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 US；2005/1/27；60/647,482
2. 美國 US；2005/9/12；60/716,177
3. 美國 US；2005/11/7；60/734,331
4. 美國 US；2005/12/23；11/318,381

☐ 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】

本發明係有關無線通信安全。更特別是，本發明係有關使用未由他人分享聯合隨機(JRNSO)衍生秘鑰之方法及系統。

【先前技術】

IEEE 802.11i係被用來確保IEEE 802.11標準下操作之無線區域網路(WLAN)可藉由使用計數器模式(CTR)與依序使用先進加密標準(AES)演算法之訊息驗證碼(CBC-MAC)協定(CCMP)概括技術鏈結之加密阻隔安全地作資料通信。為達成此目的， IEEE 802.11i係提供可促使一對通信節點衍生可被用來加密被交換封包之鑰匙之兩方案。

第一方案係以需遠端驗證伺服器(如 RADIUS 伺服器)之IEEE 802.1x驗證技術為基礎。 IEEE 802.1x中，一存取點(AP)可當作欲與該存取點連結之一無線傳送/接收單元(WTRU)及一驗證伺服器間之一路由器。該驗證伺服器可經由該存取點對該無線傳送/接收單元提供一公共鑰匙。無線傳送/接收單元可藉由該驗證伺服器所提供之數位憑證對其檢查來驗證此公共鑰匙。無線傳送/接收單元接著衍生隨機秘密(也就是主秘密)，並以所提供之公共鑰匙對其加密傳送該主秘密至該驗證伺服器。因此，僅該驗證伺服器可使用對應私用鑰匙來解密該主秘密。該驗證伺服器及該無線傳送/接收單元可使用

此主秘密來衍生主鑰匙(MK)。該驗證伺服器及該無線傳送/接收單元接著從該主鑰匙衍生成對主鑰匙(PMK)。該驗證伺服器提供此成對主鑰匙至該存取點。該存取點及該無線傳送/接收單元接著使用該成對主鑰匙來衍生成對瞬變鑰匙(PTK)。一部分此成對瞬變鑰匙係為被用於加密封包之訊息驗證碼協定技術中之實際鑰匙之暫時鑰匙(TK)。因為此方案使用遠端驗證伺服器及及數位憑證(目前很昂貴)，所以該方案通常被實施於企業無線區域網路中。

較適用於家庭或小型企業網路之第二方案係使用先分享鑰匙(PSK)。此方案中，256 位元使用者可配置秘鑰係被儲存於該通信節點上。正如同 IEEE 802.1x 系統中，當無線傳送/接收單元欲與該存取點連結時，該無線傳送/接收單元可將先分享鑰匙當作成對主鑰匙(不衍生主秘密及主鑰匙)，並衍生成對瞬變鑰匙及使用一部分該成對瞬變鑰匙當作暫時鑰匙。

IEEE 802.11i 系統中係具有至少兩問題。首先，最終暫時鑰匙僅如被交換於 IEEE 802.1x 網路例中之主秘密，或如家庭或小型企業網路例中之先分享鑰匙般安全。IEEE 802.11x 系統中，入侵者可藉由竊取該驗證伺服器之私用鑰匙來解密該主秘密。家庭網路中，先分享鑰匙可使用蠻力入侵者(家中先分享鑰匙被不定期改變或被產生自"弱"密碼作業)或藉由竊取該鑰匙而被推演。知道主秘密或先分享鑰匙係使該入侵者可以如兩合

法通信節點之相同方式到達成對主鑰匙之同等值，並衍生同等成對瞬變鑰匙值。因此，知道認證係足以知道被衍生秘鑰。再者，當鑰遲於對話期間被更新時，主鑰匙及成對主鑰匙通常保持不變，僅使用成對主鑰匙及清除中被交換之資訊來衍生新成對瞬變鑰匙(其被假設為秘密)。當成對主鑰匙不改變時，成對瞬變鑰匙並不是新的，所以不是新鑰匙。

再者，鑰匙衍生程序非常複雜且具有許多階段(如主鑰匙，成對主鑰匙，成對瞬變鑰匙及暫時鑰匙)。此消耗時間及資源。

鑰匙可被認為是位元序列。N 位元長度之完全隨機秘鑰係為實體所分享之 N 位元序列，S。假設所有資訊均於系統中可得，則任何人對有關此鑰持序列可為何之估測粗略同等機率地被分配於所有可能 2^NN 位元序列上。

先前技術密碼系統係仰賴其極難從可計算資源觀點來猜測該密碼鑰匙之事實。然而，大多數這些系統中，一旦產生正確猜測，則非常容易驗證此的確為該正確猜測。事實上，先前技術係意指此可應用至任何公共鑰匙系統(也就是秘鑰為公共，而解密鑰匙保持秘密者)。

例如，假設 p 及 q 為兩大質數而 s=pq，則熟知解出兩大質數乘積因子之問題係極難以計算。若一方秘密選擇 p 及 q 並公開地獲得其乘積 s，其接著被當作加密系統之秘鑰，則除非知道 p 及 q，否則其不能輕易地被解

密。欲攔截加密訊息之偷聽者可能藉由嘗試已知很難計算之因子 s 來開始。然而，若該偷聽者猜測 p，則其相當容易驗證其具有正確答案。知道該正確答案之能力係以區別可計算秘密及完全秘密之猜測來獲得。完全秘密意指即使該入侵者正確猜測該鑰匙，其均無決定其的確如此之能力。

因此，預期藉由不限於先前技術之鑰匙來產生加密。IEEE 802.11i 係被用來確保 IEEE 802.11 標準下操作之無線區域網路(WLAN)可藉由使用計數器模式(CTR)與依序使用先進加密標準(AES)演算法之訊息驗證碼(CBC-MAC)協定(CCMP)概括技術鏈結之加密阻隔安全地作資料通信。為達成此目的， IEEE 802.11i 係提供可促使一對通信節點衍生可被用來加密被交換封包之鑰匙之兩方案。

第一方案係以需遠端驗證伺服器(如 RADIUS 伺服器)之 IEEE 802.1x 驗證技術為基礎。 IEEE 802.1x 中，一存取點(AP)可當作欲與該存取點連結之一無線傳送/接收單元(WTRU)及一驗證伺服器間之一路由器。該驗證伺服器可經由該存取點對該無線傳送/接收單元提供一公共鑰匙。無線傳送/接收單元可藉由該驗證伺服器所提供之數位憑證對其檢查來驗證此公共鑰匙。無線傳送/接收單元接著衍生隨機秘密(也就是主秘密)，並以所提供之公共鑰匙對其加密傳送該主秘密至該驗證伺服器。因此，僅該驗證伺服器可使用對應私用鑰匙來解密

該主秘密。該驗證伺服器及該無線傳送/接收單元可使用此主秘密來衍生主鑰匙(MK)。該驗證伺服器及該無線傳送/接收單元接著從該主鑰匙衍生成對主鑰匙(PMK)。該驗證伺服器提供此成對主鑰匙至該存取點。該存取點及該無線傳送/接收單元接著使用該成對主鑰匙來衍生成對瞬變鑰匙(PTK)。一部分此成對瞬變鑰匙係為被用於加密封包之訊息驗證碼協定技術中之實際鑰匙之暫時鑰匙(TK)。因為此方案使用遠端驗證伺服器及及數位憑證(目前很昂貴)，所以該方案通常被實施於企業無線區域網路中。

較適用於家庭或小型企業網路之第二方案係使用先分享鑰匙(PSK)。此方案中，256 位元使用者可配置秘鑰係被儲存於該通信節點上。正如同 IEEE 802.1x 系統中，當無線傳送/接收單元欲與該存取點連結時，該無線傳送/接收單元可將先分享鑰匙當作成對主鑰匙(不衍生主秘密及主鑰匙)，並衍生成對瞬變鑰匙及使用一部分該成對瞬變鑰匙當作暫時鑰匙。

IEEE 802.11i 系統中係具有至少兩問題。首先，最終暫時鑰匙僅如被交換於 IEEE 802.1x 網路例中之主秘密，或如家庭或小型企業網路例中之先分享鑰匙般安全。IEEE 802.11x 系統中，入侵者可藉由竊取該驗證伺服器之私用鑰匙來解密該主秘密。家庭網路中，先分享鑰匙可使用蠻力入侵者(家中先分享鑰匙被不定期改變或被產生自"弱"密碼作業)或藉由竊取該鑰匙而被推

演。知道主秘密或先分享鑰匙係使該入侵者可以如兩合法通信節點之相同方式到達成對主鑰匙之同等值，並衍生同等成對瞬變鑰匙值。因此，知道認證係足以知道被衍生秘鑰。再者，當鑰遲於對話期間被更新時，主鑰匙及成對主鑰匙通常保持不變，僅使用成對主鑰匙及清除中被交換之資訊來衍生新成對瞬變鑰匙(其被假設為秘密)。當成對主鑰匙不改變時，成對瞬變鑰匙並不是新的，所以不是新鑰匙。

再者，鑰匙衍生程序非常複雜且具有許多階段(如主鑰匙，成對主鑰匙，成對瞬變鑰匙及暫時鑰匙)。此消耗時間及資源。

鑰匙可被認為是位元序列。N 位元長度之完全隨機秘鑰係為實體所分享之 N 位元序列，S。假設所有資訊均於系統中可得，則任何人對有關此鑰持序列可為何之估測粗略同等機率地被分配於所有可能 2^NN 位元序列上。

先前技術密碼系統係仰賴其極難從可計算資源觀點來猜測該密碼鑰匙之事實。然而，大多數這些系統中，一旦產生正確猜測，則非常容易驗證此的確為該正確猜測。事實上，先前技術係意指此可應用至任何公共鑰匙系統(也就是秘鑰為公共，而解密鑰匙保持秘密者)。

例如，假設 p 及 q 為兩大質數而 s=pq，則熟知解出兩大質數乘積因子之問題係極難以計算。若一方秘密選擇 p 及 q 並公開地獲得其乘積 s，其接著被當作加密系

統之秘鑰，則除非知道 p 及 q，否則其不能輕易地被解密。欲攔截加密訊息之偷聽者可能藉由嘗試已知很難計算之因子 s 來開始。然而，若該偷聽者猜測 p，則其相當容易驗證其具有正確答案。知道該正確答案之能力係以區別可計算秘密及完全秘密之猜測來獲得。完全秘密意指即使該入侵者正確猜測該鑰匙，其均無決定其的確如此之能力。

因此，預期藉由不限於先前技術之鑰匙來產生加密。

【發明內容】

本發明係有關使用未由他人分享聯合隨機衍生秘鑰之方法及系統。通信實體係從頻道脈衝響應(CIR)估測產生未由他人分享聯合隨機位元，而該未由他人分享聯合隨機位元係被用於產生秘鑰。該驗證類型可為 IEEE 802.1x 或先分享鑰匙系統。 IEEE 802.1x 系統中，主鑰匙，成對主鑰匙及/或成對瞬變鑰匙係可使用該未由他人分享聯合隨機位元來產生。該秘鑰可使用 Diffie-Hellman 鑰匙衍生演算法來產生。

