(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201132141 A1
(43)公開日： 中華民國 100 (2011) 年 09 月 16 日

(21)申請案號：099109709 (22)申請日： 中華民國 99 (2010) 年 03 月 30 日
(51)Int. Cl.： *H04W12/02 (2009.01)*
(30)優先權：2009/03/30 美國 12/414,630
(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：蕭倫 XIAO, LU (CA) ；金勇進 KIM, YONG JIN (KR) ；賈和芬 JIA, ZHANFENG (CN) ；朱立亞 大衛 強那森 JULIAN, DAVID JONATHAN (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：35 項 圖式數：5 共 28 頁

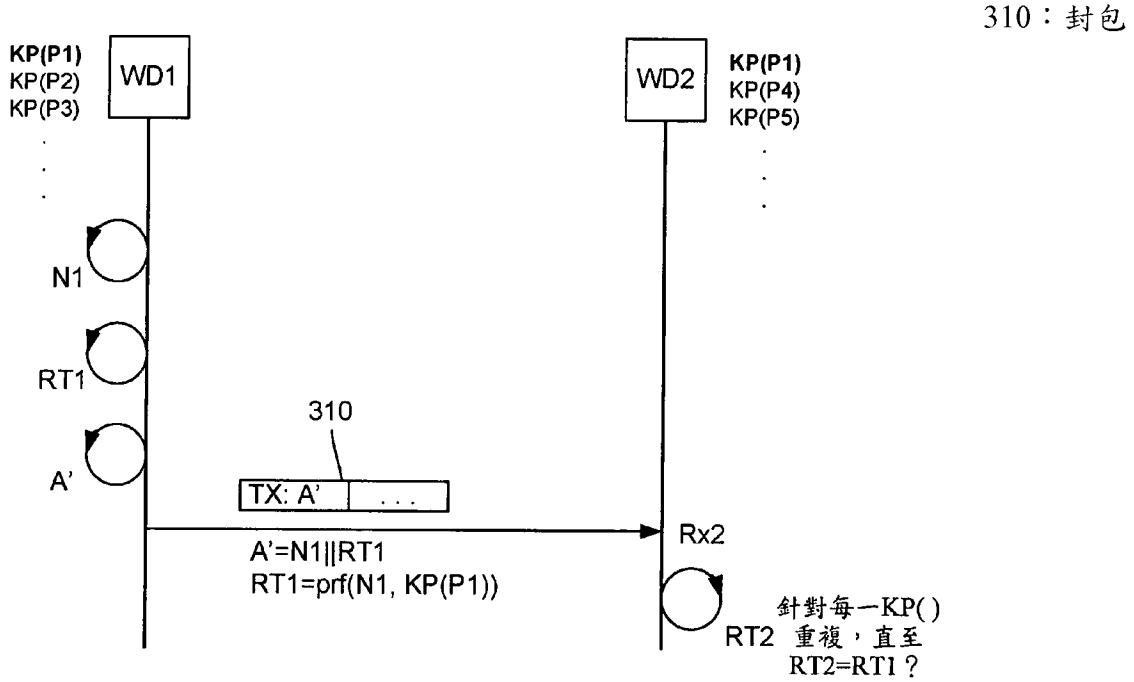
(54)名稱

接收器導向通道中位址隱私保護之裝置及方法

APPARATUS AND METHOD FOR ADDRESS PRIVACY PROTECTION IN RECEIVER ORIENTED CHANNELS

(57)摘要

本發明揭示一種用於位址隱私保護之方法，其係用於與一第二無線器件共用一隱私密鑰之一第一無線器件。在該方法中，使用具有種子值之一偽隨機函數及該隱私密鑰作為輸入引數而在該第一無線器件處產生一第一解析標籤。該隱私密鑰僅為該第一無線器件及該第二無線器件所知。基於該種子值及該第一解析標籤來產生該第一無線器件之一隱私位址。將一封包自該第一無線器件傳輸至該第二無線器件。該封包包括該隱私位址及該第一解析標籤。



(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201132141 A1
(43)公開日： 中華民國 100 (2011) 年 09 月 16 日

(21)申請案號：099109709 (22)申請日： 中華民國 99 (2010) 年 03 月 30 日
(51)Int. Cl.： *H04W12/02 (2009.01)*
(30)優先權：2009/03/30 美國 12/414,630
(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：蕭倫 XIAO, LU (CA) ；金勇進 KIM, YONG JIN (KR) ；賈和芬 JIA, ZHANFENG (CN) ；朱立亞 大衛 強那森 JULIAN, DAVID JONATHAN (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：35 項 圖式數：5 共 28 頁

