



(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 I703850 B

(45)公告日：中華民國 109 (2020) 年 09 月 01 日

(21)申請案號：105108848

(22)申請日：中華民國 105 (2016) 年 03 月 22 日

(51)Int. Cl. : *H04L9/14 (2006.01)**H04W12/04 (2009.01)**H04L5/00 (2006.01)*

(30)優先權：2015/04/10 美國

62/146,170

2016/03/21 美國

15/076,087

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：伊史考特愛德利恩愛德華 ESCOTT, ADRIAN EDWARD (GB)；汎德汶麥可拉
VANDERVEEN, MICHAELA (US)

(74)代理人：李世章

(56)參考文獻：

GB 2499247A

WO 2014/114711A1

WO 2014/208032A1

WO 2014/208034A1

審查人員：黃偉倫

申請專利範圍項數：56 項 圖式數：20 共 91 頁

(54)名稱

用於保護用於受限探索的所構造鄰近度服務代碼的安全的方法和裝置

(57)摘要

提供了用於無線通訊的方法、裝置和電腦程式產品。該裝置可以是 UE。UE 接收探索代碼以及與探索代碼相關聯的金鑰資訊。探索訊息可以基於探索代碼來產生。UE 使用金鑰資訊來轉變探索訊息。UE 隨後廣播經轉變的探索訊息。在第二配置中，UE 接收第一探索代碼、與第一探索代碼相關聯的金鑰資訊、以及包含第二探索代碼的探索訊息。UE 使用金鑰資訊對探索訊息解擾以獲取第二探索代碼。將第一探索代碼與第二探索代碼進行比較。若第一和第二探索代碼匹配，則 UE 可使用金鑰資訊檢查探索訊息的完整性及/或從探索訊息中移除機密性。

A method, an apparatus, and a computer program product for wireless communication are provided. The apparatus may be a UE. The UE receives a discovery code and key information associated with the discovery code. A discovery message may be generated based on the discovery code. The UE transforms the discovery message using the key information. The UE then broadcasts the transformed discovery message. In a second configuration, the UE receives a first discovery code, key information associated with the first discovery code, and a discovery message containing a second discovery code. The UE unscrambles the discovery message using the key information to obtain the second discovery code. The first discovery code and the second discovery code are compared. If the first and second discovery codes match, the UE may check the integrity of the discovery message and/or remove confidentiality of the discovery message using the key information.

指定代表圖：

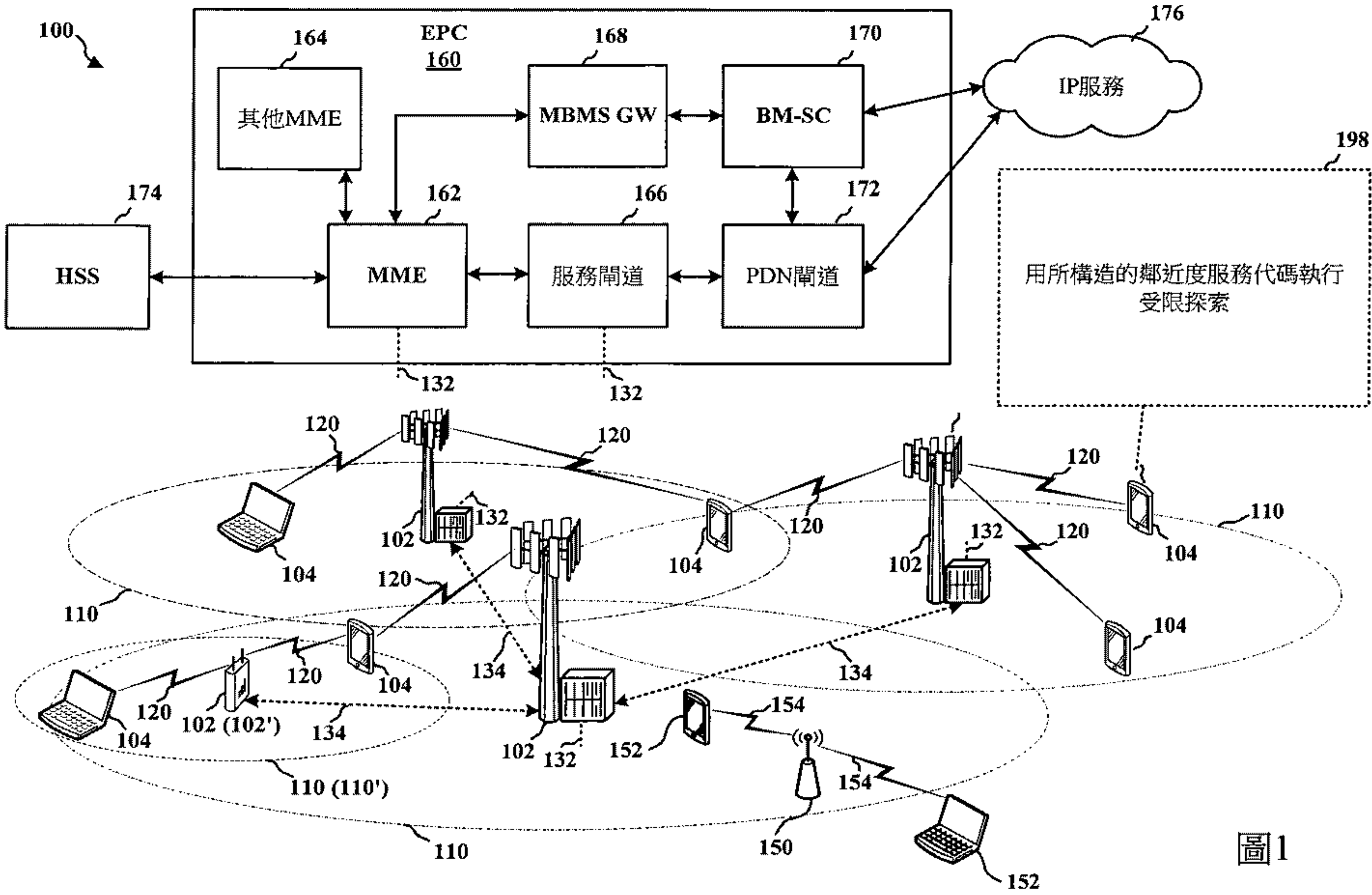


圖1

符號簡單說明：

- 100 . . . 無線通訊系統和存取網路
- 102 . . . 基地台
- 102' . . . 小型細胞服務區
- 104 . . . UE
- 110 . . . 地理覆蓋區域
- 110' . . . 覆蓋區域
- 120 . . . 通訊鏈路
- 132 . . . 回載鏈路
- 134 . . . 回載鏈路
- 150 . . . Wi-Fi 存取點(AP)
- 152 . . . Wi-Fi(STA)
- 154 . . . 通訊鏈路
- 160 . . . EPC
- 162 . . . 行動性管理實體(MME)
- 164 . . . 其他 MME
- 166 . . . 服務閘道
- 168 . . . 多媒體廣播多播服務(MBMS)閘道
- 170 . . . 廣播多播服務中心(BM-SC)
- 172 . . . 封包資料網路(PDN)閘道
- 174 . . . 歸屬用戶伺服器(HSS)
- 176 . . . IP 服務
- 198 . . . 操作

I703850

【發明摘要】

【中文發明名稱】用於保護用於受限探索的所構造鄰近度服務代碼的安全的方法和裝置

【英文發明名稱】METHOD AND APPARATUS FOR SECURING
STRUCTURED PROXIMITY SERVICE CODES FOR RESTRICTED
DISCOVERY

【中文】

提供了用於無線通訊的方法、裝置和電腦程式產品。該裝置可以是UE。UE接收探索代碼以及與探索代碼相關聯的金鑰資訊。探索訊息可以基於探索代碼來產生。UE使用金鑰資訊來轉變探索訊息。UE隨後廣播經轉變的探索訊息。在第二配置中，UE接收第一探索代碼、與第一探索代碼相關聯的金鑰資訊、以及包含第二探索代碼的探索訊息。UE使用金鑰資訊對探索訊息解擾以獲取第二探索代碼。將第一探索代碼與第二探索代碼進行比較。若第一和第二探索代碼匹配，則UE可使用金鑰資訊檢查探索訊息的完整性及/或從探索訊息中移除機密性。

【英文】

A method, an apparatus, and a computer program product for wireless communication are provided. The apparatus may be a UE. The UE receives a discovery code and key information associated with the discovery code. A discovery message may be generated based on the discovery code. The UE transforms the discovery message using the key information. The UE then broadcasts the transformed discovery message. In a second configuration, the UE

receives a first discovery code, key information associated with the first discovery code, and a discovery message containing a second discovery code. The UE unscrambles the discovery message using the key information to obtain the second discovery code. The first discovery code and the second discovery code are compared. If the first and second discovery codes match, the UE may check the integrity of the discovery message and/or remove confidentiality of the discovery message using the key information.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

1 0 0 無線通訊系統和存取網路

1 0 2 基地台

1 0 2' 小型細胞服務區

1 0 4 U E

1 1 0 地理覆蓋區域

1 1 0' 覆蓋區域

1 2 0 通訊鏈路

1 3 2 回載鏈路

1 3 4 回載鏈路

1 5 0 W i - F i 存取點（ A P ）

1 5 2 W i - F i （ S T A ）

1 5 4 通訊鏈路

1 6 0 E P C

1 6 2 行動性管理實體（ M M E ）

1 6 4 其他 M M E

1 6 6 服 務 閘 道

1 6 8 多 媒 體 廣 播 多 播 服 務 (M B M S) 閘 道

1 7 0 廣 播 多 播 服 務 中 心 (B M - S C)

1 7 2 封 包 資 料 網 路 (P D N) 閘 道

1 7 4 歸 屬 用 戶 伺 服 器 (H S S)

1 7 6 I P 服 務

1 9 8 操 作

【特徵化學式】

無

【發明說明書】

【中文發明名稱】用於保護用於受限探索的所構造鄰近度服務代碼的安全的方法和裝置

【英文發明名稱】METHOD AND APPARATUS FOR SECURING
STRUCTURED PROXIMITY SERVICE CODES FOR RESTRICTED
DISCOVERY

【相關申請的交叉引用】

【0001】 本專利申請案請求於2015年4月10日提出申請的題為「METHODS FOR SECURING STRUCTURED SERVICE CODES FOR RESTRICTED DISCOVERY（用於保護用於受限探索的所構造鄰近度服務代碼的安全的方法和裝置）」的美國臨時申請案第62/146,170號的權益，其經由援引全部明確納入於此。

【技術領域】

【0002】 本案大體係關於通訊系統，特定言之係關於設備探索。

【先前技術】

【0003】 無線通訊系統被廣泛部署以提供諸如電話、視訊、資料、訊息收發和廣播等各種電信服務。典型的無線通訊系統可採用能夠藉由共享可用的系統資源來支援與多使用者通訊的多工存取技術。這類多工存取技術的實例包括分碼多工存取（CDMA）系統、分時多工存取（TDMA）系統、分頻多工存取（FDMA）系統、正

交分頻多工存取（OFDMA）系統、單載波分頻多工存取（SC-FDMA）系統和分時同步分碼多工存取（TD-SCDMA）系統。

【0004】該等多工存取技術已在各種電信標準中被採納以提供使不同的無線設備能夠在城市、國家、地區、以及甚至全球級別上進行通訊的共同協定。示例電信標準是長期進化（LTE）。LTE是由第三代夥伴項目（3GPP）頒佈的通用行動電信系統（UMTS）行動服務標準的增強集。LTE被設計成經由改善頻譜效率、降低成本、改善服務、在下行鏈路上使用OFDMA、在上行鏈路上使用SC-FDMA、以及使用多輸入多輸出（MIMO）天線技術來支援行動寬頻存取。然而，隨著對行動寬頻存取的需求持續增長，存在對LTE技術中的進一步改進的需要。該等改進亦可適用於其他多工存取技術以及採用該等技術的電信標準。

【發明內容】

【0005】以下提供一或多個態樣的簡要概述以提供對該等態樣的基本理解。此概述不是所有構想到的態樣的詳盡綜覽，並且既非意欲標識出所有態樣的關鍵性或決定性要素亦非試圖界定任何或所有態樣的範圍。其唯一的目的是要以簡化形式提供一或多個態樣的一些概念以作為稍後提供的更加詳細的描述之序。

【0006】在本案的一態樣中，提供了一種方法、電腦程式產品和裝置。該裝置可以是宣告方使用者裝備（UE

）。UE 接收探索代碼。UE 基於探索代碼產生探索訊息。UE 亦接收與探索代碼相關聯的金鑰資訊。UE 使用金鑰資訊來轉變探索訊息。UE 隨後廣播經轉變的探索訊息。

【0007】 在本案的另一態樣中，提供了一種方法、電腦程式產品和裝置。該裝置可以是監視方UE。UE 接收第一探索代碼。UE 接收包含第二探索代碼的探索訊息。UE 接收與第一探索代碼相關聯的金鑰資訊。UE 使用金鑰資訊對探索訊息解擾以獲取第二探索代碼。UE 將第一探索代碼與第二探索代碼進行比較。

【0008】 為能達成前述及相關目的，該一或多個態樣包括在下文中充分描述並在所附請求項中特別指出的特徵。以下描述和附圖詳細闡述了該一或多個態樣的某些說明性特徵。但是，該等特徵僅僅是指示了可採用各種態樣的原理的各種方式中的若干種，並且本描述意欲涵蓋所有此類態樣及其等效方案。

【圖式簡單說明】

【0009】 圖1是圖示無線通訊系統和存取網路的示例的示圖。

【0010】 圖2A、2B、2C和2D是分別圖示DL訊框結構、DL訊框結構內的DL通道、UL訊框結構以及UL訊框結構內的UL通道的LTE示例的示圖。

【0011】 圖3是圖示存取網路中的進化型B節點(eNB)和使用者裝備(UE)的示例的示圖。

【0012】圖4是設備到設備通訊系統的示圖。

【0013】圖5是圖示探索訊息的結構的示例示圖。

【0014】圖6是圖示探索訊息的變換的示例示圖。

【0015】圖7是圖示由UE對探索訊息的加擾/解擾的示例示圖。

【0016】圖8是圖示由UE提供/移除與探索訊息相關的機密性的示例示圖。

【0017】圖9是圖示由UE計算用於探索訊息的MIC的示例示圖。

【0018】圖10是無線通訊方法的流程圖。

【0019】圖11是無線通訊方法的流程圖。

【0020】圖12是無線通訊方法的流程圖。

【0021】圖13是無線通訊方法的流程圖。

【0022】圖14是無線通訊方法的流程圖。

【0023】圖15是圖示示例性裝置中的不同模組/構件/元件之間的資料流的概念性資料流圖。

【0024】圖16是圖示採用處理系統的裝置的硬體實現的示例的示圖。

【0025】圖17是無線通訊方法的流程圖。

【0026】圖18是無線通訊方法的流程圖。

【0027】圖19是圖示示例性裝置中的不同模組/構件/元件之間的資料流的概念性資料流圖。

【0028】圖20是圖示採用處理系統的裝置的硬體實現的示例的示圖。

【實施方式】

【0029】 以下結合附圖闡述的詳細描述意欲作為各種配置的描述，而無意表示可實踐本文所描述的概念的僅有配置。本詳細描述包括具體細節以提供對各種概念的透徹理解。然而，對於本領域技藝人士將顯而易見的是，沒有該等具體細節亦可實踐該等概念。在一些情況中，以方塊圖形式示出眾所周知的結構和元件以便避免淡化此類概念。

【0030】 現在將參照各種裝置和方法提供電信系統的若干態樣。該等裝置和方法將在以下詳細描述中進行描述並在附圖中由各種方塊、元件、電路、程序、演算法等（統稱為「元素」）來圖示。該等元素可使用電子硬體、電腦軟體或其任何組合來實現。此類元素是實現成硬體還是軟體取決於具體應用和加諸於整體系統上的設計約束。

【0031】 作為實例，元素，或元素的任何部分，或者元素的任何組合可被實現為包括一或多個處理器的「處理系統」。處理器的實例包括：微處理器、微控制器、圖形處理單元（GPU）、中央處理單元（CPU）、應用處理器、數位訊號處理器（DSP）、精簡指令集計算（RISC）處理器、片上系統（SoC）、基頻處理器、現場可程式化閘陣列（FPGA）、可程式化邏輯裝置（PLD）、狀態機、閘控邏輯、個別的硬體電路以及其他配置成執行本文中通篇描述的各種功能的合適硬體。處理系

統中的一或多個處理器可以執行軟體。軟體應當被寬泛地解釋成意為指令、指令集、代碼、代碼片段、程式碼、程式、副程式、軟體元件、應用、軟體應用、套裝軟體、常式、子常式、物件、可執行件、執行的執行緒、規程、函數等，無論其是用軟體、韌體、仲介軟體、微代碼、硬體描述語言、還是其他術語來述及皆是如此。

【0032】相應地，在一或多個示例實施例中，所描述的功能可以在硬體、軟體，或其任何組合中實現。若在軟體中實現，則各功能可作為一或多數指令或代碼儲存或編碼在電腦可讀取媒體上。電腦可讀取媒體包括電腦儲存媒體。儲存媒體可以是能被電腦存取的任何可用媒體。作為示例而非限定，此類電腦可讀取媒體可包括隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電子可抹除可程式化ROM（EEPROM）、光碟儲存、磁碟儲存、其他磁存放裝置，或上述類型的電腦可讀取媒體的組合，或可被用來儲存指令或資料結構形式的電腦可執行代碼且能被電腦存取的任何其他媒體。

【0033】圖1是圖示無線通訊系統和存取網路100的示例的示圖。無線通訊系統（亦稱為無線廣域網路（WWAN））包括基地台102、UE 104、以及進化型封包核心（EPC）160。基地台102可包括巨集細胞服務區（高功率蜂巢基地台）及/或小型細胞服務區（低功率蜂巢基地台）。巨集細胞服務區包括eNB。小型細胞服

務區包括毫微微細胞服務區、微微細胞服務區和微細胞服務區。

【0034】 基地台102（統稱為進化型通用行動電信系統（UMTS）地面無線電存取網路（E-UTRAN））經由回載鏈路132（例如，S1介面）與EPC 160對接。除了其他功能，基地台102可執行以下功能中的一者或多者：使用者資料的傳遞、無線電通道加密和解密、完整性保護、標頭壓縮、行動性控制功能（例如，交遞、雙連通性）、細胞服務區間干擾協調、連接建立和釋放、負載平衡、非存取階層（NAS）訊息的分發、NAS節點選擇、同步、無線電存取網路（RAN）共享、多媒體廣播多播服務（MBMS）、用戶和裝備追蹤、RAN資訊管理（RIM）、傳呼、定位、以及警告訊息的遞送。基地台102可在回載鏈路134（例如，X2介面）上彼此直接或間接（例如，經由EPC 160）通訊。回載鏈路134可以是有線或無線的。

【0035】 基地台102可與UE 104無線通訊。每個基地台102可為各自相應的地理覆蓋區域110提供通訊覆蓋。可能存在交疊的地理覆蓋區域110。例如，小型細胞服務區102'可具有與一或多個巨集基地台102的覆蓋區域110交疊的覆蓋區域110'。包括小型細胞服務區和巨集細胞服務區的網路可被稱為異質網路。異質網路亦可包括歸屬進化型B節點（eNB）（HeNB），該HeNB可向被稱為封閉用戶群（CSG）的受限群提供服務。基

地台 102 與 UE 104 之間的通訊鏈路 120 可包括從 UE 104 到基地台 102 的上行鏈路 (UL) (亦稱為反向鏈路) 傳輸及 / 或從基地台 102 到 UE 104 的下行鏈路 (DL) (亦稱為前向鏈路) 傳輸。通訊鏈路 120 可使用 MIMO 天線技術，包括空間多工、波束成形，及 / 或發射分集。該等通訊鏈路可經由一或多個載波。對於在每個方向上用於傳輸的總共最多達 $Y \times \text{MHz}$ (x 個分量載波) 的載波聚集中分配的每個載波，基地台 102 / UE 104 可使用最多達 $Y \text{ MHz}$ (例如，5、10、15、20 MHz) 頻寬的頻譜。該等載波可以或者可以不彼此毗鄰。載波的分配可以關於 DL 和 UL 是非對稱的 (例如，與 UL 相比可將更多或更少載波分配給 DL)。分量載波可包括主分量載波和一或多個副分量載波。主分量載波可被稱為主細胞服務區 (PCell)，並且副分量載波可被稱為副細胞服務區 (SCell)。