【實施方式】

此後，”無線傳送/接收單元”名詞係包含但不限於使用者設備，站(STA)，固定或行動用戶單元，呼叫器，或可操作於無線環境中之任何其他類型元件。此後，當被稱為”存取點(AP)”名詞者係包含但不限於 B 節點，基地台，位址控制器，或無線環境中之任何其他接介裝置。

本發明特性可被併入積體電路(IC)或被配置於包含

複數互連組件之電路中。本發明可被實施為數位信號處理器(DSP)，軟體，中間件，硬體，應用或未來系統架構。該元件可為大型通信系統或特定應用積體電路(ASIC)之子組件，而若干或所有該處理元件可被其他元件分享。

無線通信系統中，雖然相關隨機資源為無先前通信難以產生之先驗，但無線頻道係提供頻道脈衝響應型式之該資源。明確地說，特定通信系統中，雙方(如 Alice 及 Bob)通信將測量非常類似頻道脈衝響應估測。寬頻分碼多重存取(WCDMA)分時多工(TDD)系統係具有此特性。另一方面，任何不與 Alice 及 Bob 實際共處之一方係可能觀察到與 Alice 及 Bob 非常少連結之頻道脈衝響應。此差異可被開發來產生完全秘鑰。該頻道係為未由他人分享聯合隨機資源，而該頻道脈衝響應估測係為被採用自該頻道之樣本。

Diffie-Hellman 鑰匙衍生程序係被解釋如下。 Alice 及 Bob 同意使用質數 p 及基數 g。Alice 選擇秘密整數 a，接著傳送 g^a 模 p 給 Bob。Bob 選擇秘密整數 b，接著傳送 g^b 模 p 給 Alice。Alice 計算 $(g^b \text{ 模 } p)^a$ 模 p。 Bob 計算 $(g^a \text{ 模 } p)^b$ 模 p。 $(g^b \text{ 模 } p)^a$ 模 p 及 $(g^a \text{ 模 } p)^b$ 模 p 係為相同。例如， Alice 及 Bob 同意使用質數 p=23 及基數 g=3。Alice 選擇秘密整數 a=6，接著傳送 g^a 模 $p=3^6$ 模 23=16 給 Bob。Bob 選擇秘密整數 b=15，接著傳送 g^b 模 $p=3^{15}$ 模 23=12 給 Alice。Alice 計算 $(g^b \text{ 模 } p)^a$ 模 $p=12^6$ 模 23=9。

Bob 計算$(g^a$ 模 $p)^b$ 模 $p=16^{15}$ 模 23=9。

使此方案安全係需許多較大數字。若 p 為大於 300 數位之質數，而 a 及 b 大於 100 數位，則因為該計算太資源密集，所以實際上不可能入侵(即使是合法通信方)。如此，此使該協定不致被實施於電池受限之行動裝置上。

若使用未由他人分享聯合隨機來秘密同意數字 p 及 q 之一(或兩者)，則此會促成該兩通信節點針對 a，b，p 及/或 q 使用較小數而達成相當安全性。 Diffie-Hellman 分享鑰匙可當作秘鑰或被用來加密及傳送該實際秘鑰。所使用較小數可使該鑰匙衍生處理較不資源密集，而使其得以被用於行動裝置上。

第 1 圖為依據本發明包含可衍生未由他人分享聯合隨機位元及秘鑰之兩通信實體(第一節點 110 及第二節點 150)之系統 100 區塊圖。

該實體之一可為無線傳送/接收單元而另一者可為存取點。為了簡化，僅具有兩通信實體 110，150 之點對點通信系統係被說明於第 1 圖。然而，本發明可被應用至牽涉兩實體以上之點對多點通信系統。亦應注意該第一節點及第二節點實質上係為包含相同元件之相同實體，但為了簡化，第 1 圖僅描繪該第一節點及第二節點之相關元件，該第一節點被假設率先產生未由他人分享聯合隨機位元及秘鑰，其將被詳細解釋如下。

依據本發明，該通信實體之一率先。假設第一節點

110率先。第一節點110係包含一頻道估測器112，一後處理器114(可選)，一誤差修正編碼器118，一同步化編碼產生器120(可選)，一秘鑰產生器116及一多工器122。

第一節點之頻道估測器112係以被接收自第二節點150之信號111為基礎來產生頻道脈衝響應估測113。第二節點150中之頻道估測器152亦以第一節點110所傳送之傳輸為基礎來產生頻道脈衝響應估測153。頻道估測器112，152係為該頻道脈衝響應估測之數位化表示。任何先前技術方法均可被用來產生頻道脈衝響應估測。例如，實體110，150可傳送特殊信號或前導序列至其他節點來協助產生頻道脈衝響應估測。頻道脈衝響應估測可以包含但不限於時域，頻域或可使用抽象向量空間表示或類似者之任何方式來產生或儲存。可產生頻道脈衝響應估測及表示方案之方法於第一節點110及第二節點150中應相同。

視實施而定，僅頻道脈衝響應估測部分資訊可為互反而適用於產生共用秘鑰。例如，實體110，150可選擇僅使用該頻道脈衝響應估測之振幅/功率輪廓資訊且可忽略相位資訊。

後處理器114可選擇性使用先前技術方法來處理該頻道脈衝響應估測。後處理器114(如低通濾波器或內插濾波器)係可移除雜訊及冗餘。實體被裝設用於多輸入多輸出(MIMO)之多天線之例中亦需後處理器114，因此天線數量及天線圖案差異可能導致該頻道脈衝響應估測

有所不同。此例中，實體 110，150 可能必須交換其天線配置相關資訊。

因為頻道互反，第一節點 110 及第二節點 150 所產生之頻道脈衝響應估測係被預期非常類似。然而，具有導入該頻道脈衝響應估測差異之三個主要誤差源。第一，該頻道互反係假設兩實體處之頻道同時估測。該同時性差異會導致頻道估測中某些差異。第二，該被數位化頻道脈衝響應估測可能必須與該起始點同步化。例如，若該頻道脈衝響應估測於時域中被數位化，則該頻道脈衝響應估測有意義部分起始可能發生於該兩實體 110，150 中之參考零時不同位置處。此問題係被描繪於第 2 圖中。另一例，若該頻道脈衝響應估測使用頻域表示被儲存，則決定儲存參數時可能假設不同起始頻率/參考相位。第三，該頻道脈衝響應估測亦會因無線通信中固有之干擾所產生之誤差而有所不同。

有關第一誤差源，為了確保頻道估測同時性，該頻道估測時點可被連結至特定系統時間，如無線幀或槽邊界。可替代是，同步化信號可被嵌入實體 110，150 傳送以支援頻道估測之信號中(如前導信號)。同步化在不需嵌入特殊信號下即可從該前導信號獲得。可替代是，頻道估測可參考如全球定位系統(GPS)之絕對時間參考來執行。可替代是，來回延遲可被測量，而同步化可以此來回延遲為基礎來達成。

有關第二誤差源，該頻道脈衝響應估測起始點可被

紀錄於第一節點 110 處且可被傳送至第二節點 150。可替代是，特殊同步化節點(如無逗點密碼)可被使用。因為同步化問題通常被限制為僅若干樣本，所以該密碼僅需有限效能。與共用時序源相關之特殊同步化信號係可藉由終端來產生，而頻道脈衝響應量測可針對該信號而達成。該同步化問題可藉由於並非議題之領域中處理該頻道脈衝響應來處理。例如，假設相位資訊可被忽略，則該同步化問題不會出現於頻域中。

視頻道干擾位準而定，秘密比率損失可大或最小。例如，非常吵雜頻道中，相位資訊可能高度不可靠，因而忽略其將產生最小秘密比率損失。

再參考第 1 圖，後處理頻道脈衝響應估測 115 係被饋送至秘鑰產生器 116，誤差修正編碼器 118 及同步化編碼產生器 120。秘鑰產生器 116 可從頻道脈衝響應估測 115 產生秘鑰 117，其為未由他人分享聯合隨機位元。

同步化編碼產生器 120 可產生用於同時性及同步化"起始點"之同步化信號/編碼 121。誤差修正編碼器 118 可對頻道脈衝響應估測 115 執行誤差修正編碼並產生同位位元 119。誤差修正編碼可為區塊編碼或迴旋編碼。本發明使用系統誤差修正編碼，使得原始訊息(也就是係頻道脈衝響應估測 115 之編碼器輸入)亦被輸出自誤差修正編碼器 118。依據本發明，僅同位位元 119 於被多工器 122 以同步化信號/編碼 121 多工之後被傳送至第二節點 150。該被多工位元流 123 係被傳送至第二節點

150。

第二節點 150 包含一頻道估測器 152，一同步化位元解調器 154，一同位位元解調器 156，一後處理器 158(可選)，一同步化單元 160，一誤差修正解碼器 162 及一秘鑰產生器 164。頻道估測器 152 可從第一節點 110 所傳送之被接收信號 151 產生之頻道脈衝響應估測。頻道脈衝響應估測 153 係選擇性藉由上述同位位元解調器 156 來處理。同步化位元解調器 154 可解調該被接收信號 151 來回復同步化信號/編碼 155。同位位元解調器 156 可解調該被接收信號 151 來回復同位位元 157。同步化信號/編碼 155 係被饋送至同步化單元 160，而同位位元 157 係被饋送至誤差修正解碼器 162。後處理頻道脈衝響應估測 159 係藉由同步化單元 160 處理。同步化單元 160 可依據同步化信號/編碼 155 來修正因缺乏同時性及/或起始點錯誤校準導致之頻道脈衝響應估測差異。

誤差修正解碼器 162 可執行誤差修正解碼將同步化單元 160 所處理之頻道脈衝響應估測 159 當作編碼字元訊息部分，其可能包含誤差並使用該被接收同位位元 157 來修正該誤差。若區塊編碼被良好選擇，則誤差修正解碼器 162 之輸出 163 係與第一節點 110 以非常高機率所產生之頻道脈衝響應估測相同。因此，第一節點 110 及第二節點 150 成功獲得相同資料序列，但僅公開地揭示其若干部分(也就是同位位元)且可衍生相同未由他人分享聯合隨機位元。

誤差修正解碼器 162 可被用來支援被數位化頻道脈衝響應估測起始點之同步化。第二節點 150 可產生一組頻道脈衝響應估測，並以同位位元 157 解碼各可能頻道脈衝響應估測。誤差修正解碼器 162 可計數各頻道脈衝響應估測中之誤差數。由於非常高機率，僅修正者會產生非常高修正數；而修正者產生非常低修正數。此法中，誤差修正解碼處理可支援該起始點同步化。

