I618440

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I618440 B**

(45)公告日： 中華民國 107 (2018) 年 03 月 11 日

(21)申請案號：102131397 (22)申請日： 中華民國 102 (2013) 年 08 月 30 日

(51)Int. Cl.： ***H04W88/04 (2009.01)*** ***H04W12/08 (2009.01)***

(30)優先權：2012/08/30 美國 61/695,022

2012/08/30 歐洲專利局 12182285.2

(71)申請人：皇家飛利浦有限公司 (荷蘭) KONINKLIJKE PHILIPS N.V. (NL)
荷蘭

(72)發明人：迪斯 華特 DEES, WALTER (NL)；彼恩森 喬哈奈斯 亞諾杜斯 寇尼利 BERNSEN, JOHANNES ARNOLDUS CORNELIS (NL)

(74)代理人：林嘉興

(56)參考文獻：

US 6965816B2 US 2010/0153727A1

WO 03/056746A1

審查人員：張智杰

申請專利範圍項數：15 項 圖式數：4 共 36 頁

(54)名稱

群組中之無線裝置之配對

PAIRING WITHIN A GROUP OF WIRELESS DEVICES

(57)摘要

本發明揭示一種用於無線通信之系統，其包括一群組無線裝置(110、120、130、140)，該群組無線裝置(110、120、130、140)包含基於由該群組共用之第一密碼資料(240)而安全連接之至少一無線主機裝置(100)。基於第二密碼資料(250)建立介於一可攜式無線裝置(200)與一無線主機裝置之間之一第二安全連接。指示該等無線裝置之至少一者以應用一第三密碼資料以用於建立與該可攜式無線裝置(200)之一直接無線安全連接。又，經由該第二安全連接指示該可攜式無線裝置以應用該第三密碼資料以用於基於該第三密碼資料建立與無線裝置之直接安全連接。最後，基於該第三密碼資料建立介於該第二裝置與一各自無線裝置之間之一各自直接無線安全連接。有利的是，在一安全無線銜接系統中減少延時。

System for wireless communication comprises a group of wireless devices (110,120,130,140) that include at least one wireless host device (100) securely connected based on first secret data (240) shared by the group. A second secure connection is set-up between a portable wireless device (200) and a wireless host device based on second secret data (250). At least one of the wireless devices is instructed to apply a third secret data for setting up a direct wireless secure connection with the portable wireless device (200). Also the portable wireless device is instructed via the second secure connection to apply the third secret data for setting up the direct secure connections with the wireless devices based on the third secret data. Finally a respective direct wireless secure connection is set-up between the second device and a respective wireless device based on the third secret data. Advantageously latency is reduced in a secure wireless docking system.

指定代表圖：

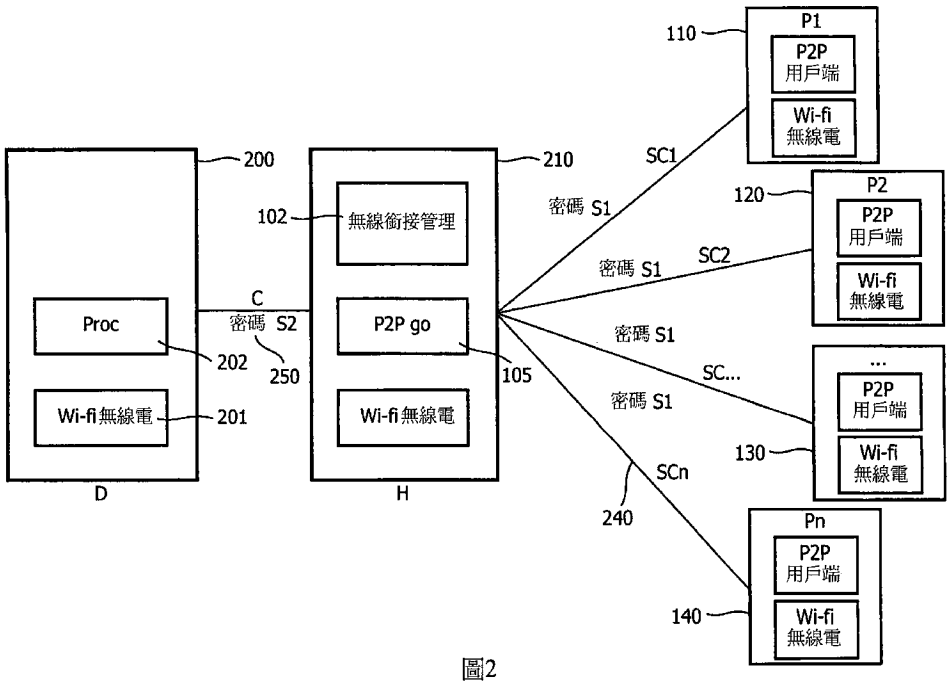

圖2

符號簡單說明：

102・・・主機通信處理器(亦稱為無線銜接管理)

110・・・無線周邊設備裝置 P1...Pn

120・・・無線周邊設備裝置 P1...Pn

130・・・無線周邊設備裝置 P1...Pn

140・・・無線周邊設備裝置 P1...Pn

200・・・可攜式裝置/銜接器 D

201・・・Wi-Fi 無線電收發器

202・・・通信處理器 PROC

210・・・無線銜接主機 H/第二無線裝置

240・・・第一密碼資料/連接線

250・・・第二密碼資料

S1・・・共同密碼/複雜密碼/密碼資料

S2・・・第二密碼資料

SC1...SCn・・・Wi-Fi Direct 連接

P1...Pn・・・無線周邊設備裝置

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】

群組中之無線裝置之配對

PAIRING WITHIN A GROUP OF WIRELESS DEVICES

【技術領域】

本發明係關於一種用於無線通信之系統，其包括一群組無線裝置及一可攜式裝置，各裝置包括用於與其他裝置無線交換資料之一無線電收發器，

- 該群組之一第一無線裝置提供一第一主機功能及該群組之一第二無線裝置提供一第二主機功能，該第一無線裝置及該第二無線裝置爲相同無線裝置或不同無線裝置；

- 該群組無線裝置共用第一密碼資料且經組態用於經由基於第一密碼資料之各自第一安全連接至提供第一主機功能之第一無線裝置之無線通信。

本發明進一步係關於用在上文用於無線通信之系統中之可攜式裝置、一主機裝置、一無線裝置、一方法及一電腦程式產品。

本發明係關於安全無線通信(例如，經由Wi-Fi)之領域，且更具體而言係關於用於一無線銜接系統之一安全建立。

【先前技術】

在無線通信(諸如自IEEE 802.11文件已知之Wi-Fi)中，需要配對裝置以建立一安全連接，例如，如經由**www.wi-fi.org**可用之文件「2004年8月由Wi-Fi聯盟發佈之基於IEEE P802.11i標準之Wi-Fi Protected Access (WPA), Enhanced Security Implementation，第3.1版」中所描述般。儘管使用Wi-Fi系統進一步闡明本發明，然應注

5

意，本發明可類似地應用於其他無線通信系統中，諸如Bluetooth(例如，參見2007年7月26日發佈之BLUETOOTH SPECIFICATION，核心封裝版本2.1+EDR)。

使用諸如WPA2之技術藉由密碼編譯構件保護Wi-Fi連接之機密性及完整性。WPA2中之安全性可基於兩個系統。第一系統爲預共用密鑰模式(PSK，亦稱爲個人模式)且經設計用於家用網路及小辦公室網路。第二系統依靠使用一802.1X鑑認伺服器且經設計用於企業網路。

在PSK模式中，彼此通信之全部裝置共用亦稱爲「複雜密碼(Passphrase)」之一256個位元密鑰。自文件「Wi-Fi Simple Configuration, Technical Specification，2011年第2.0.2版」，亦自Wi-Fi聯盟已知之Wi-Fi簡單組態(亦稱Wi-Fi保護建立)係允許知道複雜密碼之一第一裝置(例如，一無線LAN存取點)以一安全方式將該複雜密碼發送至一第二裝置而使用者不必在該第二裝置中輸入複雜密碼之一標準。代替性地，使用者可(例如)在一有限時間內在兩個裝置上推動一按鈕或將列於第一裝置上之一8個數字之PIN輸入第二裝置中以接收一複雜密碼。此通常涉及一使用者動作，即，一所謂使用者配對動作。

US2010/0153727描述多個無線裝置之間之直接鏈路通信之經改良安全性，該等無線裝置交換用於產生一共同隨機數之隨機數。自至少該共同隨機數產生一群組識別資訊元件且將其轉送至一鑑認伺服器。該鑑認伺服器自該群組識別資訊元件產生一群組直接鏈路主密鑰以匹配裝置而作爲一密鑰協議群組之部分。群組密鑰亦係基於共同隨機數產生。因此產生用於直接鏈路通信之一安全群組裝置。

【發明內容】

在Wi-Fi基礎結構中，一存取點(AP)(或更確切地其註冊器)儲存及管理其所負責之網路之認證。希望存取一AP之Wi-Fi基礎結構網路之一Wi-Fi裝置需要在與該AP之一配對操作中獲得網路認證。一旦建

立與AP之安全連接，Wi-Fi裝置即可與其他Wi-Fi裝置(其等與該AP相關聯)通信。傳統基礎結構具有連接係間接之缺點，此係因爲全部通信需要通過存取點。然而，在許多情況中，裝置將能夠建立彼此之間之一直接鏈路而不必透過存取點中繼訊務係有益的(例如，用於減少延時，改善連接速度)。已產生兩種技術Wi-Fi Direct及隧道式直接鏈路建立(TDLS)以能夠建立裝置之間之此直接Wi-Fi鏈路。