【0036】無線通訊系統可進一步包括在 5 GHz 未授權頻譜中經由通訊鏈路 154 與 Wi-Fi (STA) 152 處於通訊的 Wi-Fi 存取點 (AP) 150。當在未授權頻譜中通訊時，STA 152 / AP 150 可在通訊之前執行暢通通道評估 (CCA) 以決定該通道是否可用。

【0037】小型細胞服務區 102' 可在經授權及 / 或未授權頻譜中操作。當在未授權頻譜中操作時，小型細胞服務區 102' 可採用 LTE 並且使用與由 Wi-Fi AP 150 使用的頻譜相同的 5 GHz 未授權頻譜。在未授權頻譜中採

用LTE的小型細胞服務區102'可推升存取網路的覆蓋及/或增加存取網路的容量。未授權頻譜中的LTE可被稱為LTE未授權（LTE-U）、經授權輔助式存取（LAA），或MuLTEfire。

【0038】 EPC 160可包括行動性管理實體（MME）162、其他MME 164、服務閘道166、多媒體廣播多播服務（MBMS）閘道168、廣播多播服務中心（BM-SC）170、以及封包資料網路（PDN）閘道172。MME 162可以與歸屬用戶伺服器（HSS）174處於通訊。MME 162是處理UE 104與EPC 160之間的訊號傳遞的控制節點。一般而言，MME 162提供承載和連接管理。所有使用者網際網路協定（IP）封包經由服務閘道166來傳遞，服務閘道166自身連接到PDN閘道172。PDN閘道172提供UE IP位址分配以及其他功能。PDN閘道172和BM-SC 170連接到IP服務176。IP服務176可包括網際網路、網內網路、IP多媒體子系統（IMS）、PS流送服務（PSS），及/或其他IP服務。BM-SC 170可提供用於MBMS使用者服務置備和遞送的功能。BM-SC 170可用作內容提供者MBMS傳輸的進入點、可用來授權和發起公用陸上行動網路（PLMN）內的MBMS承載服務、並且可用來排程MBMS傳輸。MBMS閘道168可用來向屬於廣播特定服務的多播廣播單頻網路（MBSFN）區域的基地台102分發MBMS話務，並

且可負責通信期管理（開始/停止）並負責收集eMBMS相關的收費資訊。

【0039】 基地台亦可被稱為B節點、進化型B節點（eNB）、存取點、基地收發機站、無線電基地台、無線電收發機、收發機功能、基本服務集（BSS）、擴展服務集（ESS），或其他某個合適的術語。基地台102可以為UE 104提供去往EPC 160的存取點。UE 104的實例包括蜂巢式電話、智慧型電話、通信期啟動協定（SIP）電話、膝上型設備、個人數位助理（PDA）、衛星無線電、全球定位系統、多媒體設備、視訊設備、數位音訊播放機（例如，MP3播放機）、相機、遊戲控制台、平板設備、智慧設備、可穿戴設備，或任何其他類似的功能設備。UE 104亦可被稱為站、行動站、用戶站、行動單元、用戶單元、無線單元、遠端單元、行動設備、無線設備、無線通訊設備、遠端設備、行動用戶站、存取終端、行動終端、無線終端、遠端終端機、手持機、使用者代理、行動服務客戶端、客戶端，或其他某個合適的術語。

【0040】 再次參照圖1，在某些態樣中，UE 104可被配置成使用所構造的鄰近度服務代碼來執行（198）受限探索。198處執行的操作的詳情在以下參照圖4-20描述。

【0041】 圖2A是圖示LTE中的DL訊框結構的示例的示圖200。圖2B是圖示LTE中的DL訊框結構內的通道

的示例的示圖 230。圖 2C 是圖示 LTE 中的 UL 訊框結構的示例的示圖 250。圖 2D 是圖示 LTE 中的 UL 訊框結構內的通道的示例的示圖 280。其他無線通訊技術可具有不同的訊框結構及 / 或不同的通道。在 LTE 中，訊框 (10 ms) 可被劃分成 10 個相等大小的子訊框。每個子訊框可包括兩個連貫的時槽。資源網格可被用於表示這兩個時槽，每個時槽包括一或多個時間併發的資源區塊 (RB) (亦稱為實體 RB (PRB))。該資源網格被劃分成多個資源元素 (RE)。在 LTE 中，對於正常循環字首而言，RB 包含頻域中的 12 個連貫次載波以及時域中的 7 個連貫符號 (對於 DL 為 OFDM 符號；對於 UL 為 SC-FDMA 符號)，總共 84 個 RE。對於擴展循環字首而言，RB 包含頻域中的 12 個連貫次載波以及時域中的 6 個連貫符號，總共 72 個 RE。由每個 RE 攜帶的位元數可取決於調制方案。

【0042】 如圖 2A 中圖示的，一些 RE 攜帶用於 UE 處的通道估計的 DL 參考 (引導頻) 信號 (DL-RS)。DL-RS 可以包括因細胞服務區而異的參考信號 (CRS) (有時亦稱為共用 RS)、因 UE 而異的參考信號 (UE-RS)、以及通道狀態資訊參考信號 (CSI-RS)。圖 2A 圖示了用於天線埠 0、1、2 和 3 的 CRS (分別指示為 R_0 、 R_1 、 R_2 和 R_3)、用於天線埠 5 的 UE-RS (指示為 R_5)、以及用於天線埠 15 的 CSI-RS (指示為 R)。圖 2B 圖示了訊框的 DL 子訊框內的各種通道的實例。實體控制格式指

示符通道（PCFICH）在時槽0的符號0內，並且攜帶指示實體下行鏈路控制通道（PDCCH）佔據1個、2個、還是3個符號（圖2B圖示了佔據3個符號的PDCCH）的控制格式指示符（CFI）。PDCCH在一或多個控制通道元素（CCE）內攜帶下行鏈路控制資訊（DCI），每個CCE包括9個RE群（REG），每個REG包括OFDM符號中的4個連貫RE。UE可用因UE而異的亦攜帶DCI的增強型PDCCH（ePDCCH）來配置。ePDCCH可具有2個、4個，或8個RB對（圖2B圖示2個RB對，每個子集包括1個RB對）。實體混合自動重複請求（ARQ）（HARQ）指示符通道（PHICH）亦在時槽0的符號0內，並且攜帶基於實體上行鏈路共享通道（PUSCH）來指示HARQ確收（ACK）/否定ACK（NACK）回饋的HARQ指示符（HI）。主同步通道（PSSCH）在訊框的子訊框0和5內的時槽0的符號6內，並且攜帶由UE用於決定子訊框時序和實體層身份的主要同步信號（PSS）。副同步通道（SSCH）在訊框的子訊框0和5內的時槽0的符號5內，並且攜帶由UE用於決定實體層細胞服務區身份群號的副同步信號（SSS）。基於實體層身份和實體層細胞服務區身份群號，UE可決定實體細胞服務區識別符（PCI）。基於PCI，UE可決定上述DL-RS的位置。實體廣播通道（PBCH）在訊框的子訊框0的時槽1的符號0、1、2、3內，並且攜帶主區塊（MIB）。MIB提供DL系統頻寬中的RB的數目、PHICH配置、

以及系統訊框號（SFN）。實體下行鏈路共享通道（PDSCH）攜帶使用者資料、不經由PBCH傳送的廣播系統資訊（諸如系統區塊（SIB））、以及傳呼訊息。

【0043】如圖2C中圖示的，一些RE攜帶用於eNB處的通道估計的解調參考信號（DM-RS）。UE可在訊框的最後一個符號中附加地傳送探通參考信號（SRS）。SRS可具有梳狀結構，並且UE可在梳齒（comb）之一上傳送SRS。SRS可由eNB用於通道品質估計以在UL上啟用取決於頻率的排程。圖2D圖示了訊框的UL子訊框內的各種通道的實例。實體隨機存取通道（PRACH）可基於PRACH配置在訊框的一或多個子訊框內。PRACH可包括子訊框內的6個連貫RB對。PRACH允許UE執行初始系統存取並且達成UL同步。實體上行鏈路控制通道（PUCCH）可位於UL系統頻寬的邊緣。PUCCH攜帶上行鏈路控制資訊（UCI），諸如排程請求、通道品質指示符（CQI）、預編碼矩陣指示符（PMI）、秩指示符（RI）、以及HARQ ACK/NACK回饋。PUSCH攜帶資料，並且可附加地用於攜帶緩衝器狀態報告（BSR）、功率餘裕報告（PHR），及/或UCI。

【0044】圖3是存取網路中與UE 350處於通訊的eNB 310的方塊圖。在DL中，來自EPC 160的IP封包可被提供給控制器/處理器375。控制器/處理器375實現層3和層2功能。層3包括無線電資源控制（RRC）層

，並且層2包括封包資料彙聚協定（PDCP）層、無線電鏈路控制（RLC）層、以及媒體存取控制（MAC）層。控制器/處理器375提供與系統資訊（例如，MIB、SIB）的廣播、RRC連接控制（例如，RRC連接傳呼、RRC連接建立、RRC連接修改、以及RRC連接釋放）、無線電存取技術（RAT）間行動性、以及UE量測報告的量測配置相關聯的RRC層功能；與標頭壓縮/解壓縮、安全性（加密、解密、完整性保護、完整性驗證）、以及交遞支援功能相關聯的PDCP層功能；與上層封包資料單元（PDU）的傳遞、經由ARQ的糾錯、級聯、分段、RLC服務資料單元（SDU）的重新組裝、RLC資料PDU的重新分段、以及RLC資料PDU的重新排序相關聯的RLC層功能；及與邏輯通道與傳輸通道之間的映射、將MAC SDU多工到傳輸塊（TB）上、MAC SDU從TB解除多工、排程資訊報告、經由HARQ的糾錯、優先順序處置、以及邏輯通道優先順序區分相關聯的MAC層功能。

【0045】發射（TX）處理器316和接收（RX）處理器370實現與各種信號處理功能相關聯的層1功能。包括實體（PHY）層的層1可包括傳輸通道上的錯誤偵測、傳輸通道的前向糾錯（FEC）編碼/解碼、交錯、速率匹配、映射到實體通道上、實體通道的調制/解調、以及MIMO天線處理。TX處理器316基於各種調制方案（例如，二元移相鍵控（BPSK）、正交移相鍵控（QPSK

）、 M 移相鍵控（ M -PSK）、 M 正交調幅（ M -QAM）來處置至信號群集的映射。經編碼和經調制的符號可隨後被拆分成並行串流。每個串流可隨後被映射到OFDM次載波、在時域及/或頻域中與參考信號（例如，引導頻）多工、並且隨後使用快速傅裡葉逆變換（IFFT）組合到一起以產生攜帶時域OFDM符號串流的實體通道。該OFDM串流被空間預編碼以產生多個空間串流。來自通道估計器374的通道估計可被用來決定編碼和調制方案以及用於空間處理。該通道估計可以從由UE 350傳送的參考信號及/或通道狀況回饋推導出來。每個空間串流隨後可經由分開的發射器318TX被提供給一不同的天線320。每個發射器318TX可用相應空間串流來調制RF載波以供傳輸。

【0046】 在UE 350處，每個接收器354RX經由其各自相應的天線352來接收信號。每個接收器354RX恢復出調制到RF載波上的資訊並將該資訊提供給接收（RX）處理器356。TX處理器368和RX處理器356實現與各種信號處理功能相關聯的層1功能。RX處理器356可對該資訊執行空間處理以恢復出以UE 350為目的地的任何空間串流。若有多個空間串流以UE 350為目的地，則其可由RX處理器356組合成單個OFDM符號串流。RX處理器356隨後使用快速傅裡葉變換（FFT）將該OFDM符號串流從時域轉換到頻域。該頻域信號對該OFDM信號的每個次載波包括單獨的OFDM符號串流

。藉由決定最有可能由 eNB 310 傳送了的信號群集點來恢復和解調每個次載波上的符號、以及參考信號。該等軟判決可以基於由通道估計器 358 計算出的通道估計。該等軟判決隨後被解碼和解交錯以恢復出原始由 eNB 310 在實體通道上傳送的資料和控制信號。該等資料和控制信號隨後被提供給實現層 3 和層 2 功能的控制器/處理器 359。

【0047】 控制器/處理器 359 可以與儲存程式碼和資料的記憶體 360 相關聯。記憶體 360 可稱為電腦可讀取媒體。在 UL 中，控制器/處理器 359 提供傳輸通道與邏輯通道之間的解多工、封包重組、解密、標頭解壓縮以及控制信號處理以恢復出來自 EPC 160 的 IP 封包。控制器/處理器 359 亦負責使用 ACK 及 / 或 NACK 協定進行檢錯以支援 HARQ 操作。

【0048】 類似於結合由 eNB 310 進行的 DL 傳輸所描述的功能，控制器/處理器 359 提供與系統資訊（例如，MIB、SIB）擷取、RRC 連接、以及量測報告相關聯的 RRC 層功能；與標頭壓縮/解壓縮、以及安全性（加密、解密、完整性保護、完整性驗證）相關聯的 PDCP 層功能；與上層 PDU 的傳遞、經由 ARQ 的糾錯、級聯、分段、RLC SDU 的重新組裝、RLC 資料 PDU 的重新分段、以及 RLC 資料 PDU 的重新排序相關聯的 RLC 層功能；及與邏輯通道與傳輸通道之間的映射、將 MAC SDU 多工到 TB 上、從 TB 解多工 MAC SDU、排程資訊報告

、經由HARQ的糾錯、優先順序處置、以及邏輯通道優先順序區分相關聯的MAC層功能。

【0049】 由通道估計器358從由eNB 310傳送的參考信號或者回饋推導出的通道估計可由TX處理器368用來選擇合適的編碼和調制方案並促成空間處理。由TX處理器368產生的空間串流可經由分開的發射器354TX被提供給不同的天線352。每個發射器354TX可用相應空間串流來調制RF載波以供傳輸。

【0050】 在eNB 310處以與結合UE 350處的接收器功能所描述的方式相類似的方式來處理UL傳輸。每個接收器318RX經由其各自相應的天線320來接收信號。每個接收器318RX恢復出調制到RF載波上的資訊並將該資訊提供給RX處理器370。

【0051】 控制器/處理器375可以與儲存程式碼和資料的記憶體376相關聯。記憶體376可稱為電腦可讀取媒體。在UL中，控制器/處理器375提供傳輸通道與邏輯通道之間的解多工、封包重新組裝、解密、標頭解壓縮、控制信號處理以恢復出來自UE 350的IP封包。來自控制器/處理器375的IP封包可被提供給EPC 160。控制器/處理器375亦負責使用ACK及/或NACK協定進行檢錯以支援HARQ操作。

【0052】 圖4是設備到設備（D2D）通訊系統460的示圖。D2D通訊系統460包括複數個UE 464、466、468、470。D2D通訊系統460可與諸如舉例而言

W W A N 之類的蜂巢通訊系統交疊。U E 4 6 4 、4 6 6 、4 6 8 、4 7 0 中的一些可以使用 D L / U L W W A N 頻譜按 D 2 D 通訊方式來一起通訊，一些可與基地台 4 6 2 通訊，而一些可進行這兩種通訊。例如，如圖 4 中所示，U E 4 6 8 、4 7 0 處於 D 2 D 通訊中，且 U E 4 6 4 、4 6 6 處於 D 2 D 通訊中。U E 4 6 4 、4 6 6 亦正與基地台 4 6 2 通訊。D 2 D 通訊可經由一或多個側鏈路通道，諸如實體側鏈路廣播通道（P S B C H）、實體側鏈路探索通道（P S D C H）、實體側鏈路共享通道（P S S C H）、以及實體側鏈路控制通道（P S C C H）。

【0053】 下文中論述的示例性方法和裝置可適用於各種無線 D 2 D 通訊系統中的任一種，諸如舉例而言基於 F l a s h L i n Q 、W i M e d i a 、藍芽、Z i g B e e 或以 I E E E 8 0 2 . 1 1 標準為基礎的 W i - F i 的無線設備到設備通訊系統。為了簡化論述，在 L T E 的上下文內論述了示例性的方法和裝置。然而，本領域一般技藝人士將理解，該等示例性方法和裝置更一般可適用於各種其他無線設備到設備通訊系統。

【0054】 U E 可使用從鄰點 U E 接收到的探索訊息來標識鄰點 U E 以便建立或進行設備到設備通訊。具體而言，鄰近度服務（P r o S e）直接探索訊息可被用於設備到設備無線通訊以探索鄰點 U E。例如，從鄰點 U E 接收到的探索訊息可包括關於該鄰點 U E 的資訊，使得該鄰點 U E 可基於該探索訊息來標識。

【0055】 廣播探索訊息的UE是宣告方UE。監聽由相鄰UE傳送的探索訊息的UE是監視方UE。探索訊息可包含受限探索代碼，受限探索代碼對於已被宣告方UE專門授權的鄰近監視方UE有意義。在一種配置中，受限探索代碼是包含一結構的ProSe代碼。

【0056】 圖5是圖示探索訊息的結構的示例示圖500。在一種配置中，探索訊息560包括ProSe代碼。如所圖示的，探索訊息560具有首碼部分510和後置部分520。在一種配置中，首碼部分510被網路伺服器指派並且後置部分520被UE或ProSe應用控制。該探索訊息結構允許ProSe代碼的部分被保留用於ProSe應用，並且其可允許數個行動服務，例如，群探索、註明日期、廣告等。該探索訊息結構亦允許ProSe碼的部分匹配。出於此目的，受限ProSe應用使用者ID可由應用按分層格式來配置。ProSe功能（亦即，網路伺服器）產生與受限ProSe應用使用者ID的分層格式相對應的ProSe代碼。該等代碼的意圖是允許代碼的某一（一些）部分獨立於該代碼的其他部分來匹配，例如，匹配群識別符（首碼）但不匹配成員識別符（後置）。

【0057】 由於所構造的該等代碼是受限探索代碼，因此其需要被保護以對抗追蹤（被被動或未獲授權UE追蹤）、假冒（被任何其他UE假冒）、以及重放（稍後時間對所宣告的ProSe代碼的重放）。另外，存在對於該等受限代碼的完整性和機密性保護的要求。另外，較佳

ProSe代碼的結構經由應用安全性量測以保護該等代碼的程序來保持。

【0058】 達成對受限探索ProSe代碼的某種追蹤/重放保護的一種簡單解決方案涉及使用基於UTC的計數器的時間散列化。這有效地對所宣告的代碼加擾以使得其看起來逐個探索時槽皆不同。圖6是圖示根據本案的一態樣的探索訊息的變換的示例示圖600。例如，可藉由對探索訊息610編碼以產生安全探索訊息670來使得探索訊息610變得安全。探索訊息610包括首碼部分620和後置部分630。首碼部分620可包括群ID（諸如，層2（L2）群ID）和群金鑰ID（諸如，ProSe群金鑰ID（PGK ID））。後置部分630包括UE自己的ID（例如，L2 ID）、UE自己的層級、UE的鄰點UE的ID（例如，L2 ID）、以及UE的鄰點UE的層級值。

【0059】 UE基於以通用時間座標（UTC）為基礎的計數器650應用單向散列函數640以對首碼部分620中的群ID和群金鑰ID編碼。在一種配置中，基於UTC的計數器650具有與在開放探索中使用的相同的系統時間。首碼部分680藉由基於單向散列函數640和基於UTC的計數器650對群ID和群金鑰ID編碼來產生。來自單向散列函數640的輸出的一部分藉由XOR（異或）運算660與後置部分630相組合以產生受安全保護的探索訊息670的後置部分690。因此，受安全保護的探索訊息670包括受限首碼部分680和本質上開放的後置部分690。

【0060】 接收到包括所宣告的探索訊息670的探索訊息的監視方UE可嘗試首先對首碼部分680解碼。若監視方UE具有與探索訊息610的首碼部分620的群ID和群金鑰ID相同的群ID和群金鑰ID，則監視方UE將能夠對所宣告的探索訊息670的首碼部分680解碼。隨後，監視方UE可對所宣告探索訊息670的後置部分690解碼，例如藉由用後置部分690以及群ID和群金鑰ID的單向散列函數的輸出的一部分執行XOR運算。因此，後置經由與XOR運算660類似的XOR運算來解碼。