一旦頻道脈衝響應估測已於第一節點 110 及第二節點 150 之間被校準，秘鑰產生器 164 係可產生與第一節點 110 所產生之秘鑰 117 相同之秘鑰 165。

第 3 圖為依據本發明衍生用於無線系統之未由他人分享聯合隨機位元及秘鑰之處理 300 流程圖。第一節點可從被第二節點傳送之傳輸產生頻道脈衝響應估測，而第二節點可從被第一節點傳送之傳輸產生頻道脈衝響應估測(步驟 302)。為了修正第一節點所產生之頻道脈衝響應估測及第二節點所產生之頻道脈衝響應估測間之差異(及選擇性支援該頻道脈衝響應估測之同步化)，該第一節點可傳送同位位元(及選擇性同步化信號/編碼)至該第二節點(步驟 304)。該同位位元可藉由該第一節點所產生之頻道脈衝響應估測上之誤差修正編碼來產生。該第二節點可使用該第一節點所傳送之同步化信號/編碼或使用上述某些其他方案將該第二節點所產生之頻道脈衝響應估測與該第一節點所產生之頻道脈衝響應估測同步化(步驟 306)。該第二節點接著藉由該同位位

元對該被同步化頻道脈衝響應估測執行誤差修正解碼來修正對該被同步化頻道脈衝響應估測及該第一節點所產生之頻道脈衝響應估測間之差異(步驟 308)。步驟 302-308 可被重複若干次。此法中，第一節點及第二節點可獲得相同頻道脈衝響應估測(未由他人分享聯合隨機位元)。第一節點及第二節點接著可從該相同頻道脈衝響應估測產生秘鑰(步驟 310)。

第 4 圖為依據本發明一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理 400 流程圖。一旦無線傳送/接收單元於步驟 402 被與存取點連結，則可決定無線網路所支援之驗證類型是 IEEE802.1x 或先分享鑰匙(步驟 404)。若 IEEE802.1x 被支援，則驗證，授權及會計(AAA)伺服器及無線傳送/接收單元可使用數位憑證來彼此驗證(步驟 406)。當部份驗證信號發送時，無線傳送/接收單元係傳送使用該驗證，授權及會計伺服器之公共鑰匙被加密之秘密至該驗證，授權及會計伺服器，使得僅該驗證，授權及會計伺服器得以使用對應私用鑰匙來解密它。此秘密係被當作衍生秘鑰之種子。該驗證，授權及會計伺服器接著傳送該秘密至存取點(步驟 408)。若被支援驗證類型為先分享鑰匙，則該先分享鑰匙係被設定為預設秘密(步驟 410)。

存取點及無線傳送/接收單元可使用上述說明之處理來產生未由他人分享聯合隨機位元(步驟 412)。應注意，未由他人分享聯合隨機位元不僅於秘密被轉送之

後，並於該秘鑰產生之前任何步驟被產生。存取點及無線傳送/接收單元可使用該秘密及未由他人分享聯合隨機位元來衍生秘鑰(步驟 414)。存取點及無線傳送/接收單元接著交換一部份秘鑰來確認鑰匙及身分(步驟 416)。群組鑰匙可如 IEEE 802.1i 目前所做者使用秘鑰當作成對瞬變鑰匙被衍生及傳送至無線傳送/接收單元(步驟 418)。

秘鑰準備被衍生時尚未產生充足未由他人分享聯合隨機位元之事件中，依據 IEEE 802.11i 標準之處理係可被遵循。應注意，起始衍生係需步驟 402-410，而秘鑰更新或再新僅可藉由衍生新未由他人分享聯合隨機位元來執行。

為了更新鑰匙，802.1x 例中，新秘密可被交換且新未由他人分享聯合隨機位元可被產生，或可替代地，具有舊秘密之新未由他人分享聯合隨機位元可被使用。僅第二部份可用於先分享鑰匙例。歷史資料可被用來驗證未由他人分享聯合隨機位元。雙方可快取某些早期鑰匙事先同意部份。入侵者不能僅使用被偷竊私用鑰匙，還必須猜測被衍生之先前鑰匙來解密該主秘密。

此處理明確地分隔系統中之驗證及鑰匙產生角色。驗證，授權及會計伺服器僅處理驗證客戶，而存取點處理鑰匙產生。此與 IEEE 802.1x 不同，其中驗證，授權及會計伺服器被牽涉鑰匙衍生及驗證。未由他人分享聯合隨機可促使新及最新秘鑰動態地每幾百分之一

秒(視頻道情況而定)被衍生。此與先前技術不同，其中鑰匙更新係被事先程式設計且不為新密碼，而新秘密係於產生新鑰匙之處必須被交換。本發明處理 400 中並無主鑰匙或成對主鑰匙。因此，該處理較先前技術簡單。

既存 802.11i 協定中，知道驗證憑據(802.1x 例中)或先分享鑰匙(先分享鑰匙驗證例中)之入侵者僅必須偷聽信號發送交換來知道秘鑰。相對地，使用本發明方法時，當處理驗證憑據(如數位憑證或先分享鑰匙驗證)之入侵者不分享無線傳送/接收單元及存取點所分享之相同頻道時，其不能衍生秘鑰，因而不能做出相同未由他人分享聯合隨機位元。

現行 IEEE 802 標準下，鑰匙更新並不真正密碼安全，因為僅成對瞬變鑰匙改變而主鑰匙及成對主鑰匙維持相同。若入侵者猜到成對主鑰匙，則當成對瞬變鑰匙剛好是成對主鑰匙加上清除中被交換之隨機資訊時，更新鑰匙並不服務任何密碼術目的。被用來衍生主鑰匙及成對主鑰匙之主秘密係服務密碼術目的而非常長(如 48 位元組)。因此，針對 IEEE 802.11i 中之新鑰匙，必須交換已被真正隨機衍生之長 48 位元組數(其為資源密集)。然而，依據本發明，該被交換秘密可驗證被衍生自未由他人分享聯合隨機位元之秘鑰，而僅需長得足以阻止蠻力入侵者(如約 16 位元組)。此使其可於每次鑰匙必須以未由他人分享聯合隨機更新時重新產生它。本發明提供僅一被交換短秘密及一組被衍生鑰匙，而非一被交換長

鑰匙及 3 組被衍生鑰匙(也就是主鑰匙，成對主鑰匙及成對瞬變鑰匙)之較簡單鑰匙衍生方法。此可節省行動裝置之電源。

第 5 圖為依據本發明另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理 500 流程圖。處理 500 類似處理 400。步驟 502-512 與步驟 402-412 相同，為了簡化不再解釋。秘密被轉送至存取點且未由他人分享聯合隨機位元被產生之後，存取點及無線傳送/接收單元可使用該秘密及未由他人分享聯合隨機位元來衍生成對主鑰匙(步驟 514)。群組鑰匙接著可如 IEEE 802.11i 目前所做者被衍生及傳送至無線傳送/接收單元(步驟 516)。

第 6 圖為依據本發明再另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理 600 流程圖。一旦無線傳送/接收單元於步驟 602 被與存取點連結，則可決定無線網路所支援之驗證類型是 IEEE802.1x 或先分享鑰匙(步驟 604)。若 IEEE802.1x 被支援，則驗證，授權及會計伺服器及無線傳送/接收單元可使用數位憑證來彼此驗證並交換主秘密(步驟 606)。驗證，授權及會計伺服器及無線傳送/接收單元接著使用該主秘密來衍生主鑰匙(步驟 608)。驗證，授權及會計伺服器及無線傳送/接收單元接著從該主鑰匙衍生成對主鑰匙，而驗證，授權及會計伺服器將此成對主鑰匙傳送至存取點(步驟 610)。若被支援驗證類型為先分享鑰匙，則該先分享鑰匙係被設定為成對主鑰匙(步驟 611)。

存取點及無線傳送/接收單元使用上述說明之處理來產生未由他人分享聯合隨機位元(步驟 612)。應注意，未由他人分享聯合隨機位元不僅於成對主鑰匙被轉送之後，並於該秘鑰產生之前任何步驟被產生。其可於衍生成對主鑰匙之前被執行(802.1x 例中)來加速鑰匙衍生處理。亦可於 4 向交握處理期間被達成以衍生成對瞬變鑰匙。此使系統得以與先分享鑰匙驗證相容。同位檢查亦可於衍生成對瞬變鑰匙之前任何時間被執行。

存取點及無線傳送/接收單元使用成對主鑰匙及未由他人分享聯合隨機位元來衍生成對瞬變鑰匙(步驟 614)。成對瞬變鑰匙可被衍生如下：

PTK＝PRF(成對主鑰匙，清除中之資訊，未由他人分享聯合隨機位元)。

群組鑰匙接著可如 IEEE 802.11i 目前所做者被衍生及交換(步驟 616)。

第 7 圖為依據本發明仍再另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理 700 流程圖。一旦無線傳送/接收單元於步驟 702 被與存取點連結，則可決定無線網路所支援之驗證類型是 IEEE802.1x 或先分享鑰匙(步驟 704)。此實施例中，先分享鑰匙不被支援而僅 IEEE802.1x 被支援。若先分享鑰匙為網路所支援類型，則該處理結束。若 IEEE802.1x 被支援，則驗證，授權及會計伺服器及無線傳送/接收單元可交換先主秘密，而驗證，授權及會計伺服器傳送該主秘密至存取點(步驟

706)。

驗證，授權及會計伺服器及存取點使用該先主秘密來衍生主鑰匙(步驟 710)。無線傳送/接收單元及存取點接著使用該主鑰匙及未由他人分享聯合隨機位元來衍生成對主鑰匙(步驟 712)。存取點及無線傳送/接收單元使用該成對主鑰匙來衍生成對瞬變鑰匙(步驟 714)。群組鑰匙接著可如 IEEE 802.11i 目前所做者被衍生及交換(步驟 716)。

第 8 圖為依據本發明使用 Diffie-Hellman 協定衍生秘鑰之處理 800 流程圖。無線傳送/接收單元 802 及存取點 804 同意使用未由他人分享聯合隨機藉由交換未由他人分享聯合隨機起始訊息來驅動鑰匙至存取點及未由他人分享聯合隨機起始確認(步驟 812，814)。無線傳送/接收單元 802 及存取點 804 係以頻道脈衝響應估測為基礎從彼此間之傳輸產生未由他人分享聯合隨機位元(步驟 816，818)。無線傳送/接收單元 802(率先)藉由對被產生頻道脈衝響應估測執行誤差修正編碼來產生同位位元並傳送該同位位元至存取點 804(步驟 820)。存取點 804 使用該被接收同位位元來執行誤差修正解碼且可選擇性傳送確認(步驟 822)。步驟 816-822 可被重複若干次。