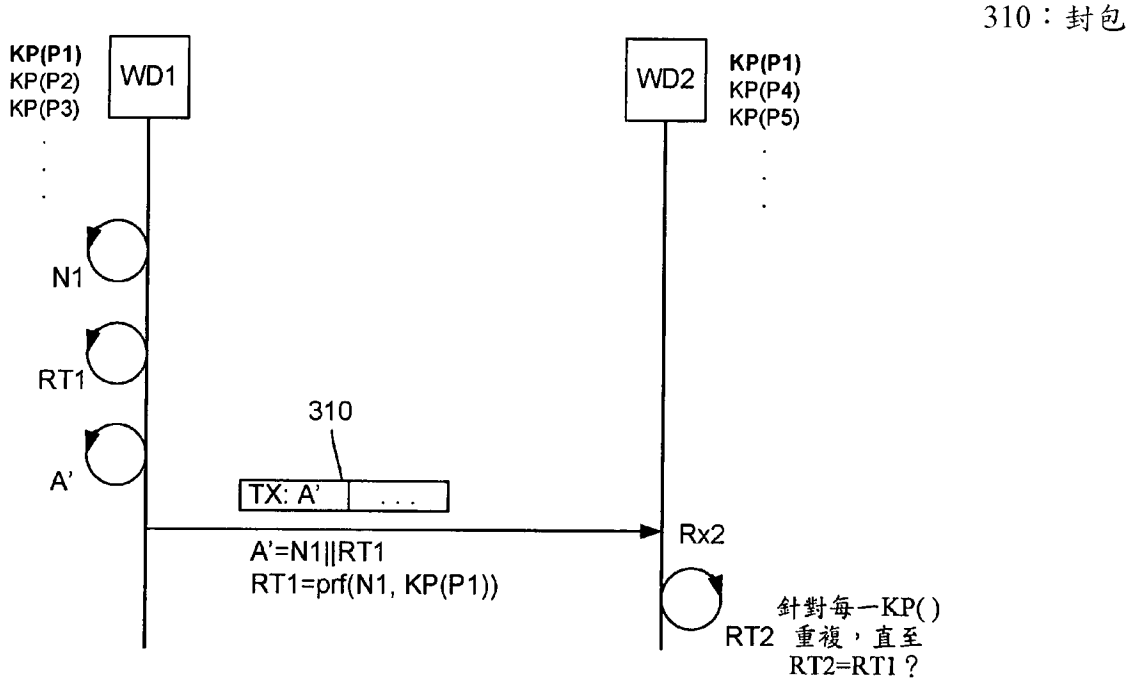
(54)名稱

接收器導向通道中位址隱私保護之裝置及方法

APPARATUS AND METHOD FOR ADDRESS PRIVACY PROTECTION IN RECEIVER ORIENTED CHANNELS

(57)摘要

本發明揭示一種用於位址隱私保護之方法，其係用於與一第二無線器件共用一隱私密鑰之一第一無線器件。在該方法中，使用具有種子值之一偽隨機函數及該隱私密鑰作為輸入引數而在該第一無線器件處產生一第一解析標籤。該隱私密鑰僅為該第一無線器件及該第二無線器件所知。基於該種子值及該第一解析標籤來產生該第一無線器件之一隱私位址。將一封包自該第一無線器件傳輸至該第二無線器件。該封包包括該隱私位址及該第一解析標籤。



六、發明說明：

【發明所屬之技術領域】

本發明大體而言係關於接收器導向無線通道中之位址隱私保護。

【先前技術】

在短距離內以無線方式傳送資料之同級間網路歸因於優於使用電纜之傳統有線連接的優勢而正變得普及。Bluetooth及ZigBee為短程同級網路之標準的實例。

然而，同級器件之間的無線通信可易受追蹤及攻擊。在空中以無線方式傳輸之封包通常識別其來源及目的地，以便被正確地遞送。通常藉由各別位址來識別來源及目的地。結果，竊聽者可被動地接聽接收通道且追蹤哪一來源位址或目的地位址被涉及。因此，竊聽者知道一個實體正在發送或接收封包。

在短程無線通信中，位址追蹤之此可能性係不良的。封包中之來源位址或目的地位址通常與特定器件相關聯。器件之存在可揭示諸如器件擁有者之位置及時間型樣的有用資訊。

因此，需要一種用於位址隱私保護之技術。

【發明內容】

本發明之一態樣可駐留於一種用於位址隱私保護之方法中，該方法係用於與一第二無線器件共用一隱私密鑰之一第一無線器件。在該方法中，使用具有一種子值(seed value)之一偽隨機函數及該隱私密鑰作為輸入引數而在該

第一無線器件處產生一第一解析標籤(resolution tag)。該隱私密鑰僅為該第一無線器件及該第二無線器件所知。基於該種子值及該第一解析標籤來產生該第一無線器件之一隱私位址。將一封包自該第一無線器件傳輸至該第二無線器件。該封包包括該隱私位址及該第一解析標籤。

在本發明之更詳細態樣中，該偽隨機函數可產生一已截斷密鑰式雜湊訊息驗證碼(truncated keyed hash message authentication code)，或一基於加密之訊息驗證碼(cipher-based message authentication code)。該隱私密鑰可為基於該第一無線器件與該第二無線器件之一配對所產生的一已配對器件密鑰。

該封包可進一步包括該種子值。該種子值可為一臨時標誌(nonce)。或者，該種子值可為一時間戳記，或由該第一無線器件及該第二無線器件所維持之一計數器值。因此，該封包可包括用於使該種子值在該第一無線器件與該第二無線器件之間同步的該種子值之一部分。該隱私位址可為與該第一解析標籤串連之該種子值。若該第二器件以其他方式知道該種子值，則該隱私位址可僅含有該第一解析標籤。

在本發明之其他更詳細態樣中，該第二無線器件可經由僅與該第二無線器件相關聯之一無線接收通道而自該第一無線器件接收該封包。該第二無線器件可使用具有該種子值之該偽隨機函數及該隱私密鑰作為輸入引數來產生一第二解析標籤。該第二無線器件可在該第二解析標籤匹配於

該第一解析標籤時將該隱私位址映射至該第一無線器件。另外，該第一無線器件可在一廣播匿名傳呼通道上將該封包傳輸至該第二無線器件，且該第二無線器件可在由該第一無線器件之該隱私位址所定義的一無線接收通道上將一第二封包轉遞至該第一無線器件。

本發明之另一態樣可駐留於一種裝置中，該裝置具有位址隱私保護且與一第二無線器件共用一隱私密鑰。該裝置可包括：用於使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數來產生一第一解析標籤之構件，其中該隱私密鑰僅為該裝置及該第二無線器件所知；用於基於該種子值及該第一解析標籤來產生該裝置之一隱私位址之構件；及用於將一封包傳輸至該第二無線器件之構件，其中該封包包括該隱私位址及該第一解析標籤。該裝置可包含一手錶、一頭戴式耳機或一感測器件。

本發明之另一態樣可駐留於一種電腦程式產品中，該電腦程式產品包含電腦可讀媒體，該電腦可讀媒體包含：用於使一電腦使用具有一種子值之一偽隨機函數及一隱私密鑰作為輸入引數來產生一第一解析標籤之程式碼，其中該隱私密鑰僅為該電腦及一第二無線器件所知；用於使一電腦基於該種子值及該第一解析標籤來產生一隱私位址之程式碼；及用於使一電腦將一封包傳輸至該第二無線器件之程式碼，其中該封包包括該隱私位址及該第一解析標籤。

【實施方式】

詞語「例示性」在本文中用以意謂「充當實例、例子或

說明」。未必將本文中描述為「例示性」之任何實施例解釋為比其他實施例較佳或有利。

參看圖1至圖3，本發明之一態樣可駐留於用於位址隱私保護之方法200中，方法200係用於與第二無線器件WD2及114共用隱私密鑰KP之第一無線器件WD1(諸如行動台102)。在該方法中，使用具有種子值S1之偽隨機函數及隱私密鑰作為輸入引數而在第一無線器件處產生第一解析標籤RT1(步驟210)。隱私密鑰僅為第一無線器件及第二無線器件所知。基於種子值及第一解析標籤來產生第一無線器件之隱私位址A'(步驟220)。將封包310自第一無線器件傳輸至第二無線器件(步驟230)。該封包包括隱私位址及第一解析標籤。