【0061】 探索訊息的首碼提前被監視方UE知曉，而探索訊息的後置（其可包含監視方UE未提前知曉的資訊（例如，應用控制的資訊））可僅在首碼被匹配之後被解碼。在一種配置中，為了勾畫要被匹配的位元與應當在匹配之後解碼的彼等位元之間的拆分，網路伺服器向宣告方UE和監視方UE兩者提供ProSe代碼、匹配位元遮罩及/或可設置位元遮罩。首碼可經由匹配位元遮罩，或者匹配位元遮罩加上因使用者而異的獲指派位元來選擇。

【0062】 ProSe代碼的抗重放/追蹤/假冒可藉由向訊息應用時間散列化來達成，如以下描述的。宣告方UE和監視方UE兩者可被提供金鑰資訊（例如，來自網路）以便匯出將要與時間散列聯用的加擾金鑰。在一種配置中，UE所接收到的金鑰資訊可以是不同金鑰的集合。在此類配置中，加擾金鑰可以藉由從該金鑰的集合中選擇對

應金鑰來匯出。在一種配置中，UE所接收到的金鑰資訊可以是主金鑰。在此類配置中，加擾金鑰可以從主金鑰算術地匯出。在一種配置中，主金鑰可以是不同金鑰的級聯。在此類配置中，加擾金鑰可藉由標識主金鑰內的加擾金鑰（例如，藉由對主金鑰應用預配置的位元遮罩）來匯出。

【0063】 在一種配置中，因使用者而異的位元的機密性可藉由對因使用者而異的位元與從由網路伺服器提供的一金鑰匯出的與獲指派的首碼相關聯的金鑰串流執行XOR運算來達成。在一種配置中，該金鑰串流可從網路伺服器提供的金鑰以算術方法匯出。在一種配置中，網路伺服器提供的金鑰可以是不同金鑰的集合，並且金鑰串流可基於從該金鑰的集合中選擇的一或多個金鑰來匯出。在一種配置中，網路伺服器提供的金鑰可以是不同金鑰的級聯，並且金鑰串流可基於在網路伺服器提供的金鑰內所標識的一或多個金鑰來匯出。在僅找到一個UE的探索過濾的情形中，因使用者而異的位元的機密性可藉由上述用於抗重放/追蹤/假冒的時間散列來達成。否則，因使用者而異的位元的機密性可如以下所述地使用專用於機密性的金鑰來達成並且應當對於每個UE皆不同。

【0064】 在一種配置中，整個ProSe代碼的完整性可經由網路伺服器檢查的訊息完整性代碼（MIC）（就像用於開放探索的）或者經由本端檢查的MIC（如本案所

描述的)來達成。在前一情形中，網路伺服器可向宣告方/監視方UE提供探索金鑰。在後一情形中，宣告方UE和監視方UE兩者皆可被提供(例如從網路提供)能夠匯出完整性金鑰的資訊。在一種配置中，UE所接收到的該資訊可以是不同金鑰的集合。在此類配置中，完整性金鑰可以藉由從該金鑰的集合中選擇對應金鑰來匯出。在一種配置中，UE所接收到的該資訊可以是主金鑰。在此類配置中，完整性金鑰可以從主金鑰以算術方法匯出。在一種配置中，主金鑰可以是不同金鑰的級聯。在此類配置中，完整性金鑰可藉由標識主金鑰內的完整性金鑰(例如，藉由對主金鑰應用預配置的位元遮罩)來匯出。

【0065】實現以上所有三個量測的一種解決方案可如下：UE(其發送或接收探索訊息)被提供用於獲指派ProSe代碼(或ProSe代碼首碼)的金鑰資訊(例如，探索使用者主金鑰(DUMK))。從該金鑰信息，UE依須求匯出：探索使用者加擾金鑰(DUSK)以計算時間散列位元序列；探索使用者完整性金鑰(DUIK)，在存在因使用者而異的位元但不期望匹配報告的情況下需要該金鑰；探索使用者機密性金鑰(DUCK)以在存在一個後置的情況下保護該後置。在一種配置中，UE使用不同的金鑰推導函數來從金鑰資訊匯出DUSK、DUIK和DUCK。在一種配置中，該金鑰資訊可以是金鑰的集合或級聯，並且UE可藉由從該金鑰的集合或級聯

中選擇/標識對應金鑰來從該金鑰資訊匯出DUSK、DUICK和DUCK。網路伺服器亦可提供遮罩（皆具有與ProSe代碼相同的長度）以指示若干所需參數。該等遮罩和其他參數的存在可通知UE要應用何種安全性。

【0066】金鑰計算遮罩選擇訊息的哪些位元被用來從接收自網路的金鑰資訊（例如，DUMK）計算DUCK/DUICK。若宣告方UE獲得金鑰計算遮罩並且不存在來自網路伺服器的針對特定ProSe代碼的探索金鑰，則其應使用關聯到該ProSe代碼的DUICK向包含該ProSe代碼的訊息應用完整性。類似地，若監視方UE獲得金鑰計算遮罩並且沒有要進行匹配報告的指示，則其使用與特定探索過濾相關聯的DUICK來檢查針對該特定探索過濾的訊息的完整性。在一種配置中，用於計算探索訊息的DUCK和DUICK的金鑰計算遮罩可以不同。在另一配置中，用於計算探索訊息的DUCK和DUICK的金鑰計算遮罩可以相同。

【0067】經加密位元遮罩選擇哪些位元受DUCK（與DUSK形成對比）保護。這在沒有後置的情況下可被設為全零。在一種配置中，若宣告方UE或監視方UE從網路伺服器獲得金鑰計算遮罩和經加密位元遮罩兩者，則其基於DUCK分別應用或移除機密性。

【0068】經加擾位元遮罩選擇加擾保護（在發送之前或接收之後應用的時間散列）哪些位元。這可被設為全一（亦即，選擇ProSe代碼中的所有位元）。在一種配

置中，若宣告方或監視方UE獲得經加擾位元遮罩，則其可在時間散列化中應用其。

【0069】 匹配位元遮罩選擇收到ProSe代碼中應對其執行匹配的位元。匹配位元遮罩發信號通知假定對代碼的哪一部分（例如，首碼）進行匹配。

【0070】 可設置位元遮罩選擇要被宣告的ProSe代碼中可由應用或UE設置的位元。可設置位元遮罩從後置勾畫首碼，亦即，代碼的信號結構。

【0071】 圖7是圖示根據本案的一態樣的由UE對探索訊息的加擾/解擾的示例示圖700。該方法可由宣告方UE或監視方UE執行。宣告方UE執行該方法以對原始探索訊息加擾。監視方UE執行該方法以對所宣告的探索訊息解擾。

【0072】 如圖7中所圖示的，UE使用金鑰推導函數704從接收自網路的金鑰資訊（例如，DUMK 702）匯出DUSK 706。在一種配置中，DUMK 702可以是金鑰的集合或級聯，並且金鑰推導函數704可被用來從該金鑰的集合或級聯中標識或選擇DUSK 706。UE隨後使用金鑰散列函數710來基於DUSK 706和基於UTC的計數器708獲取時間散列值714。在一種配置中，UE首先對時間散列值714和經加擾位元遮罩712執行邏輯與運算718。UE隨後對邏輯與運算718的輸出和輸入訊息716執行XOR運算720以產生輸出訊息722。在另一配置中，不使用經加擾位元遮罩，並且XOR運算720對

時間散列值 714 和輸入訊息 716 執行以產生輸出訊息 722。

【0073】對於宣告方 UE，輸入訊息 716 是沒有應用任何其他保護情況下的原始探索訊息或者應用了其他保護的原始探索訊息，並且輸出訊息 722 是所宣告探索訊息。對於監視方 UE，輸入訊息 716 是接收到的所宣告探索訊息，並且輸出訊息 722 是恢復出的原始探索訊息或應用了其他保護的原始探索訊息。一旦監視方 UE 具有輸出訊息 722，監視方 UE 就可檢查 ProSe 代碼的匹配。

【0074】圖 8 是圖示根據本案的一態樣的由 UE 提供 / 移除與探索訊息相關的機密性的示例示圖 800。該方法可由宣告方 UE 或監視方 UE 執行。宣告方 UE 執行該方法以向原始探索訊息提供機密性。監視方 UE 執行該方法以從所宣告的探索訊息移除機密性。

【0075】如圖 8 中所圖示的，UE 對金鑰計算遮罩和輸入訊息執行邏輯與運算。UE 隨後使用金鑰推導函數 804 基於接收自網路的金鑰資訊（例如，DUMK）和邏輯與運算的結果匯出 DUCK。在一種配置中，DUMK 可以是金鑰的集合或級聯。UE 使用金鑰散列函數基於 DUCK 和基於 UTC 的計數器來獲取金鑰串流。UE 進一步對金鑰串流和經加密位元遮罩執行邏輯與運算。在一種配置中，經加密位元遮罩可以是金鑰計算遮罩的邏輯補。UE 隨後對邏輯與運算的結果和輸入訊息執行 XOR 運算以產生輸出訊息。

【0076】對於宣告方UE，輸入訊息是原始探索訊息並且輸出訊息是所宣告探索訊息。對於監視方UE，輸入訊息是移除了加擾的收到所宣告探索訊息並且輸出訊息是恢復出的原始探索訊息。

【0077】圖9是圖示根據本案的一態樣的由UE計算用於探索訊息的MIC的示例示圖900。該方法可由宣告方UE或監視方UE執行。宣告方UE執行該方法以產生要被添加到原始探索訊息的MIC。監視方UE執行該方法以產生要與所宣告探索訊息內包含的MIC進行比較以便驗證所宣告探索訊息的MIC。

【0078】如圖9中所圖示的，UE對金鑰計算遮罩和輸入訊息執行邏輯與運算。在一種配置中，金鑰計算遮罩可選擇不被加密的任何事項。金鑰計算遮罩所指示的位置中的位元可被UE設為亂數以使從探索訊息洩露資訊最小化。提前給予宣告方UE和監視方UE金鑰計算遮罩。UE使用金鑰推導函數904基於接收自網路的金鑰資訊（例如，DUMK）和邏輯與運算的結果匯出DUIK。在一種配置中，DUMK可以是金鑰的集合或級聯。UE隨後使用MIC函數基於DUIK、輸入訊息和基於UTC的計數器來產生MIC。

【0079】對於宣告方UE，輸入訊息是原始探索訊息或者應用了機密性的原始探索訊息。宣告方UE處產生的MIC被添加到探索訊息。對於監視方UE，輸入訊息是加擾和機密性均被移除的收到所宣告探索訊息（其為原

始探索訊息），或者僅加擾被移除的收到所宣告探索訊息（其為應用了機密性的原始探索訊息）。監視方UE處產生的MIC將與接收到的所宣告探索訊息內包含的MIC進行比較以驗證所宣告探索訊息的完整性。

【0080】圖10是無線通訊方法的流程圖1000。該方法可由宣告方UE執行。在1002，UE從網路伺服器接收探索代碼以及與探索代碼相關聯的金鑰資訊（例如，DUMK）。在一種配置中，該金鑰資訊可以是金鑰的集合或級聯。在一種配置中，探索代碼是包括首碼部分和後置部分的ProSe代碼，如以上在圖5中描述的。

【0081】在1004，UE基於探索代碼產生探索訊息。在一種配置中，UE從網路伺服器接收可設置位元遮罩。UE將其想要發送的所選位元設定。UE隨後藉由對探索代碼以及所選位元和可設置位元遮罩的邏輯與執行XOR運算來產生探索訊息。

【0082】在1006，UE使用金鑰資訊來轉變探索訊息。在一種配置中，1006處的操作是在以下圖11中描述的操作。最後，在1008，UE廣播/宣告經轉變的探索訊息。

【0083】圖11是無線通訊方法的流程圖1100。該方法可由宣告方UE執行。在一種配置中，該方法執行在以上圖10的1006處描述的操作。在1102，UE使用從網路接收到的金鑰資訊向探索訊息添加因訊息而異的機密性。在一種配置中，1102處的操作可以是以下圖13中

描述的操作。在一種配置中，1102處的操作在沒有因使用者而異的位元的情況下可被省略。

【0084】 在1104，UE使用金鑰資訊來計算用於探索訊息的訊息完整性代碼（MIC）。在一種配置中，1104處的操作可以是以下圖14中描述的操作。在1106，UE向探索訊息添加MIC。在一種配置中，1104和1106處的操作在沒有因使用者而異的位元並且匹配報告未被網路請求的情況下可被省略。在1108，UE使用金鑰資訊對探索訊息加擾。在一種配置中，1108處的操作可以是以下圖12中描述的操作。

【0085】 在一種配置中，1102處的操作在1104處的操作之前執行，並且在1104處MIC基於經由1102處的操作更新的探索訊息來計算。在另一配置中，1104處的操作在1102處的操作之前執行。在一種配置中，1102處的操作可被省略。在另一配置中，1104和1106處的操作可被省略。在又一配置中，1102-1106處的操作可被省略。

【0086】 圖12是無線通訊方法的流程圖1200。該方法可由宣告方UE或監視方UE執行。該方法在由宣告方UE執行時對原始探索訊息加擾。該方法在由監視方UE執行時對所宣告探索訊息解擾。在一種配置中，該方法執行在以上圖11的1108中描述的操作。在一種配置中，該方法執行在以上圖7中描述的操作。

【0087】 在1202，UE從網路伺服器接收經加擾位元遮罩。在1204，UE基於從網路接收到的金鑰資訊來計算DUSK。在1206，UE基於DUSK和探索訊息的時間來計算時間散列值。

【0088】 最後，在1208，UE對探索訊息以及時間散列值和經加擾位元遮罩的邏輯與執行XOR運算來更新探索訊息。在一種配置中，不使用經加擾位元遮罩，並且1208處的XOR運算對時間散列值和探索訊息執行以產生經加擾探索訊息。在一種配置中，1208處的輸入探索訊息是以上圖11的1102或1106處的操作的輸出探索訊息。在一種配置中，1208處的輸入探索訊息是以下圖17的1704處接收的所宣告探索訊息。

【0089】 圖13是無線通訊方法的流程圖1300。該方法可由宣告方UE或監視方UE執行。在一種配置中，該方法執行在以上圖11的1102中描述的操作。在另一配置中，該方法執行將在以下圖17的1716處描述的操作。在一種配置中，該方法執行在以上圖8中描述的操作。在1302，UE從網路伺服器接收金鑰計算遮罩及/或經加密位元遮罩。在一種配置中，經加密位元遮罩和金鑰計算遮罩可以是彼此的邏輯補。在此類配置中，UE可接收經加密位元遮罩和金鑰計算遮罩之一，並且將另一個計算為接收到的那一個的邏輯補。

【0090】 在1306，UE基於接收到的金鑰資訊、添加了MIC的探索訊息和金鑰計算遮罩的邏輯與、以及探索

訊息的時間來計算金鑰串流。在一種配置中，UE可基於接收到的金鑰資訊以及探索訊息和金鑰計算遮罩的邏輯與來匯出DUCK。在一種配置中，1306處的輸入探索訊息可以是以上圖10的1004處的操作的輸出探索訊息。在另一配置中，1306處的輸入探索訊息可以是以上圖11的1106處的操作的輸出探索訊息。在又一配置中，1306處的輸入探索訊息可以是以下圖17的1708或1712處的操作的輸出探索訊息。在一種配置中，DUCK可以基於接收到的金鑰資訊以及添加了MIC的探索訊息和金鑰計算遮罩的邏輯與來匯出。

【0091】最後，在1308，UE對探索訊息以及金鑰串流和經加密位元遮罩的邏輯與執行XOR運算來更新探索訊息。在一種配置中，1308處的輸入探索訊息是以上圖10的1004處的操作的輸出探索訊息。在另一配置中，1308處的輸入探索訊息是以上圖11的1106處的操作的輸出探索訊息。在又一配置中，1308處的輸入探索訊息是以下圖17的1708或1712處的操作的輸出探索訊息。

【0092】圖14是無線通訊方法的流程圖1400。該方法可由宣告方UE執行。在一種配置中，該方法執行在以上圖11的1104中描述的操作。在一種配置中，該方法執行在以上圖9中描述的操作。在1402，UE從網路伺服器接收金鑰計算遮罩或者從接收到的經加密位元遮罩匯出金鑰計算遮罩。

【0093】 在1404，UE基於接收到的金鑰資訊（例如，DUMK）以及探索訊息和金鑰計算遮罩的邏輯與來計算DUICK。在一種配置中，1404處的輸入探索訊息是以上圖10的1004處的操作的輸出探索訊息。在另一配置中，1404處的輸入探索訊息是以上圖11的1102處的操作的輸出探索訊息。在一種配置中，DUICK基於接收到的金鑰資訊以及添加了暫時全零的MIC的探索訊息和金鑰計算遮罩的邏輯與來計算。在1406，UE基於DUICK和探索訊息的時間來計算MIC。

【0094】 圖15是圖示示例性裝置1502中的不同模組/構件/元件之間的資料流的概念性資料流圖1500。該裝置可以是宣告方UE。裝置1502包括傳送元件1510，其向監視方UE 1550或其他監視方UE（未圖示）傳送探索訊息。裝置1502亦包括接收元件1504，其嘗試從UE 1550和其他UE（未圖示）接收設備到設備訊息。接收元件1504亦從網路伺服器接收探索代碼、金鑰資訊（例如，DUMK）以及各種遮罩。

【0095】 裝置1502可包括訊息產生元件1512，其基於接收到的探索代碼產生探索訊息。在一種配置中，訊息產生元件1512可執行以上參照圖10的1004描述的操作。

【0096】 裝置1502可包括機密性元件1514，其使用金鑰資訊向探索訊息添加因訊息而異的機密性。在一種

配置中，機密性元件 1514 可執行以上參照圖 13 或圖 11 的 1102 描述的操作。

【0097】裝置 1502 可包括完整性元件 1516，其使用金鑰資訊向探索訊息添加 MIC。在一種配置中，完整性元件 1516 可執行以上參照圖 14 或圖 11 的 1104、1106 描述的操作。

【0098】裝置 1502 可包括加擾元件 1518，其使用金鑰資訊對探索訊息加擾。在一種配置中，加擾元件 1518 可執行以上參照圖 12 或圖 11 的 1108 描述的操作。

【0099】該裝置可包括執行前述圖 10-14 的流程圖中的演算法的每個框的附加元件。如此，前述圖 10-14 的流程圖之每一框可由一元件執行且該裝置可包括彼等元件中的一或多個元件。各元件可以是專門配置成實施該程序/演算法的一或多個硬體元件、由配置成執行該程序/演算法的處理器實現、儲存在電腦可讀取媒體中以供由處理器實現，或其某個組合。

【0100】圖 16 是圖示採用處理系統 1614 的裝置 1502' 的硬體實現的示例的示圖 1600。處理系統 1614 可實現成具有由匯流排 1624 一般化地表示的匯流排架構。取決於處理系統 1614 的具體應用和整體設計約束，匯流排 1624 可包括任何數目的互連匯流排和橋接器。匯流排 1624 將各種電路連結在一起，包括一或多個處理器及/或硬體元件（由處理器 1604，組件 1504、1510、1512、1514、1516、1518 以及電腦可讀取媒體/記憶

體 1606 表示)。匯流排 1624 亦可連結各種其他電路，諸如時序源、周邊設備、穩壓器和功率管理電路，該等電路在本領域中是眾所周知的，且因此將不再進一步描述。

【0101】處理系統 1614 可耦合至收發機 1610。收發機 1610 被耦合至一或多個天線 1620。收發機 1610 提供用於經由傳輸媒體與各種其他裝置通訊的構件。收發機 1610 從一或多個天線 1620 接收信號，從接收到的信號中提取資訊，並向處理系統 1614（具體而言是接收元件 1504）提供所提取的資訊。另外，收發機 1610 從處理系統 1614（具體而言是傳輸元件 1510）接收資訊，並基於接收到的資訊來產生將應用於一或多個天線 1620 的信號。處理系統 1614 包括耦合到電腦可讀取媒體/記憶體 1606 的處理器 1604。處理器 1604 負責一般性處理，包括執行儲存在電腦可讀取媒體/記憶體 1606 上的軟體。該軟體在由處理器 1604 執行時使處理系統 1614 執行上文針對任何特定裝置描述的各種功能。電腦可讀取媒體/記憶體 1606 亦可被用於儲存由處理器 1604 在執行軟體時操縱的資料。處理系統進一步包括元件 1504、1510、1512、1514、1516 和 1518 中的至少一個元件。該等元件可以是在處理器 1604 中執行的軟體元件、常駐/儲存在電腦可讀取媒體/記憶體 1606 中的軟體元件、耦合至處理器 1604 的一或多個硬體元件，或其某種組合。處理系統 1614 可以是 UE 350 的元件且可包