無線傳送/接收單元 802 及存取點 804 係具有可儲存映射未由他人分享聯合隨機位元至 p 及 q 值之秘密數 p 及 q(質數)之預定查找表(LUT)。例如，若未由他人分享聯合隨機測量可產生 5 位元秘密資料，無線傳送/接收單

元 802 及存取點 804 可針對質數 p 選擇 16 可能唯一值之一及針對基數 g 選擇另 16 值。應注意，熟練技術人士所明瞭之其他方案係可替代查找表被使用。因為依據本發明具有 p 及 g 秘密之安全性附加層，所以被儲存質數應該很大，但不必與傳統 Diffie-Hellman 協定般大。較佳地，該質數大小階亦應不同使入侵者很難猜測模數值範圍。雖然公開已知未由他人分享聯合隨機位元對查找表值之映射，但因為入侵者不能偷聽未由他人分享聯合隨機測量，所以其並不知何值實際被選用。

無線傳送/接收單元 802 及存取點 804 分別選擇秘密整數 a 及 b，並分別傳送 g^a 模 p 及 g^b 模 q 至另一方，並分別驅動 b 及 a(步驟 824，826)。無線傳送/接收單元 802 及存取點 804 使用此來衍生共享秘密(步驟 828)。無線傳送/接收單元 802 及存取點 804 使用該共享秘密來傳送被加密未由他人分享聯合隨機鑰匙或將該共享秘密當作未由他人分享聯合隨機鑰匙(步驟 830)。

雖然本發明之特性及元件被以特定組合說明於較佳實施例中，但各特性及元件係不需較佳實施例之其他特性及元件，或有或無本發明其他特性及元件之各種組合中被單獨使用。

【圖式簡單說明】

第 1 圖為依據本發明包含可衍生秘鑰之兩通信實體之系統區塊圖。

第 2 圖說明因第一節點及第二節點處之不同起始點

所造成之頻道脈衝響應估測差異問題。

第 3 圖為依據本發明衍生秘鑰之處理流程圖。

第 4 圖為依據本發明一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理流程圖。

第 5 圖為依據本發明另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理流程圖。

第 6 圖為依據本發明再另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理流程圖。

第 7 圖為依據本發明仍再另一實施例使用未由他人分享聯合隨機位元衍生秘鑰之處理流程圖。

第 8 圖為依據本發明使用 Diffie-Hellman 鑰匙衍生演算法衍生秘鑰之處理流程圖。

【主要元件符號說明】

100	區塊圖
110、150	節點
113、115、153、159	頻道脈衝響應估測
117、165	秘鑰
119、157	位元
121、155	信號/編碼
123	位元流
163	輸出
300、400、500、600、700、800	流程圖
AP	存取點
a、b	秘密整數

g	基數
p、q	質數
PSK	先分享鑰匙
WTRU	無線傳送/接收單元

五、中文發明摘要

本發明與一種使用未由他人分享聯合隨機而衍生秘鑰之方法及系統有關。通信實體係從頻道脈衝響應(CIR)估測產生未由他人分享聯合隨機位元，而該未由他人分享聯合隨機位元係用於產生秘鑰。該驗證類型可為 IEEE 802.1x 或先分享鑰匙系統。 IEEE 802.1x 系統中，主鑰匙，成對主鑰匙或成對瞬變鑰匙係可使用該未由他人分享聯合隨機位元來產生。該秘鑰可使用 Diffie-Hellman 鑰匙衍生演算法來產生。

六、英文發明摘要

The present invention is related to a method and system for deriving an encryption key using joint randomness not shared by others (JRNSO). Communicating entities generate JRNSO bits from a channel impulse response (CIR) estimate and the JRNSO bits are used in generation of an encryption key. The authentication type may be IEEE 802.1x or a pre-shared key system. In an IEEE 802.1x system, a master key, a pairwise master key or a pairwise transient key may be generated using the JRNSO bits. The encryption key may be generated by using a Diffie-Hellman key derivation algorithm.

生。

5. 如申請專利範圍第 1 項的方法，其中該第一節點傳送一同步化編碼至該第二節點，藉此該第二節點使用該同步化編碼同步化該第二頻道脈衝響應估測與該第一頻道脈衝響應估測。

6. 如申請專利範圍第 1 項的方法，其中該第一節點與該第二節點藉由使用全球定位系統(GPS)信號來同步化該第二頻道脈衝響應估測與該第一頻道脈衝響應估測。

7. 如申請專利範圍第 1 項的方法，更包含：

該第一節點與該第二節點使用該未由他人分享聯合隨機位元衍生出一秘鑰。

8. 如申請專利範圍第 7 項的方法，更包含：

該第一節點與一驗證伺服器彼此驗證；以及

該第一節點與該驗證伺服器交換一秘密，其中該第一節點與該第二節點更以該祕密為基礎來產生該秘鑰。

9. 如申請專利範圍第 8 項的方法，更包含：

該第二節點自該秘鑰中衍生出一群組鑰匙；以及

該第二節點將該群組鑰匙提供至該第一節點以便在該第一節點與該第二節點間通信。

10. 如申請專利範圍第 7 項的方法，其中該第一節點與該第二節點更以一先分享鑰匙為基礎來產生該秘鑰。

11. 如申請專利範圍第 7 項的方法，其中該第一節點與該第二節點週期性地產生該未由他人分享聯合隨機位元以產生一新秘鑰。

12. 如申請專利範圍第 7 項的方法，其中該秘鑰為一成對主鑰匙。

13. 如申請專利範圍第 7 項的方法，更包含：

該第一節點與一驗證伺服器彼此驗證；

該第一節點與該驗證伺服器交換一主秘密；以及

該第一節點與該第二節點自該主秘密中衍生出一成對主鑰匙，其中該第一節點與該第二節點更以該成對主鑰匙為基礎來產生該秘鑰。

14. 如申請專利範圍第 13 項的方法，更包含：

該第二節點自該秘鑰中衍生出一群組鑰匙；以及

該第二節點將該群組鑰匙提供至該第一節點以便在該第一節點與該第二節點間通信。

15. 如申請專利範圍第 12 項的方法，其中該第一節點與該第二節點將一先分享鑰匙設定為該成對主鑰匙。

16. 如申請專利範圍第 7 項的方法，更包含：

該第一節點與一驗證伺服器彼此驗證；

該第一節點與該驗證伺服器交換一先主秘密；

該驗證伺服器將該先主秘密轉送至該第二節點；

該第一節點與該第二節點使用該先主秘密與該未由他人分享聯合隨機位元而衍生出一主鑰匙，以及

該第一節點與該第二節點使用該主秘密與該未由他人分享聯合隨機位元而衍生出一成對主鑰匙，其中該第一節點與該第二節點使用該成對主鑰匙與該未由他人分享聯合隨機位元來衍生出該秘鑰。

17. 如申請專利範圍第 16 項所述的方法，更包含：

該第二節點自該秘鑰中衍生出一群組鑰匙；以及

該第二節點將該群組鑰匙提供至該第一節點以便在該第一節點與該第二節點間通信。

18. 一種第一節點，用於在包含該第一節點及一第二節點的一無線通信系統中確保在該第一節點及該第二節點間無線通信的安全，該第一節點包含：

一頻道估測器，用於從該第二節點所傳送的傳輸中產生一第一頻道脈衝響應估測；以及

一誤差修正編碼器，用於藉由對該第一頻道脈衝響應估測執行誤差修正編碼來產生同位位元，該同位位元被傳送至該第二節點，該第二節點從該第一節點所傳送的傳輸中產生一第二頻道脈衝響應估測，並以該同位位元對該第二頻道脈衝響應執行一誤差修正解碼，藉此該第一節點與該第二節點取得相同的頻道脈衝響應估測以作為未由他人分享聯合隨機位元。

19. 如申請專利範圍第 18 項的第一節點，更包含：

一後處理器，用以對該第一頻道脈衝響應估測執行後處理，藉此，該第一節點在後處理後以該第一頻道脈衝響應估測來執行該誤差修正編碼。

20. 如申請專利範圍第 18 項的第一節點，其中該誤差修正編碼器藉由在該第一頻道脈衝響應估測上應用區塊編碼以產生該同位位元。

21. 如申請專利範圍第 18 項的第一節點，其中該誤差修正編碼器藉由在該第一頻道脈衝響應估測上應用系統

迴旋編碼以產生該同位位元。

22. 如申請專利範圍第 18 項的第一節點，更包含：

一同步化編碼產生器，用以產生將傳送至該第二節點的一同步化編碼，藉此該第二節點使用該同步化編碼同步化該第二頻道脈衝響應估測與該第一頻道脈衝響應估測。

23. 如申請專利範圍第 18 項的第一節點，更包含：

一秘密鑰匙產生器，用於使用該未由他人分享聯合隨機位元來產生一秘鑰。

24. 如申請專利範圍第 23 項的第一節點，其中該第一節點與一驗證伺服器彼此驗證並交換一秘密，其中該第一節點與該第二節點更以該祕密為基礎來產生該秘鑰。

25. 如申請專利範圍第 23 項的第一節點，其中該祕密鑰匙產生器更以一先分享鑰匙為基礎來產生該秘鑰。

26. 如申請專利範圍第 23 項的第一節點，其中該第一節點週期性地產生該未由他人分享聯合隨機位元以產生一新秘鑰。

27. 如申請專利範圍第 23 項的第一節點，其中該秘鑰為一成對主鑰匙。

28. 如申請專利範圍第 23 項的第一節點，其中該第一節點與一驗證伺服器彼此驗證並交換一主秘密，該祕密鑰匙產生器自該主祕密中衍生出一成對主鑰匙且更以該成對主鑰匙為基礎來產生該秘鑰。

29. 如申請專利範圍第 23 項的第一節點，其中該祕密鑰

匙產生器將一先分享鑰匙設定為一成對主鑰匙，並以該成對主鑰匙為基礎來產生該秘鑰。

30. 如申請專利範圍第 23 項的第一節點，其中該第一節點與一驗證伺服器彼此驗證並交換一先主秘密，而且該秘密鑰匙產生器使用該先主秘密與該未由他人分享聯合隨機位元而衍生出一主鑰匙、使用該主鑰匙與該未由他人分享聯合隨機位元來衍生出一成對主鑰匙、並使用該成對主鑰匙與該未由他人分享聯合隨機位元來衍生出該秘鑰。

31. 一種第二節點，用於在包含一第一節點及該第二節點的一無線通信系統中確保在該第一節點及該第二節點間無線通信的安全，該第二節點包含：

一頻道估測器，用於從該第一節點所傳送的傳輸中產生一第二頻道脈衝響應估測；以及

一誤差修正解碼器，用於以同位位元對該第二頻道脈衝響應執行誤差修正解碼，該同位位元是由該第一節點透過對從該第二節點傳送出的傳輸產生的一第一頻道脈衝響應估測執行誤差修正編碼而產生的，藉此該第一節點與該第二節點取得相同的頻道脈衝響應估測以作為未由他人分享聯合隨機位元。