偽隨機函數可產生已截斷密鑰式雜湊訊息驗證碼(HMAC)，或基於加密之訊息驗證碼(CMAC)。偽隨機函數在密碼編譯方面應較強，使得自隱私位址A'導出共用隱私密鑰KP係不可行的。隱私密鑰可為基於第一無線器件與第二無線器件之配對所產生的已配對器件密鑰。為了使該等器件配對，使用者可手動地將一程式碼鍵入至每一器件中，或以其他方式建立此等兩個器件之間的安全關聯。種子值S1可為臨時標誌N1、計數器值或時間戳記。隱私位址A'可為與第一解析標籤串連之種子值，使得A'=S1||RT1，其中RT1=prf(S1, KP)。當種子值S1為計數器值或時間戳記時，取決於接收端器件是否能夠以其他方式得到其確切值，可在隱私位址中包括、部分地包括或省略種子值。如

圖3所示，當種子值為臨時標誌N1時，該臨時標誌係在第一無線器件WD1處得以產生，且在封包310中作為隱私位址A'之部分得以傳輸。

另外，第二無線器件WD2可經由僅與第二無線器件相關聯之無線接收通道Rx2而自第一無線器件WD1接收封包。第二無線器件可使用具有種子值(諸如臨時標誌N1)之偽隨機函數及隱私密鑰作為輸入引數來產生第二解析標籤RT2。第二無線器件可在第二解析標籤匹配於第一解析標籤時將隱私位址映射至第一無線器件。第一無線器件及第二無線器件可與複數個其他器件配對。每一對(P1, ..., PN)具有一關聯隱私密鑰KP( )。該器件藉由產生每一隱私密鑰KP(P1, ... , PN)之解析標籤直至發現解析標籤之匹配來映射隱私位址。

參看圖4，第一無線器件WD1可在廣播匿名傳呼通道Rx0上將封包310傳輸至第二無線器件，且第二無線器件WD2可在由第一無線器件之隱私位址A'所定義的無線接收通道RxA'上將第二封包320轉遞至第一無線器件。另外，第二無線器件可產生第二種子值(諸如臨時標誌N2)，以用於基於第二臨時標誌以及使用第二臨時標誌及隱私密鑰PK所產生之第三解析標籤RT3來產生其自己的隱私位址A2'。第一無線器件可藉由產生第四解析標籤RT4且使其匹配於第三解析標籤而將第二隱私位址A2'映射至第二無線器件。

在一時段之後，一無線器件應改變其隱私位址。因此，與該器件相關聯之共同接收通道可改變，例如，自RxA'改

變至RxA''。

本發明之技術不依賴於由與該器件配對之所有器件共用(諸如在Bluetooth Low-Energy(LE)中)的秘密(諸如識別根(IR))。取而代之，以成對方式保護位址隱私。因此，即使與一器件配對之一個器件被損害，攻擊者亦不能追蹤與除了所損害之器件以外之其他器件的活動。

參看圖5，本發明之另一態樣可駐留於裝置500中，裝置500具有位址隱私保護且與第二無線器件WD2共用隱私密鑰KP。該裝置可包括：用於使用具有種子值之偽隨機函數及隱私密鑰作為輸入引數來產生第一解析標籤RT1之構件(處理器510)，其中隱私密鑰僅為該裝置及第二無線器件所知；用於基於種子值及第一解析標籤來產生該裝置之隱私位址A'之構件；及用於將封包310傳輸至第二無線器件之構件，其中該封包包括隱私位址及第一解析標籤。該裝置可包含手錶、頭戴式耳機、感測器件或行動台102。

該裝置可進一步包括儲存媒體520(諸如記憶體)、顯示器530及輸入器件540(諸如鍵盤)。該裝置可包括無線連接550。

本發明之另一態樣可駐留於電腦程式產品中，電腦程式產品包含電腦可讀媒體520，電腦可讀媒體520包含：用於使電腦500使用具有種子值之偽隨機函數及隱私密鑰KP作為輸入引數來產生第一解析標籤RT1之程式碼，其中隱私密鑰僅為該電腦及第二無線器件所知；用於使電腦基於種子值及第一解析標籤來產生隱私位址A'之程式碼；及用於

使電腦將封包310傳輸至第二無線器件之程式碼，其中該封包包括隱私位址及第一解析標籤。

無線器件可包括基於由無線器件發射或在無線器件處接收之信號來執行功能的各種組件。舉例而言，無線頭戴式耳機可包括經調適以基於經由接收器所接收之信號來提供音訊輸出的傳感器。無線手錶可包括經調適以基於經由接收器所接收之信號來提供指示的使用者介面。無線感測器件可包括經調適以提供待傳輸至另一器件之資料的感測器。

再次參看圖1，無線行動台(MS)102可與無線通信系統100之一或多個基地台(BS)104通信。無線通信系統100可進一步包括一或多個基地台控制器(BSC)106，及核心網路108。核心網路可經由適合回載傳輸而連接至網際網路110及公眾交換電話網路(PSTN)112。典型無線行動台可包括手持型電話或膝上型電腦。無線通信系統100可使用許多多重存取技術中之任一者，諸如分碼多重存取(CDMA)、分時多重存取(TDMA)、分頻多重存取(FDMA)、分域多重存取(SDMA)、分極多重存取(polarization division multiple access, PDMA)，或此項技術中已知之其他調變技術。

無線器件114可經由一或多個無線通信鏈路進行通信，該一或多個無線通信鏈路係基於任何適合無線通信技術或以其他方式支援任何適合無線通信技術。舉例而言，在一些態樣中，一無線器件可與一網路相關聯。在一些態樣中，該網路可包含人體區域網路或個人區域網路(例如，

超寬頻網路)。在一些態樣中，該網路可包含區域網路或廣域網路。一無線器件可支援或以其他方式使用多種無線通信技術、協定或標準(諸如CDMA、TDMA、OFDM、OFDMA、WiMAX及Wi-Fi)中之一或多者。類似地，一無線器件可支援或以其他方式使用多種對應調變或多工方案中之一或多者。因此，一無線器件可包括適當組件(例如，空中介面)，以使用以上或其他無線通信技術來建立一或多個無線通信鏈路且經由該一或多個無線通信鏈路進行通信。舉例而言，一器件可包含具有關聯發射器組件及接收器組件(例如，發射器及接收器)之無線收發器，關聯發射器組件及接收器組件可包括促進經由無線媒體之通信的各種組件(例如，信號產生器及信號處理器)。