括記憶體 360 及 / 或包括 TX 處理器 368、RX 處理器 356 和控制器 / 處理器 359 中的至少一者。

【0102】 在一種配置中，用於無線通訊的裝置 1502/1502' 包括：用於接收探索代碼以及與探索代碼相關聯的金鑰資訊的構件，用於基於探索代碼產生探索訊息的構件，用於使用金鑰資訊來轉變探索訊息的構件，以及用於廣播經轉變的探索訊息的構件。

【0103】 在一種配置中，用於轉變探索訊息的構件被配置成使用金鑰資訊來對探索訊息加擾。在一種配置中，為了對探索訊息加擾，用於轉變探索訊息的構件被配置成：基於金鑰資訊匯出探索使用者加擾金鑰；基於探索使用者加擾金鑰和探索訊息的時間來計算時間散列值；及對探索訊息和時間散列值執行 XOR 運算以對探索訊息加擾。在一種配置中，用於轉變探索訊息的構件被進一步配置成：使用金鑰資訊計算用於探索訊息的 MIC；及向探索訊息添加 MIC。

【0104】 在一種配置中，用於轉變探索訊息的構件被進一步配置成使用金鑰資訊向探索訊息添加因訊息而異的機密性。在一種配置中，用於轉變探索訊息的構件被進一步配置成：使用金鑰資訊計算用於探索訊息的 MIC；及向探索訊息添加 MIC。

【0105】 在一種配置中，為了添加因訊息而異的機密性，用於轉變探索訊息的構件被進一步配置成：接收經加密位元遮罩；及將金鑰計算遮罩計算為經加密位元遮

罩的邏輯補。在一種配置中，為了添加因訊息而異的機密性，用於轉變探索訊息的構件被進一步配置成：基於金鑰資訊、添加了MIC的探索訊息和金鑰計算遮罩的邏輯與、以及探索訊息的時間來計算金鑰串流；及對探索訊息以及金鑰串流和經加密位元遮罩的邏輯與執行XOR運算來更新探索訊息。在一種配置中，為了計算MIC，用於轉變探索訊息的構件被進一步配置成：基於金鑰資訊計算探索使用者完整性金鑰；及基於探索使用者完整性金鑰和探索訊息的時間來計算MIC。

【0106】 前述構件可以是裝置1502的前述元件及/或裝置1502'的處理系統1614中被配置成執行由前述構件敘述的功能的一或多個元件。如前述，處理系統1614可包括TX處理器368、RX處理器356、以及控制器/處理器359。如此，在一種配置中，前述構件可以是被配置成執行由前述構件所敘述的功能的TX處理器368、RX處理器356、以及控制器/處理器359。

【0107】 圖17是無線通訊方法的流程圖1700。該方法可由監視方UE來執行。在1702，UE接收第一探索代碼以及與第一探索代碼相關聯的金鑰資訊。在1704，UE接收包含第二探索代碼的探索訊息。在一種配置中，該探索訊息接收自宣告方UE。在一種配置中，第一和第二探索代碼是ProSe代碼，其每一個包括首碼部分和後置部分，如以上在圖5中描述的。

【0108】 在1706，UE使用金鑰資訊對探索訊息解擾以獲取第二探索代碼。在一種配置中，1706處的操作的詳情在以上圖12中描述。

【0109】 在1708，UE將第一探索代碼與第二探索代碼進行比較。在1710，UE決定第一和第二探索代碼是否匹配。若兩個探索代碼不匹配，則該方法結束。然而，若兩個探索代碼匹配，則該方法行進至1712。

【0110】 在1712，UE使用接收到的金鑰資訊檢查探索訊息的MIC。在一種配置中，1712處的操作的詳情在以下圖18中進一步描述。在步驟1714，UE決定探索訊息的完整性是否被損害。若完整性被損害，該方法結束。若完整性是完整的，則該方法行進至框1716。

【0111】 在1716，UE使用接收到的金鑰資訊從探索訊息中移除因訊息而異的機密性。在一種配置中，1716處的操作的詳情在以上圖13中描述。

【0112】 在一種配置中，1712處的操作在1716處的操作之前執行。在另一配置中，1716處的操作在1712處的操作之前執行。在一種配置中，1712和1716處的操作的次序是探索訊息被宣告方UE產生時機密性和完整性被添加的相反次序。在一種配置中，可省略1712和1714處的操作。在另一配置中，可省略1716處的操作。在又一配置中，可省略1712-1716處的操作。

【0113】 圖18是無線通訊方法的流程圖1800。該方法可由監視方UE來執行。在一種配置中，該方法執行在

以上圖 17 的 1712 中描述的操作。在一種配置中，該方法執行在以上圖 9 中描述的操作。在 1802，UE 從網路伺服器接收金鑰計算遮罩或者從接收自網路伺服器的經加密位元遮罩匯出金鑰計算遮罩。

【0114】 在 1804，UE 基於金鑰資訊來計算 DUIK。在一種配置中，1804 處的輸入探索訊息是以上圖 17 的 1708 處的操作的輸出探索訊息。在另一配置中，1804 處的輸入探索訊息是以上圖 17 的 1716 處的操作的輸出探索訊息。在一種配置中，DUIK 基於金鑰資訊以及探索訊息和金鑰計算遮罩的邏輯與來計算。在一種配置中，DUIK 基於金鑰資訊以及添加了暫時全零的 MIC 的探索訊息和金鑰計算遮罩的邏輯與來計算。

【0115】 在 1806，UE 基於 DUIK 和探索訊息的時間來計算新的 MIC。在 1808，UE 將探索訊息內包含的 MIC 與新 MIC 進行比較。若兩個 MIC 相同，則探索訊息的完整性是完整的。否則，探索訊息的完整性被損害。

【0116】 圖 19 是圖示示例性裝置 1902 中的不同模組 / 構件 / 元件之間的資料流的概念性資料流圖 1900。該裝置可以是監視方 UE。裝置 1902 包括傳送元件 1910，其向 UE 1950 或其他 UE（未圖示）傳送設備到設備訊息。裝置 1902 亦包括接收元件 1904，其從 UE 1950 或其他宣告方 UE（未圖示）接收探索訊息。接收元件 1904 亦從網路伺服器接收第一探索代碼、金鑰資訊以及各種遮罩。

【0117】 裝置1902可包括解擾元件1912，其使用金鑰資訊對探索訊息解擾以獲取第二探索代碼。在一種配置中，解擾元件1912可執行以上參照圖12或圖17的1706描述的操作。

【0118】 裝置1902可包括代碼比較元件1914，其將第一探索代碼與第二探索代碼進行比較。在一種配置中，代碼比較元件1914可執行以上參照圖17的1708描述的操作。

【0119】 裝置1902可包括完整性檢查組件1916，其使用金鑰資訊檢查探索訊息的MIC。在一種配置中，完整性檢查組件1916可執行以上參照圖18或圖17的1712描述的操作。

【0120】 裝置1902可包括機密性移除元件1918，其使用金鑰資訊從探索訊息中移除因訊息而異的機密性。在一種配置中，機密性移除元件1918可執行以上參照圖13或圖17的1716描述的操作。

【0121】 該裝置可包括執行前述圖12-13和17-18的流程圖中的演算法的每個框的附加元件。如此，前述圖12-13和17-18的流程圖之每一框可由一元件執行且該裝置可包括彼等元件中的一或多個元件。各元件可以是專門配置成實施該程序/演算法的一或多個硬體元件、由配置成執行該程序/演算法的處理器實現、儲存在電腦可讀取媒體中以供由處理器實現，或其某個組合。

【0122】圖20是圖示採用處理系統2014的裝置1902'的硬體實現的示例的示圖2000。處理系統2014可實現成具有由匯流排2024一般化地表示的匯流排架構。取決於處理系統2014的具體應用和整體設計約束，匯流排2024可包括任何數目的互連匯流排和橋接器。匯流排2024將各種電路連結在一起，包括一或多個處理器及/或硬體元件（由處理器2004，組件1904、1910、1912、1914、1916、1918以及電腦可讀取媒體/記憶體2006表示）。匯流排2024亦可連結各種其他電路，諸如時序源、周邊設備、穩壓器和功率管理電路，該等電路在本領域中是眾所周知的，且因此將不再進一步描述。

【0123】處理系統2014可耦合至收發機2010。收發機2010被耦合至一或多個天線2020。收發機2010提供用於經由傳輸媒體與各種其他裝置通訊的構件。收發機2010從一或多個天線2020接收信號，從接收到的信號中提取資訊，並向處理系統2014（具體而言是接收元件1904）提供所提取的資訊。另外，收發機2010從處理系統2014（具體而言是傳輸元件1910）接收資訊，並基於接收到的資訊來產生將應用於一或多個天線2020的信號。處理系統2014包括耦合到電腦可讀取媒體/記憶體2006的處理器2004。處理器2004負責一般性處理，包括執行儲存在電腦可讀取媒體/記憶體2006上的軟體。該軟體在由處理器2004執行時使處理系統2014

執行上文針對任何特定裝置描述的各種功能。電腦可讀取媒體/記憶體2006亦可被用於儲存由處理器2004在執行軟體時操縱的資料。處理系統進一步包括元件1904、1910、1912、1914、1916和1918中的至少一個元件。該等元件可以是在處理器2004中執行的軟體元件、常駐/儲存在電腦可讀取媒體/記憶體2006中的軟體元件、耦合至處理器2004的一或多個硬體元件，或其某種組合。處理系統2014可以是UE 350的元件且可包括記憶體360及/或包括TX處理器368、RX處理器356和控制器/處理器359中的至少一者。

【0124】 在一種配置中，用於無線通訊的裝置1902/1902'包括：用於接收第一探索代碼以及與第一探索代碼相關聯的金鑰資訊的構件，用於接收包含第二探索代碼的探索訊息的構件，用於使用金鑰資訊對探索訊息解擾以獲取第二探索代碼的構件，以及用於將第一探索代碼與第二探索代碼進行比較的構件。

【0125】 在一種配置中，用於將第一探索代碼與第二探索代碼進行比較的構件被配置成將第一探索代碼的首碼部分與第二探索代碼的首碼部分進行比較。在一種配置中，用於對探索訊息解擾的構件被配置成：基於金鑰資訊匯出探索使用者加擾金鑰；基於探索使用者加擾金鑰和探索訊息的時間來計算時間散列值；及對探索訊息和時間散列值執行XOR運算以對探索訊息解擾。

【0126】 在一種配置中，裝置1902/1902'進一步包括用於使用金鑰資訊檢查探索訊息的第一MIC的構件。在一種配置中，用於檢查第一MIC的構件被配置成：基於金鑰資訊計算探索使用者完整性金鑰；基於探索使用者完整性金鑰和探索訊息的時間來計算第二MIC；及將第一MIC和第二MIC進行比較。

【0127】 在一種配置中，裝置1902/1902'進一步包括用於使用金鑰資訊從探索訊息中移除因訊息而異的機密性的構件。在一種配置中，用於移除因訊息而異的機密性的構件被配置成：基於金鑰資訊、添加了訊息完整性代碼（MIC）的探索訊息和金鑰計算遮罩的邏輯與、以及探索訊息的時間來計算金鑰串流；及對探索訊息以及金鑰串流和經加密位元遮罩的邏輯與執行XOR運算來恢復探索訊息。在一種配置中，用於移除因訊息而異的機密性的構件被配置成：接收經加密位元遮罩；及將金鑰計算遮罩計算為經加密位元遮罩的邏輯補。

【0128】 前述構件可以是裝置1902的前述元件及/或裝置1902'的處理系統2014中被配置成執行由前述構件敘述的功能的一或多個元件。如前述，處理系統2014可包括TX處理器368、RX處理器356、以及控制器/處理器359。如此，在一種配置中，前述構件可以是被配置成執行由前述裝構件敘述的功能的TX處理器368、RX處理器356、以及控制器/處理器359。

【0129】應理解，所揭示的程序/流程圖中的各個框的具體次序或層次是示例性辦法的圖示。應理解，基於設計偏好，可以重新編排該等程序/流程圖中的各個框的具體次序或層次。此外，一些框可被組合或被略去。所附方法請求項以範例次序呈現各種框的要素，且並不意味著被限定於所呈現的具體次序或層次。

【0130】提供先前描述是為了使本領域任何技藝人士均能夠實踐本文中所描述的各種態樣。對該等態樣的各種改動將容易為本領域技藝人士所明白，並且在本文中所定義的普適原理可被應用於其他態樣。因此，請求項並非意欲被限定於本文中所示出的態樣，而是應被授予與語言上的請求項相一致的全部範圍，其中對要素的單數形式的引述除非特別聲明，否則並非意欲表示「有且僅有一個」，而是「一或多個」。本文使用術語「示例性」意指「用作示例、實例或圖示」。本文中描述為「示例性」的任何態樣不必被解釋成優於或勝過其他態樣。除非特別另外聲明，否則術語「一些」指的是一或多個。諸如「A、B或C中的至少一者」、「A、B或C中的一者或多者」、「A、B和C中的至少一者」、「A、B和C中的一者或多者」以及「A、B、C或其任何組合」之類的組合包括A、B及/或C的任何組合，並且可包括多個A、多個B或者多個C。具體地，諸如「A、B或C中的至少一者」、「A、B或C中的一者或多者」、「A、B和C中的至少一者」、「A、B和C中的一者或多者」、以及

「A、B、C或其任何組合」之類的組合可以是僅A、僅B、僅C、A和B、A和C、B和C，或者A和B和C，其中任何此類組合可包含A、B或C中的一或多個成員。本案通篇描述的各種態樣的要素為本領域一般技藝人士當前或今後所知的所有結構上和功能上的等效方案經由引述被明確納入於此，且意欲被請求項所涵蓋。此外，本文中所揭示的任何內容皆並非意欲貢獻給公眾，無論此種揭示是否在申請專利範圍中被顯式地敘述。措辭「元件」、「機制」、「元件」、「設備」以及諸如此類可以不是措辭「構件」的代替。如此，沒有任何請求項元素應被解釋為手段功能，除非該元素是使用短語「用於……的構件」來明確敘述的。

【符號說明】

【0131】

100 無線通訊系統和存取網路

102 基地台

102' 小型細胞服務區

104 UE

110 地理覆蓋區域

110' 覆蓋區域

120 通訊鏈路

132 回載鏈路

134 回載鏈路

150 Wi-Fi存取點 (AP)

1 5 2 W i - F i (S T A)

1 5 4 通 訊 鏈 路

1 6 0 E P C

1 6 2 行 動 性 管 理 實 體 (M M E)

1 6 4 其 他 M M E

1 6 6 服 務 閘 道

1 6 8 多 媒 體 廣 播 多 播 服 務 (M B M S) 閘 道

1 7 0 廣 播 多 播 服 務 中 心 (B M - S C)

1 7 2 封 包 資 料 網 路 (P D N) 閘 道

1 7 4 歸 屬 用 戶 伺 服 器 (H S S)

1 7 6 I P 服 務

1 9 8 操 作

2 0 0 示 圖

2 3 0 示 圖

2 5 0 示 圖

2 8 0 示 圖

3 1 0 e N B

3 1 6 發 射 (T X) 處 理 器

3 1 8 發 射 器

3 2 0 天 線

3 5 0 U E

3 5 2 天 線

3 5 4 接 收 器

3 5 6 接 收 (R X) 處 理 器

- 3 5 8 通 道 估 計 器
- 3 5 9 控 制 器 / 處 理 器
- 3 6 0 記 憶 體
- 3 6 8 T X 處 理 器
- 3 7 0 R X 處 理 器
- 3 7 4 通 道 估 計 器
- 3 7 5 控 制 器 / 處 理 器
- 3 7 6 記 憶 體
- 4 6 0 設 備 (D 2 D) 通 訊 系 統
- 4 6 2 基 地 台
- 4 6 4 U E
- 4 6 6 U E
- 4 6 8 U E
- 4 7 0 U E
- 5 0 0 示 圖
- 5 6 0 探 索 訊 息
- 6 0 0 示 例 示 圖
- 6 1 0 探 索 訊 息
- 6 2 0 首 碼 部 分
- 6 3 0 後 置 部 分
- 6 4 0 單 向 散 列 函 數
- 6 5 0 計 數 器
- 6 6 0 X O R (異 或) 運 算
- 6 7 0 探 索 訊 息

6 8 0	受 限 首 碼 部 分
6 9 0	後 置 部 分
7 0 0	示 例 示 圖
7 0 2	操 作
7 0 4	金 鑰 推 導 函 數
7 0 6	D U S K
7 0 8	計 數 器
7 1 0	金 鑰 散 列 函 數
7 1 2	經 加 擾 位 元 遮 罩
7 1 4	時 間 散 列 值
7 1 6	輸 入 訊 息
7 1 8	執 行 邏 輯 與 運 算
7 2 0	X O R 運 算
7 2 2	輸 出 訊 息
8 0 0	示 例 示 圖
8 0 4	金 鑰 推 導 函 數
8 1 0	首 碼
8 2 0	後 置
9 0 0	示 例 示 圖
9 0 4	金 鑰 推 導 函 數
1 0 0 0	流 程 圖
1 0 0 2	步 驟
1 0 0 4	步 驟
1 0 0 6	步 驟

1 0 0 8 步 驟

1 1 0 0 流 程 圖

1 1 0 2 步 驟

1 1 0 4 步 驟

1 1 0 6 步 驟

1 1 0 8 步 驟

1 2 0 0 流 程 圖

1 2 0 2 步 驟

1 2 0 4 步 驟

1 2 0 6 步 驟

1 2 0 8 步 驟

1 3 0 0 流 程 圖

1 3 0 2 步 驟

1 3 0 6 步 驟

1 3 0 8 步 驟

1 4 0 0 流 程 圖

1 4 0 2 步 驟

1 4 0 4 步 驟

1 4 0 6 步 驟

1 5 0 0 概 念 性 資 料 流 圖

1 5 0 2 裝 置

1 5 0 2' 裝 置

1 5 0 4 接 收 元 件

1 5 1 0 傳 送 元 件

1 5 1 2 訊 息 產 生 元 件

1 5 1 4 機 密 性 元 件

1 5 1 6 完 整 性 元 件

1 5 1 8 加 擾 元 件

1 5 5 0 監 視 方 U E

1 6 0 0 示 圖

1 6 0 4 處 理 器

1 6 0 6 電 腦 可 讀 取 媒 體 / 記 憶 體

1 6 1 0 收 發 機

1 6 1 4 處 理 系 統

1 6 2 0 天 線

1 6 2 4 匯 流 排

1 7 0 0 流 程 圖

1 7 0 2 步 驟

1 7 0 4 步 驟

1 7 0 6 步 驟

1 7 0 8 步 驟

1 7 1 0 步 驟

1 7 1 2 步 驟

1 7 1 4 步 驟

1 7 1 6 步 驟

1 8 0 0 流 程 圖

1 8 0 2 步 驟

1 8 0 4 步 驟

1 8 0 6 步 驟

1 8 0 8 步 驟

1 9 0 0 概 念 性 資 料 流 圖

1 9 0 2 裝 置

1 9 0 2' 的 裝 置

1 9 0 4 接 收 元 件

1 9 1 0 傳 送 元 件

1 9 1 2 解 擾 元 件

1 9 1 4 代 碼 比 較 元 件

1 9 1 6 完 整 性 檢 查 組 件

1 9 1 8 機 密 性 移 除 元 件

1 9 5 0 U E

2 0 0 0 示 圖

2 0 0 4 處 理 器

2 0 0 6 電 腦 可 讀 取 媒 體 / 記 憶 體

2 0 1 0 收 發 機

2 0 1 4 處 理 系 統

2 0 2 0 天 線

2 0 2 4 匯 流 排

【生物材料寄存】

【 0 1 3 2 】 國內寄存資訊 (請依寄存機構、日期、號碼順序註記)

無

【 0 1 3 3 】 國外寄存資訊 (請依寄存國家、機構、日期、號碼順序註記)

無

.

.

.

.

【序列表】(請換頁單獨記載)

無

.

.

.

.