自文件「Wi-Fi Wi-Fi Peer-to-Peer (P2P) Technical Specification，2010年第1.1版」，亦自Wi-Fi聯盟已知之Wi-Fi Direct(亦稱Wi-Fi點對點)係允許Wi-Fi裝置彼此連接而無需一無線存取點之一標準。Wi-Fi Direct發揮用於連接獨立無線裝置及周邊設備(諸如支援Wi-Fi顯示器之顯示裝置/周邊設備及支援Wi-Fi串列匯流排之I/O裝置/周邊設備(例如，無線滑鼠、鍵盤、印表機、USB集線器))之一重要作用。因此，Wi-Fi Direct係用於無線銜接(使一可攜式裝置能夠連接至大量無線周邊設備之一技術)之一重要技術。在Wi-Fi Direct中，通常需要對所產生之每一個新Wi-Fi Direct連接執行一使用者配對步驟。當兩個Wi-Fi Direct裝置想要通信時，其等之一者成爲所謂群組擁有者(GO)。另一裝置承擔用戶端角色。其等一起形成一所謂P2P群組。一GO與一AP具有許多相似性。例如，其可允許其他裝置加入該P2P群組，且提供將訊務分配於該P2P群組中之不同裝置之間之可能性。然而，如之前所提及般，裝置將能夠彼此直接通信而不必中繼訊務係有益的。在Wi-Fi Direct之情況下，此將意謂你將必須個別連接至其他裝置之各者且與其他裝置之各者個別配對。尤其若涉及多個裝置，則此係繁複的。例如，對於具有大量無線周邊設備之一可攜式裝置之無線銜接，若使用者將需要個別執行與各無線周邊設備之一使用者配對步驟，則其將對使用者非常不友好。因此保持配對動作之量至一最小值係非常重要的。

自文件「2010年10月14日由IEEE出版之IEEE Std 802.11z-2010第11部分：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) 規格，第7修正案：Extensions to Direct-Link Setup (DLS)」已知之隧道式直接鏈路建立(TDLS)係能夠建立皆連接至相同Wi-Fi存取點之兩個裝置之間之一直接鏈路而無需再次配對以建立一安全直接連接之Wi-Fi中之一選項。按如下般完成此。一旦一經TDLS啓用之Wi-Fi裝置連接至AP，其即可將一請求發送至連接至相同AP之另一經TDLS啓用之裝置以建立一直接連接。在交換諸如安全性認證之資訊及關於使用哪一個Wi-Fi頻道之資訊之後，兩個裝置可開始該兩個裝置之間之一私密安全直接鏈路。

然而，TDLS具有若干缺點：

所涉及之全部裝置必須支援同時操作(以同時維持至另一裝置之一直接鏈路及至AP之一鏈路，包含在兩個不同頻率上操作)，而許多可攜式裝置及無線周邊設備裝置僅能夠建立及維持一單一Wi-Fi連接及/或單頻Wi-Fi連接。

TDLS在用於一Wi-Fi Direct網路中時(例如，TDLS透過Wi-Fi Direct GO建立一Wi-Fi Direct P2P群組內之不同裝置之間之一直接鏈路)具有若干相容性問題。例如，Wi-Fi Direct與TDLS之電力節省機構並不相容且可引起衝突。

透過一TDLS同級密鑰(TPK)交握完成TDLS直接鏈路之安全性認證之交換。問題在於：經由AP完成兩個TDLS裝置之間之此交握。因爲AP可解密所涉及之TDLS裝置之訊息，此意謂AP可竊聽此交握且能夠回復TDLS裝置對直接連接達成一致之密鑰。當使用PSK模式時，與相同AP相關聯之其他裝置亦將能夠竊聽此訊務，例如以下列方式：當一Wi-Fi裝置使用PSK與一AP相關聯時，其使用一所謂四向交握中之複雜密碼及其他資訊以產生/導出稱爲成對瞬時密鑰(PTK)之一

鏈路密鑰。該PTK用於該Wi-Fi裝置與AP之間之訊務之加密及鑑認。藉由AP使用AP及其他裝置自複雜密碼導出之鏈路密鑰(PTK)重新加密用於另一裝置之訊務。儘管AP對各相關聯Wi-Fi裝置具有一不同PTK，然與AP相關聯之持有複雜密碼之任何裝置可藉由聆聽另一裝置與AP之間之四向交握而計算所使用之PTK。因爲藉由使用此PTK該裝置可解密另一裝置與AP之間之通信，所以此意謂其亦可竊聽TDLS同級密鑰交握且計算用於保護兩個TDLS裝置之間之TDLS直接鏈路之密鑰。因此，預設TDLS不提供經由直接鏈路之安全私密通信。

一無線裝置之配對與連接建立總是不得不通過群組中之全部裝置必須連接至之存取點。你不能與群組中之用戶端/站(例如，顯示器)之任一者直接連接，除非你首先建立與存取點/群組擁有者之一連接。此意謂你可需要實體接近存取點/群組擁有者以執行配對步驟，此係因爲你不能透過群組中之其他裝置之一者與該群組連接。

本發明之一目的係提供用於安全通信之一系統，該系統保持使用者配對步驟之數目至一最小值，防止竊聽介於裝置之間之直接鏈路且提供連接至群組之靈活性。

爲此目的，在如【技術領域】中所描述般之用於無線通信之系統中，

可攜式裝置包括一裝置通信處理器，該裝置通信處理器用於

- 使用基於不同於第一密碼資料之第二密碼資料之一配對程序建立與提供第二主機功能之第二無線裝置之一第二安全連接，

- 經由該第二安全連接接收一第二指令，且根據該第二指令，

- 使用基於第三密碼資料之一各自配對程序建立與群組之至少一無線裝置之一各自直接無線安全連接，該第三密碼資料不同於第一密碼資料；

提供第二主機功能之第二無線裝置包括一主機通信處理器，該

主機通信處理器用於

- 使用基於第二密碼資料之配對程序建立與可攜式裝置之第二安全連接，

- 經由第一安全連接將一第一指令傳送至至少一無線裝置以應用第三密碼資料以用於建立與可攜式裝置之一直接無線安全連接，及

- 經由第二安全連接將一第二指令傳送至可攜式裝置以應用第三密碼資料以用於基於該第三密碼資料建立與該至少一無線裝置之直接無線安全連接；

該至少一無線裝置包括一通信處理器，該通信處理器用於

- 經由第一安全連接接收第一指令，且根據該第一指令，

- 使用基於第三密碼資料之各自配對程序建立與可攜式裝置之各自直接無線安全連接。

爲此目的，根據本發明之一進一步態樣，在如【技術領域】中所描述般之無線裝置系統中之無線通信之方法包括

- 使用基於不同於第一密碼資料之第二密碼資料之一配對程序建立可攜式裝置與提供第二主機功能之第二無線裝置之間之一第二安全連接；

- 經由第一安全連接將一第一指令傳送至該群組之至少一無線裝置以應用一第三密碼資料以用於建立與可攜式裝置之一直接無線安全連接，該第三密碼資料不同於第一密碼資料(240)，及

- 經由第二安全連接將一第二指令傳送至可攜式裝置以應用第三密碼資料以用於基於該第三密碼資料建立與該至少一無線裝置之直接無線安全連接；

- 使用基於該第三密碼資料之一各自配對程序建立可攜式裝置與該至少一無線裝置之間之一各自直接無線安全連接。

安全系統及方法之主要元件啓用一可攜式裝置A (例如，Wi-Fi

Direct相容)以連接至一群組G無線裝置。該群組G經預組態以作爲連接至提供一第一主機功能之一無線裝置之一群組且共用一共同密碼S1(其用於使該群組內之通信安全)。該群組可(例如)包括一無線銜接主機及無線周邊設備。裝置A連接至無線裝置之在群組中藉由提供一第二主機功能而作爲一第二主機裝置之使用密碼S2用於使經由第二安全連接之通信安全之一者。隨後，該群組中之裝置及裝置A得到關於另一密碼S3之指示，接著裝置A開始聆聽連入連接，接著一或多個裝置使用與裝置A自動配對(例如，以與Wi-Fi Direct相容之一方式)之密碼S3建立與裝置A之一直接安全無線連接。視需要，第二主機裝置係與提供第一主機功能之無線裝置相同之裝置。因此，可在一單一無線裝置中實施第一主機功能及第二主機功能。此外，群組G可含有僅能夠支援一P2P用戶端或一Wi-Fi站(STA)角色且非支援一P2P群組擁有者或Wi-Fi存取點(AP)角色之裝置。

該等措施具有提供一無線安全通信系統及安全協定用於分配密碼(該等密碼用於使用最小使用者配對步驟以防止竊聽介於裝置之間之直接鏈路之一方式建立安全直接鏈路)之效應，且此外該效應藉由允許能夠執行第二主機之功能之任何裝置成爲至執行一功能之群組無線裝置之進口點而提供額外靈活性。例如，該群組裝置可針對如一智慧型手機之一可攜式裝置(亦稱銜接器(dockee))提供一銜接環境。特定言之，銜接器並非總是必須使用銜接系統中用於與該群組連接之相同裝置(例如，一AP或GO)，而是可連接至該群組中提供該第二主機功能之任何裝置。

本發明亦基於以下認知(使用Wi-Fi環境作爲一實例)。當一群組Wi-Fi Direct裝置針對另一無線裝置一起執行功能(諸如無線銜接)時，期望另一無線裝置能夠建立與群組中之無線裝置之任一者之一或多個點對點鏈路而無需個別執行與來自該群組之此等裝置之各者之一使用