可將本文中之教示併入至多種裝置(例如，器件)中(例如，實施於多種裝置(例如，器件)內，或由多種裝置(例如，器件)執行)。舉例而言，本文中所教示之一或多個態樣可併入至電話(例如，蜂巢式電話)、個人資料助理(「PDA」)、娛樂器件(例如，音樂或視訊器件)、頭戴式耳機(例如，耳機、聽筒，等等)、麥克風、醫療器件(例如，生物測定感測器、心跳速率監視器、計步器、EKG器件，等等)、使用者I/O器件(例如，手錶、遙控器、燈開關、鍵盤、滑鼠，等等)、輪胎氣壓監視器、電腦、銷售點器件、娛樂器件、助聽器、機上盒或任何其他適合器件中。

此等器件可具有不同之功率及資料要求。在一些態樣

中，本文中之教示可經調適以用於低功率應用中(例如，經由使用基於脈衝之傳信方案及低工作循環模式)，且可支援包括相對較高之資料速率的多種資料速率(例如，經由使用高頻寬脈衝)。

在一些態樣中，無線器件可包含用於通信系統之存取器件(例如，Wi-Fi存取點)。此存取器件可提供(例如)經由有線或無線通信鏈路而至另一網路(例如，諸如網際網路或蜂巢式網路之廣域網路)之連接性。因此，該存取器件可使另一器件(例如，Wi-Fi台)能夠存取該另一網路或某其他功能性。另外，應瞭解，該等器件中之一者或兩者可為攜帶型的，或在一些狀況下，其可為相對非攜帶型的。

熟習此項技術者應理解，可使用多種不同技術中之任一者來表示資訊及信號。舉例而言，可藉由電壓、電流、電磁波、磁場或磁性粒子、光場或光學粒子或其任何組合來表示可貫穿以上描述所引用之資料、指令、命令、資訊、信號、位元、符號及碼片。

熟習此項技術者應進一步瞭解，結合本文中所揭示之實施例而描述之各種說明性邏輯區塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或此兩者之組合。為了清楚地說明硬體與軟體之此互換性，上文已大體上在功能性方面描述各種說明性組件、區塊、模組、電路及步驟。此功能性係實施為硬體或是軟體取決於特定應用及強加於整個系統之設計約束。熟習此項技術者可針對每一特定應用而以變化之方式來實施所描述之功能性，但不應將此等

實施決策解釋為導致脫離本發明之範疇。

結合本文中所揭示之實施例而描述之各種說明性邏輯區塊、模組及電路可藉由通用處理器、數位信號處理器(DSP)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)或其他可程式化邏輯器件、離散閘或電晶體邏輯、離散硬體組件或其經設計以執行本文中所描述之功能的任何組合加以實施或執行。通用處理器可為微處理器，但在替代例中，處理器可為任何習知處理器、控制器、微控制器或狀態機。處理器亦可實施為計算器件之組合，例如，DSP與微處理器之組合、複數個微處理器、結合DSP核心之一或多個微處理器，或任何其他此組態。

結合本文中所揭示之實施例而描述之方法或演算法的步驟可直接體現於硬體中、由處理器執行之軟體模組中，或此兩者之組合中。軟體模組可駐留於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、抽取式磁碟、CD-ROM或此項技術中已知的任何其他形式之儲存媒體中。例示性儲存媒體耦接至處理器，使得處理器可自儲存媒體讀取資訊及將資訊寫入至儲存媒體。在替代例中，儲存媒體可與處理器成整體。處理器及儲存媒體可駐留於ASIC中。ASIC可駐留於使用者終端機中。在替代例中，處理器及儲存媒體可作為離散組件而駐留於使用者終端機中。

在一或多個例示性實施例中，可以硬體、軟體、韌體或其任何組合來實施所描述之功能。若作為電腦程式產品而

以軟體加以實施，則該等功能可作為一或多個指令或程式碼而儲存於電腦可讀媒體上或經由電腦可讀媒體進行傳輸。電腦可讀媒體包括電腦儲存媒體及通信媒體兩者，通信媒體包括促進電腦程式自一處至另一處之傳送的任何媒體。儲存媒體可為可由電腦存取之任何可用媒體。藉由實例而非限制，此電腦可讀媒體可包含RAM、ROM、EEPROM、CD-ROM或其他光碟儲存器件、磁碟儲存器件或其他磁性儲存器件，或可用以載運或儲存呈指令或資料結構形式之所要程式碼且可由電腦存取的任何其他媒體。又，將任何連接恰當地稱為電腦可讀媒體。舉例而言，若使用同軸電纜、光纖電纜、雙絞線、數位用戶線(DSL)或無線技術(諸如紅外線、無線電及微波)而自網站、伺服器或其他遠端源傳輸軟體，則同軸電纜、光纖電纜、雙絞線、DSL或無線技術(諸如紅外線、無線電及微波)包括於媒體之定義中。如本文中所使用，磁碟及光碟包括緊密光碟(CD)、雷射光碟、光碟、數位多功能光碟(DVD)、軟性磁碟及藍光光碟，其中磁碟通常以磁性方式再生資料，而光碟藉由雷射以光學方式再生資料。上述各物之組合亦應包括於電腦可讀媒體之範疇內。

所揭示之實施例之先前描述經提供以使熟習此項技術者能夠製造或使用本發明。在不脫離本發明之精神或範疇的情況下，對此等實施例之各種修改對於熟習此項技術者將顯而易見，且可將本文中所界定之一般原理應用於其他實施例。因此，本發明不意欲限於本文中所展示之實施例，

而應符合與本文中所揭示之原理及新穎特徵相一致的最廣範疇。

【圖式簡單說明】

圖1為無線通信系統之實例的方塊圖。

圖2為用於位址隱私保護之方法的流程圖，該方法係用於與第二無線器件共用隱私密鑰之第一無線器件。

圖3為說明用於位址隱私保護之方法的流程圖。

圖4為說明用於位址隱私保護之方法的另一流程圖。

圖5為包括處理器及記憶體之電腦的方塊圖。

【主要元件符號說明】

100	無線通信系統
102	行動台
104	基地台
106	基地台控制器
108	核心網路
110	網際網路
112	公眾交換電話網路
114	無線器件
310	封包
320	封包
500	裝置/電腦
510	處理器
520	儲存媒體/電腦可讀媒體
530	顯示器