32. 如申請專利範圍第 31 項的第二節點，更包含：

一後處理器，用以對該第二頻道脈衝響應估測執行後處理，藉此，該誤差修正解碼器在後處理後對該第二頻道脈衝響應估測執行該誤差修正解碼。

33. 如申請專利範圍第 31 項的第二節點，更包含：

點與一驗證伺服器彼此驗證並交換一主秘密，該祕密鑰匙產生器自該主祕密中衍生出一成對主鑰匙且更以該成對主鑰匙為基礎來產生該秘鑰。

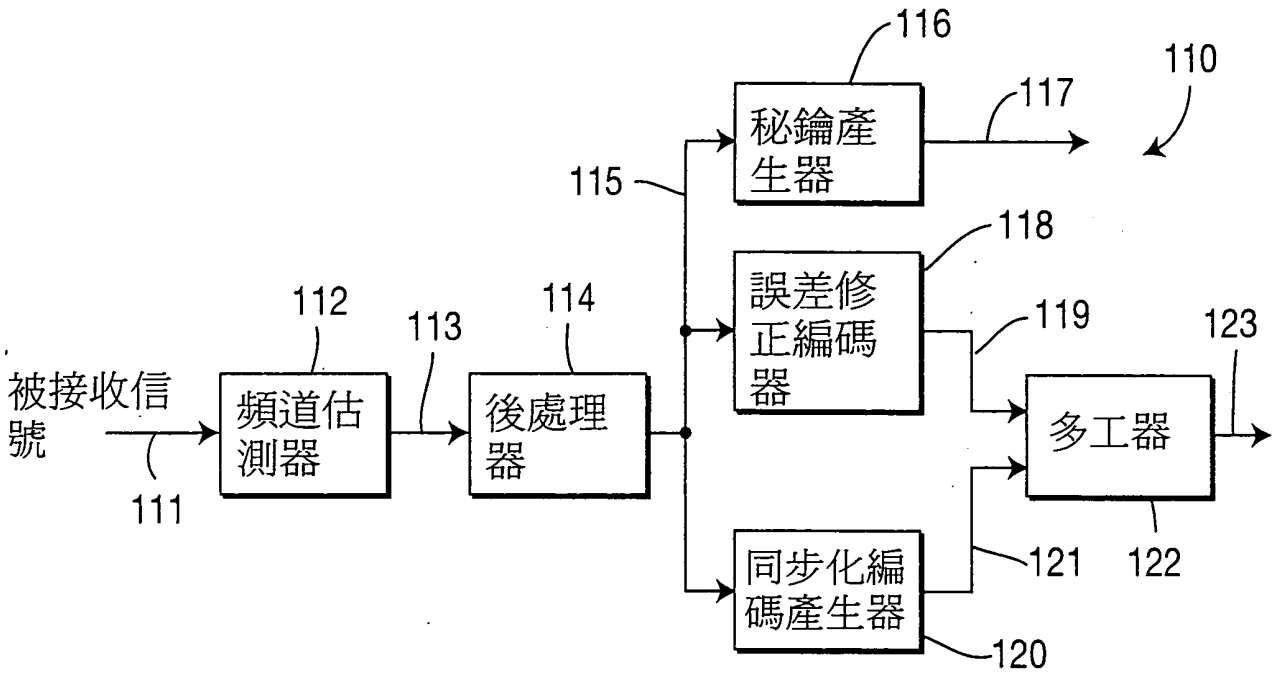
42. 如申請專利範圍第 41 項的第二節點，其中該祕密鑰匙產生器自該秘鑰中衍生出一群組鑰匙且為了在該第一節點與該第二節點間的通信而把該群組鑰匙供至該第一節點。

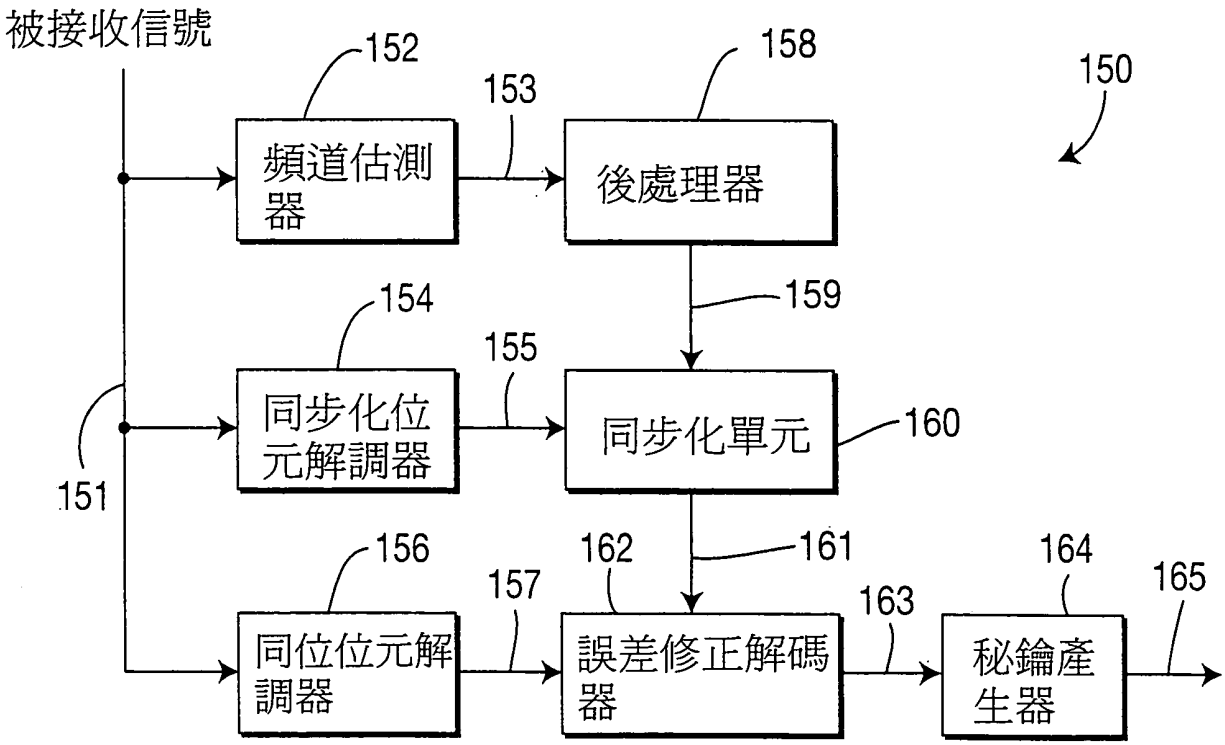
43. 如申請專利範圍第 35 項的第二節點，其中該第一節點與該第二節點將一先分享鑰匙設定為一成對主鑰匙，並以該成對主鑰匙為基礎來產生該秘鑰。

44. 如申請專利範圍第 35 項的第二節點，其中該第一節點與一驗證伺服器彼此驗證並交換一先主秘密，而且該祕密鑰匙產生器使用該先主祕密與該未由他人分享聯合隨機位元而衍生出一主鑰匙、使用該主鑰匙與該未由他人分享聯合隨機位元來衍生出一成對主鑰匙、並使用該成對主鑰匙與該未由他人分享聯合隨機位元來衍生出該秘鑰。

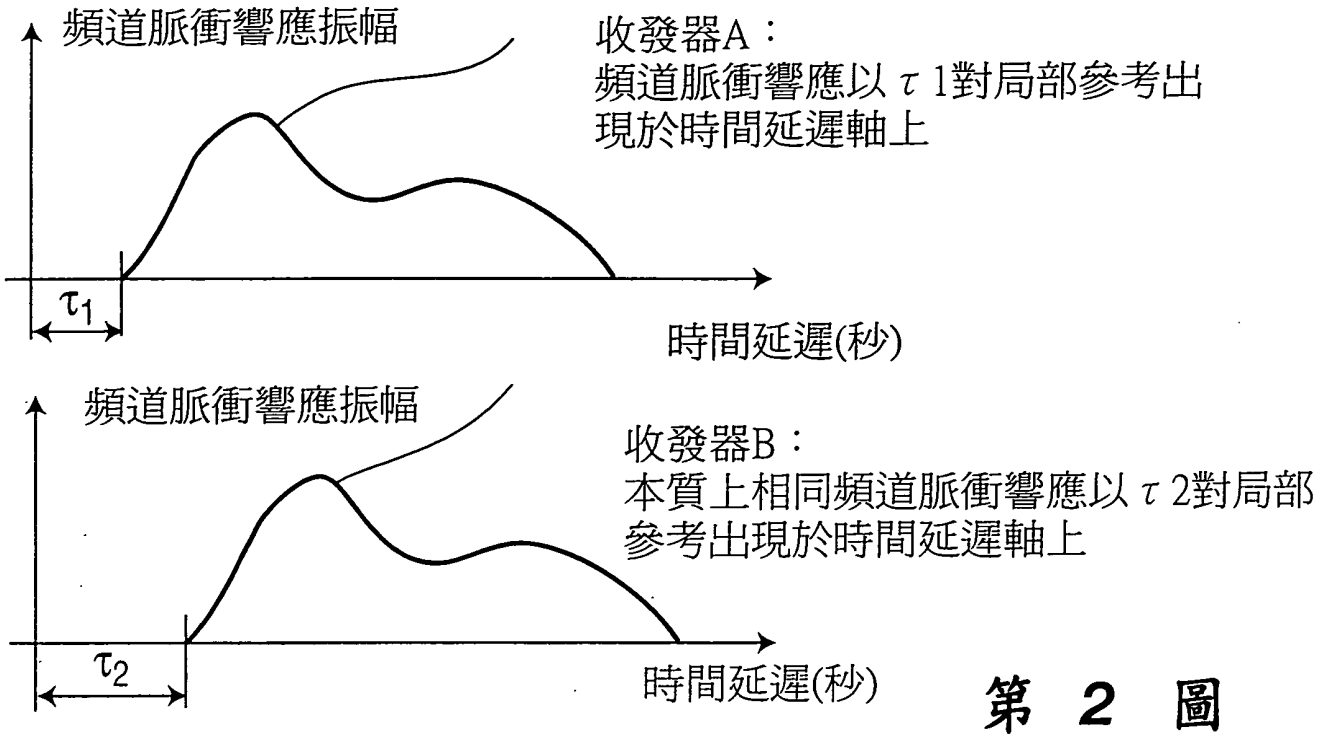
45. 如申請專利範圍第 44 項的第二節點，其中該祕密鑰匙產生器自該秘鑰中衍生出一群組鑰匙且為了在該第一節點與該第二節點間的通信而把該群組鑰匙供至該第一節點。