者配對動作。

Wi-Fi Direct具有一群組擁有者(GO)之概念。若該群組中之全部Wi-Fi Direct裝置將連接至相同GO，且該GO支援Wi-Fi Direct之所謂Intra-BSS分配特徵，則足以使另一無線裝置連接至此GO以能夠與該群組中之全部裝置通信。一Intra-BSS分配域指示P2P裝置是否正在主持(hosting)或意欲主持一P2P群組，該P2P群組在該P2P群組中之用戶端之間提供一資料分配服務。然而，全部通信將不得不通過該GO。此係非常無效率的且增加通信之延時。對於諸如無線銜接之功能，延時係一重要的問題。與無線顯示器、滑鼠、鍵盤等之連接需要盡可能低的延時。因此，能夠建立與群組之多個或甚至全部成員之直接(即，點對點)連接係重要的。然而，此將需要針對想要連接至此群組周邊設備之每一個無線銜接器執行之多個使用者配對步驟。出於先前章節所提及之原因，使用TDLS並非克服此問題之一選項。

另一問題在於，Wi-Fi Direct對裝置施加特定限制，諸如一P2P裝置僅可連接至一單一GO之限制。一旦該P2P裝置連接至一GO，其即改變角色，即，該裝置成爲一P2P用戶端。Wi-Fi Direct定義針對P2P用戶端之各種限制，諸如對可發現性及在P2P用戶端之間通信之限制。此外，通常可在一單一裝置上運行之同時P2P用戶端執行個體之數目亦非常有限的。預期許多低階無線周邊設備(諸如一Wi-Fi滑鼠或鍵盤)歸因於其等之資源限制而甚至具有進一步限制，諸如僅支援P2P用戶端角色且僅支援一單一Wi-Fi鏈路。

發明者已知藉由安全協定克服以上問題，該安全協定經由第二主機產生第三密碼資料且指示可攜式裝置(銜接器)及群組之無線裝置以應用該第三密碼資料以用於將第一裝置連接至該群組之選定無線裝置，例如，構成一預組態銜接環境。

視需要，在可攜式裝置中，裝置通信處理器進一步經配置用於

作爲一群組擁有者控制經由該直接無線連接之通信。一般而言，在一無線網路系統中一裝置可作爲一群組擁有者(例如，在無線區域網路(WLAN)中執行AP角色)控制--群組裝置。在Wi-Fi中之一實例中，第一裝置在建立進一步無線裝置之一子集G'中之裝置與第一裝置之間之Wi-Fi Direct P2P連接時承擔一Wi-Fi Direct群組擁有者角色。

視需要，在可攜式裝置中，裝置通信處理器進一步經配置用於使用基於各自不同第三密碼資料之一各自配對程序建立與各自不同子集之各自無線裝置之各自不同直接無線安全連接。有利的是，提供多個子集以經由第三密碼資料之不同執行個體與第一裝置通信。

視需要，在可攜式裝置中，裝置通信處理器進一步經配置用於接收包含用於多個子集之各自不同第三密碼資料之第二指令。有利的是，提供多個子集以經由一單一指令與可攜式裝置通信。

視需要，在可攜式裝置中，裝置通信處理器進一步經配置用於產生第三密碼資料且將該第三密碼資料傳送至提供第二主機功能之裝置。有利的是，該可攜式裝置藉由控制該第三密碼資料之產生而控制安全性。

視需要，在可攜式裝置中，裝置通信處理器經配置用於在起始建立與子集之一各自無線裝置之各自直接無線安全連接之前斷開第二安全連接。有利的是，需要更少無線電收發器能力且使用更少容量之無線媒體。

視需要，在可攜式裝置中，裝置通信處理器經配置用於提供一持久分組，且因此用於在斷開基於該第三密碼資料之各自直接無線安全連接之後，再次基於該第三密碼資料建立一進一步各自直接無線安全連接。有利的是，當一可攜式裝置(例如，一銜接器)重新連接時，更快恢復安全通信。

視需要，在可攜式裝置中，裝置通信處理器經配置用於：當在

斷開基於該第三密碼資料之各自直接無線安全連接之後，使用在初期配對期間獲取之第二密碼資料或第三密碼資料與子集之各自無線裝置重新連接以用於建立一各自直接無線安全連接。有利的是，當一可攜式裝置(例如，一銜接器)重新連接時，更快恢復安全通信。

視需要，第二安全連接包括一Wi-Fi Direct P2P連接。實務上，該連接可爲一Wi-Fi Direct P2P連接且其中第二密碼資料(S2)係一Wi-Fi複雜密碼，例如，Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK)。

視需要，各自直接無線安全連接包括一Wi-Fi Direct點對點連接，及/或該各自直接無線安全連接包括一隧道式直接鏈路建立(TDLS)連接。實務上，子集G'中之裝置與第一裝置之間之直接連接可爲Wi-Fi Direct P2P連接且其中第三密碼資料係一Wi-Fi複雜密碼，例如，Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK)。或者，子集G'中之裝置與第一裝置之間之直接連接爲TDLS連接。此外，配對程序可包括一Wi-Fi保護存取(WPA/WPA2)或Wi-Fi簡單組態程序。有利的是，此已知配對程序可已經在無線裝置中可用且可被共用。

視需要，一預組態步驟涉及：指定提供第二主機功能之裝置爲由第二主機裝置及群組G中之裝置組成之一P2P群組之一Wi-Fi Direct P2P群組擁有者；及將群組中之裝置之各者與第二主機裝置配對以自該第二主機裝置得到共同密碼S1且其中S1係複雜密碼(Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK))。

視需要，在主機裝置中，主機通信處理器經配置用於產生第三密碼資料。有利的是，主機裝置藉由控制該第三密碼資料之產生而控制安全性。

視需要，在主機裝置中，主機通信處理器經配置用於針對第一裝置之各自、不同執行個體產生一組各自、不同第三密碼資料。有利

的是，在不同第一裝置中防止竊聽通信。

視需要，在主機裝置中，主機通信處理器經配置用於當裝置(A)在斷開第二安全連接之後之一各自、進一步時間建立第二安全連接時產生一組各自、不同第三密碼資料。有利的是，藉由產生不同組第三密碼資料而避免重播攻擊。

視需要，在主機裝置中，主機通信處理器經配置用於針對群組中之各自、不同無線裝置之一子集產生一組各自、不同第三密碼資料。有利的是，提供多個子集以經由第三密碼資料之不同執行個體與第一裝置通信。

視需要，在主機裝置中，主機通信處理器經配置用於產生基於或等於第二密碼資料之第三密碼資料。基本上，可選擇不同於第二密碼資料之第三密碼資料，該第三密碼資料改良安全性。有利的是，可基於第二密碼資料產生第三密碼資料，該第三密碼資料改良效率。又，可選擇等於第二密碼資料之第三密碼資料，該第三密碼資料在需要傳送更少資料時改良速度。

視需要，在主機裝置中，主機通信處理器經配置用於指派一有限壽命至第三密碼資料，及/或取決於裝置(A)之一授權層級指派一壽命至第三密碼資料。有利的是，在時間上限制安全系統之存取，或可指派一客體或擁有者不同權利。

視需要，在主機裝置中，主機通信處理器經配置用於將一第三指令傳送至子集之各自無線裝置以用於在建立至裝置之各自直接無線安全連接之前斷開第一安全連接。有利的是，需要更少無線電收發器能力且使用更少容量之無線媒體。

視需要，主機裝置係一無線銜接主機或一無線銜接站。實務上，該主機裝置可爲與第一無線主機裝置及/或第二無線主機裝置相同的裝置。因此，可在一單一銜接主機或無線銜接站中實施第一主機

功能及第二主機功能。

視需要，在無線裝置中，各自通信處理器經配置用於起始至可攜式裝置之各自直接無線安全連接之建立。有利的是，該無線裝置控制該建立。

視需要，在無線裝置中，各自通信處理器經配置用於在建立至可攜式裝置之各自直接無線安全連接之前斷開第一安全連接。有利的是，需要更少無線電收發器能力且使用更少容量之無線媒體。

視需要，在無線裝置中，各自通信處理器經配置用於在斷開至可攜式裝置之各自直接無線安全連接之後恢復第一安全連接。有利的是，在斷開第一裝置之後自動重新連接預組態群組。

視需要，主機裝置能夠爲兩個獨立Wi-Fi Direct P2P群組之部分，一群組由群組G中之裝置組成且一群組由具有與該主機裝置之一P2P連接之可攜式裝置組成。

視需要，在可攜式裝置A連接之前，主機裝置將密碼S3通知給群組G中之其他裝置。有利的是，更快完成該可攜式裝置至該群組之連接(例如，銜接程序)。

視需要，主機裝置支援Wi-Fi Direct持久群組操作。視需要，主機裝置使用Wi-Fi Direct P2P邀請程序邀請群組G中之裝置連接至該主機裝置。視需要，自動配對程序係基於Wi-Fi保護存取(例如，WPA或WPA2)。視需要，自動配對程序係基於Wi-Fi簡單組態。視需要，可攜式裝置支援Wi-Fi Direct intra-BSS分配使得群組G中之無線裝置可仍然彼此通信以一起執行一功能，而無需一骨幹。視需要，可攜式裝置支援Wi-Fi Direct持久分組操作且使用在透過第二主機裝置與群組之一第一連接期間擷取之第三密碼資料在隨後連接中連接至子集G'之裝置。有利的是，此等選項係經Wi-Fi啓用裝置之現有元件之延伸。