540 輸入器件

550 無線連接

201132141

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：99109709

※申請日：99.3.30　　※IPC 分類：H04W 12/02 (2009.01)

一、發明名稱：(中文/英文)

接收器導向通道中位址隱私保護之裝置及方法

APPARATUS AND METHOD FOR ADDRESS PRIVACY PROTECTION IN RECEIVER ORIENTED CHANNELS

二、中文發明摘要：

本發明揭示一種用於位址隱私保護之方法，其係用於與一第二無線器件共用一隱私密鑰之一第一無線器件。在該方法中，使用具有種子值之一偽隨機函數及該隱私密鑰作為輸入引數而在該第一無線器件處產生一第一解析標籤。該隱私密鑰僅為該第一無線器件及該第二無線器件所知。基於該種子值及該第一解析標籤來產生該第一無線器件之一隱私位址。將一封包自該第一無線器件傳輸至該第二無線器件。該封包包括該隱私位址及該第一解析標籤。

三、英文發明摘要：

Disclosed is a method for address privacy protection for a first wireless device sharing a privacy key with a second wireless device. In the method, a first resolution tag is generated at the first wireless device using a pseudo-random function with the seed value and the privacy key as input arguments. The privacy key is only known to the first and second wireless devices. A privacy address is generated for the first wireless device based on the seed value and the first resolution tag. A packet is transmitted from the first wireless device to the second wireless device. The packet includes the privacy address and the first resolution tag.

七、申請專利範圍：

1. 一種用於位址隱私保護之方法，其係用於與一第二無線器件共用一隱私密鑰之一第一無線器件，該方法包含：

使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數而在該第一無線器件處產生一第一解析標籤，其中該隱私密鑰僅為該第一無線器件及該第二無線器件所知；

基於該種子值及該第一解析標籤來產生該第一無線器件之一隱私位址；及

將一封包自該第一無線器件傳輸至該第二無線器件，其中該封包包括該隱私位址及該第一解析標籤。

2. 如請求項1之用於位址隱私保護之方法，其中該偽隨機函數產生一已截斷密鑰式雜湊訊息驗證碼。

3. 如請求項1之用於位址隱私保護之方法，其中該偽隨機函數產生一基於加密之訊息驗證碼。

4. 如請求項1之用於位址隱私保護之方法，其中該隱私密鑰為基於該第一無線器件與該第二無線器件之一配對所產生的一已配對器件密鑰。

5. 如請求項1之用於位址隱私保護之方法，其中該封包進一步包括該種子值。

6. 如請求項5之用於位址隱私保護之方法，其中該種子值為一臨時標誌。

7. 如請求項1之用於位址隱私保護之方法，其中該種子值為由該第一無線器件及該第二無線器件所維持之一計數

器值。

8. 如請求項1之用於位址隱私保護之方法，其中該種子值為一時間戳記。

9. 如請求項1之用於位址隱私保護之方法，其中該封包包括用於使該種子值在該第一無線器件與該第二無線器件之間同步的該種子值之一部分。

10. 如請求項1之用於位址隱私保護之方法，其中該隱私位址為與該第一解析標籤串連之該種子值。

11. 如請求項1之用於位址隱私保護之方法，其進一步包含：

該第二無線器件經由僅與該第二無線器件相關聯之一無線接收通道而自該第一無線器件接收該封包；

該第二無線器件使用具有該種子值之該偽隨機函數及該隱私密鑰作為輸入引數來產生一第二解析標籤；及

該第二無線器件在該第二解析標籤匹配於該第一解析標籤時將該隱私位址映射至該第一無線器件。

12. 如請求項11之用於位址隱私保護之方法，其中：

該第一無線器件在一廣播匿名傳呼通道上將該封包傳輸至該第二無線器件；且

該方法進一步包含：該第二無線器件在由該第一無線器件之該隱私位址所定義的一無線接收通道上將一第二封包轉遞至該第一無線器件。

13. 一種裝置，其具有位址隱私保護且與一第二無線器件共用一隱私密鑰，該裝置包含：

用於使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數來產生一第一解析標籤之構件，其中該隱私密鑰僅為該裝置及該第二無線器件所知；