十一、圖式：

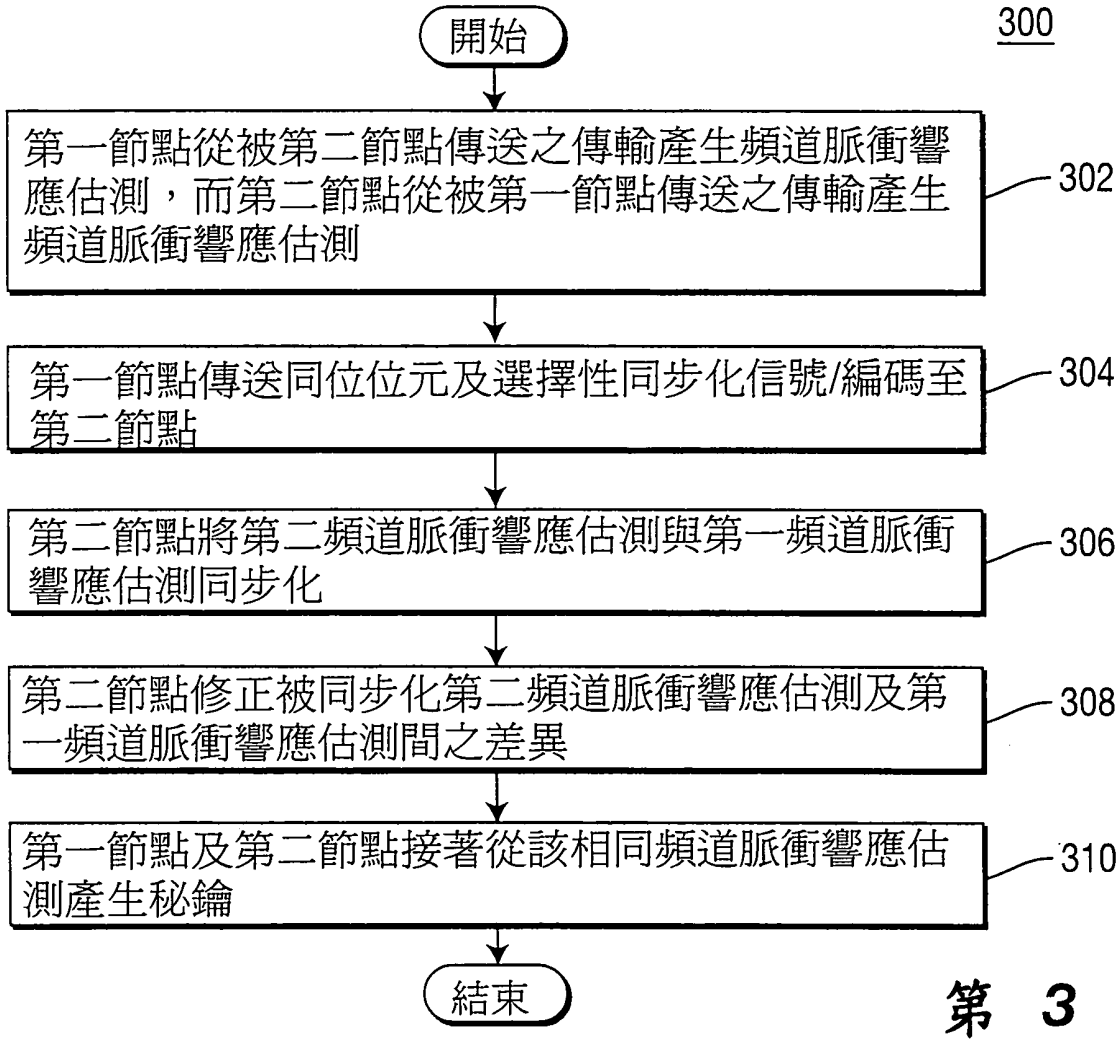

100
116
110
秘鑰產生器
117
115
118
誤差修正編碼器
119
123
112
113
114
被接收信號
頻道估測器
後處理器
多工器
111
同步化編碼產生器
121
122
120


被接收信號
152
158
150
153
頻道估測器
後處理器
154
159
155
同步化位元解調器
同步化單元
160
151
156
162
161
164
165
157
163
同位位元解調器
誤差修正解碼器
秘鑰產生器

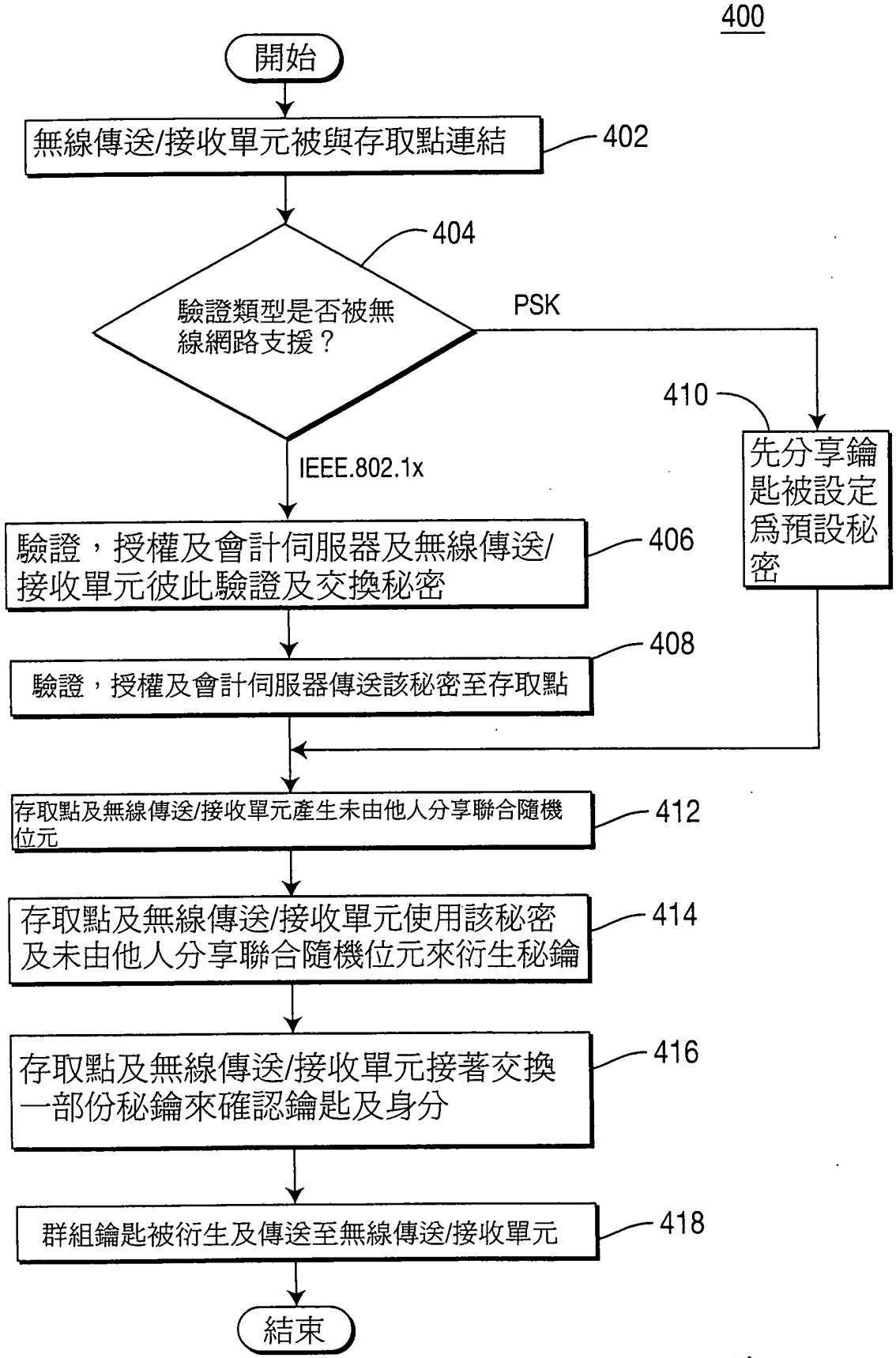
第 1 圖


頻道脈衝響應振幅
收發器A：
頻道脈衝響應以τ1對局部參考出現於時間延遲軸上
τ1
時間延遲(秒)
頻道脈衝響應振幅
收發器B：
本質上相同頻道脈衝響應以τ2對局部參考出現於時間延遲軸上
τ2
時間延遲(秒)

