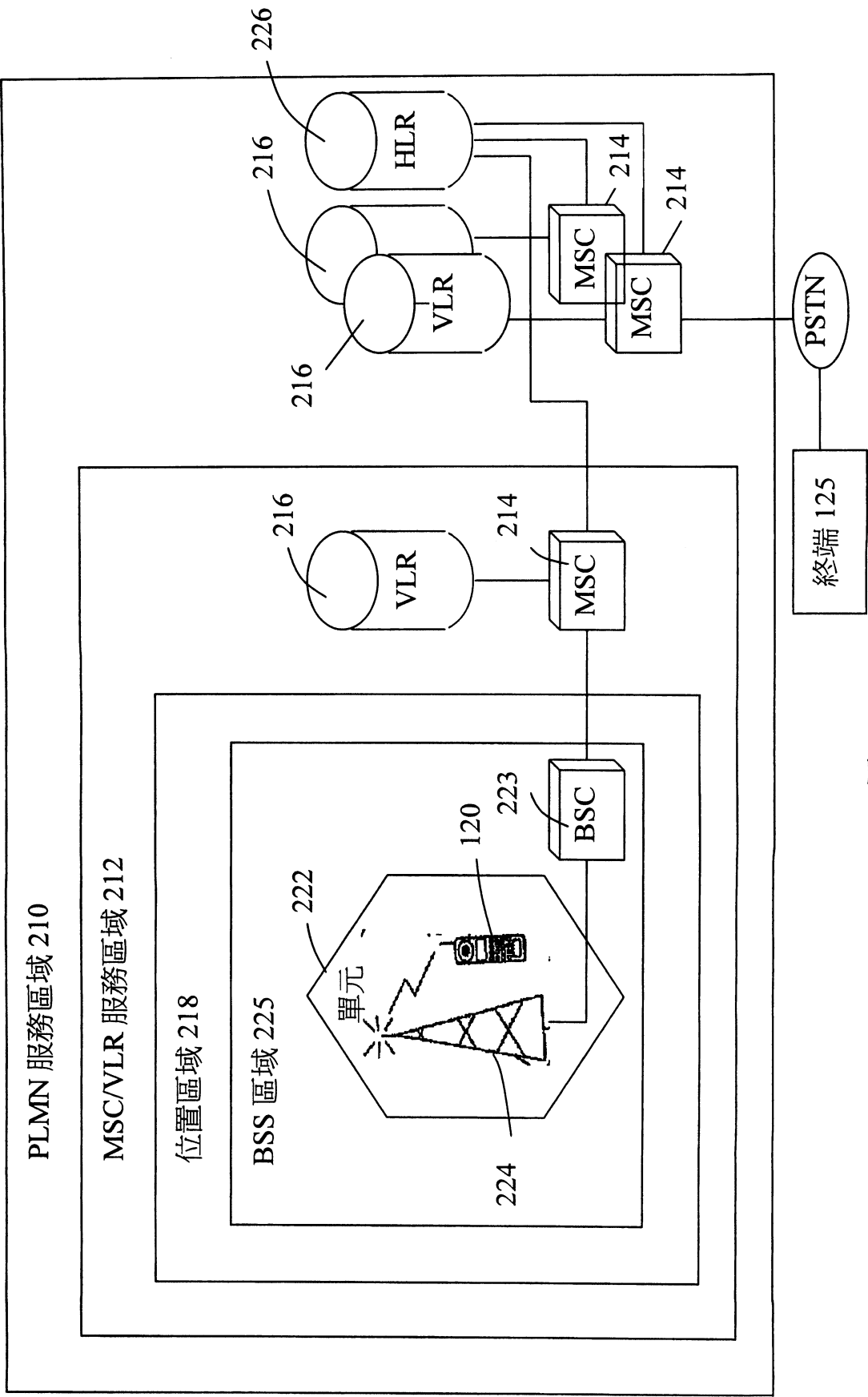


圖 2

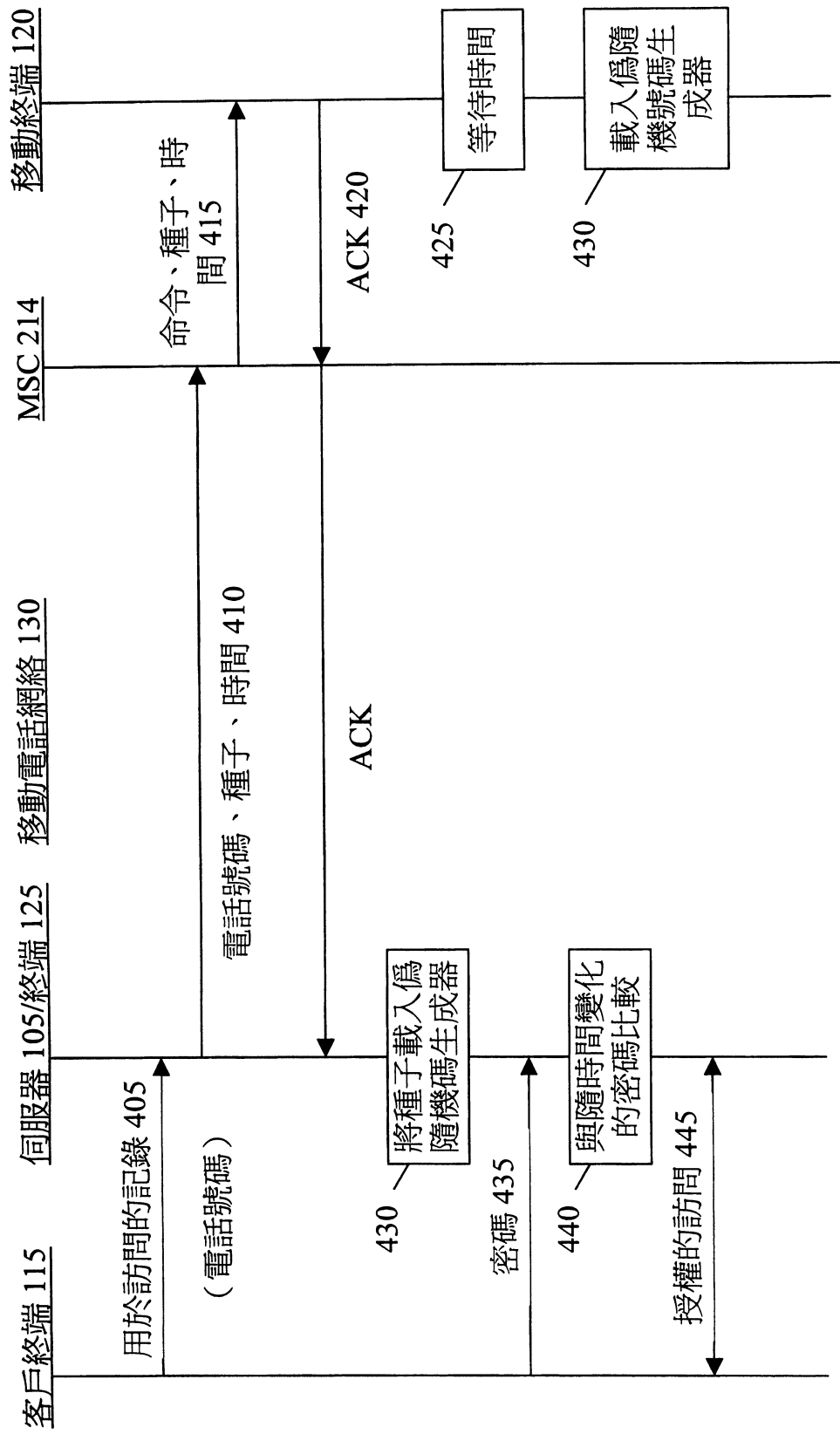


圖 4

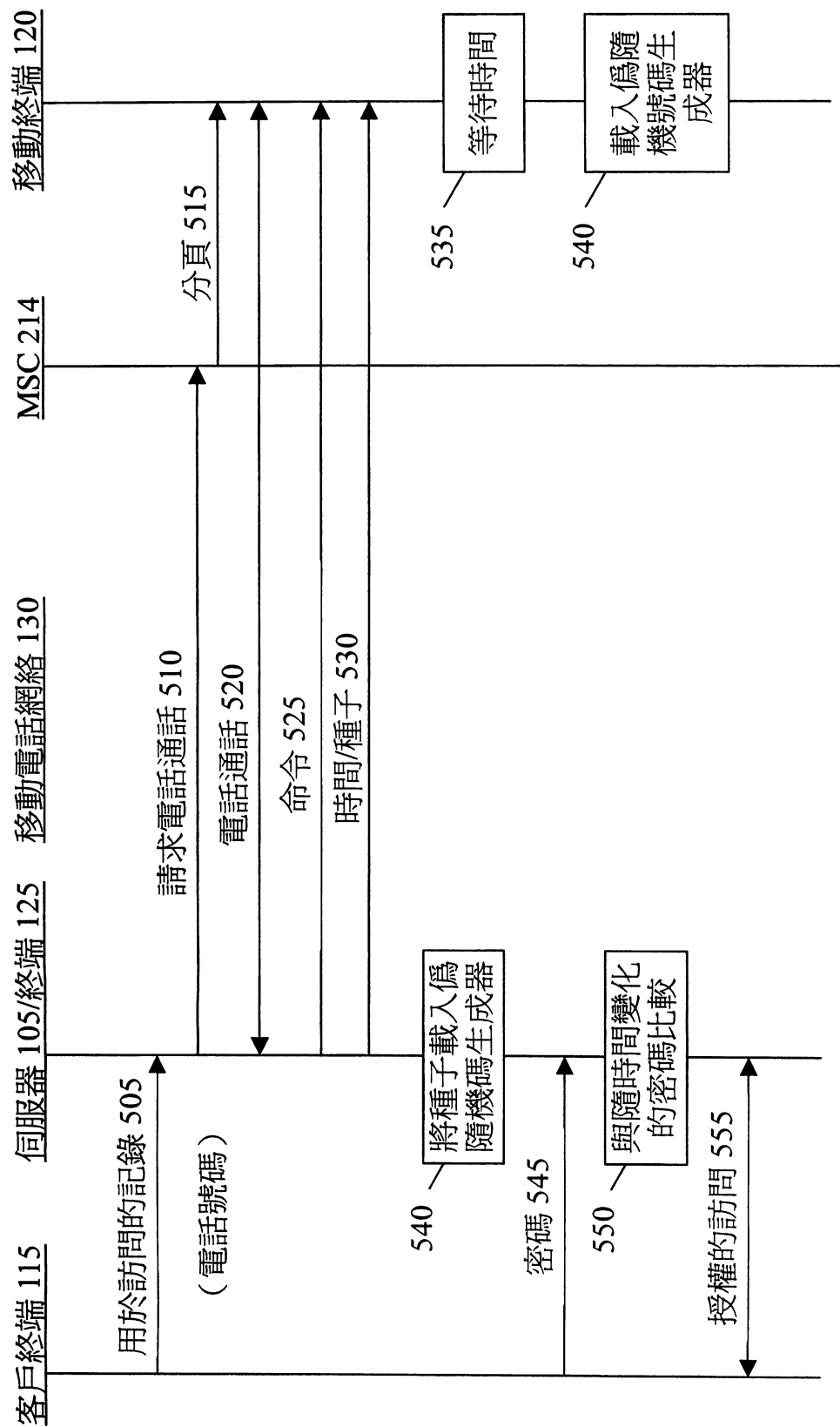


圖 5

七、指定代表圖：

(一)本案指定代表圖為：第 (4) 圖。

(二)本代表圖之元件符號簡單說明：

伺服器 105

客戶終端 115

移動終端 120

終端 125

移動電話網絡 130

移動轉換中心 (MSC) 214

信號 405、410、415、420、435、445

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

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：941082004

※ 申請日期：94.3.16

※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：(中文/英文)

安全認證方法和集成安全認證邏輯之移動電話

INTEGRATION OF SECURE IDENTIFICATION LOGIC INTO CELL
PHONE

二、申請人：(共1人)

姓名或名稱：(中文/英文)(簽章) ID：

美國博通公司/Broadcom Corporation

☐ 指定 為應受送達人

代表人：(中文/英文)(簽章) 狄·韓德森/Dee Henderson

住居所或營業所地址：(中文/英文)

美國加州爾灣市奧爾頓公園路 16215 號 92618-7013

16215 Alton Parkway, Irvine, California USA, 92618-7013

國 籍：(中文/英文) 美國/U.S.A.

電話/傳真/手機：

E-MAIL：

三、發明人：(共3人)

姓 名：(中文/英文) ID：

1. 瑞賈得·卡爾/Rajendra Khare

2. 桑迪普·雷蘭/Sandeep Relan

3. 布雷傑班德休·米什雷/Brajabandhu Mishra

國 籍：(中文/英文)

1.2.3：美國/U.S.A.