在隨附申請專利範圍中給出根據本發明之裝置及方法之進一步

較佳實施例，其等之揭示內容以引用的方式併入本文中。

【圖式簡單說明】

自藉由以下描述中之實例且參考附圖描述之實施例將明白本發明之此等態樣及其他態樣且進一步參考該等實施例闡明本發明之此等態樣及其他態樣，其中

圖1展示在預組態期間之一無線銜接系統，

圖2展示建置至一主機之一連接之一無線裝置，

圖3展示指示經連接無線裝置之一無線主機，及

圖4展示直接連接進一步無線裝置之一無線裝置。

該等圖係純粹圖解的且並不按比例繪製。在該等圖中，對應於已描述元件之元件可具有相同元件符號。

【實施方式】

現論述一無線銜接系統之一詳細實施方案實例。無線銜接係關於啓用可攜式裝置(所謂無線銜接器或WD)以無線連接至一群組無線周邊設備使得該可攜式裝置上之應用可利用此等周邊設備以改善與此等應用一起作業/交互作用之體驗及生產力。藉由一所謂無線銜接主機(WDH)執行分組周邊設備、發現群組周邊設備、管理至群組周邊設備之連接。

可能無線銜接器包含(但不限於)行動電話、膝上型電腦、平板電腦、可攜式媒體播放器、相機。可能WDH包含(但不限於)專用無線銜接站裝置、顯示裝置、音訊裝置、印表機、個人電腦(PC)。可能周邊設備包含(但不限於)無線滑鼠、鍵盤、顯示裝置、音訊裝置、網路攝影機、印表機、儲存裝置、USB集線器。此等周邊設備應視爲支援諸如Wi-Fi串列匯流排及Wi-Fi顯示器之標準以使其等功能性透過無線網路可用於其他裝置(諸如銜接器及WDH)。有線周邊設備可藉由經由導線將其等連接至一中間裝置而連接至無線網路，且該中間裝置如在

此文件中所定義般可無線連接，例如，支援Wi-Fi串列匯流排之一USB集線器裝置。周邊設備及銜接器其等本身亦可爲WDH。

圖1展示在預組態期間之一無線銜接系統。該無線銜接系統具有一無線銜接主機裝置H 100，及若干無線周邊設備裝置P1...Pn 110、120、130、140。該等裝置全部具有一Wi-Fi無線電收發器101、111且支援參與一Wi-Fi Direct P2P群組。一些周邊設備裝置可限制於僅支援作爲一P2P用戶端或一舊型用戶端。

圖1繪示預組態一組用於無線銜接之周邊設備之一起始情形。該等周邊設備裝置形成透過Wi-Fi Direct連接150 SC1...SCn連接至一主機裝置H 100之一群組190之無線裝置，該主機裝置H 100作爲由H及作爲P2P用戶端之周邊設備P1...Pn形成之P2P群組之群組擁有者(P2P GO)。其中無線裝置具有展示爲具有P2P用戶端之功能之一各自通信處理器112。實務上，如此已知此等無線裝置及/或主機裝置之通信處理器且可在一專用積體電路中、在一可程式化電路中及/或在韌體(在一微控制器或專用處理器上執行該韌體)中實施該通信處理器。該等通信處理器經配置以如下文所闡釋般執行通信處理程序。

建立Wi-Fi Direct連接SC1...SCn需要一配對步驟(例如，使用Wi-Fi簡單組態(WSC))。在該配對步驟期間，藉由H提供一共同密碼S1以基於Wi-Fi保護存取(WPA/WPA2)建置一安全連接。該密碼S1可爲複雜密碼(Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK))，其用於四向交握中以建立Wi-Fi保護存取(WPA/WPA2)。

存在分配密碼S1之許多可能性，例如，可使用Wi-Fi簡單組態分配密碼S1或可將密碼S1預組態於全部相關裝置中。無線銜接主機裝置H亦具有一主機通信處理器102(亦稱爲無線銜接管理)以儲存關於周邊設備之資訊、持續追蹤連接、建置密碼、指示其他裝置以組態一起形成一無線銜接環境之周邊設備。

圖2展示建置至一主機之一連接之一無線裝置。該無線裝置200稱爲一銜接器D且展示於類似於上文圖1之一無線銜接系統中。該無線裝置具有一Wi-Fi無線電收發器201及用於控制通信處理程序之一通信處理器PROC 202。

在該系統中無線銜接器D建置與一無線銜接主機H 210之一Wi-Fi Direct連接C 250以與一組周邊設備銜接。此特定實施方案實例僅展示解決方案以藉此該銜接器建立至該無線銜接主機H且非至裝置P1...Pn之任一者之一起始銜接連接(所謂導頻連接)。應注意，類似地，當此等進一步無線裝置之任一者經配置以執行用於建立起始連接之主機功能時，該銜接器可建立至該等進一步無線裝置P1...Pn之任一者之起始連接。因此，主機功能可藉由一單一裝置執行或可分配於不同裝置中。

在爲建立連接C之D與H之間之配對步驟期間，H確保出於安全原因藉由H提供不等於S1之一密碼S2以基於Wi-Fi保護存取(WPA/WPA2)建置一安全連接。類似於如連接線240所指示般之基於密碼資料S1之連接SC1...SCn，密碼S2係複雜密碼(Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK))，其用於四向交握中以建立Wi-Fi保護存取(WPA/WPA2)。存在分配密碼S2之許多可能性，例如，可使用Wi-Fi簡單組態分配密碼S2或可將密碼S2預組態於全部相關裝置中。在此實施方案實例中，D連接至H之P2P GO，藉此D自動成爲P2P用戶端。或者，D與H形成獨立於在H與周邊設備之間建置之P2P群組之一新P2P群組，藉此D或H可成爲P2P GO。

圖3展示指示經連接無線裝置之一無線主機。一無線主機H 310係展示於類似於上文圖1及圖2之無線銜接系統中。該圖繪示自該無線銜接主機H 310接收指令之銜接器D 200及周邊設備P1...Pn 110、120。

該圖展示H透過指令I1...In 320指示一或多個周邊設備且亦透過

指令DI 330指示銜接器關於在該等周邊設備與D之間之一自動配對步驟期間使用密碼S3。此等指令及訊息可使用許多不同通信協定而採取任何格式(自MAC訊框中之二進制編碼指令至經由HTTP之XML編碼指令之範圍)。

除了密碼資料S3之外，該等指令亦可包含關於裝置在接收該等指令之後需要執行哪些動作(諸如斷開與H之連接且建立與D之一連接)之資訊。周邊設備可需要具有關於D將使用於告示其之Wi-Fi Direct能力之服務組識別符SSID之資訊，且D可需要具有諸如將建置一連接之周邊設備之唯一識別符之資訊。一或多個周邊設備裝置Pi亦可保持連接至H。此等裝置可接收保持連接至H或自H斷開之一指令。在圖3中，假定裝置P3...Pn-1接收保持連接至H之一指令。

使用藉由自密碼資料S2導出之一密鑰保護之頻道C，亦將密碼資料S3發送至銜接器D。此意謂D與一或多個周邊設備可使用四向交握直接建立WPA/WPA2保護連接且意謂並不需要執行涉及輸入PIN碼之可能使用者互動之一Wi-Fi簡單組態程序。不必執行該Wi-Fi簡單組態程序亦加速銜接程序。

圖4展示直接連接進一步無線裝置之一無線裝置。一無線裝置D 400係展示於類似於上文圖1、圖2及圖3之無線銜接系統中。該圖繪示銜接器D 400及一子集(例如，經直接連接且視需要自無線銜接主機H 100斷開(藉由虛線430指示)之周邊設備P1...Pn之三個周邊設備110、120、140)。在該圖中，一周邊設備130並未連接至銜接器D且保持僅連接至無線銜接主機100。

該圖展示其中裝置P1、P2及Pn已使用藉由420指示之密碼資料S3(複雜密碼S3)建立與銜接器裝置D之直接連接SP1、SP2及SPn之情形。D作爲SD1、SD2及SDn之一Wi-Fi Direct群組擁有者(藉由圖中之P2P GO單元403指示)。與H之連接SC1、SC2及SCn可釋放或可保持

主動。圖4中之點狀線反映此。銜接涉及銜接器D改變角色及成爲無線周邊設備之子集之一P2P GO。在WPA/WPA2四向交握期間，S3可用作導出鏈路密鑰(成對瞬時密鑰)之一共同密碼(Wi-Fi成對主密鑰(PMK)或Wi-Fi預共用密鑰(PSK))。或者，S3係用於Wi-Fi保護建立配對程序中，其中代替使用者輸入(例如)一PIN碼，自S3導出該PIN。

實務上，上文無線銜接系統可應用於將一無線銜接器D直接連接至一顯示裝置或一(USB)滑鼠/鍵盤以用於降低延時。可指示該等裝置使用一預定義組態組。經斷開裝置可進入睡眠。視需要，無線主機可指示該等經斷開裝置按一特定規則時間間隔醒來以能夠發現其等且與其等再次連接。

在一實例系統中一無線周邊設備裝置P(例如，一Wi-Fi顯示器)可最初經由一安全頻道C基於一鏈路密鑰(成對瞬時密鑰)(其基於一複雜密碼S1)連接至一無線主機H。該主機作爲群組擁有者(GO)且P作爲用戶端。H及P兩者皆支援Wi-Fi Direct持久P2P分組。其中P將複雜密碼S1儲存於其記憶體中。銜接器D最初使用基於複雜密碼S2之一鏈路密鑰(成對瞬時密鑰)經由直接在一安全頻道D上之Wi-Fi與主機H連接。H經由一銜接組態協定指示銜接器D必須接受經由Wi-Fi之一負載連接。當使用一複雜密碼S3產生如周邊設備P所同意之一鏈路密鑰(成對瞬時密鑰)M時，經由在D處之一群組擁有者單元實現與周邊設備P之直接連接。H亦指示P在使用如D所同意之鏈路密鑰(成對瞬時密鑰)M時其必須連接至周邊設備D之GO。此後P可斷開與H之連接且使用鏈路密鑰(成對瞬時密鑰)M建立與D之一鏈路。若斷開P與D之間之連接(例如，若D未銜接)，則P可使用原始複雜密碼S1重新連接至H。