用於基於該種子值及該第一解析標籤來產生該裝置之一隱私位址之構件；及

用於將一封包傳輸至該第二無線器件之構件，其中該封包包括該隱私位址及該第一解析標籤。

14. 如請求項13之具有位址隱私保護之裝置，其中該偽隨機函數產生一已截斷密鑰式雜湊訊息驗證碼。

15. 如請求項13之具有位址隱私保護之裝置，其中該偽隨機函數產生一基於加密之訊息驗證碼。

16. 如請求項13之具有位址隱私保護之裝置，其中該隱私密鑰為基於該第一無線器件與該第二無線器件之一配對所產生的一已配對器件密鑰。

17. 如請求項13之具有位址隱私保護之裝置，其中該封包進一步包括該種子值。

18. 如請求項17之具有位址隱私保護之裝置，其中該種子值為一臨時標誌。

19. 如請求項13之具有位址隱私保護之裝置，其中該種子值為由該裝置及該第二無線器件所維持之一計數器值。

20. 如請求項13之具有位址隱私保護之裝置，其中該種子值為一時間戳記。

21. 如請求項13之具有位址隱私保護之裝置，其中該封包包括用於使該種子值在該第一無線器件與該第二無線器件

之間同步的該種子值之一部分。

22. 如請求項13之具有位址隱私保護之裝置，其中該隱私位址為與該第一解析標籤串連之該種子值。

23. 一種電腦程式產品，其包含：

電腦可讀媒體，其包含：

用於使一電腦使用具有一種子值之一偽隨機函數及一隱私密鑰作為輸入引數來產生一第一解析標籤之程式碼，其中該隱私密鑰僅為該電腦及一第二無線器件所知；

用於使一電腦基於該種子值及該第一解析標籤來產生一隱私位址之程式碼；及

用於使一電腦將一封包傳輸至該第二無線器件之程式碼，其中該封包包括該隱私位址及該第一解析標籤。

24. 如請求項23之電腦程式產品，其中該偽隨機函數產生一已截斷密鑰式雜湊訊息驗證碼。

25. 如請求項23之電腦程式產品，其中該偽隨機函數產生一基於加密之訊息驗證碼。

26. 如請求項23之電腦程式產品，其中該隱私密鑰為基於該電腦與該第二無線器件之一配對所產生的一已配對器件密鑰。

27. 如請求項23之電腦程式產品，其中該封包進一步包括該種子值。

28. 如請求項27之電腦程式產品，其中該種子值為一臨時標

誌。

29. 如請求項23之電腦程式產品，其中該種子值為由該電腦及該第二無線器件所維持之一計數器值。

30. 如請求項23之電腦程式產品，其中該種子值為一時間戳記。

31. 如請求項23之電腦程式產品，其中該封包包括用於使該種子值在該電腦與該第二無線器件之間同步的該種子值之一部分。

32. 如請求項23之電腦程式產品，其中該隱私位址為與該第一解析標籤串連之該種子值。

33. 一種手錶，其具有位址隱私保護且與一第二無線器件共用一隱私密鑰，該手錶包含：

用於使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數來產生一第一解析標籤之構件，其中該隱私密鑰僅為該手錶及該第二無線器件所知；

用於基於該種子值及該第一解析標籤來產生該手錶之一隱私位址之構件；及

用於將一封包傳輸至該第二無線器件之構件，其中該封包包括該隱私位址及該第一解析標籤。

34. 一種頭戴式耳機，其具有位址隱私保護且與一第二無線器件共用一隱私密鑰，該頭戴式耳機包含：

用於使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數來產生一第一解析標籤之構件，其中該隱私密鑰僅為該頭戴式耳機及該第二無線器件所知；

用於基於該種子值及該第一解析標籤來產生該頭戴式耳機之一隱私位址之構件；及

用於將一封包傳輸至該第二無線器件之構件，其中該封包包括該隱私位址及該第一解析標籤。

35. 一種感測器件，其具有位址隱私保護且與一第二無線器件共用一隱私密鑰，該感測器件包含：

用於使用具有一種子值之一偽隨機函數及該隱私密鑰作為輸入引數來產生一第一解析標籤之構件，其中該隱私密鑰僅為該感測器件及該第二無線器件所知；

用於基於該種子值及該第一解析標籤來產生該感測器件之一隱私位址之構件；及

用於將一封包傳輸至該第二無線器件之構件，其中該封包包括該隱私位址及該第一解析標籤。

八、圖式：

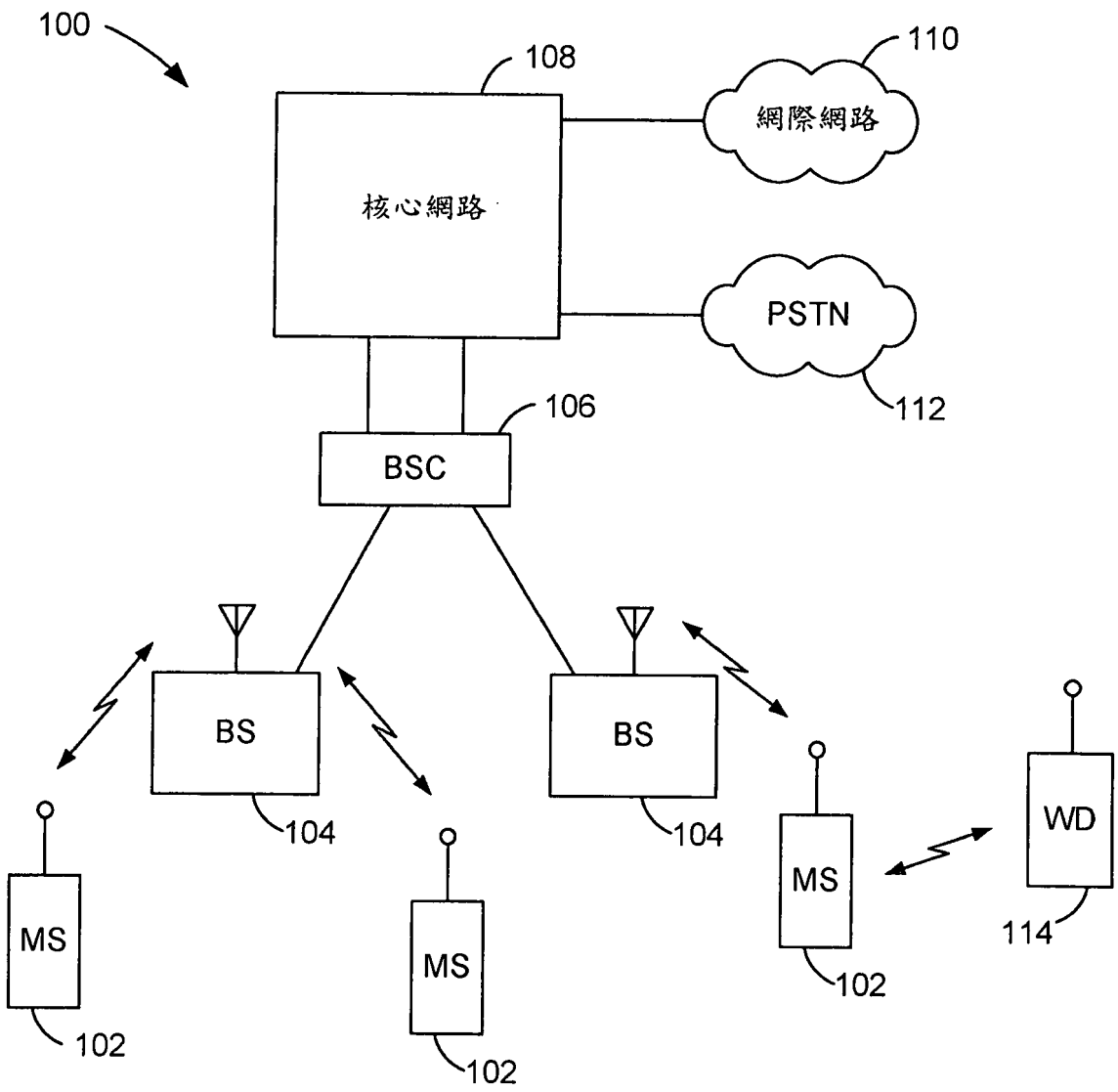

100
108
110
網際網路
核心網路
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
WD
102
102
102
114