【發明申請專利範圍】

【第1項】 一種用於一使用者裝備（UE）的無線通訊方法，包括下列步驟：

接收一探索代碼；

基於該探索代碼產生一探索訊息；

接收與該探索代碼相關聯的金鑰資訊；

使用該金鑰資訊來轉變該探索訊息；及

廣播經轉變的探索訊息，

其中轉變該探索訊息的步驟包括使用該金鑰資訊對該探索訊息加擾，對該探索訊息加擾的步驟包含：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息加擾。

【第2項】 如請求項1之方法，其中該探索代碼包括一鄰近度服務（ProSe）代碼。

【第3項】 如請求項2之方法，其中該 ProSe 代碼包括一首碼部分和一後置部分。

【第4項】 如請求項1之方法，其中轉變該探索訊息的步驟進一步包括：

使用該金鑰資訊計算用於該探索訊息的一訊息完

整性代碼（MIC）；及

向該探索訊息添加該 MIC。

【第5項】如請求項1之方法，其中轉變該探索訊息的步驟進一步包括使用該金鑰資訊向該探索訊息添加因訊息而異的機密性。

【第6項】如請求項5之方法，其中轉變該探索訊息的步驟進一步包括：

使用該金鑰資訊計算用於該探索訊息的一訊息完整性代碼（MIC）；及

向該探索訊息添加該 MIC。

【第7項】如請求項5之方法，其中添加該因訊息而異的機密性的步驟包括：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第8項】如請求項5之方法，其中添加該因訊息而異的機密性的步驟包括：

基於該金鑰資訊、添加了該 MIC 的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算一金鑰串流；及

對該探索訊息以及該金鑰串流和一經加密位元遮罩的一邏輯與執行一 XOR 運算來更新該探索訊息。

【第9項】 如請求項 4 之方法，其中計算該 MIC 的步驟包括：

基於該金鑰資訊計算一探索使用者完整性金鑰；及
基於該探索使用者完整性金鑰和該探索訊息的一時間來計算該 MIC。

【第10項】 一種用於一使用者裝備（UE）的無線通訊方法，包括下列步驟：

接收一第一探索代碼；
接收包含一第二探索代碼的一探索訊息；
接收與該第一探索代碼相關聯的金鑰資訊；
使用該金鑰資訊對該探索訊息解擾以獲取一該第二探索代碼，其中解擾該探索訊息的步驟包括：
基於該金鑰資訊匯出一探索使用者加擾金鑰；
基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及
對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息解擾；及
將該第一探索代碼與該第二探索代碼進行比較以得知該第一探索代碼與該第二探索代碼之間是否有一匹配。

【第11項】 如請求項 10 之方法，其中該第一和第二探索代碼中的每一者包括一鄰近度服務（ProSe）代

碼。

【第12項】 如請求項11之方法，其中該ProSe代碼包括一首碼部分和一後置部分。

【第13項】 如請求項12之方法，其中比較該第一探索代碼和該第二探索代碼的步驟包括將該第一探索代碼的該首碼部分與該第二探索代碼的該首碼部分進行比較。

【第14項】 如請求項10之方法，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該方法進一步包括使用該金鑰資訊檢查該探索訊息的一訊息完整性代碼（MIC）。

【第15項】 如請求項14之方法，其中該MIC是第一MIC，並且檢查該第一MIC的步驟包括：

基於該金鑰資訊計算一探索使用者完整性金鑰；

基於該探索使用者完整性金鑰和該探索訊息的一時間來計算一第二MIC；及

將該第一MIC和該第二MIC進行比較。

【第16項】 如請求項10之方法，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該方法進一步包括使用該金鑰資訊從該探索訊息中移除因訊息而異的機密性。

【第17項】 如請求項16之方法，其中移除該因訊息

而異的機密性的步驟包括：

基於該金鑰資訊、添加了一訊息完整性代碼(MIC)的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算一金鑰串流；及

對該探索訊息以及該金鑰串流和經加密位元遮罩的邏輯與執行 XOR 運算來恢復該探索訊息。

【第18項】 如請求項16之方法，其中移除該因訊息而異的機密性的步驟包括：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第19項】 一種用於無線通訊的裝置，包括：

用於接收一探索代碼的構件；

用於基於該探索代碼產生一探索訊息的構件；

用於接收與該探索代碼相關聯的金鑰資訊的構件；

用於使用該金鑰資訊來轉變該探索訊息的構件；及

用於廣播經轉變的探索訊息的構件，

其中該用於轉變該探索訊息的構件被配置成使用該金鑰資訊來對該探索訊息加擾，及其中為了對該探索訊息加擾，該用於轉變該探索訊息的構件被配置成：

基於金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息加擾。

【第20項】 如請求項19之裝置，其中該探索代碼包括一鄰近度服務（ProSe）代碼。

【第21項】 如請求項20之裝置，其中該ProSe代碼包括一首碼部分和一後置部分。

【第22項】 如請求項19之裝置，其中該用於轉變該探索訊息的構件被進一步配置成：

使用該金鑰資訊計算用於該探索訊息的一訊息完整性代碼（MIC）；及

向該探索訊息添加該MIC。

【第23項】 如請求項19之裝置，其中該用於轉變該探索訊息的構件被進一步配置成使用該金鑰資訊向該探索訊息添加因訊息而異的機密性。

【第24項】 如請求項23之裝置，其中該用於轉變該探索訊息的構件被進一步配置成：

使用該金鑰資訊計算用於該探索訊息的一訊息完整性代碼（MIC）；及

向該探索訊息添加該MIC。

【第25項】 如請求項23之裝置，其中為了添加因訊

息而異的機密性，該用於轉變該探索訊息的構件被進一步配置成：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第26項】 如請求項23之裝置，其中為了添加因訊息而異的機密性，該用於轉變該探索訊息的構件被進一步配置成：

基於該金鑰資訊、添加了MIC的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算一金鑰串流；及

對該探索訊息以及該金鑰串流和一經加密位元遮罩的一邏輯與執行一XOR運算來更新該探索訊息。

【第27項】 如請求項22之裝置，其中為了計算該MIC，該用於轉變該探索訊息的構件被進一步配置成：

基於該金鑰資訊計算一探索使用者完整性金鑰；及

基於該探索使用者完整性金鑰和該探索訊息的一時間來計算該MIC。

【第28項】 一種用於無線通訊的裝置，包括：

用於接收一第一探索代碼的構件；

用於接收包含一第二探索代碼的一探索訊息的構

件；

用於接收與該第一探索代碼相關聯的金鑰資訊的構件；

用於使用該金鑰資訊對該探索訊息解擾以獲取該第二探索代碼的構件，其中該用於對該探索訊息解擾的構件被配置成：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息解擾；及

用於將該第一探索代碼與該第二探索代碼進行比較以得知該第一探索代碼與該第二探索代碼之間是否有一匹配的構件。

【第29項】 如請求項28之裝置，其中該第一和第二探索代碼中的每一者包括一鄰近度服務（ProSe）代碼。

【第30項】 如請求項29之裝置，其中該ProSe代碼包括一首碼部分和一後置部分。

【第31項】 如請求項30之裝置，其中該用於將該第一探索代碼與該第二探索代碼進行比較的構件被配置成將該第一探索代碼的首碼部分與該第二探索代

碼的首碼部分進行比較。

【第32項】 如請求項 28 之裝置，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該裝置進一步包括用於使用該金鑰資訊檢查該探索訊息的一訊息完整性代碼（MIC）的構件。

【第33項】 如請求項 32 之裝置，其中該 MIC 是第一 MIC，其中該用於檢查該第一 MIC 的構件被配置成：

基於該金鑰資訊計算一探索使用者完整性金鑰；

基於該探索使用者完整性金鑰和該探索訊息的一時間來計算一第二 MIC；及

將該第一 MIC 和該第二 MIC 進行比較。

【第34項】 如請求項 28 之裝置，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該裝置進一步包括用於使用該金鑰資訊從該探索訊息中移除因訊息而異的機密性的構件。

【第35項】 如請求項 34 之裝置，其中該用於移除因訊息而異的機密性的構件被配置成：

基於該金鑰資訊、添加了一訊息完整性代碼（MIC）的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算金鑰串流；及

對該探索訊息以及該金鑰串流和一經加密位元遮

罩的一邏輯與執行一 XOR 運算來恢復該探索訊息。

【第36項】 如請求項34之裝置，其中該用於移除因訊息而異的機密性的構件被配置成：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第37項】 一種用於無線通訊的裝置，包括：

一記憶體；及

至少一個處理器，其耦合至該記憶體並被配置成：

接收一探索代碼；

基於該探索代碼產生一探索訊息；

接收與該探索代碼相關聯的金鑰資訊；

使用該金鑰資訊來轉變該探索訊息；及

廣播該經轉變的探索訊息，

其中為了轉變該探索訊息，該至少一個處理器被配置成使用該金鑰資訊來對該探索訊息加擾，及其中為了對該探索訊息加擾，該至少一個處理器被配置成：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息加擾。

【第38項】 如請求項37之裝置，其中該探索代碼包括一鄰近度服務（ProSe）代碼。

【第39項】 如請求項38之裝置，其中該ProSe代碼包括一首碼部分和一後置部分。

【第40項】 如請求項37之裝置，其中為了轉變該探索訊息，該至少一個處理器被進一步配置成：

使用該金鑰資訊計算用於該探索訊息的一訊息完整性代碼（MIC）；及

向該探索訊息添加該MIC。

【第41項】 如請求項37之裝置，其中為了轉變該探索訊息，該至少一個處理器被配置成使用該金鑰資訊向該探索訊息添加因訊息而異的機密性。

【第42項】 如請求項41之裝置，其中為了轉變該探索訊息，該至少一個處理器被進一步配置成：

使用該金鑰資訊計算用於該探索訊息的一訊息完整性代碼（MIC）；及

向該探索訊息添加該MIC。

【第43項】 如請求項41之裝置，其中為了添加因訊息而異的機密性，該至少一個處理器被配置成：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第44項】 如請求項41之裝置，其中為了添加因訊息而異的機密性，該至少一個處理器被配置成：

基於該金鑰資訊、添加了MIC的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算一金鑰串流；及

對該探索訊息以及該金鑰串流和一經加密位元遮罩的一邏輯與執行一XOR運算來更新該探索訊息。

【第45項】 如請求項40之裝置，其中為了計算該MIC，該至少一個處理器被配置成：

基於該金鑰資訊計算一探索使用者完整性金鑰；及

基於該探索使用者完整性金鑰和該探索訊息的一時間來計算該MIC。

【第46項】 一種用於無線通訊的裝置，包括：

一記憶體；及

至少一個處理器，其耦合至該記憶體並被配置成：

接收一第一探索代碼；

接收包含一第二探索代碼的一探索訊息；

接收與該第一探索代碼相關聯的金鑰資訊；

使用該金鑰資訊對該探索訊息解擾以獲取該第二探索代碼；及

將該第一探索代碼與該第二探索代碼進行比較以得知該第一探索代碼與該第二探索代碼之間是

否有一匹配，

其中為了對該探索訊息解擾，該至少一個處理器被配置成：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息解擾。

【第47項】 如請求項46之裝置，其中該第一和第二探索代碼中的每一者包括一鄰近度服務（ProSe）代碼。

【第48項】 如請求項47之裝置，其中該ProSe代碼包括一首碼部分和一後置部分。

【第49項】 如請求項48之裝置，其中為了將該第一探索代碼與該第二探索代碼進行比較，該至少一個處理器被配置成將該第一探索代碼的該首碼部分與該第二探索代碼的一首碼部分進行比較。

【第50項】 如請求項46之裝置，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該至少一個處理器被進一步配置成使用該金鑰資訊檢查該探索訊息的一訊息完整性代碼（MIC）。

【第51項】 如請求項50之裝置，其中該MIC是一

第一 MIC，其中為了檢查該第一 MIC，該至少一個處理器被配置成：

基於該金鑰資訊計算一探索使用者完整性金鑰；

基於該探索使用者完整性金鑰和該探索訊息的一時間來計算一第二 MIC；及

將該第一 MIC 和該第二 MIC 進行比較。

【第 52 項】 如請求項 46 之裝置，其中回應於該第一探索代碼與該第二探索代碼之間的該匹配，該至少一個處理器被進一步配置成使用該金鑰資訊從該探索訊息中移除因訊息而異的機密性。

【第 53 項】 如請求項 52 之裝置，其中為了移除因訊息而異的機密性，該至少一個處理器被配置成：

基於該金鑰資訊、添加了一訊息完整性代碼(MIC)的探索訊息和一金鑰計算遮罩的一邏輯與、以及該探索訊息的一時間來計算金鑰串流；及

對該探索訊息以及該金鑰串流和一經加密位元遮罩的一邏輯與執行一 XOR 運算來恢復該探索訊息。

【第 54 項】 如請求項 52 之裝置，其中為了移除因訊息而異的機密性，該至少一個處理器被配置成：

接收一經加密位元遮罩；及

將一金鑰計算遮罩計算為該經加密位元遮罩的一邏輯補。

【第55項】 一種儲存電腦可執行代碼的電腦可讀取媒體，包括用於以下操作的代碼：

接收一探索代碼；

基於該探索代碼產生一探索訊息；

接收與該探索代碼相關聯的金鑰資訊；

使用該金鑰資訊來轉變該探索訊息；及

廣播該經轉變的探索訊息，

其中用於使用該金鑰資訊來轉變該探索訊息的代碼包含用於使用該金鑰資訊對該探索訊息加擾的代碼，及其中用於對該探索訊息加擾的代碼包括用於以下操作的代碼：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息加擾。

【第56項】 一種儲存電腦可執行代碼的電腦可讀取媒體，包括用於以下操作的代碼：

接收一第一探索代碼；

接收包含一第二探索代碼的一探索訊息；

接收與該第一探索代碼相關聯的金鑰資訊；

使用該金鑰資訊對該探索訊息解擾以獲取該第二

探索代碼；及

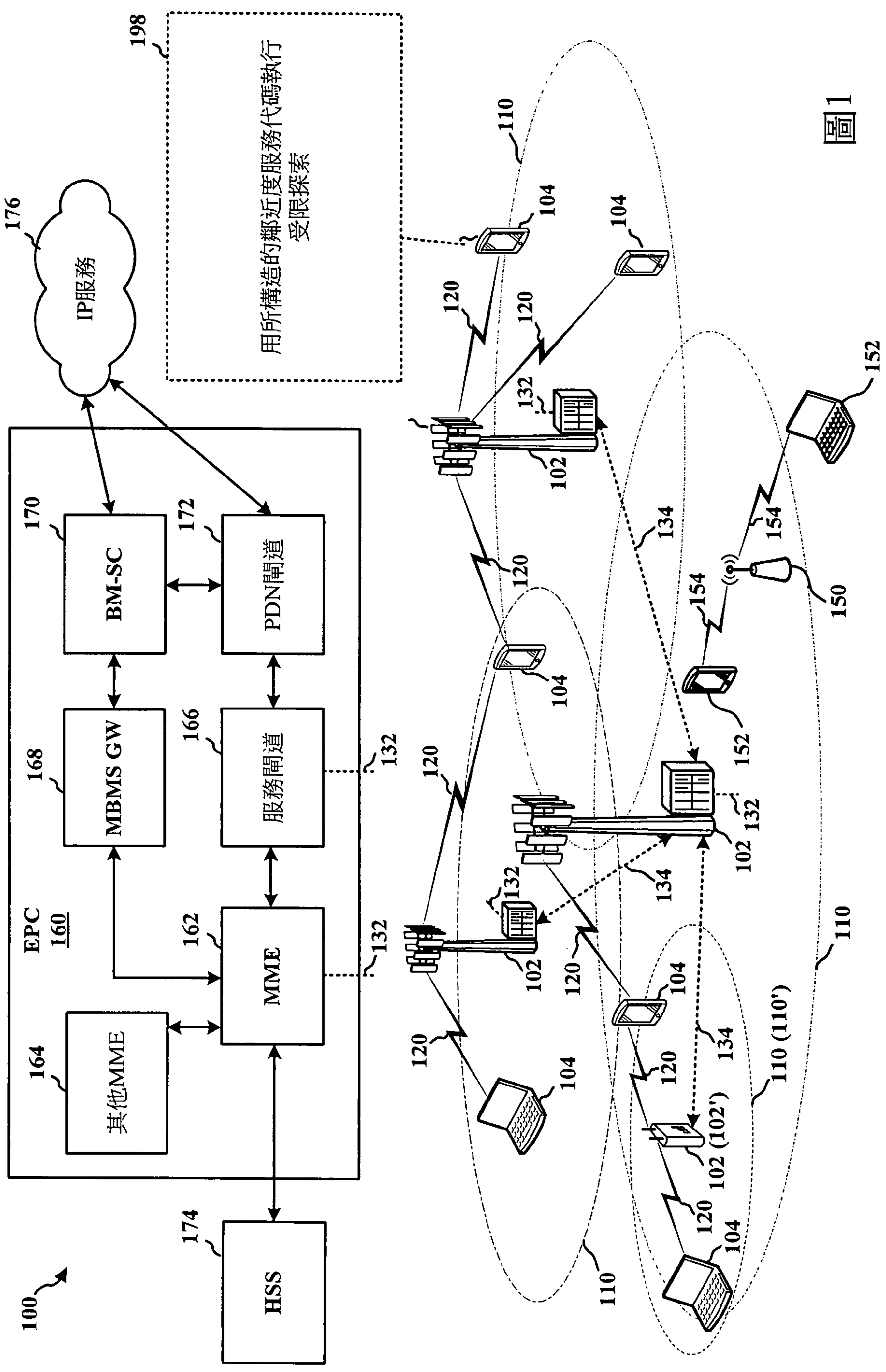
將該第一探索代碼與該第二探索代碼進行比較以得知是否該第一探索代碼與該第二探索代碼之間有一匹配，