在一實際實施例中可按如下般實施如上文所述般之經改良無線銜接系統。在實例無線銜接系統中存在一無線主機WDH(一無線裝置WD可透過其銜接)。該WDH透過有線及無線介面連接至周邊設備P。

且亦可具有內建PF。進一步假定一些無線PF具有額外內建功能性使得其等可經指示以直接連接至一經銜接WD或經裝配以執行無線主機功能。

藉由經改良無線銜接系統實現以下優點。PF可快速連接至一WD(不需要執行Wi-Fi簡單組態WSC協定)且無需使用者介入。僅經允許銜接一次之一WD在脫離銜接之後未再啓用與其原先銜接之PF或WDH再次自動連接。爲私密性及完整性保護介於一WD與該WD銜接之WDH之間之Wi-Fi通信。又，可先前與該WDH銜接之其他WD不能解密此通信或在沒有偵測之情況下惡意破壞此通信。爲私密性及完整性保護介於一WD與該WD在銜接期間直接連接之PF之間之Wi-Fi通信。又，可先前與此等PF連接之其他WD不能解密此通信或在沒有偵測之情況下惡意破壞此通信。爲私密性及完整性保護介於一WDH與一經Wi-Fi連接之PF之間之通信。又，儘管與此WDH銜接之WD將自該WDH接收一些此通信且接收源自與此WDH銜接之該WD之一些此通信，然WD不能解密此通信或在沒有偵測之情況下惡意破壞此通信。經允許銜接一次以上之一WD在其首次銜接時不得不執行WSC僅一次且在其再次銜接時可在不使用WSC之情況下銜接。一WD及WDH皆可經預組態使得該WD可總是自動銜接。

在實例經改良無線銜接系統中定義以下階段：建立(或組態)階段、未經銜接模式、銜接階段及控制或非控制之脫離銜接階段。

在一建立階段中一WDH使用SSID SSID1及複雜密碼PP1將其自身建立爲一P2P群組G1之一P2P GO。該WDH僅接受PF加入G1。許多PF使用用於獲得PP1之PBC或WSC-PIN而加入G1。亦可針對SSID1及PP1預組態該等PF。

在未經銜接模式中WDH使用SSID SSID2(但尚未決定用於G2之一複雜密碼)將其自身建立爲一P2P群組G2之一P2P GO。WDH可針對G2

發送信標訊框。WDH回應於探測請求訊框。WDH在相關資訊元件中給出其係一WDH、關於其之PF、關於其之WDE等資訊。WDH僅接受WD加入G2。

在一銜接階段中已發現G2之一WD要求加入G2。此觸發銜接動作。若不允許該WD銜接，則拒絕經請求之銜接動作。若該WD之前已銜接且若允許該WD再次銜接，則WDH將其之前與該WD一起使用之複雜密碼設定爲用於G2之複雜密碼PP2。在全部其他情況中(因此當WD之前從未銜接時，或當其之前已銜接但經允許僅銜接一次時)，WDH產生一新的隨機PP2作爲用於G2之複雜密碼。WDH使用P2P群組G1將SSID2、PP2、WD位址及WD ID發送至全部PF(因此使用自PP1導出之一密鑰加密且因此針對全部WD及全部其他裝置保持私密)。若使用用於此WDH之一複雜密碼預組態WD或該WD仍持有來自一先前銜接會期之一複雜密碼，則該WD可在一四向交握中嘗試且使用該複雜密碼。以其他方式，或當使用舊複雜密碼失效時，WD與WDH一起針對P2P群組G2執行WSC以獲得PP2。WSC可使用PBS或WSC-PIN(其使用WD或WDH PIN)。

若在加入G2之後，沒有PF將直接連接至WDH，則WD與WDH透過該WDH建立至PF之一負載連接且銜接該WD。

若一或多個PF將直接連接至WD，則該WD與WDH交換GO角色。該WDH發送支援建立一直接Wi-Fi連接之全部PF之位址/ID至該WD。其可排除出於某種原因透過該WDH安排路線之負載連接係最佳之PF之位址。吾人稱此等「直接」PF。全部其他PF稱爲「間接」PF。使用P2P群組G1作爲通信構件，WDH要求直接PF使用複雜密碼PP2加入P2P群組G2。有效的是，在此實例中第二密碼資料等於第三秘密資料。因爲直接PF現知道PP2，所以其等不需要執行WSC以加入G2，此節省大量時間(即使(例如)預佈建PIN)。此等PF使用其等知道之複雜密

碼(PP2)簡單地執行與WD之四向交握。WD已獲得所涉及之直接PF之位址因此知道哪些直接PF預期連接。透過G2之WD及透過G1之PF兩者皆可將P2P群組G2加入已成功或失效傳訊至WDH。(例如)若一PF與WD之間之距離太大，則該PF可能無法加入P2P群組G2。加入失效之直接PF成爲間接PF且保持連接至WDH。WD針對已成功加入G2之PF(即，直接PF)建立直接負載連接。使用自PP2導出之一密鑰保護此等負載連接。WD與WDH透過該WDH建立至其他PF(即，間接PF)之一負載連接且銜接該WD。若WDH同時支援一個以上WD，則其可建立一新SSID以接受一新WD用於銜接。

在一脫離銜接階段中可以一控制或非控制方式完成脫離銜接。控制脫離銜接係藉以使WD對WDH指示其想要脫離銜接。非控制脫離銜接係在WDH在沒有自WD接收到其想要脫離銜接之一指示之情況下以某種方式偵測到WD已離開或不可到達時。

在控制脫離銜接期間，當一WD想要脫離銜接時，該WD使用P2P群組G2作爲通信構件將一訊息(其意謂該WD想要脫離銜接)發送給WDH。WDH確認成功接收此訊息。在成功遞送該訊息之後，WD將藉由使用原因代碼3將解鑑認訊框發送給WDH及G2中之PF而結束P2P群組G2會期。在接收解鑑認訊框之後，PF斷開負載連接。使用P2P群組G1作爲通信構件，WDH指示直接PF刪除所使用之PP2。或者，若不允許WD再次銜接則WDH可僅完成此。在此情況中，PF必須儲存稍後用於經允許再次銜接之WD之複雜密碼及WD ID組合。此可在銜接操作期間節省一些時間。儘管如此WDH必須持續追蹤哪一PF已接收哪些複雜密碼。WDH指示間接PF斷開負載連接。WDH再次假定P2P群組G2之GO角色且設定複雜密碼爲未決定的。WDH現可再次告示未銜接狀態。

在非控制脫離銜接期間，WDH在沒有自WD接收到其想要脫離銜

接之一指示之情況下以某種方式決定WD已離開或不可到達。WDH通知全部PF斷開(直接或間接)負載連接。使用P2P群組G1作爲通信構件，WDH指示直接PF刪除所使用之PP2。或者，若不允許WD再次銜接則WDH可僅完成此。在此情況中，PF必須儲存稍後用於經允許再次銜接之WD之複雜密碼及WD ID組合。此可在銜接操作期間節省一些時間。儘管如此WDH必須持續追蹤哪一PF已接收哪些複雜密碼。WDH再次假定P2P群組G2之GO角色且設定該複雜密碼爲未決定的。WDH現可再次告示未銜接狀態。

儘管主要藉由使用無線銜接之實施例闡釋本發明，然本發明亦適用於其中一未連接無線裝置需要連接至一群組裝置之任何無線系統。本發明係相關於經Wi-Fi銜接啓用之裝置、Wi-Fi串列匯流排裝置、Wi-Fi顯示裝置及支援Wi-Fi Direct之任何其他裝置，其等在自可攜式音訊裝置、行動電話、膝上型電腦、平板電腦至Wi-Fi滑鼠、鍵盤、顯示裝置、印表機、相機之範圍內。

應注意，可以硬體及/或軟體使用可程式化組件實施本發明。用於實施本發明之一方法具有對應於針對如參考圖1所描述般之系統所定義之功能之步驟。

將理解，爲清晰起見之以上描述已參考不同功能單元及處理器描述本發明之實施例。然而，將明白，可在不偏離本發明之情況下使用不同功能單元或處理器之間之功能性之任何合適分配。例如，經繪示以藉由分離單元、處理器或控制器執行之功能性可藉由相同處理器或控制器執行。因此，對特定功能單元之參考應僅看作爲對用於提供所描述之功能性而非指示一嚴格邏輯或實體結構或組織之合適構件之參考。可以包含硬體、軟體、韌體或此等之任何組合之任何合適形式實施本發明。

應注意：在此文件中文字「包括」並不排除存在除所列出之元

件或步驟之外之其他元件或步驟且在一元件之前之文字「一」並不排除存在複數個此等元件；任何元件符號並未限制申請專利範圍之範疇；可藉由硬體及軟體兩者實施本發明；若干「構件」或「單元」可由硬體或軟體之相同品項表示且一處理器可能與硬體元件協作而可實現一或多個單元之功能。此外，本發明並不限於實施例且本發明在於每一個新穎特徵或上文所描述或敘述在相互不同申請專利範圍附屬項中之特徵之組合。

【符號說明】

100	無線銜接主機裝置H/第一無線裝置
101	Wi-Fi無線電收發器
102	主機通信處理器(亦稱爲無線銜接管理)
110	無線周邊設備裝置P1...Pn
111	Wi-Fi無線電收發器
112	通信處理器
120	無線周邊設備裝置P1...Pn
130	無線周邊設備裝置P1...Pn
140	無線周邊設備裝置P1...Pn
150	Wi-Fi Direct連接
190	群組
200	可攜式裝置/銜接器D
201	Wi-Fi無線電收發器
202	通信處理器PROC
210	無線銜接主機H/第二無線裝置
240	第一密碼資料/連接線
250	第二密碼資料
310	無線銜接主機H