圖1

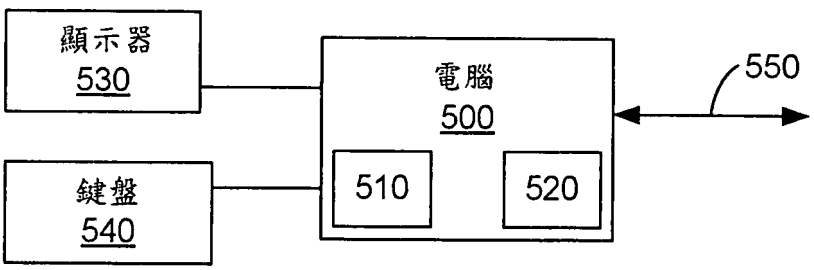

顯示器
530
電腦
500
550
鍵盤
540
510
520

圖5

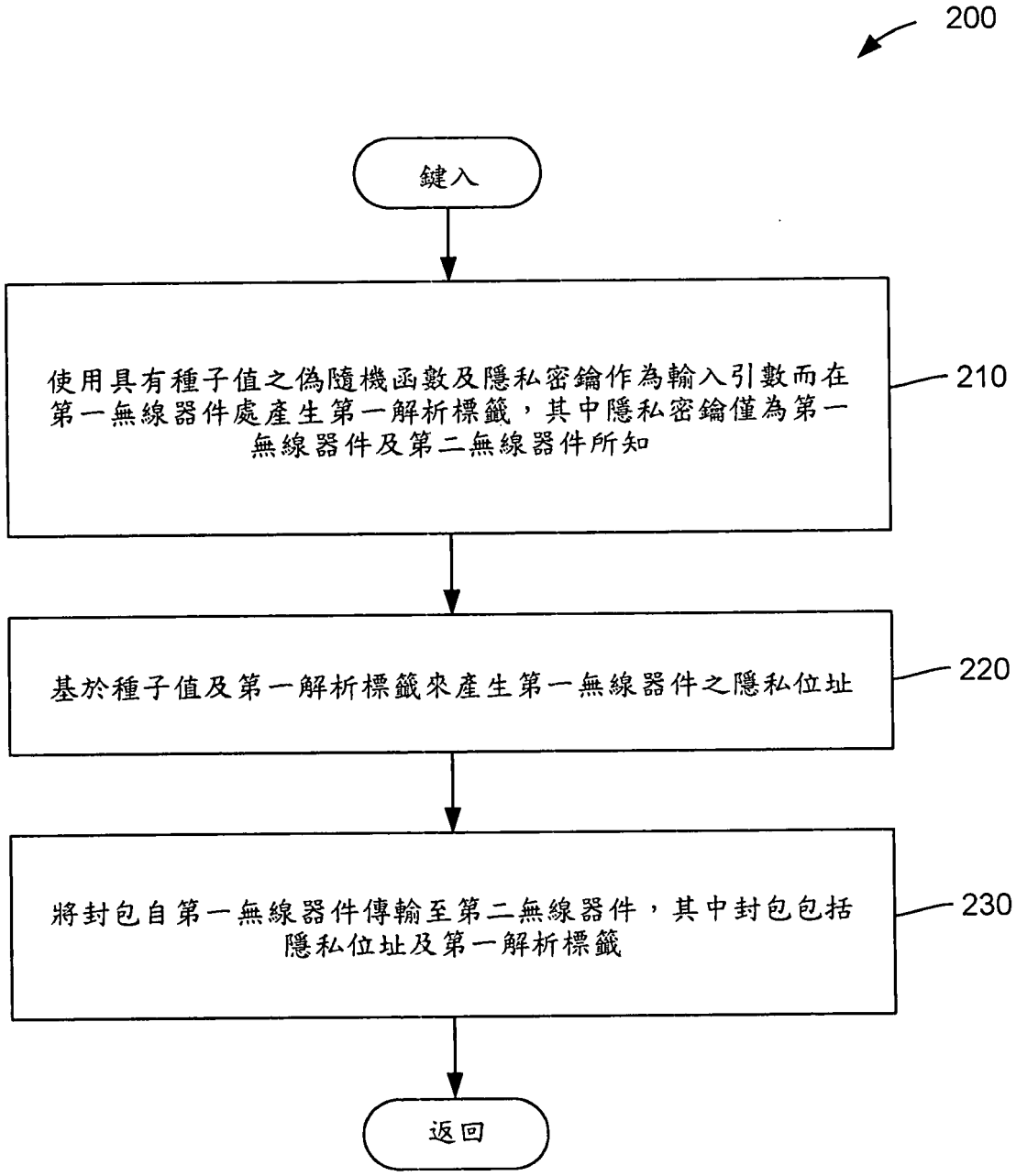

200
鍵入
使用具有種子值之偽隨機函數及隱私密鑰作為輸入引數而在第一無線器件處產生第一解析標籤，其中隱私密鑰僅為第一無線器件及第二無線器件所知
210
基於種子值及第一解析標籤來產生第一無線器件之隱私位址
220
將封包自第一無線器件傳輸至第二無線器件，其中封包包括隱私位址及第一解析標籤
230
返回