其中用於對該探索訊息解擾的代碼包括用於以下操作的代碼：

基於該金鑰資訊匯出一探索使用者加擾金鑰；

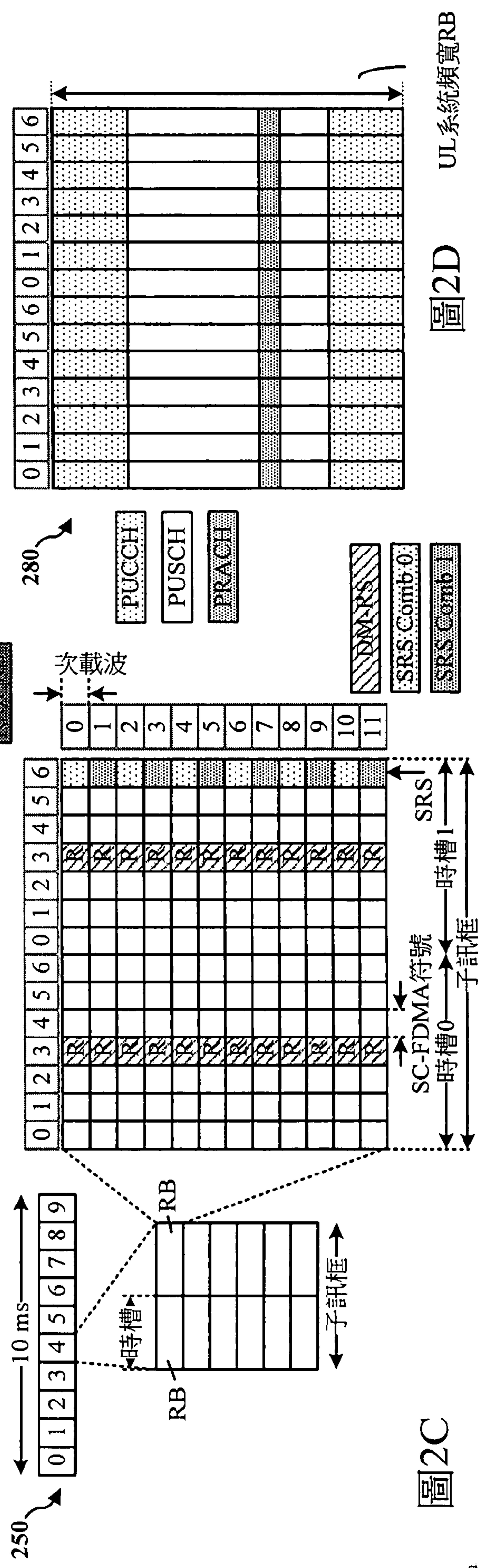
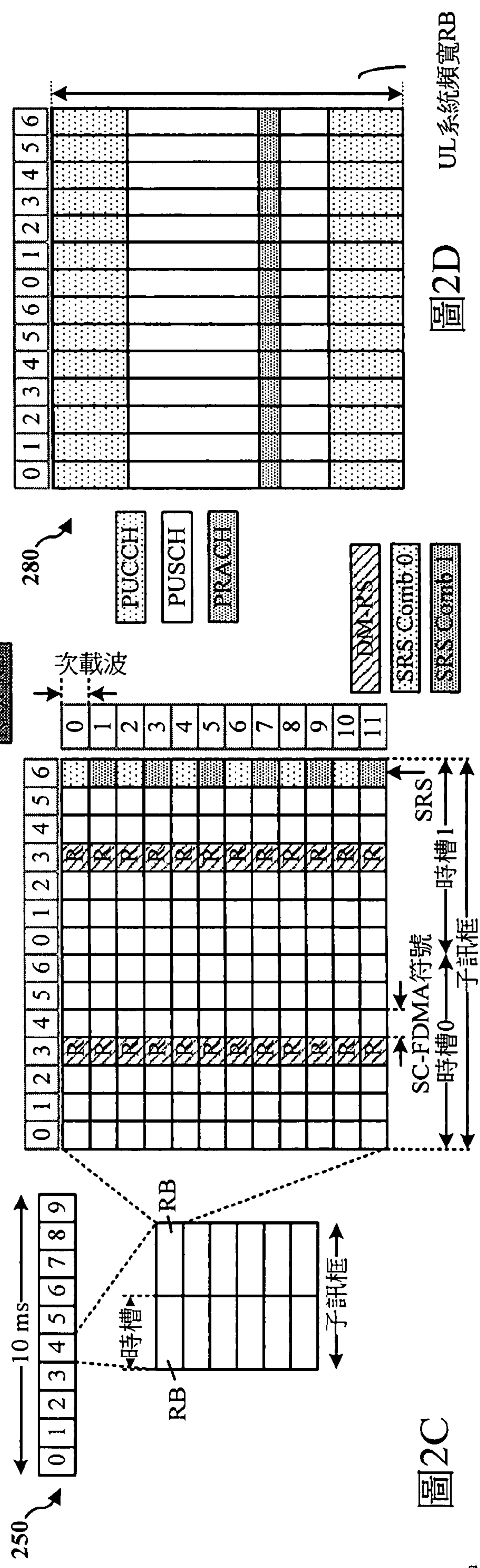
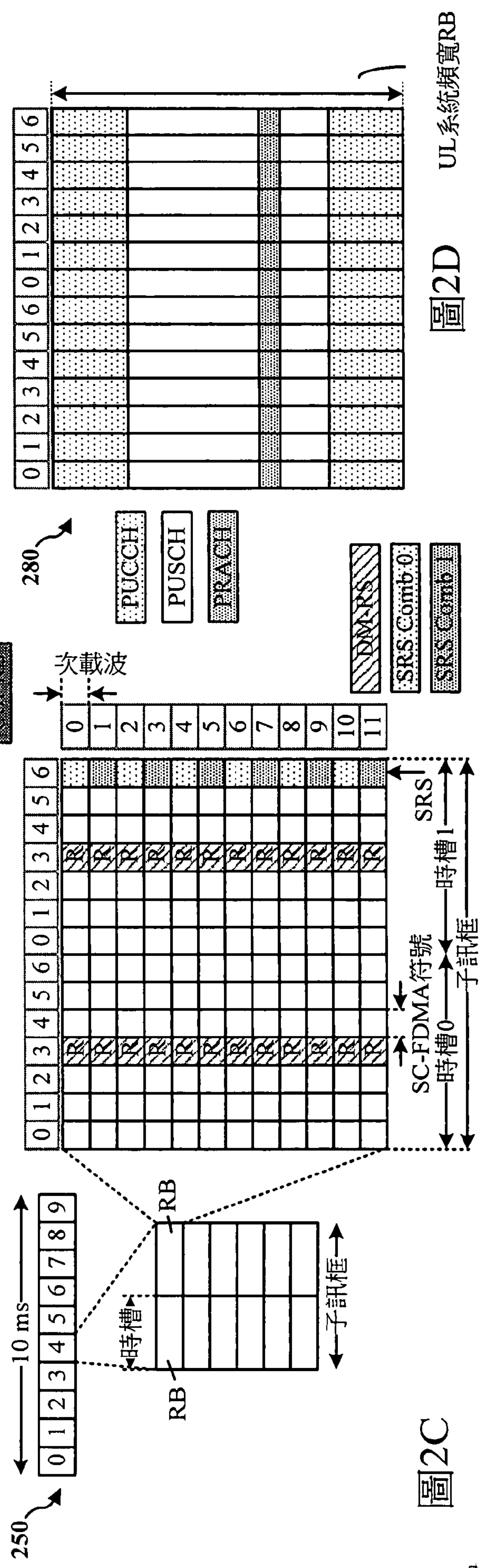
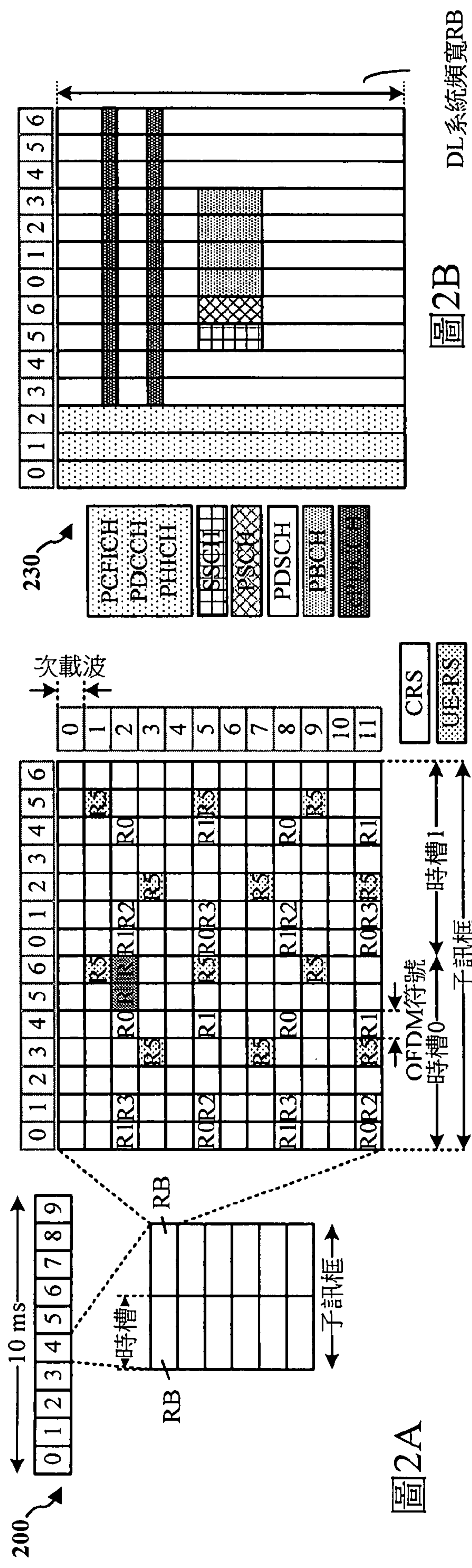
基於該探索使用者加擾金鑰和該探索訊息的一時間來計算一時間散列值；及

對該探索訊息和該時間散列值執行一 XOR 運算以對該探索訊息解擾。



圖式

圖1



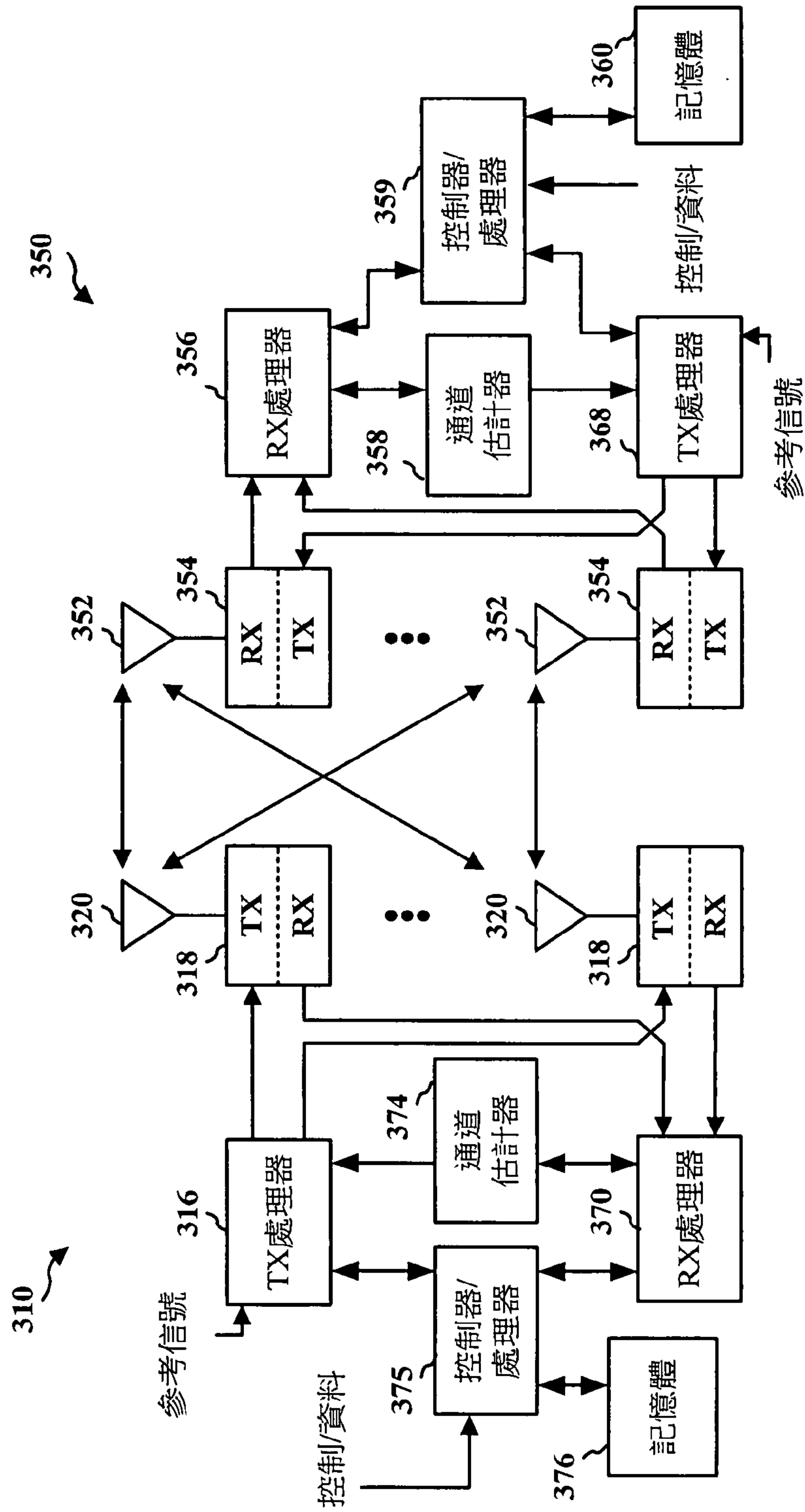
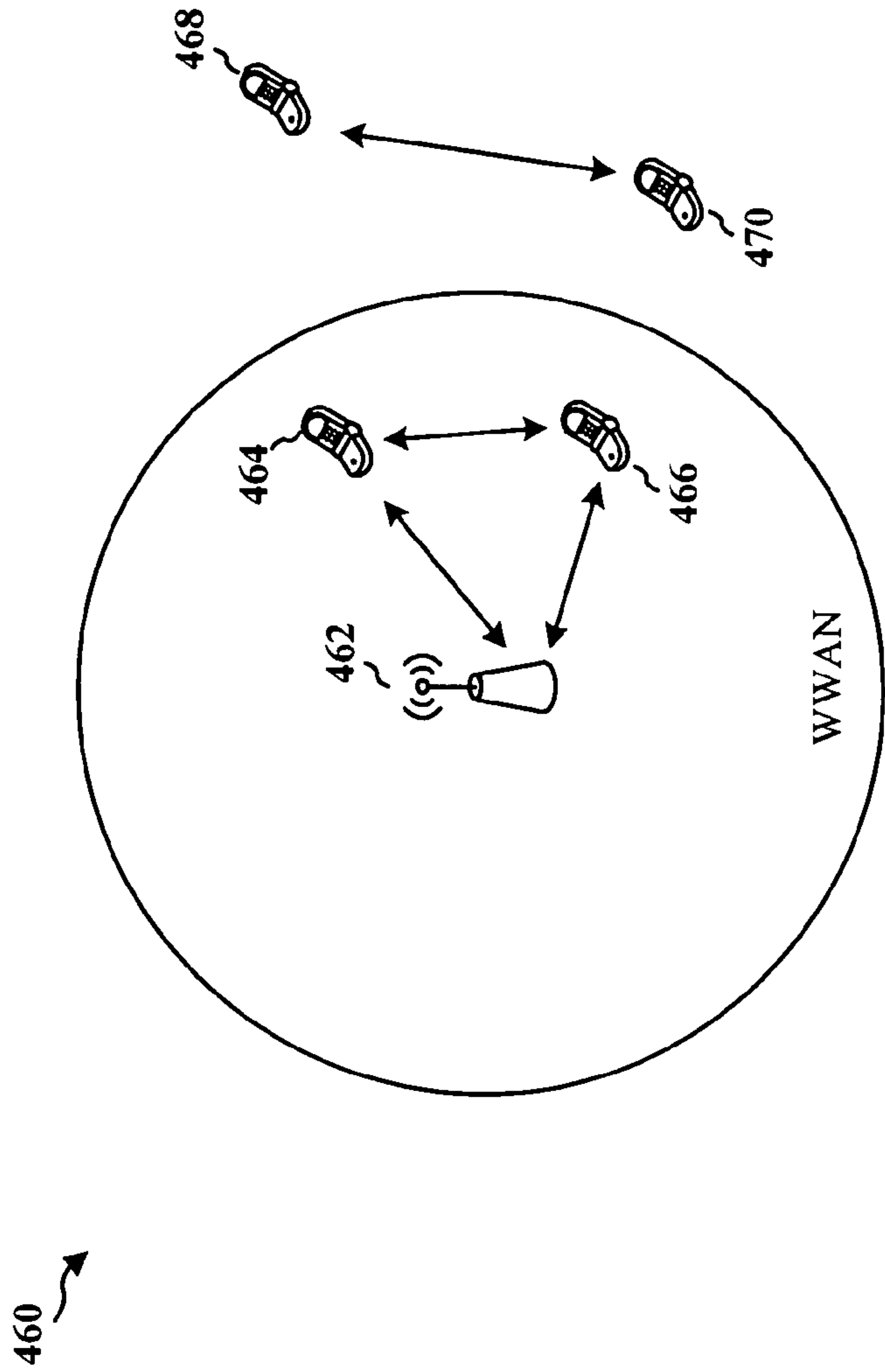


圖3



設備到設備通訊系統

圖4

.

.

.

.