320　指令I1...In

330　指令DI

400　無線裝置D/銜接器D

403　P2P GO單元

420　第三密碼資料

430　虛線

SC1...SCn　Wi-Fi Direct連接

S1　共同密碼/複雜密碼/密碼資料

S2　第二密碼資料

S3　密碼/複雜密碼/密碼資料

I1...In　指令

SP1、SP2、SPn　直接連接

P1...Pn　無線周邊設備裝置

S

公告本

發明摘要

※ 申請案號：102131397

※ 申請日： 102/08/30 ※IPC 分類：*H04W 88/04* (2009.01)
H04W 12/08 (2009.01)

【發明名稱】

群組中之無線裝置之配對

PAIRING WITHIN A GROUP OF WIRELESS DEVICES

【中文】

本發明揭示一種用於無線通信之系統，其包括一群組無線裝置(110、120、130、140)，該群組無線裝置(110、120、130、140)包含基於由該群組共用之第一密碼資料(240)而安全連接之至少一無線主機裝置(100)。基於第二密碼資料(250)建立介於一可攜式無線裝置(200)與一無線主機裝置之間之一第二安全連接。指示該等無線裝置之至少一者以應用一第三密碼資料以用於建立與該可攜式無線裝置(200)之一直接無線安全連接。又，經由該第二安全連接指示該可攜式無線裝置以應用該第三密碼資料以用於基於該第三密碼資料建立與無線裝置之直接安全連接。最後，基於該第三密碼資料建立介於該第二裝置與一各自無線裝置之間之一各自直接無線安全連接。有利的是，在一安全無線銜接系統中減少延時。

5

【英文】

System for wireless communication comprises a group of wireless devices (110,120,130,140) that include at least one wireless host device (100) securely connected based on first secret data (240) shared by the group. A second secure connection is set-up between a portable wireless device (200) and a wireless host device based on second secret data (250). At least one of the wireless devices is instructed to apply a third secret data for setting up a direct wireless secure connection with the portable wireless device (200). Also the portable wireless device is instructed via the second secure connection to apply the third secret data for setting up the direct secure connections with the wireless devices based on the third secret data. Finally a respective direct wireless secure connection is set-up between the second device and a respective wireless device based on the third secret data. Advantageously latency is reduced in a secure wireless docking system.

圖式

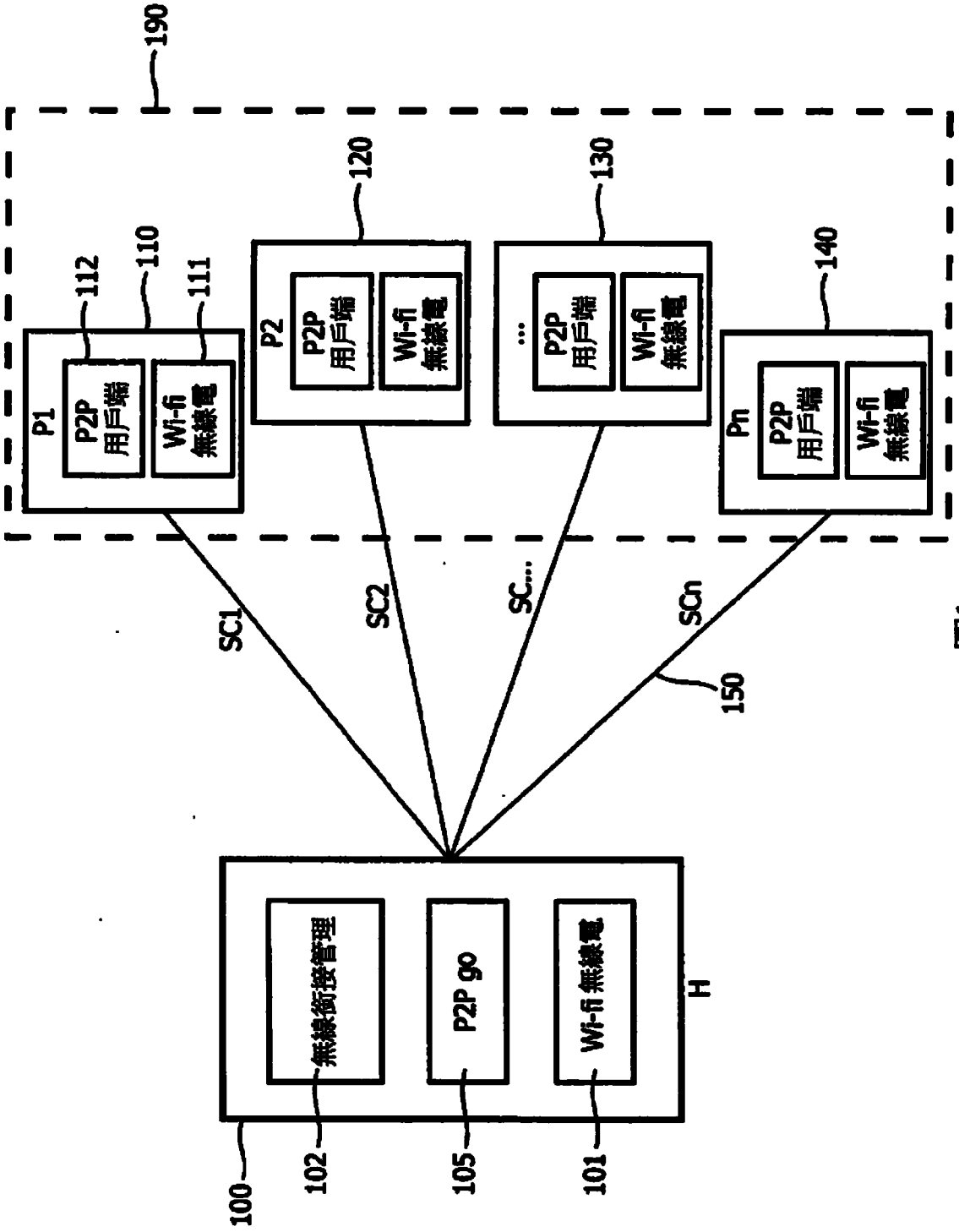
190
120
130
140
110
112
111
P2
P2P 用戶端
Wi-fi 無線電
...
P2P 用戶端
Wi-fi 無線電
P1
P2P 用戶端
Wi-fi 無線電
Pn
P2P 用戶端
Wi-fi 無線電
SC1
SC2
SC...
SCn
150
無線銜接管理
P2P go
Wi-fi 無線電
H
100
102
105
101

圖1

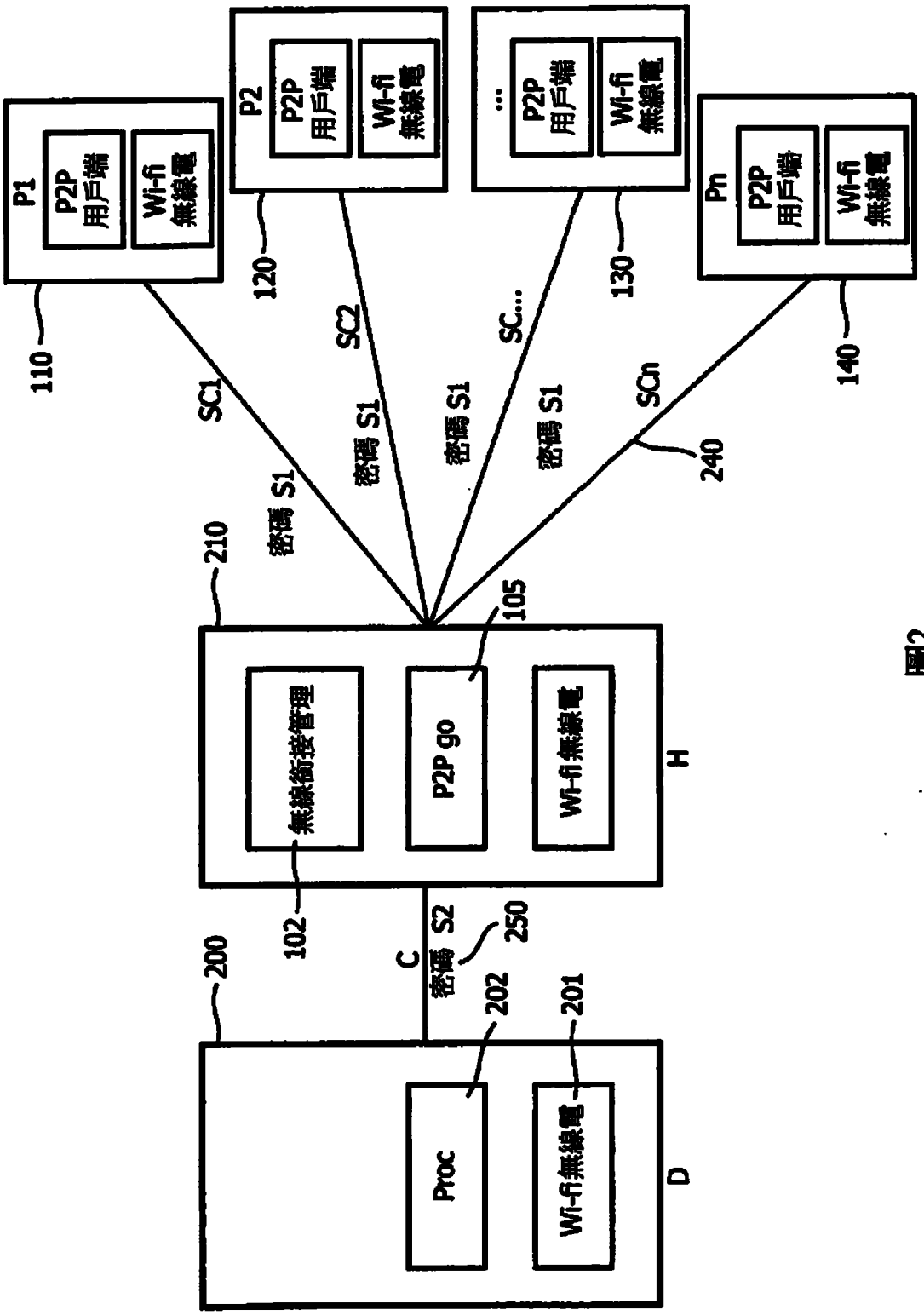
P1
P2P 用戶端
Wi-fi 無線電
110
P2
120
...
130
Pn
140
SC1
SC2
SC...
SCn
密碼 S1
240
210
105
無線銜接管理
P2P go
Wi-fi無線電
H
102
C
密碼 S2
250
200
202
201
Proc
D