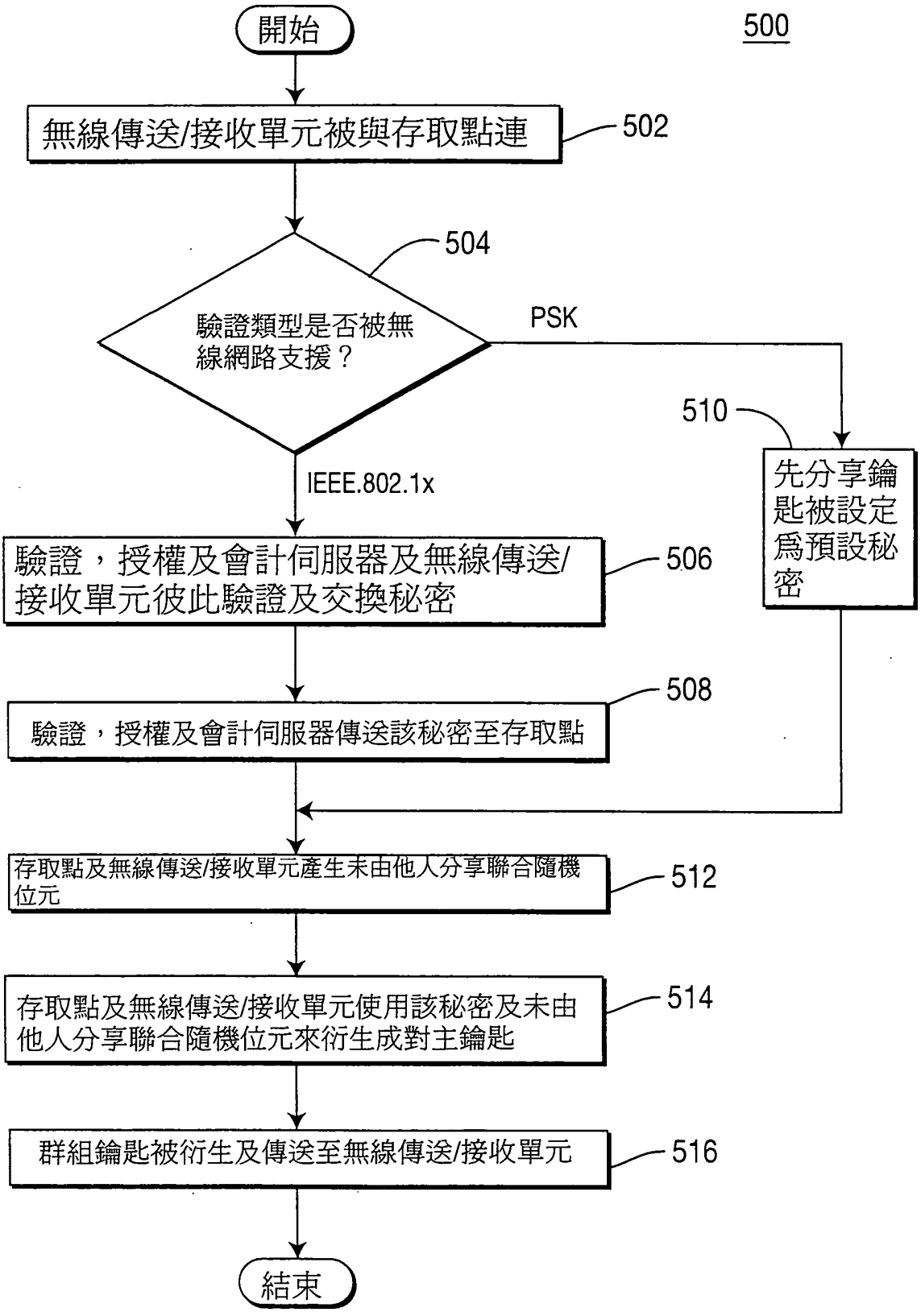
第 2 圖


300
開始
第一節點從被第二節點傳送之傳輸產生頻道脈衝響應估測，而第二節點從被第一節點傳送之傳輸產生頻道脈衝響應估測
302
第一節點傳送同位位元及選擇性同步化信號/編碼至第二節點
304
第二節點將第二頻道脈衝響應估測與第一頻道脈衝響應估測同步化
306
第二節點修正被同步化第二頻道脈衝響應估測及第一頻道脈衝響應估測間之差異
308
第一節點及第二節點接著從該相同頻道脈衝響應估測產生秘鑰
310
結束

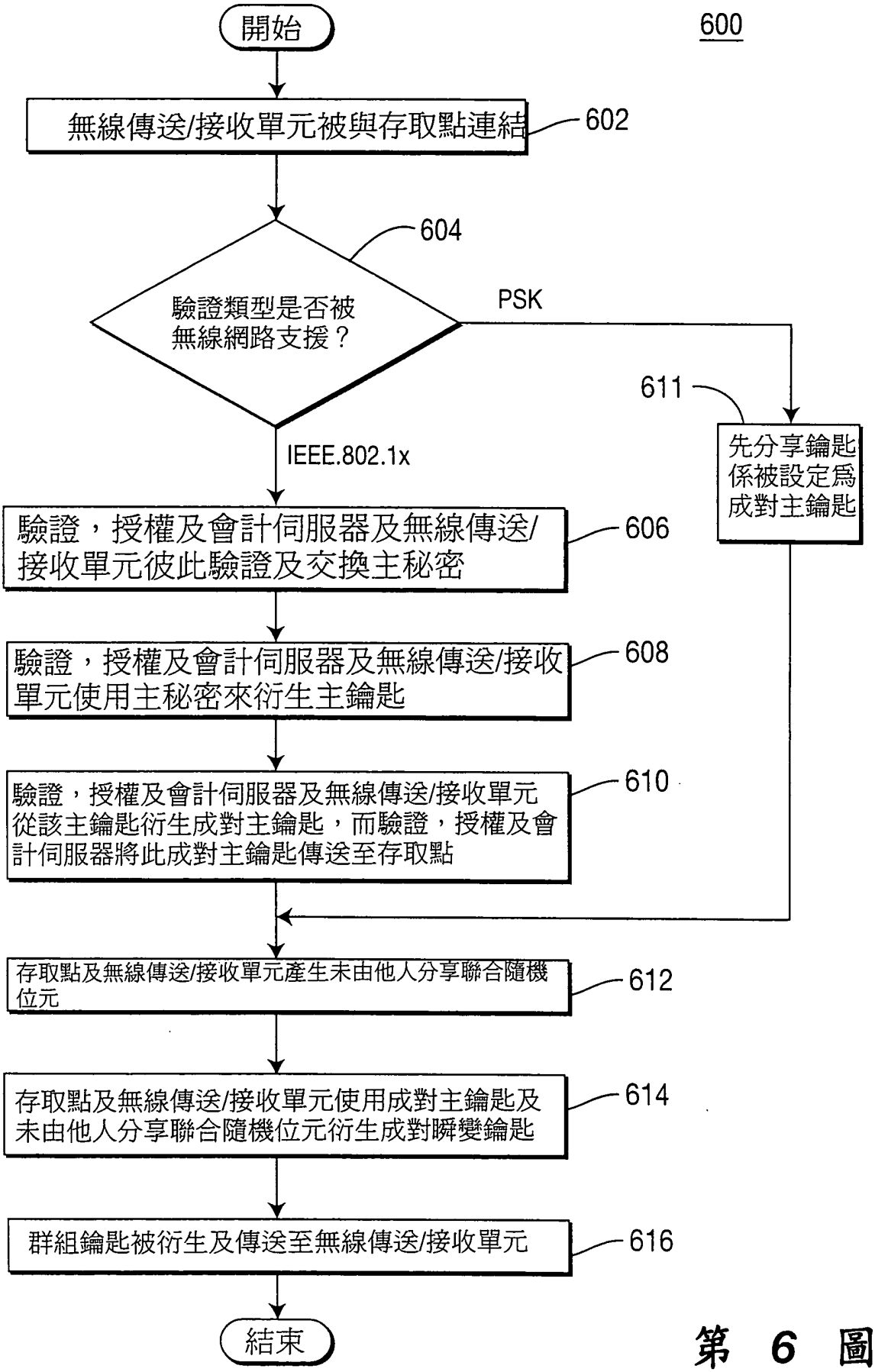
第 3 圖


400
開始
無線傳送/接收單元被與存取點連結
402
404
驗證類型是否被無線網路支援？
PSK
IEEE.802.1x
410
先分享鑰匙被設定爲預設秘密
驗證，授權及會計伺服器及無線傳送/接收單元彼此驗證及交換秘密
406
驗證，授權及會計伺服器傳送該秘密至存取點
408
存取點及無線傳送/接收單元產生未由他人分享聯合隨機位元
412
存取點及無線傳送/接收單元使用該秘密及未由他人分享聯合隨機位元來衍生秘鑰
414
存取點及無線傳送/接收單元接著交換一部份秘鑰來確認鑰匙及身分
416
群組鑰匙被衍生及傳送至無線傳送/接收單元
418
結束

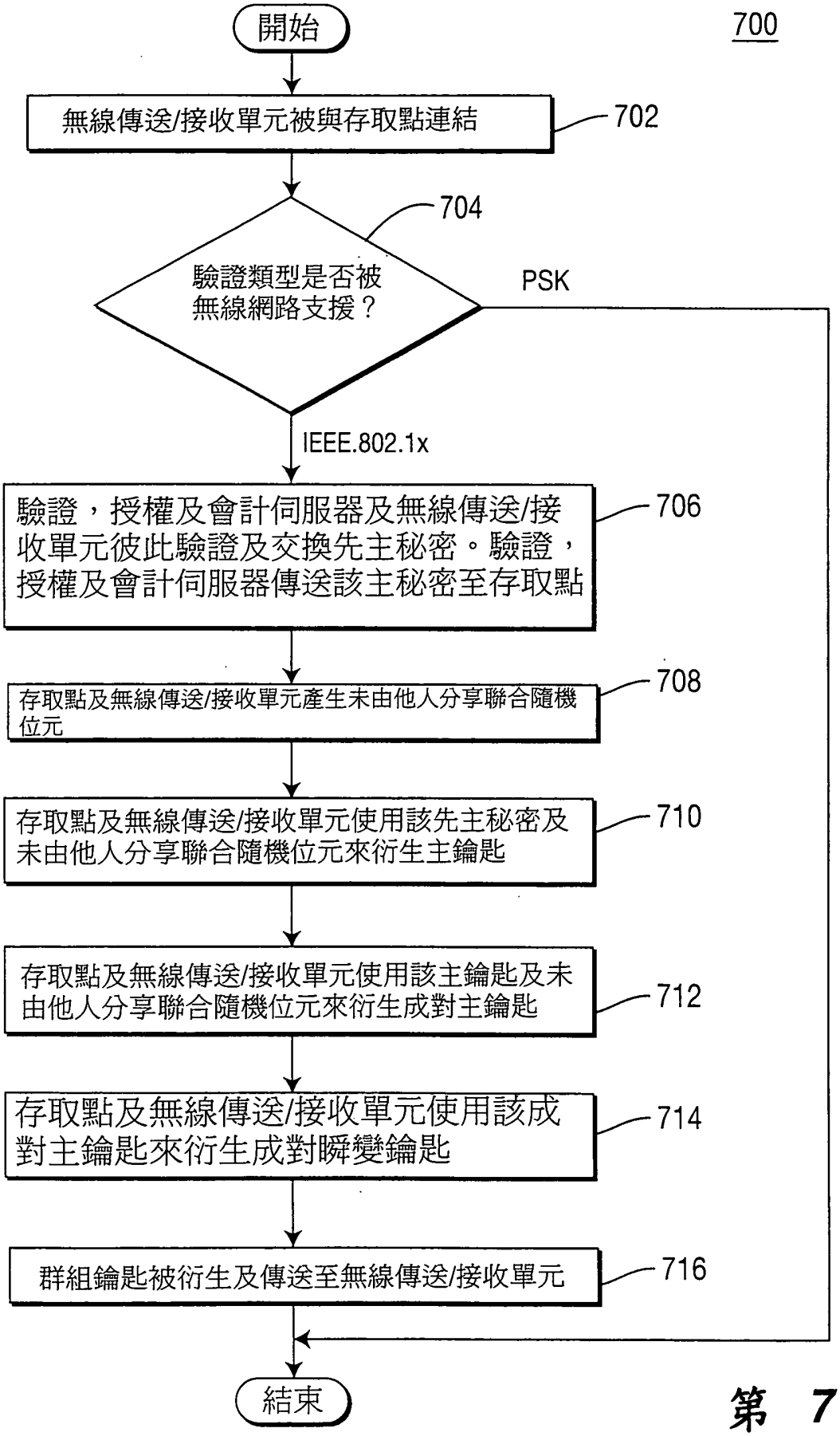
第 4 圖


開始
500
無線傳送/接收單元被與存取點連
502
504
驗證類型是否被無線網路支援？
PSK
IEEE.802.1x
510
先分享鑰匙被設定爲預設秘密
驗證，授權及會計伺服器及無線傳送/接收單元彼此驗證及交換秘密
506
驗證，授權及會計伺服器傳送該秘密至存取點
508
存取點及無線傳送/接收單元產生未由他人分享聯合隨機位元
512
存取點及無線傳送/接收單元使用該秘密及未由他人分享聯合隨機位元來衍生成對主鑰匙
514
群組鑰匙被衍生及傳送至無線傳送/接收單元
516
結束