500 ↗

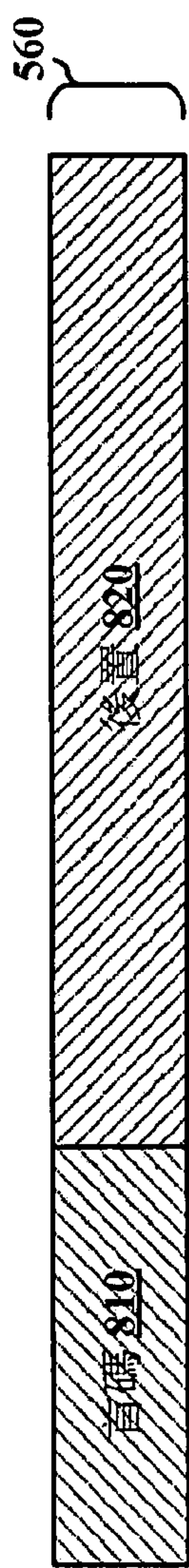


圖5

600 ↗

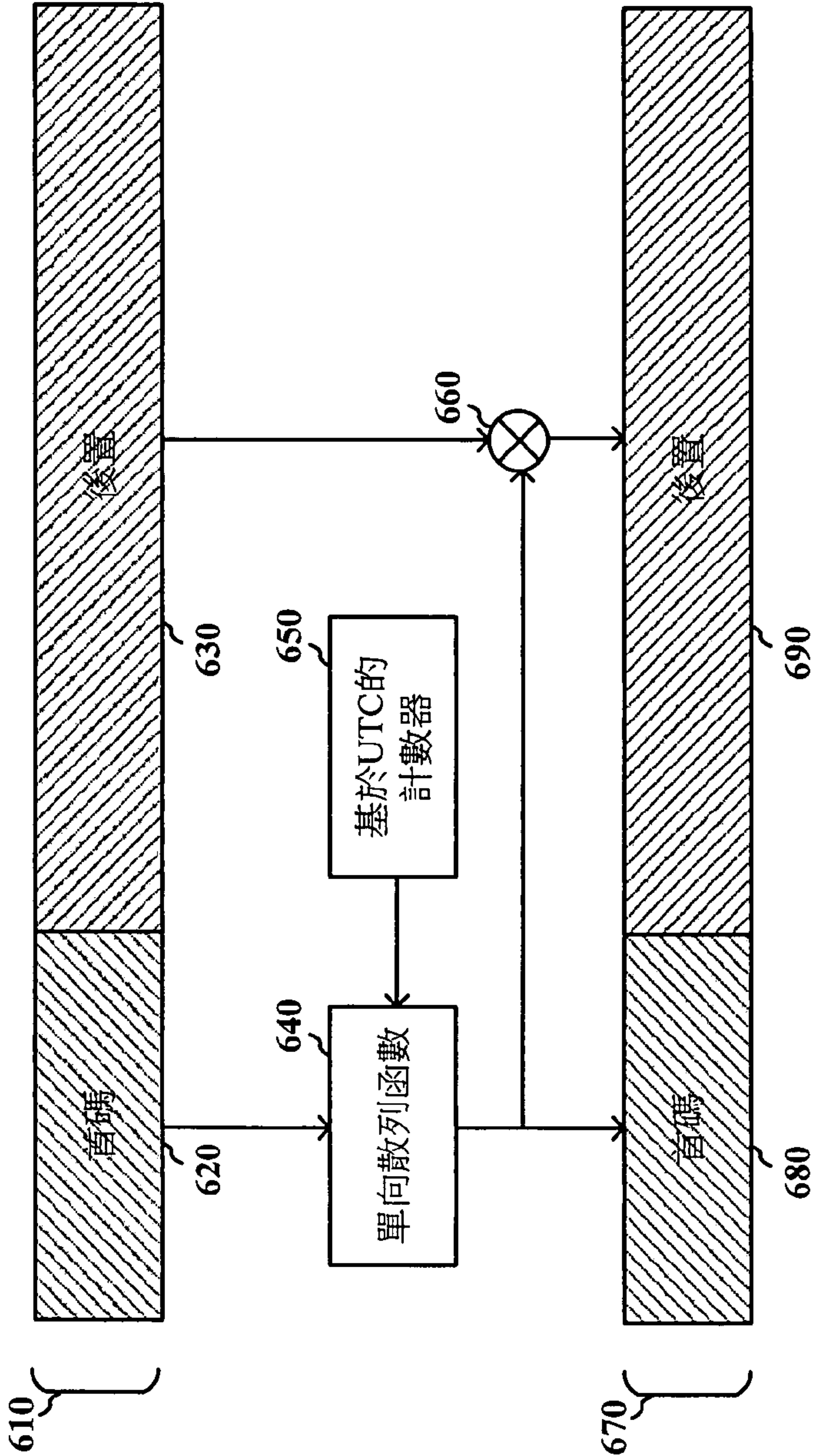


圖6

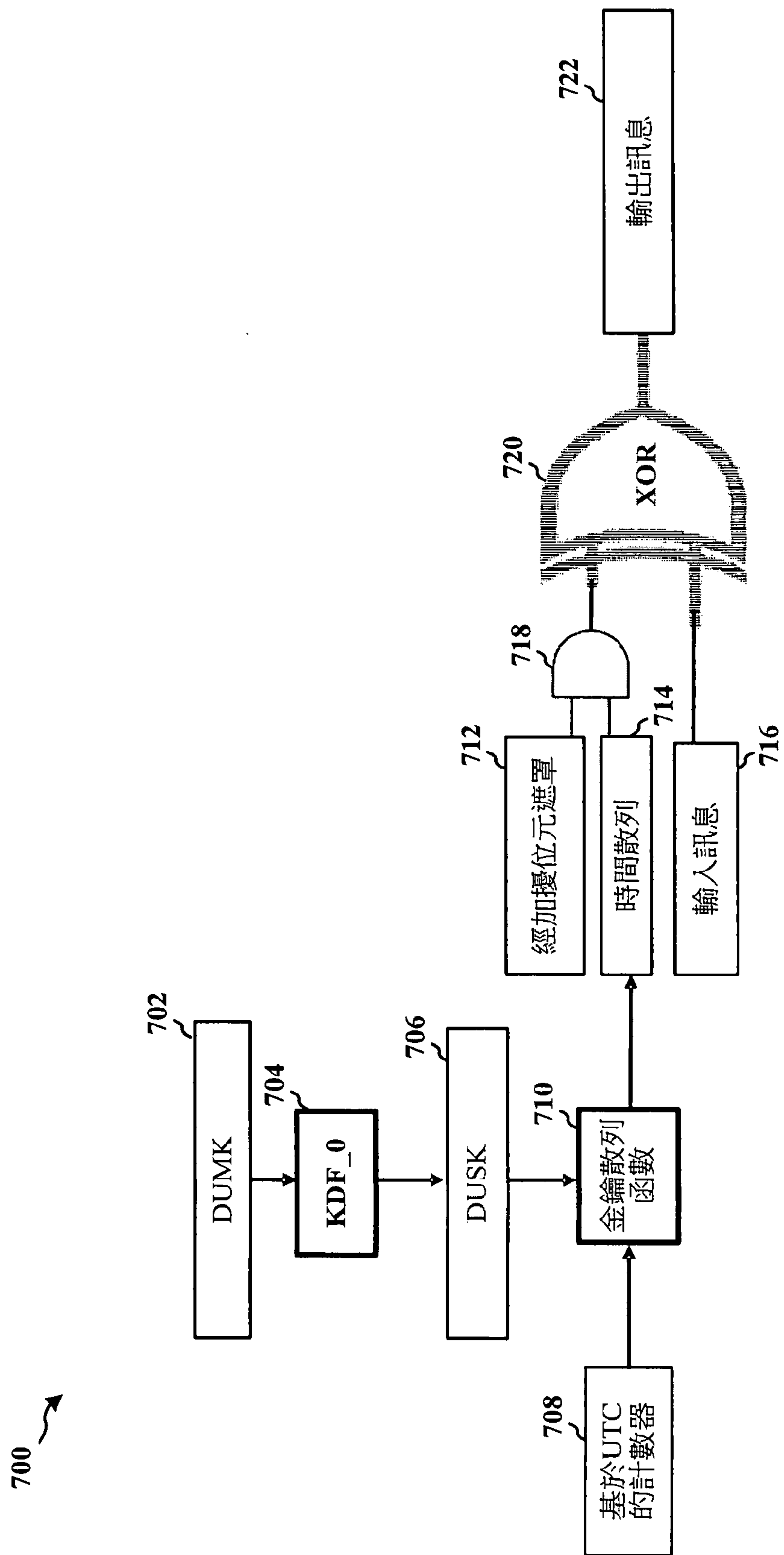


圖7

800

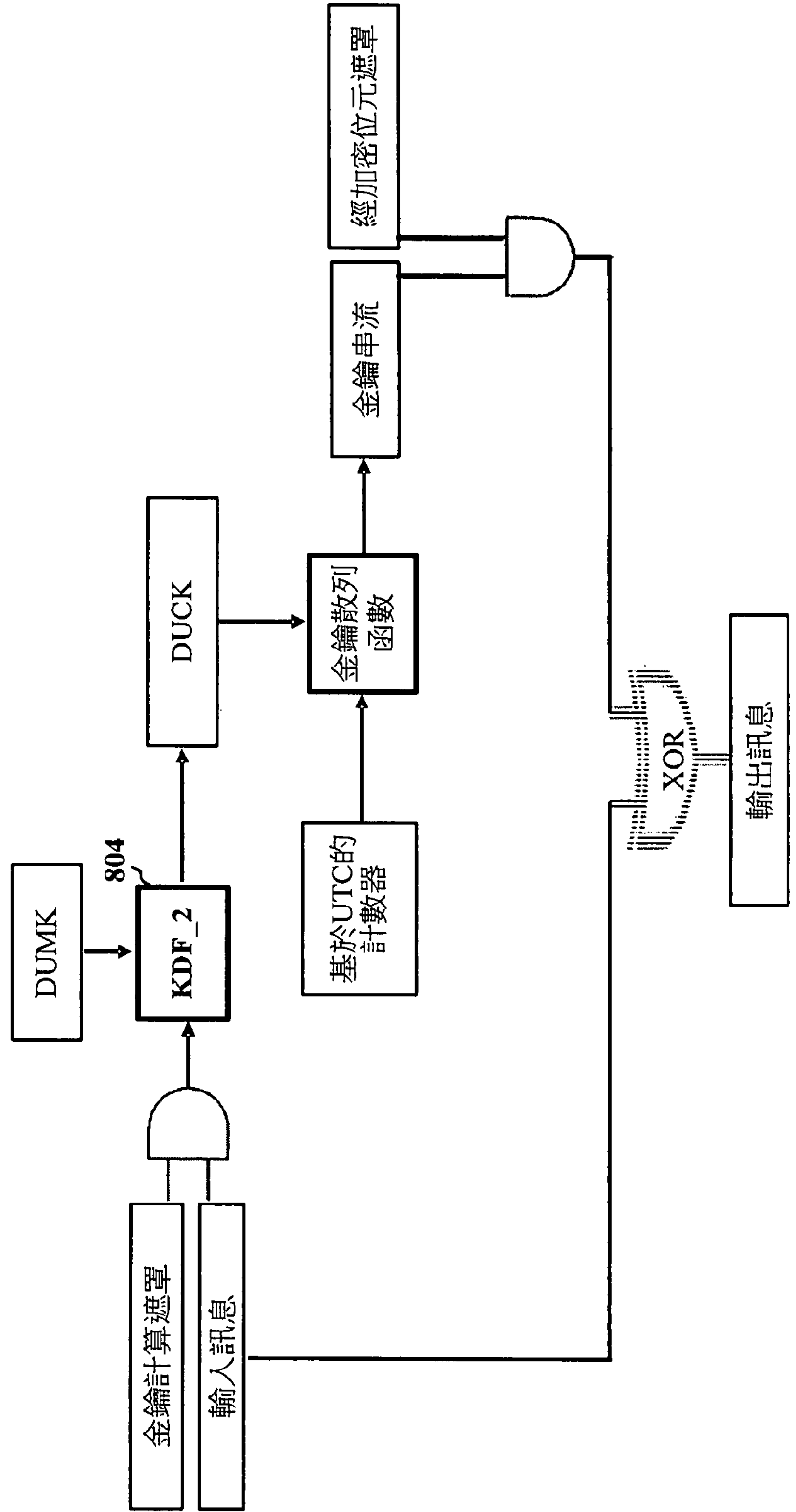


圖8

900 ↗

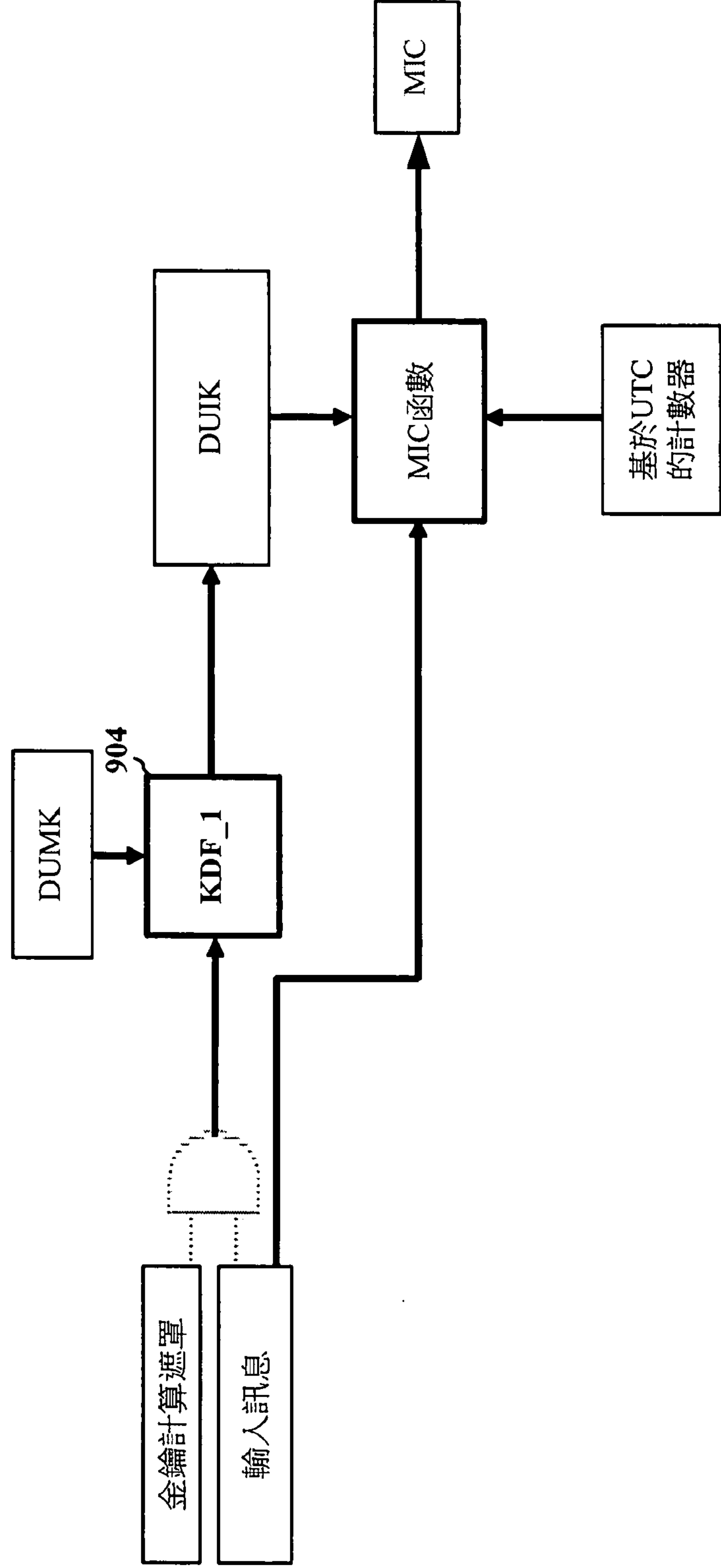


圖9

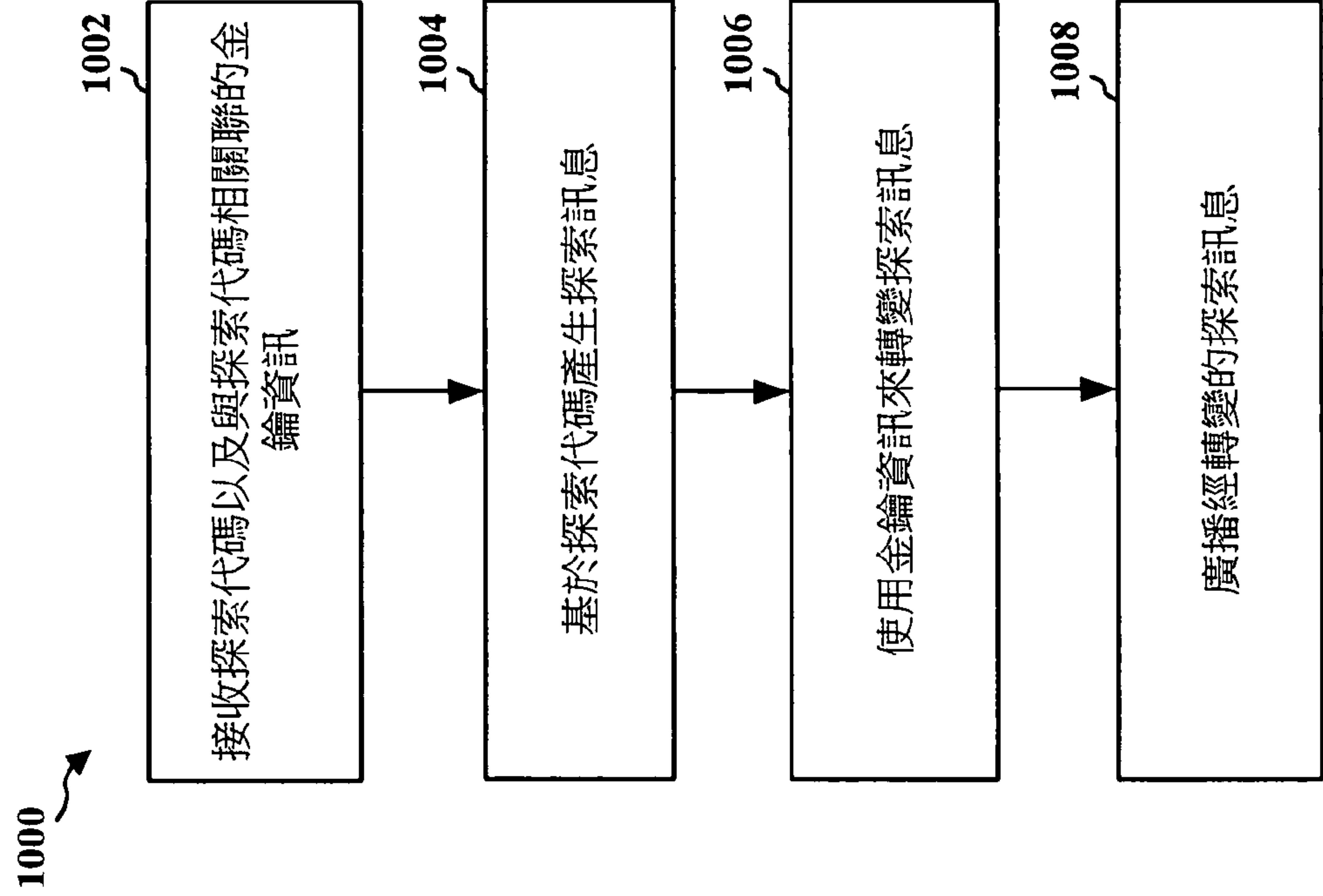


圖10