端 125 和移動終端 120 之間的通信可通過使用安全通信協定而實現保密，該通信協定比如但不局限於：諸如傳輸層安全 (TLS) 協定、安全套接字層 (SSL) 協定等等的使用數位證書的協定。

將來自特定 MSC 214 之一的控制信號傳輸到移動終端 120 可通過修改現存協定實現，該修改定義了使移動終端 120 將特定種子載入其內的偽隨機號碼生成器的命令。比如，MSC 214 可將在特定預設時間載入種子的命令以及種子一起在分頁通道上傳輸到移動終端 120。爲了增加安全性，可使用一個安全分頁通道。在接收前述信號後，在預設時間內移動終端 120 把種子載入偽隨機號碼生成器。接收種子之後，移動終端 120 可使用一個隨機訪問通道把一個肯定回應傳送到 MSC 214。

現在參見附圖 3，示出了根據本發明的一個實施例的示例性移動終端 120 的框圖。爲了清晰的目的，不準備讓此框圖作爲一個全面的圖示，並且某些元件可以被省略。

移動終端 120 包括控制器 305、非揮發性記憶體 307、小型鍵盤 310、收發器 315、揚聲器 317、麥克風 318、諸如可視螢幕 320 或者介面埠 321 的輸出、以及偽隨機號碼生成器 325。偽隨機號碼生成器 325 在規則時間內產生一個偽隨機號碼，所述時間可由系統時鐘控制。控制器 305 使當前時間變化偽隨機密碼顯示在螢幕 320 上。

隨時間變化的偽隨機密碼可以是偽隨機號碼生成器 325 產生的偽隨機號碼。可供選擇地，隨時間變化的偽隨機密碼 305 可從

理和解碼來恢復種子。

移動終端 120 通常在兩種模式之一中操作：分頁模式和活躍模式。通常，分頁模式與移動終端 120 不參與電話通話的次數有關，而活躍模式與移動終端 120 參與電話通話的次數有關。

在分頁模式期間，爲了獲得從移動電話網絡 130 上來的任何通信，移動終端 120 在規則時間間隔內掃描一個分頁通道。所述通信包括：諸如電話連接請求、時間指示符、服務質量的信號發射、以及漫遊的通知，僅僅列舉這麼一些。

分頁通道通過使用基於公共密鑰加密技術的安全協定進行保密。這樣協定的例子是 TLS、SSL，等等。這些協定交換用於授權的數位證書，並且在授權程式的最後可獲得一個唯一的會話，該會話用於在發送端加密種子，並在移動終端 120 解密種子。

在本發明一個實施例中，定義一個命令，並由 MSC 214 通過分頁通道把此命令、種子、和時間傳送到移動終端 120。依靠移動終端 120 對種子的接收使移動終端 120 在所提供時間內把種子載入偽隨機號碼生成器 325。另外，移動終端 120 經由收發器 315 傳送一個肯定回應。

相應地，非揮發性記憶體 307 可包括檢測和執行回應接收命令的前述活動的指令。前述指令可被結合爲分頁模式應用程式的一部分。

在另一模式中，依靠移動終端 120 命令的接收可在分頁模式應用程式中引起一個中斷。用於中斷的中斷處理程式在所提供時

間內可使種子被載入偽隨機號碼生成器 325。

在另一實施例中，移動終端 120 可在一個電話通話建立期間從移動電話網絡 130 接收種子。正如以上所提到的，用於終端 125 和移動終端 120 之間通信的一個預設通信協定，可包括一個指示種子將被傳送到的移動終端 120 的任意控制信號。非揮發性記憶體 307 可包括檢測任意控制信號和作用於任意控制信號的指令。在檢測任意控制信號之後，移動終端 120 準備接收種子和時間。在接收種子和時間之後，移動終端 120 在給定時間內把種子載入偽隨機號碼生成器 325。

現在參見附圖 4，示出了根據本發明的一個實施例的給偽隨機號碼生成器 325 提供一個種子的信號流程圖。在初始註冊（信號 405）期間，用戶提供與他們移動終端有關的電話號碼。作為回應，伺服器 105 為用戶分配一個種子並且確定一個同步時間。

伺服器 105 通過終端 125 經由移動電話網絡 130 傳送電話號碼、一個種子、和一個同步時間（信號 410）。移動電話網絡 130 的基礎結構識別和定位與電話號碼有關的移動終端 120，並把電話號碼、種子和同步時間路由到最接近移動終端 120 的一個 MSC 214。MSC 214 使一個基站利用一個分頁通道將種子、同步時間和一個在同步時間（信號 415）內載入種子的命令傳送到移動終端 120。