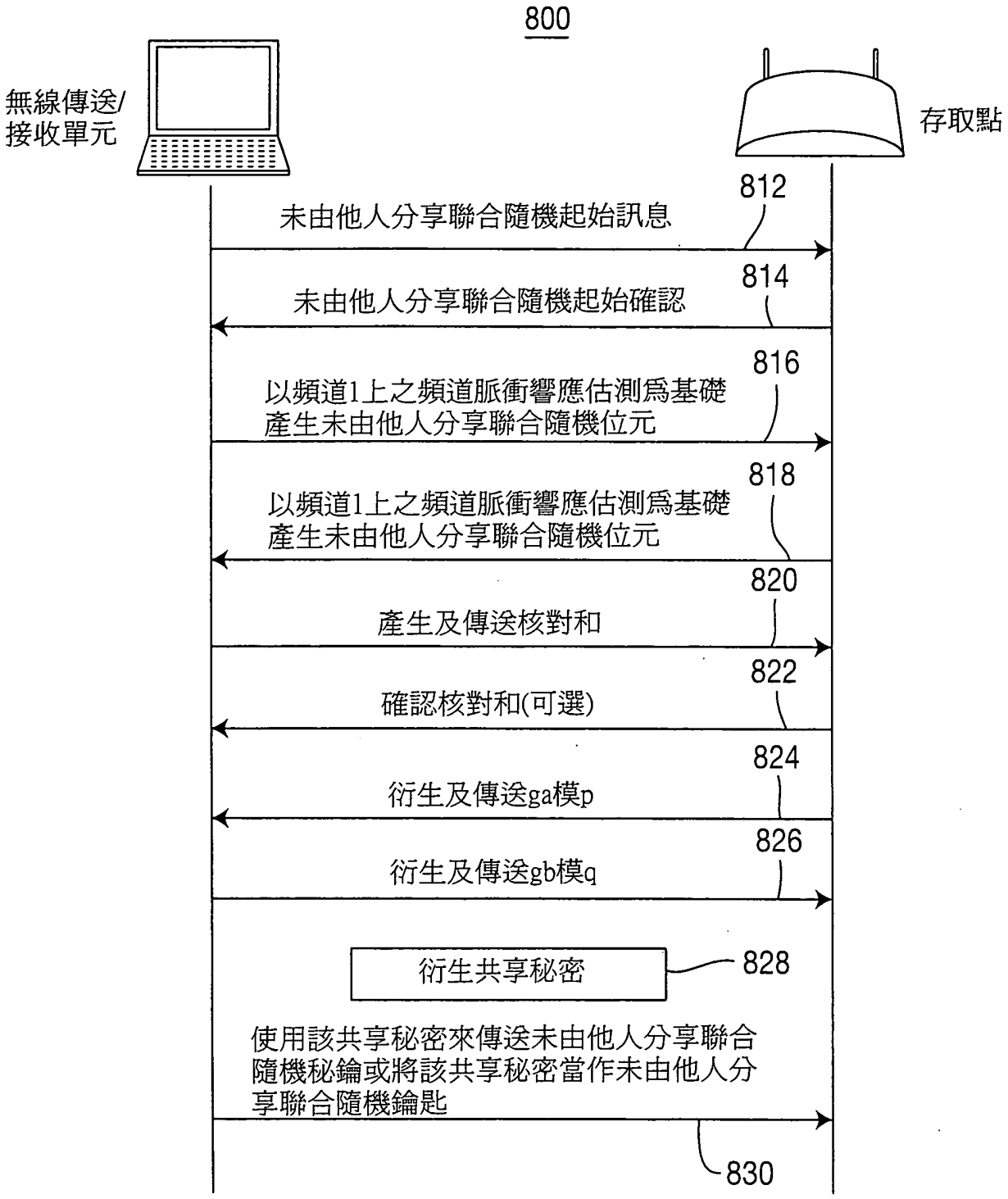
第 5 圖


600
開始
無線傳送/接收單元被與存取點連結
602
604
驗證類型是否被無線網路支援？
PSK
611
先分享鑰匙係被設定爲成對主鑰匙
IEEE.802.1x
驗證，授權及會計伺服器及無線傳送/接收單元彼此驗證及交換主秘密
606
驗證，授權及會計伺服器及無線傳送/接收單元使用主秘密來衍生主鑰匙
608
驗證，授權及會計伺服器及無線傳送/接收單元從該主鑰匙衍生成對主鑰匙，而驗證，授權及會計伺服器將此成對主鑰匙傳送至存取點
610
存取點及無線傳送/接收單元產生未由他人分享聯合隨機位元
612
存取點及無線傳送/接收單元使用成對主鑰匙及未由他人分享聯合隨機位元衍生成對瞬變鑰匙
614
群組鑰匙被衍生及傳送至無線傳送/接收單元
616
結束

第 6 圖


開始
700
無線傳送/接收單元被與存取點連結
702
704
驗證類型是否被無線網路支援？
PSK
IEEE.802.1x
驗證，授權及會計伺服器及無線傳送/接收單元彼此驗證及交換先主秘密。驗證，授權及會計伺服器傳送該主秘密至存取點
706
存取點及無線傳送/接收單元產生未由他人分享聯合隨機位元
708
存取點及無線傳送/接收單元使用該先主秘密及未由他人分享聯合隨機位元來衍生主鑰匙
710
存取點及無線傳送/接收單元使用該主鑰匙及未由他人分享聯合隨機位元來衍生成對主鑰匙
712
存取點及無線傳送/接收單元使用該成對主鑰匙來衍生成對瞬變鑰匙
714
群組鑰匙被衍生及傳送至無線傳送/接收單元
716
結束

第 7 圖


800
無線傳送/
接收單元
存取點
812
未由他人分享聯合隨機起始訊息
814
未由他人分享聯合隨機起始確認
816
以頻道1上之頻道脈衝響應估測爲基礎
產生未由他人分享聯合隨機位元
818
以頻道1上之頻道脈衝響應估測爲基礎
產生未由他人分享聯合隨機位元
820
產生及傳送核對和
822
確認核對和(可選)
824
衍生及傳送ga模p
826
衍生及傳送gb模q
衍生共享秘密
828
使用該共享秘密來傳送未由他人分享聯合
隨機秘鑰或將該共享秘密當作未由他人分
享聯合隨機鑰匙
830

第 8 圖

七、指定代表圖：

(一)本案指定代表圖為：第（8）圖。

(二)本代表圖之元件符號簡單說明:

800	流程圖
AP	存取點
a、b	秘密整數
g	基數
p、q	質數
WTRU	無線傳送/接收單元

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

102年3月19日修正頁

發明專利分割說明書

公告本

（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：95128389

※ 申請日期：95、1、20　　※IPC 分類：H04L 9/08 (2006.01)

原申請案號：095102241　　H04L 9/30 (2006.01)

一、發明名稱：（中文/英文）

確保無線通信安全之節點及其方法 / NODE FOR SECURING WIRELESS COMMUNICATIONS AND METHOD THEREOF

二、申請人：（共1人）

姓名或名稱：（中文/英文）

美商內數位科技公司 INTERDIGITAL TECHNOLOGY CORPORATION

代表人：（中文/英文）

唐納爾德・伯萊斯 DONALD M. BOLES

住居所或營業所地址：（中文/英文）

美國德拉威州 19801 威明頓德拉威大道 300 號 527 室 300 DELAWARE AVENUE, SUITE 527, WILMINGTON, DE 19801, U.S.A.

國　籍：（中文/英文）　美國/US

三、發明人：（共2人）

姓　名：（中文/英文）

1. 馬里恩・魯道夫 / MARIAN RUDOLF
2. 拉傑・普利塔・穆克吉/ RAJAT PRITAM MUKHERJEE

國　籍：（中文/英文）

1. 德國 / DE
2. 印度 / IN

十、申請專利範圍：

1. 一種用於在一第一節點及一第二節點間確保無線通信安全的方法，該方法包含：

(a) 該第一節點以該第二節點所傳送的傳輸為基礎產生一第一頻道脈衝響應估測；

(b) 該第一節點對該第一頻道脈衝響應估測執行一誤差修正編碼以產生同位位元；

(c) 該第一節點傳送該同位位元至該第二節點；

(d) 該第二節點以該第一節點所傳送的傳輸為基礎產生一第二頻道脈衝響應估測；以及

(e) 該第二節點以該接收到的同位位元來對該第二頻道脈衝響應執行一誤差修正解碼，使得該第二節點取得與該第一節點相同的頻道脈衝響應估測以作為未由他人分享聯合隨機位元。

2. 如申請專利範圍第1項的方法，進一步包含：

該第一節點後處理該第一頻道脈衝響應估測；及

該第二節點後處理該第二頻道脈衝響應估測，其中，該第一節點在後處理後以該第一頻道脈衝響應估測來執行該誤差修正編碼，以及，該第二節點在後處理後以該第二頻道脈衝響應估測來執行該誤差修正解碼。

3. 如申請專利範圍第1項的方法，其中該同位位元藉由在該第一頻道脈衝響應估測上應用區塊編碼而產生。

4. 如申請專利範圍第1項的方法，其中該同位位元藉由在該第一頻道脈衝響應估測上應用系統迴旋編碼而產

一同步化單元，用於使用該第一節點所傳送出的一同步化編碼同步化該第二頻道脈衝響應估測與該第一頻道脈衝響應估測。

34. 如申請專利範圍第31項的第二節點，其中該第二節點藉由使用全球定位系統信號來同步化該第一頻道脈衝響應估測與該第二頻道脈衝響應估測。

35. 如申請專利範圍第31項的第二節點，更包含：

一秘密鑰匙產生器，用於使用該未由他人分享聯合隨機位元來產生一秘鑰。

36. 如申請專利範圍第35項的第二節點，其中該第一節點與一驗證伺服器彼此驗證並交換一秘密，其中該祕密鑰匙產生器更以該祕密為基礎來產生該秘鑰。

37. 如申請專利範圍第36項的第二節點，其中該祕密鑰匙產生器自該秘鑰衍生出一群組鑰匙，並為了在該第一節點與該第二節點間的通信而把該群組鑰匙供至該第一節點。

38. 如申請專利範圍第35項的第二節點，其中該祕密鑰匙產生器更以一先分享鑰匙為基礎來產生該秘鑰。

39. 如申請專利範圍第35項的第二節點，其中該第二節點週期性地產生該未由他人分享聯合隨機位元以產生一新秘鑰。

40. 如申請專利範圍第35項的第二節點，其中該秘鑰為一成對主鑰匙。

41. 如申請專利範圍第35項的第二節點，其中該第一節