圖2

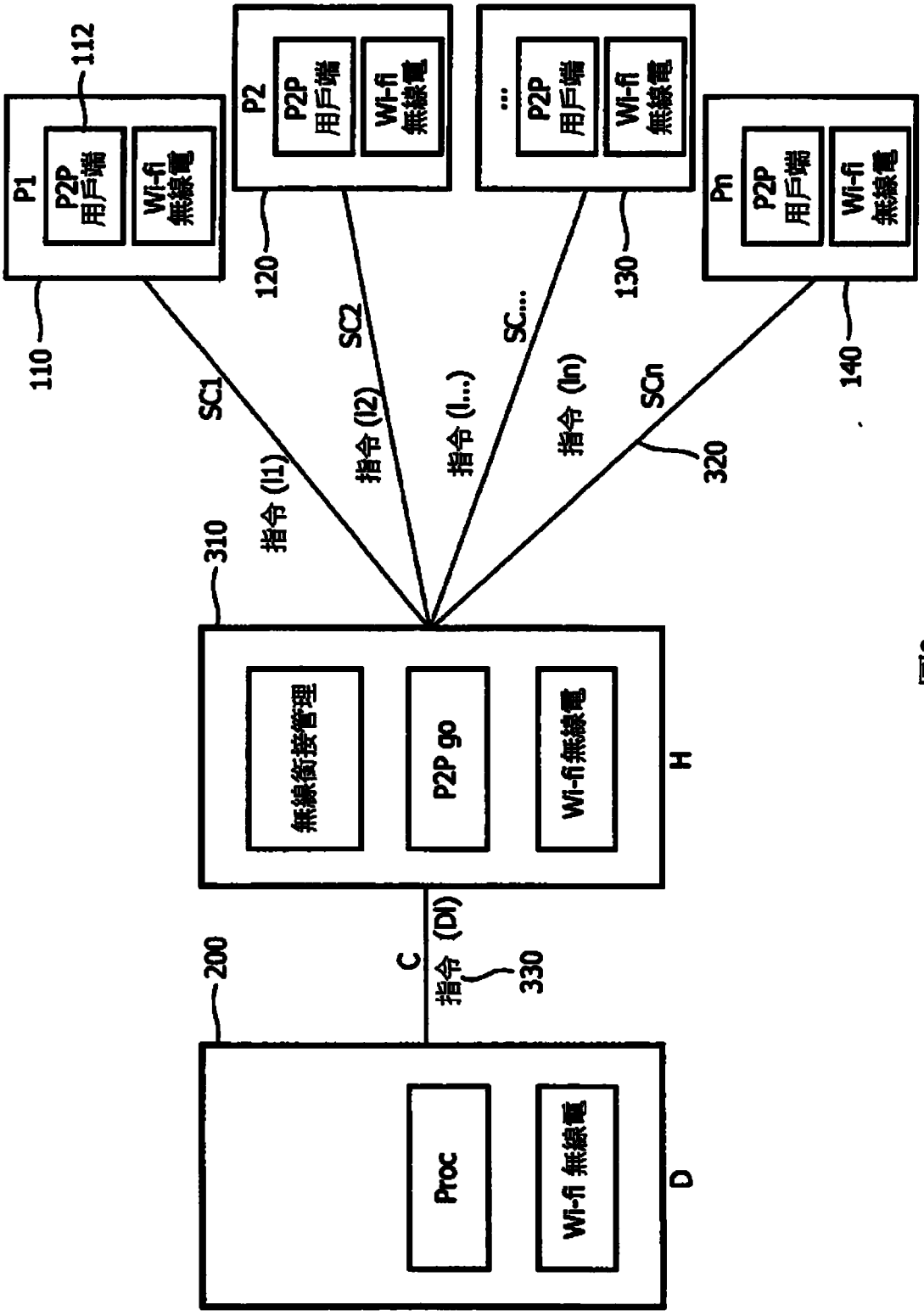
P1
P2P 用戶端
Wi-fi 無線電
112
110
P2
P2P 用戶端
Wi-fi 無線電
120
...
P2P 用戶端
Wi-fi 無線電
130
Pn
P2P 用戶端
Wi-fi 無線電
140
SC1
SC2
SC...
SCn
指令 (I1)
指令 (I2)
指令 (I...)
指令 (In)
320
310
無線銜接管理
P2P go
Wi-fi無線電
H
C
指令 (DI)
330
200
Proc
Wi-fi 無線電
D

圖3

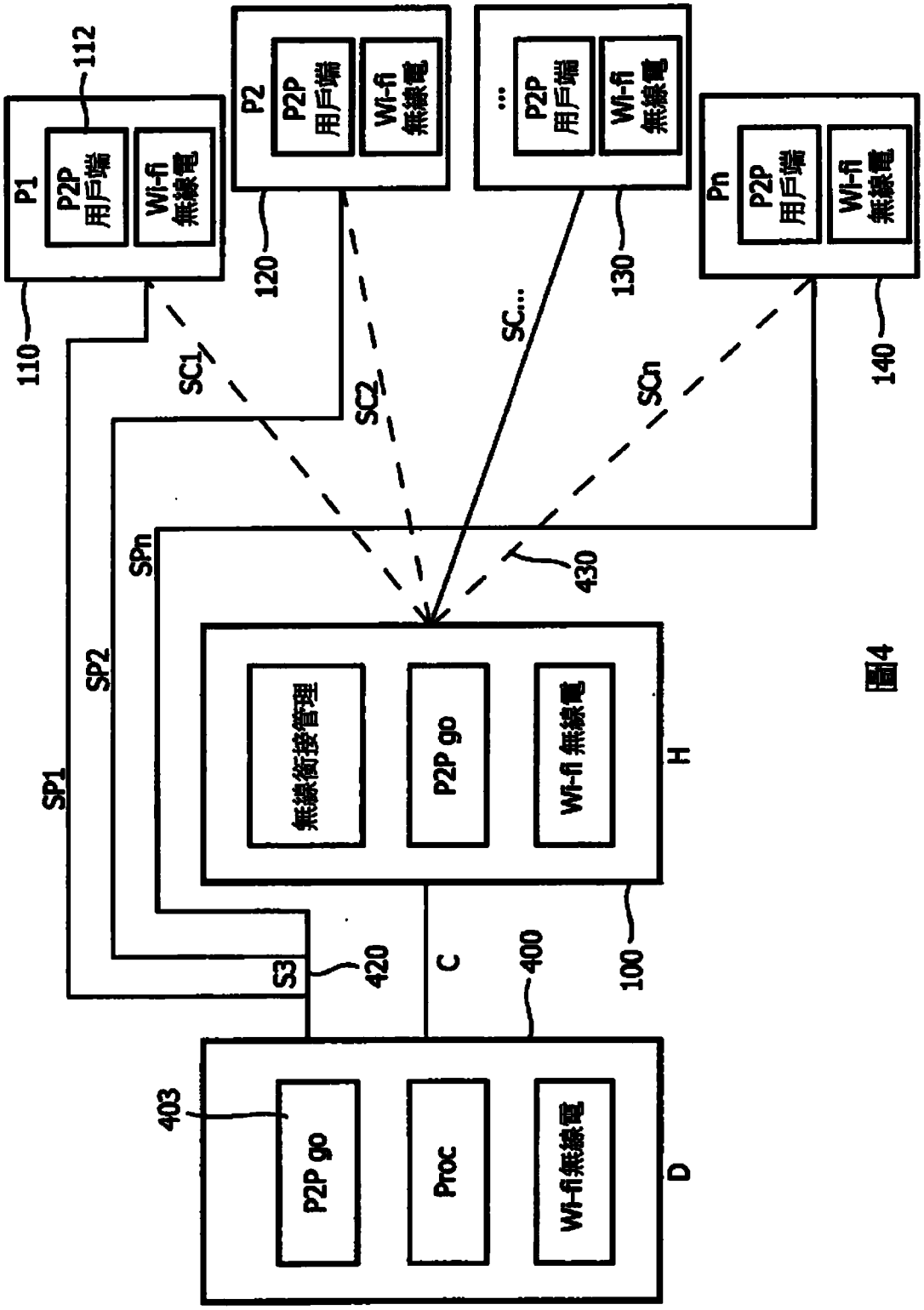
P1
P2P 用戶端
Wi-fi 無線電
112
110
P2
120
...
130
Pn
140
SC1
SC2
SC...
SCn
SPn
SP2
SP1
430
無線銜接管理
P2P go
Wi-fi 無線電
H
S3
420
C
400
100
403
P2P go
Proc
Wi-fi無線電
D