圖2

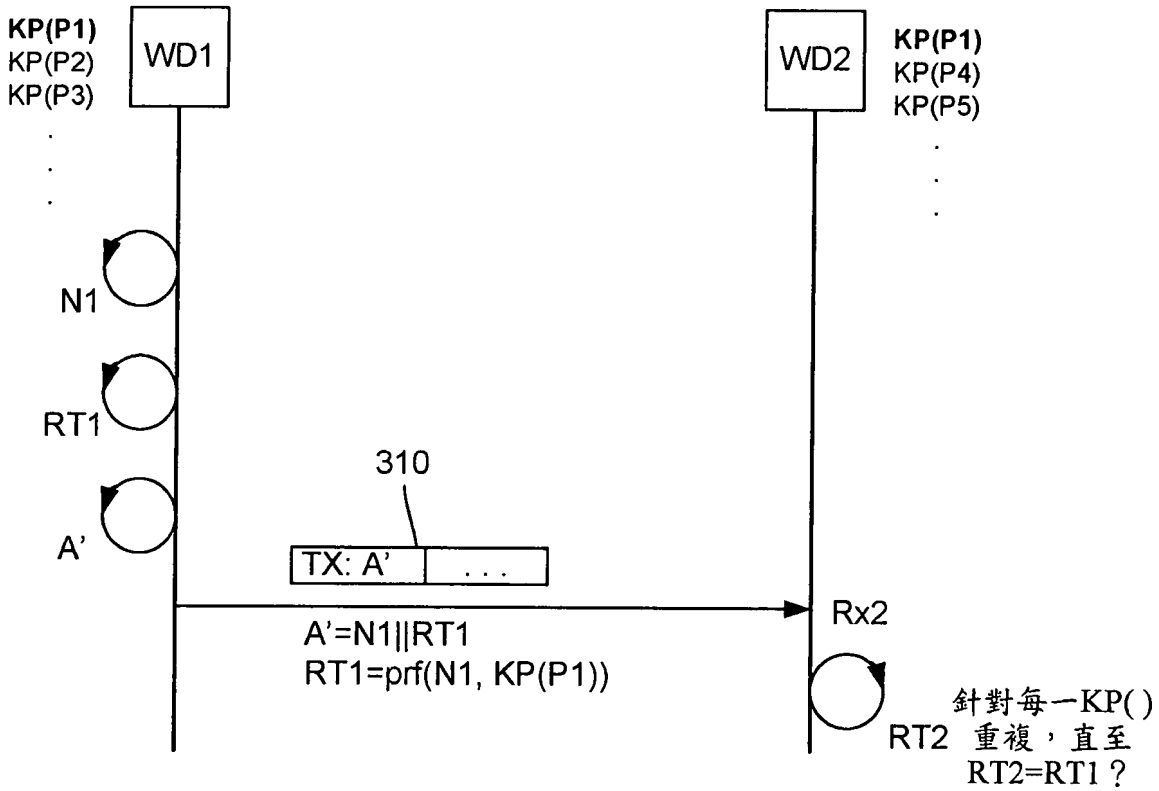

KP(P1)
KP(P2)
KP(P3)
WD1
N1
RT1
A'
310
TX: A'
. . .
A'=N1||RT1
RT1=prf(N1, KP(P1))
WD2
KP(P1)
KP(P4)
KP(P5)
Rx2
RT2
針對每一KP( )
重複，直至
RT2=RT1？

圖3

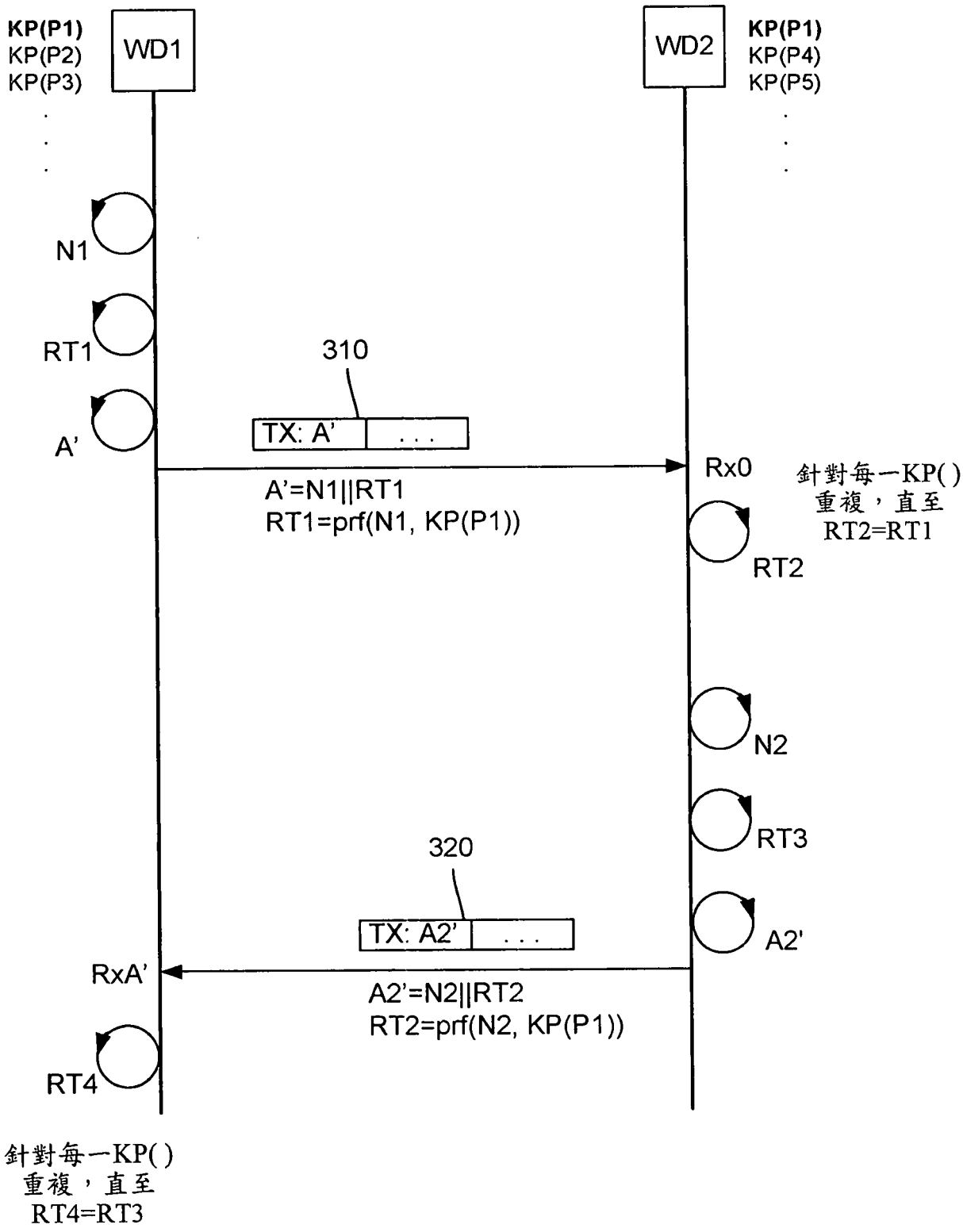

KP(P1)
KP(P2)
KP(P3)
WD1
WD2
KP(P1)
KP(P4)
KP(P5)
N1
RT1
A'
310
TX: A'
A'=N1||RT1
RT1=prf(N1, KP(P1))
Rx0
針對每一KP( )
重複，直至
RT2=RT1
RT2
N2
RT3
320
TX: A2'
A2'
RxA'
A2'=N2||RT2
RT2=prf(N2, KP(P1))
RT4
針對每一KP( )
重複，直至
RT4=RT3

圖4

四、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明：

310　　封包

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）