在接收種子和同步時間之後，移動終端 120 利用一個隨機訪問通道發出一個肯定回應（信號 420）到 MSC 214，再轉發回伺

網路的示例性全球系統的框圖；

圖 3 是根據本發明的一個實施例的示例性的移動終端的框圖；

圖 4 是根據本發明的一個實施例的信號流程圖，其用於配置移動終端以提供隨時間變化的隨機密碼；

圖 5 是根據本發明的另一實施例的信號流程圖，其用於配置移動終端以提供隨時間變化的隨機密碼。

【主要元件符號說明】

電腦網路 100	伺服器 105
客戶終端 115	移動終端 120
終端 125	移動電話網絡 130
無線電話網路 150	
公共陸地移動網路 (PLMN) 控制器 305	210
MSC/VLR 區域 212	移動轉換中心 (MSC) 214
集成訪問者位置寄存器 (VLR) 216	
位置區域 (LA) 218	單元 222
基站控制器 (BSC) 223	基收發器站 (BTS) 224
基站系統 (BSS) 225	本地位置寄存器 (HLR) 226
控制器 305	非揮發性記憶體 307
小型鍵盤 310	收發器 315
揚聲器 317	麥克風 318
可視螢幕 320	介面埠 321
偽隨機號碼生成器 325	
信號 405、410、415、420、435、445、505、510、525、530、545、555	

圖式：

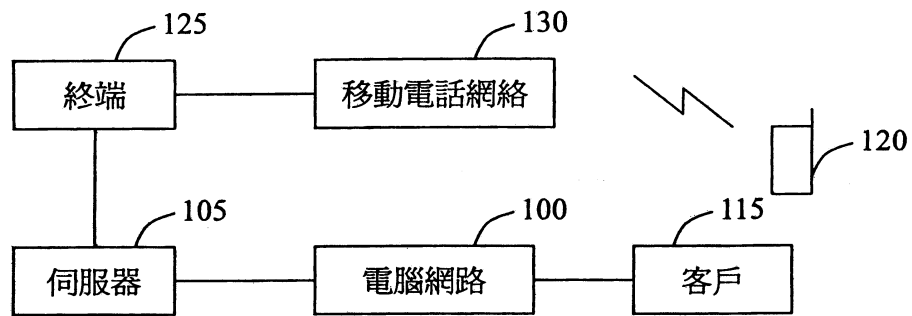


圖 1

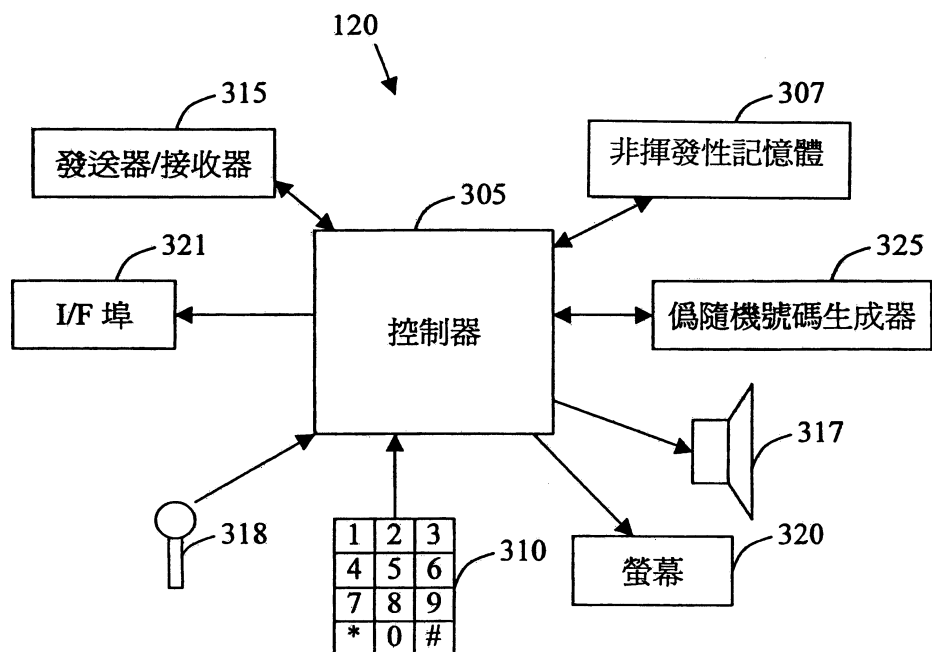


圖 3