圖4

【代表圖】

【本案指定代表圖】：第（2）圖。

【本代表圖之符號簡單說明】：

102　主機通信處理器(亦稱爲無線銜接管理)

110　無線周邊設備裝置P1...Pn

120　無線周邊設備裝置P1...Pn

130　無線周邊設備裝置P1...Pn

140　無線周邊設備裝置P1...Pn

200　可攜式裝置/銜接器D

201　Wi-Fi無線電收發器

202　通信處理器PROC

210　無線銜接主機H/第二無線裝置

240　第一密碼資料/連接線

250　第二密碼資料

S1　共同密碼/複雜密碼/密碼資料

S2　第二密碼資料

SC1...SCn　Wi-Fi Direct連接

P1...Pn　無線周邊設備裝置

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

申請專利範圍

1. 一種用於無線通信(wireless communication)之系統，其包括：

一群組之無線裝置及一可攜式(portable)裝置，該群組之各無線裝置及該可攜式裝置包括用於無線地交換資料之一無線電收發器(radio transceiver)；其中，

該群組之一第一無線裝置提供(accommodating)一第一主機功能(host function)及該群組之一第二無線裝置提供一第二主機功能，該第一無線裝置及該第二無線裝置為相同無線裝置或不同無線裝置；

該群組共用(sharing)第一密碼資料(secret data)且經組態用於經由基於該第一密碼資料之各自第一安全連接而與提供該第一主機功能之該第一無線裝置無線通信；

該可攜式裝置包括一裝置通信處理器，該裝置通信處理器經組態用於

使用基於不同於該第一密碼資料之第二密碼資料之一配對程序建立與提供該第二主機功能之該第二無線裝置之一第二安全連接，

經由該第二安全連接接收一第二指令，且

根據該第二指令，使用基於第三密碼資料之一各自配對程序(pairing procedure)建立與該群組之至少一無線裝置之一各自直接無線安全連接，該第三密碼資料不同於該第一密碼資料；

提供該第二主機功能之該第二無線裝置包括一主機通信處理器(host communication processor)，該主機通信處理器經組態用於

使用基於該第二密碼資料之該配對程序建立與該可攜式裝置之該第二安全連接，

經由該第一安全連接將一第一指令傳送至該至少一無線裝置以應用該第三密碼資料，以用於建立與該可攜式裝置之一直接無線安全連接，及

經由該第二安全連接將一第二指令傳送至該可攜式裝置以應用該第三密碼資料，以用於基於該第三密碼資料建立與該至少一無線裝置之該直接無線安全連接；及

該至少一無線裝置包括一通信處理器，該通信處理器經組態用於

經由該第一安全連接接收該第一指令，且

根據該第一指令，使用基於該第三密碼資料之一各自配對程序建立與該可攜式裝置之該各自直接無線安全連接。

2. 一種用在包括一群組之無線裝置及一可攜式裝置之一系統中之無線通信之可攜式裝置，該群組之各無線裝置及該可攜式裝置經組態用於無線地交換資料，及該群組共用第一密碼資料且經組態用於經由基於該第一密碼資料之各自第一安全連接而與該群組之一第一無線裝置無線通信，該可攜式裝置包括：

用於無線地交換資料之一無線電收發器；及

一裝置通信處理器，其經組態用於

藉由使用基於不同於該第一密碼資料之第二密碼資料之一配對程序建立與提供一主機功能之該群組之一第二無線裝置之一第二安全連接；

經由該第二安全連接接收一指令，且

根據該指令，使用基於第三密碼資料之一各自配對程序建立與該群組之至少一無線裝置之一各自直接無線安全連接，該第三密碼資料不同於該第一密碼資料。

3. 如請求項2之裝置，其中該裝置通信處理器進一步經組態用於下

列一或多者：

作為一群組擁有者(group owner)控制經由該各自直接無線連接之該通信；或

使用基於各自不同第三密碼資料之一各自配對程序建立與各自不同子集之各自無線裝置之各自不同直接無線安全連接，或

產生該第三密碼資料且將該第三密碼資料傳送至提供該主機功能之該第二無線裝置。

4. 如請求項2之裝置，其中該裝置通信處理器經組態用於下列一或多者：

在起始建立與該至少一無線裝置之該各自直接無線安全連接之前斷開該第二安全連接；或

提供一持久分組(persistent grouping)，且因此用於在斷開基於該第三密碼資料之該各自直接無線安全連接之後，再次基於該第三密碼資料建立一進一步各自直接無線安全連接，或

當在斷開基於該第三密碼資料之該各自直接無線安全連接之後，使用在初期配對期間獲取之該第二密碼資料或該第三密碼資料與該至少一無線裝置重新連接以用於建立一各自直接無線安全連接。

5. 如請求項2之裝置，其中

該第二安全連接包括一Wi-Fi Direct P2P連接，及/或

該各自直接無線安全連接包括另一Wi-Fi Direct P2P連接，或

該各自直接無線安全連接包括一隧道式直接鏈路建立連接，或

該配對程序包括一Wi-Fi保護存取程序或一Wi-Fi簡單組態程序。

6. 一種用在包括一群組之無線裝置及一可攜式裝置之系統中之無線通信之主機裝置，該群組之各無線裝置及該可攜式裝置經組

態用於無線地交換資料，及該群組共用第一密碼資料且經組態用於經由基於該第一密碼資料之各自第一安全連接而與該群組之一第一無線裝置無線通信，該主機裝置包括：

一無線電收發器，其用於無線地交換資料，及

一主機通信處理器，其經組態用於藉由以下各項提供一主機功能

使用基於不同於該第一密碼資料之第二密碼資料之一配對程序建立與該可攜式裝置之一第二安全連接，

經由該第一安全連接將一第一指令傳送至該群組之至少一無線裝置以應用第三密碼資料，以用於建立與該可攜式裝置之一直接無線安全連接，該第三密碼資料不同於該第一密碼資料，及

經由該第二安全連接將一第二指令傳送至該可攜式裝置以應用該第三密碼資料，以用於基於該第三密碼資料建立與該群組之該至少一無線裝置之該直接無線安全連接。

7. 如請求項6之主機裝置，其中該主機通信處理器經組態用於下列一或多者：

產生該第三密碼資料，或

針對該可攜式裝置之各自、不同執行個體(instances)產生一組各自、不同之該第三密碼資料，或

當該可攜式裝置在斷開該第二安全連接之後之一各自、進一步時間建立該第二安全連接時產生一組各自、不同之該第三密碼資料，或

針對各自、不同之該等無線裝置之一子集產生一組各自、不同之該第三密碼資料，或

產生基於或等於該第二密碼資料之該第三密碼資料。

8. 如請求項6之主機裝置，其中該主機通信處理器經組態用於下列

一或多者：

指派一有限壽命至該第三密碼資料，或

取決於該裝置之一授權層級指派一壽命至該第三密碼資料。

9. 如請求項6之主機裝置，其中該主機通信處理器經組態用於：

將一第三指令傳送至該至少一無線裝置以用於在建立至該可攜式裝置之該直接無線安全連接之前斷開該第一安全連接。

10. 如請求項6之主機裝置，其中該主機裝置係一無線銜接主機或一無線銜接站。

11. 一種用在包括一群組之無線裝置及一可攜式裝置之系統中之無線通信之無線裝置，該群組之各無線裝置及該可攜式裝置經組態用於無線地交換資料，及該群組共用第一密碼資料且經組態用於經由基於該第一密碼資料之各自第一安全連接而與該群組之一第一無線裝置無線通信及一第二無線裝置使用基於第二密碼資料之一配對程序建立與該可攜式裝置之一第二安全連接，該無線裝置包括：

用於無線交換資料之一無線電收發器，及

一通信處理器，其經組態用於

經由該第一安全連接接收一第一指令，該第一指令應用第三密碼資料來建立與該可攜式裝置之一直接無線安全連接，且

根據該第一指令，使用基於該第三密碼資料之一配對程序建立與該可攜式裝置之該直接無線安全連接。

12. 如請求項11之無線裝置，其中該通信處理器經組態用於：

起始至該可攜式裝置之該直接無線安全連接之該建立。

13. 如請求項11之無線裝置，其中該通信處理器(112)經組態用於下列一或多者：

在建立至該可攜式裝置之該直接無線安全連接之前斷開該各

自第一安全連接，或

在斷開至該可攜式裝置之該各自直接無線安全連接之後恢復該各自第一安全連接。

14. 一種在包括一群組之無線裝置及一可攜式裝置之無線裝置之一系統中之無線通信之方法，該群組之各無線裝置及該可攜式裝置經組態用於無線地交換資料，及該群組共用第一密碼資料且經組態用於經由基於該第一密碼資料之各自第一安全連接而與該群組之一第一無線裝置無線通信，

該方法包括

使用基於不同於該第一密碼資料之第二密碼資料之一配對程序建立該可攜式裝置與提供一第二主機功能之該群組之一第二無線裝置之間之一第二安全連接；

經由該第一安全連接將一第一指令傳送至該群組之至少一無線裝置以應用一第三密碼資料，以用於建立與該可攜式裝置之一直接無線安全連接，該第三密碼資料不同於該第一密碼資料，及

經由該第二安全連接將一第二指令傳送至該可攜式裝置以應用該第三密碼資料，以用於基於該第三密碼資料建立與該至少一無線裝置之該直接無線安全連接；

使用基於該第三密碼資料之一各自配對程序建立該可攜式裝置與該至少一無線裝置之間之一各自直接無線安全連接。

15. 一種非暫態電腦可讀媒體(non-transitory computer readable medium)，其包括可操作以引起一處理器執行如請求項14之方法的一程式(program)。