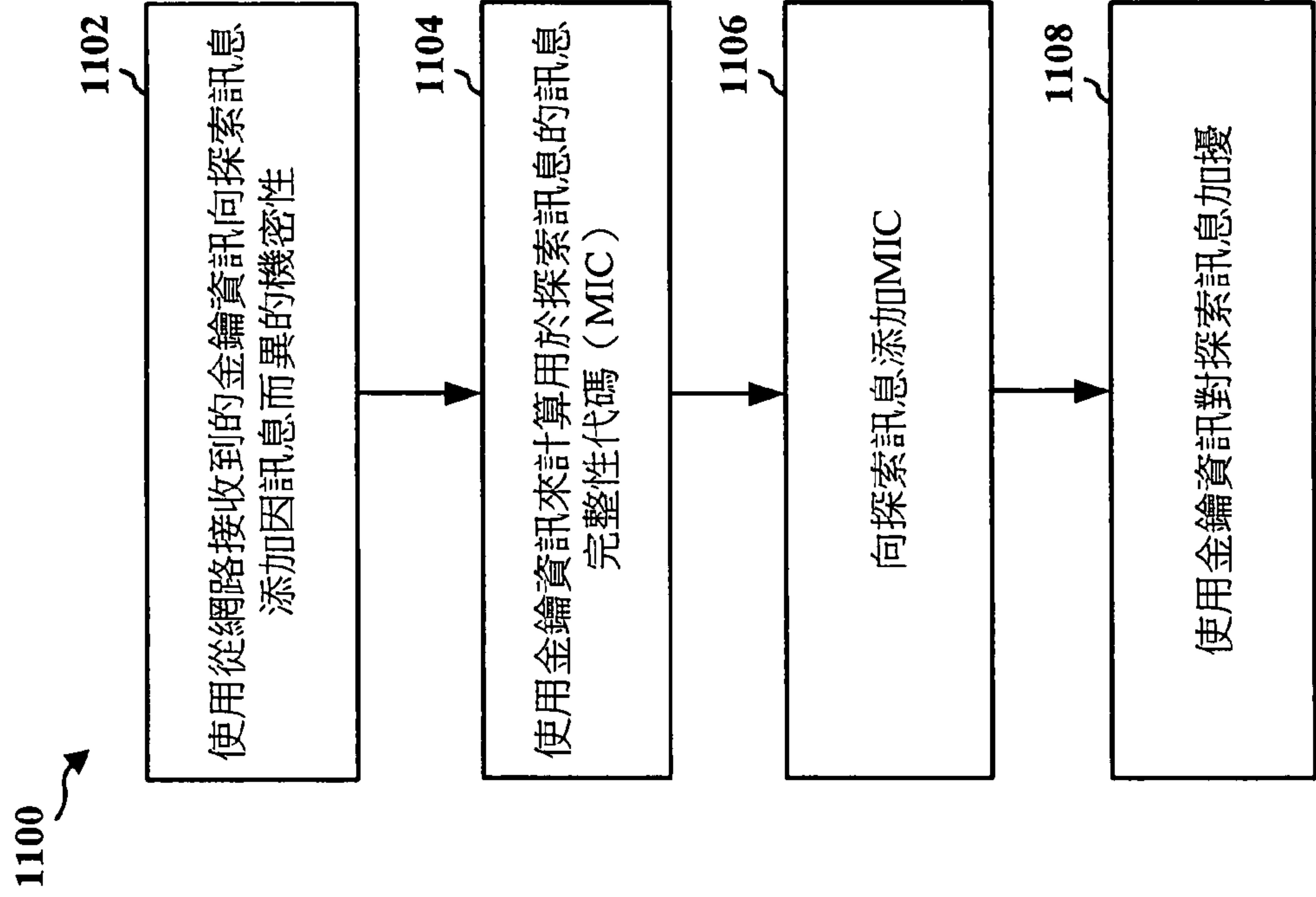


圖11

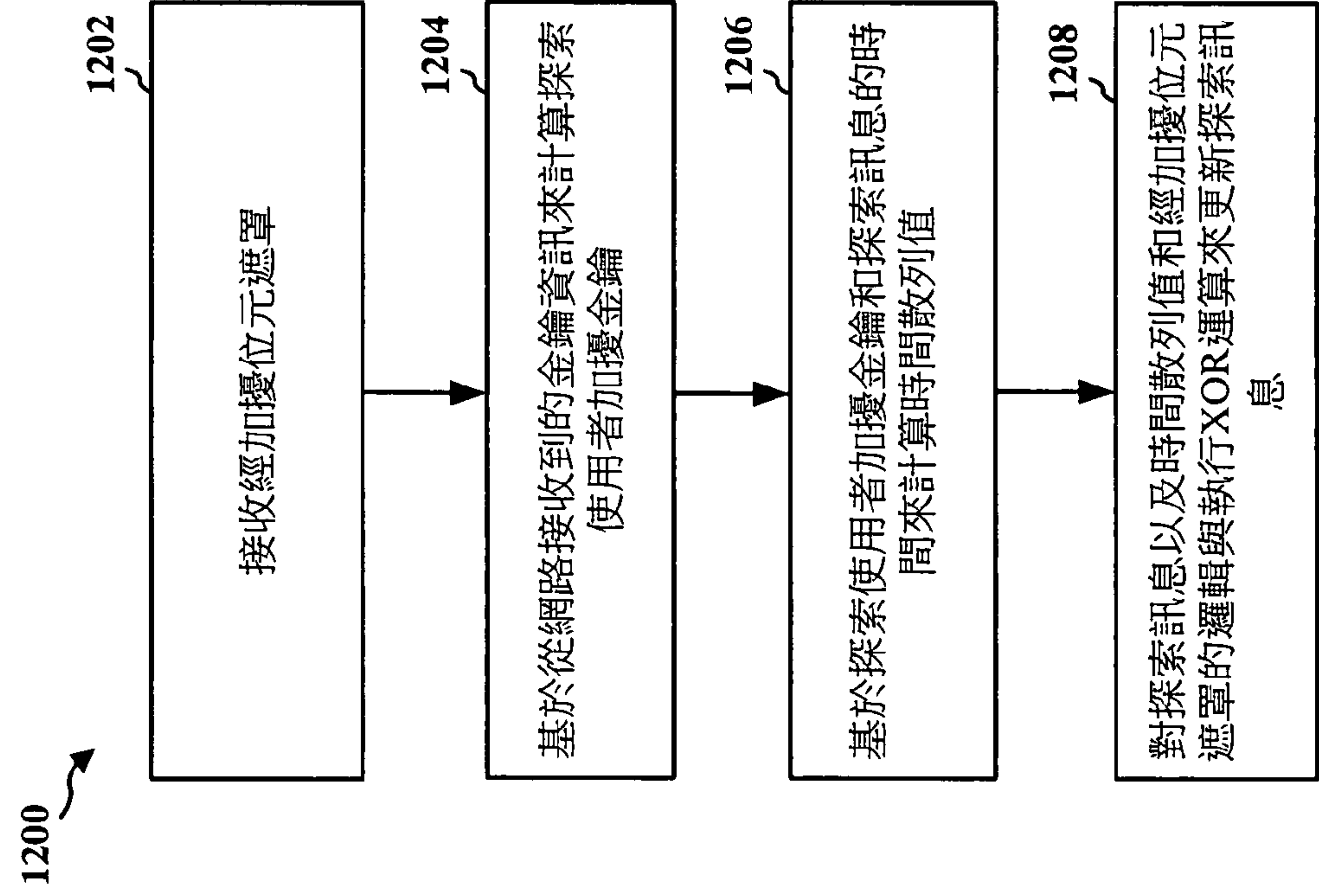


圖12

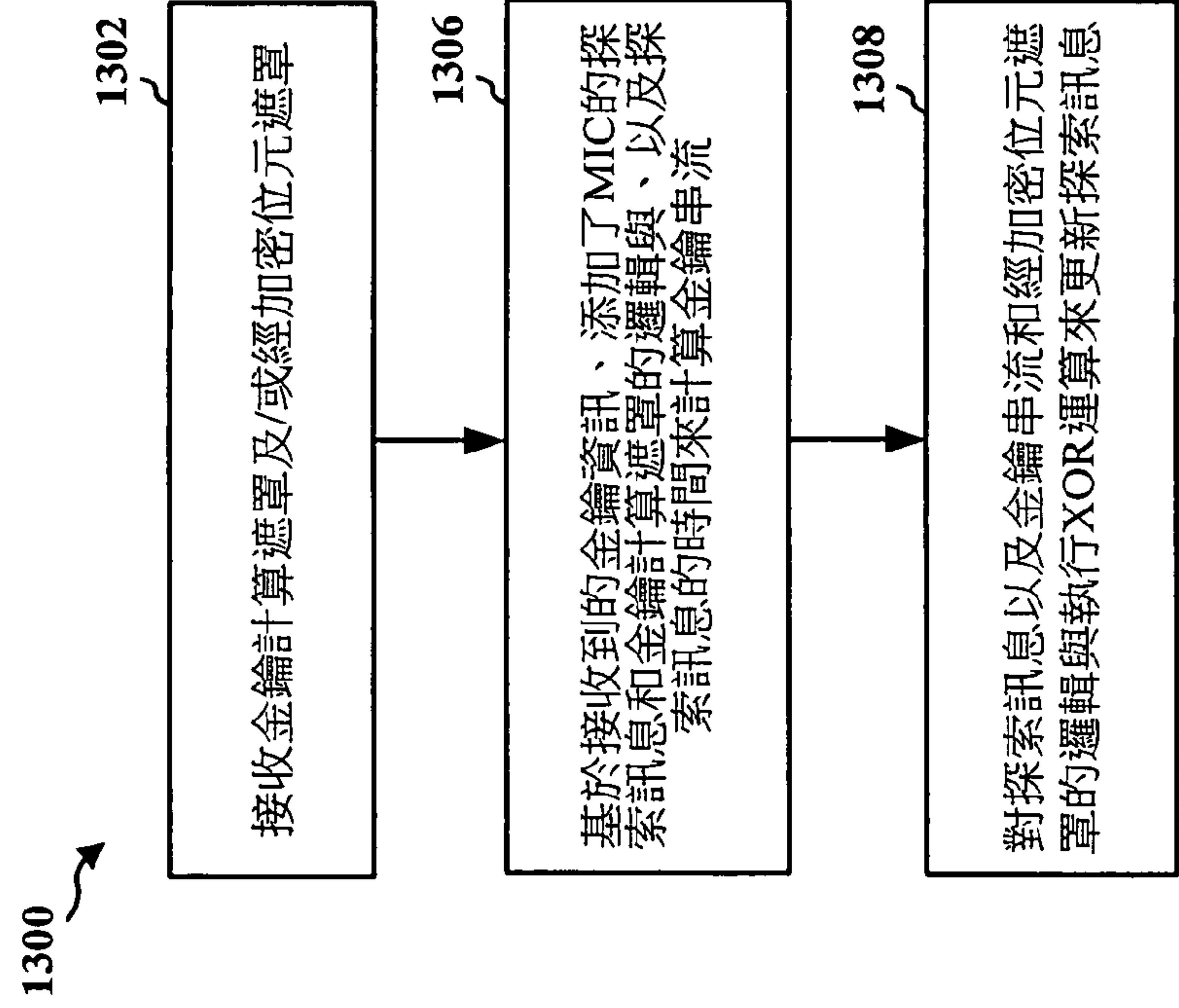


圖13

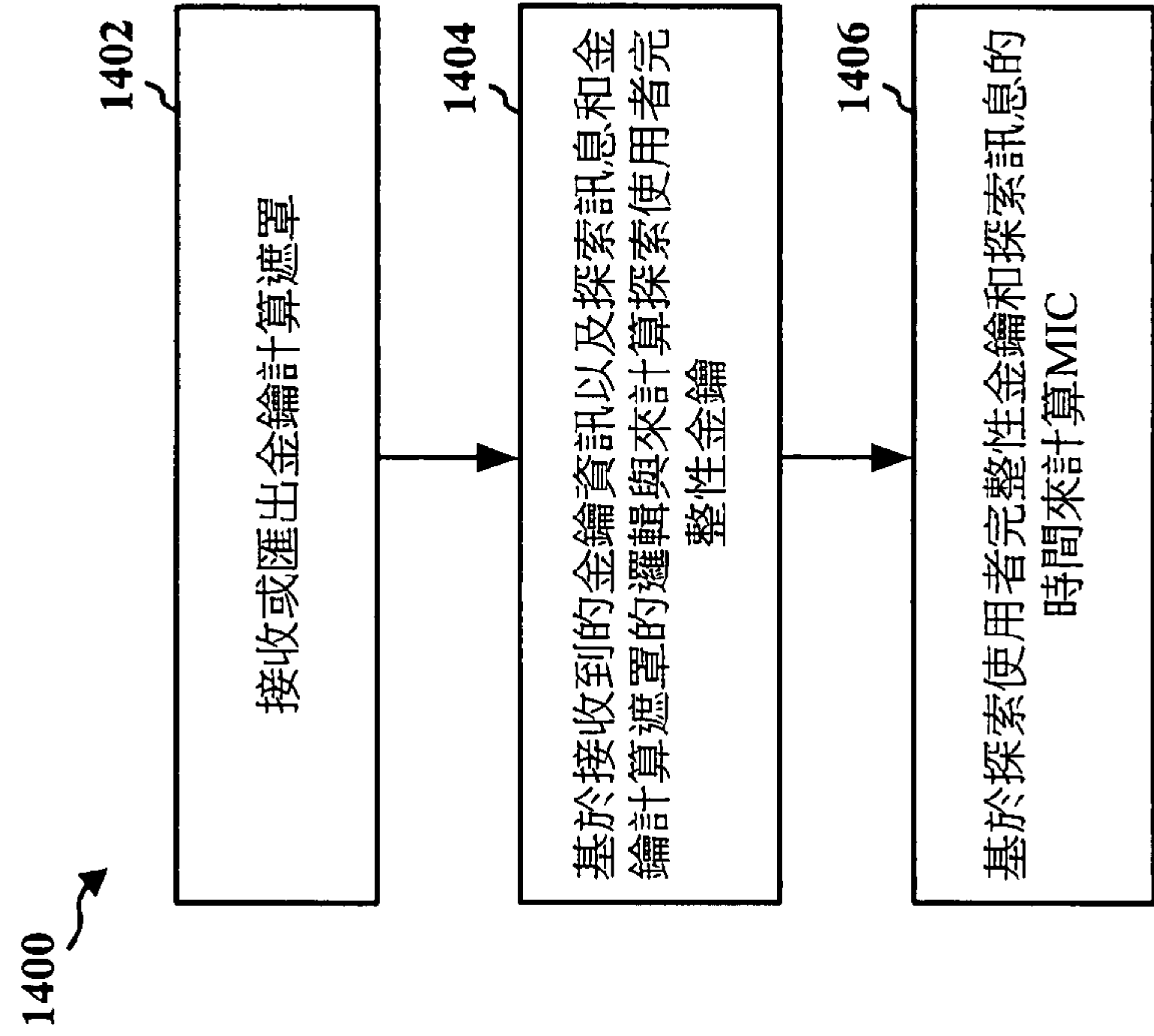


圖14

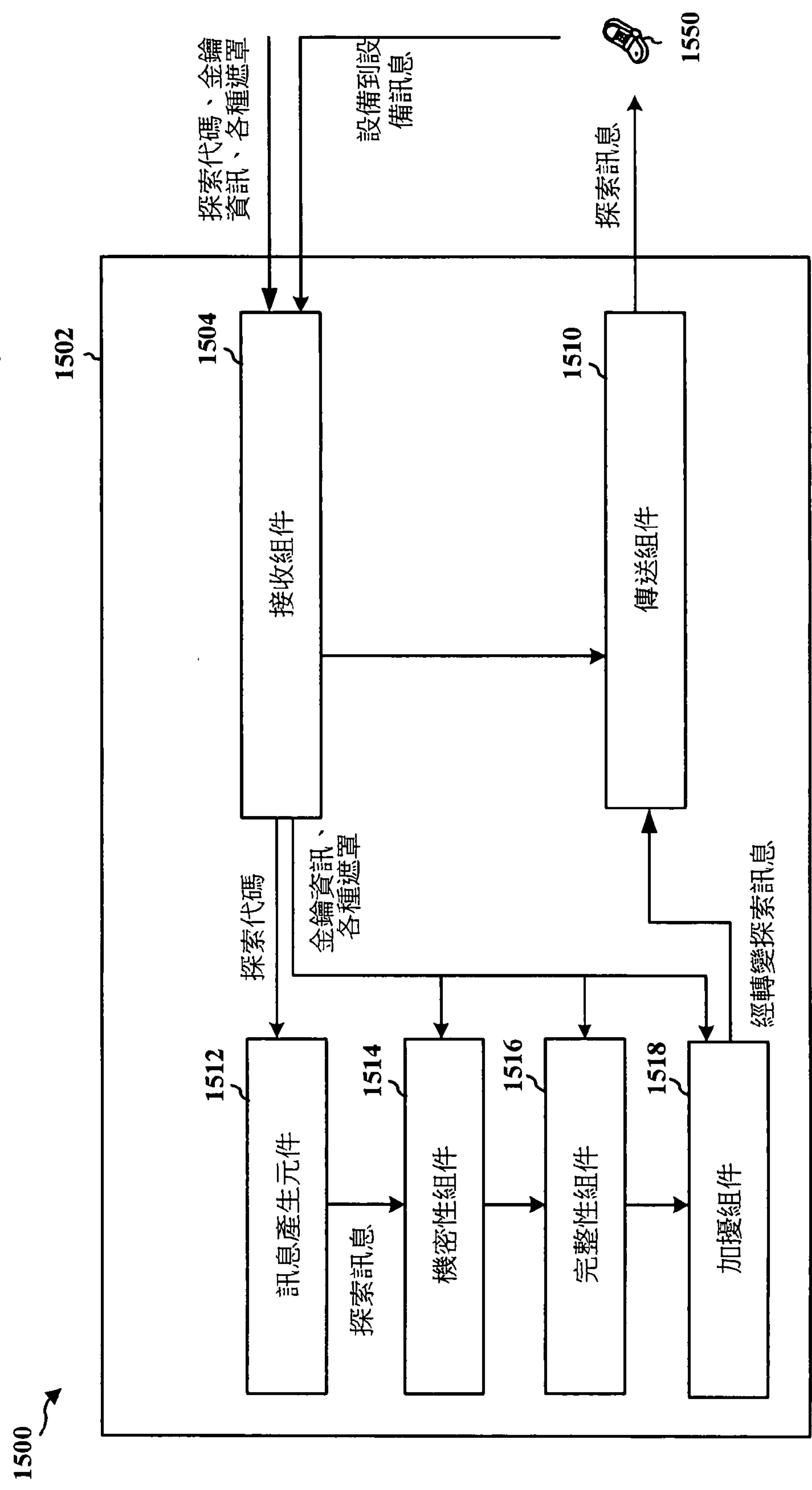


圖15

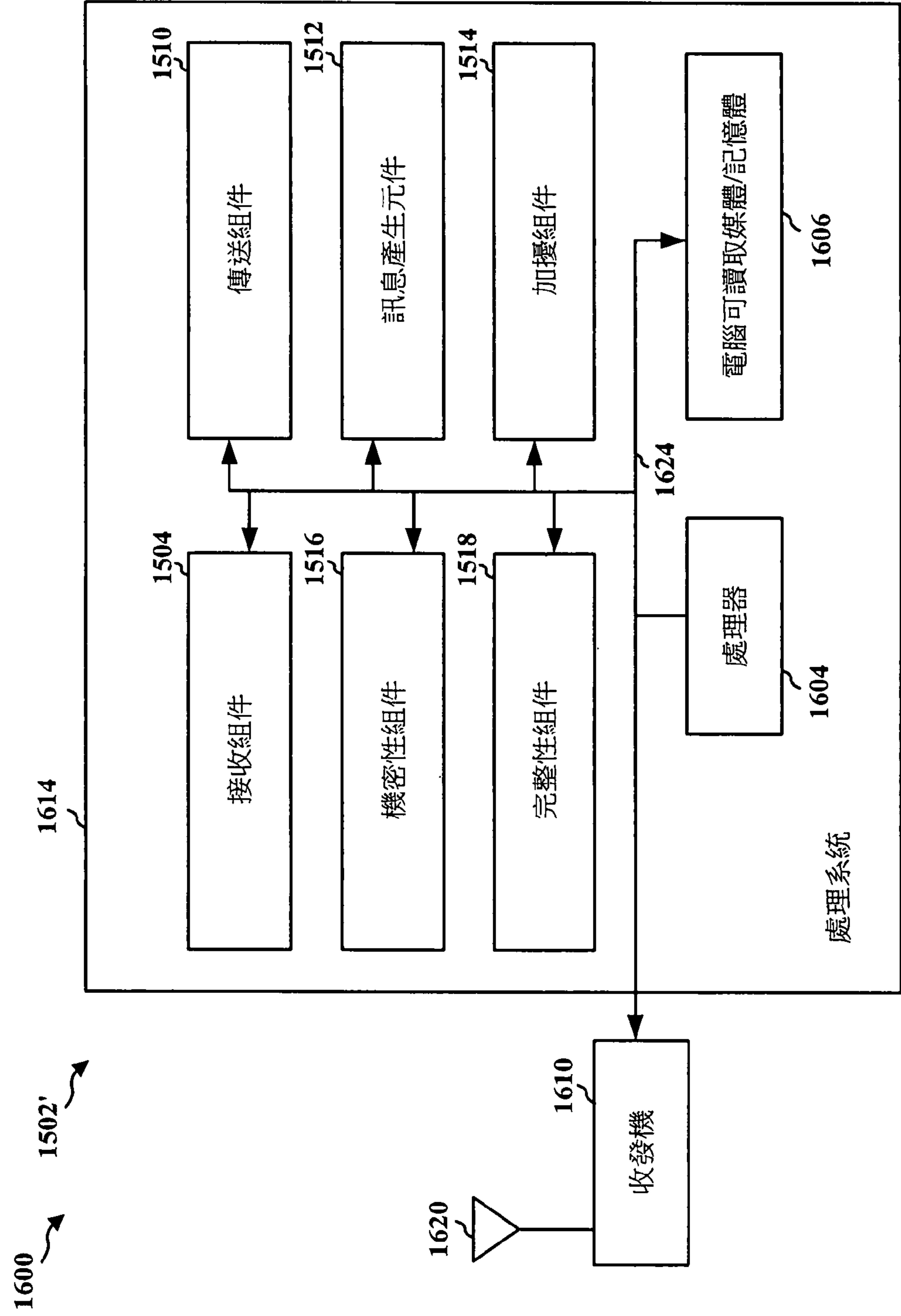


圖16

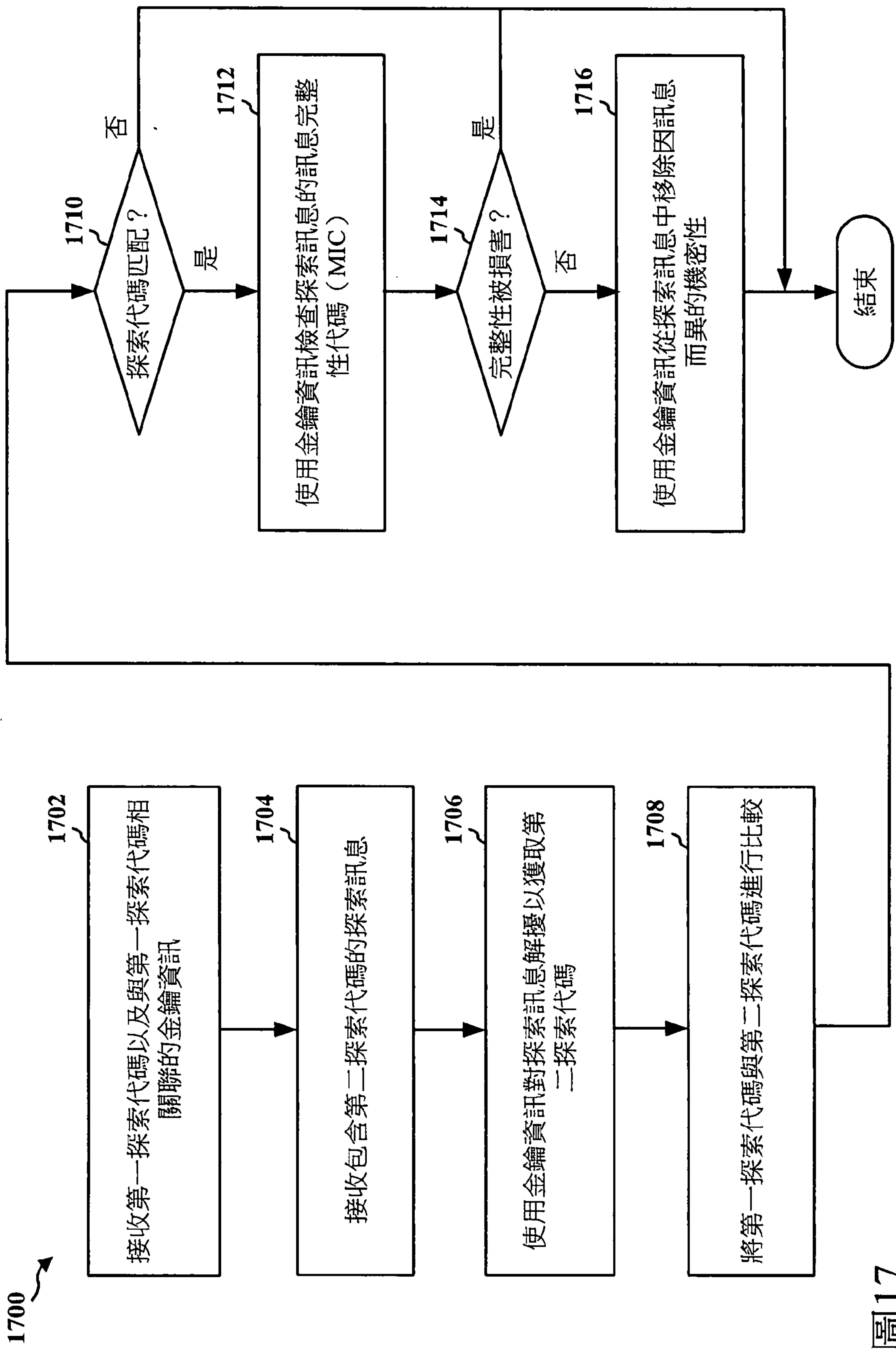


圖17

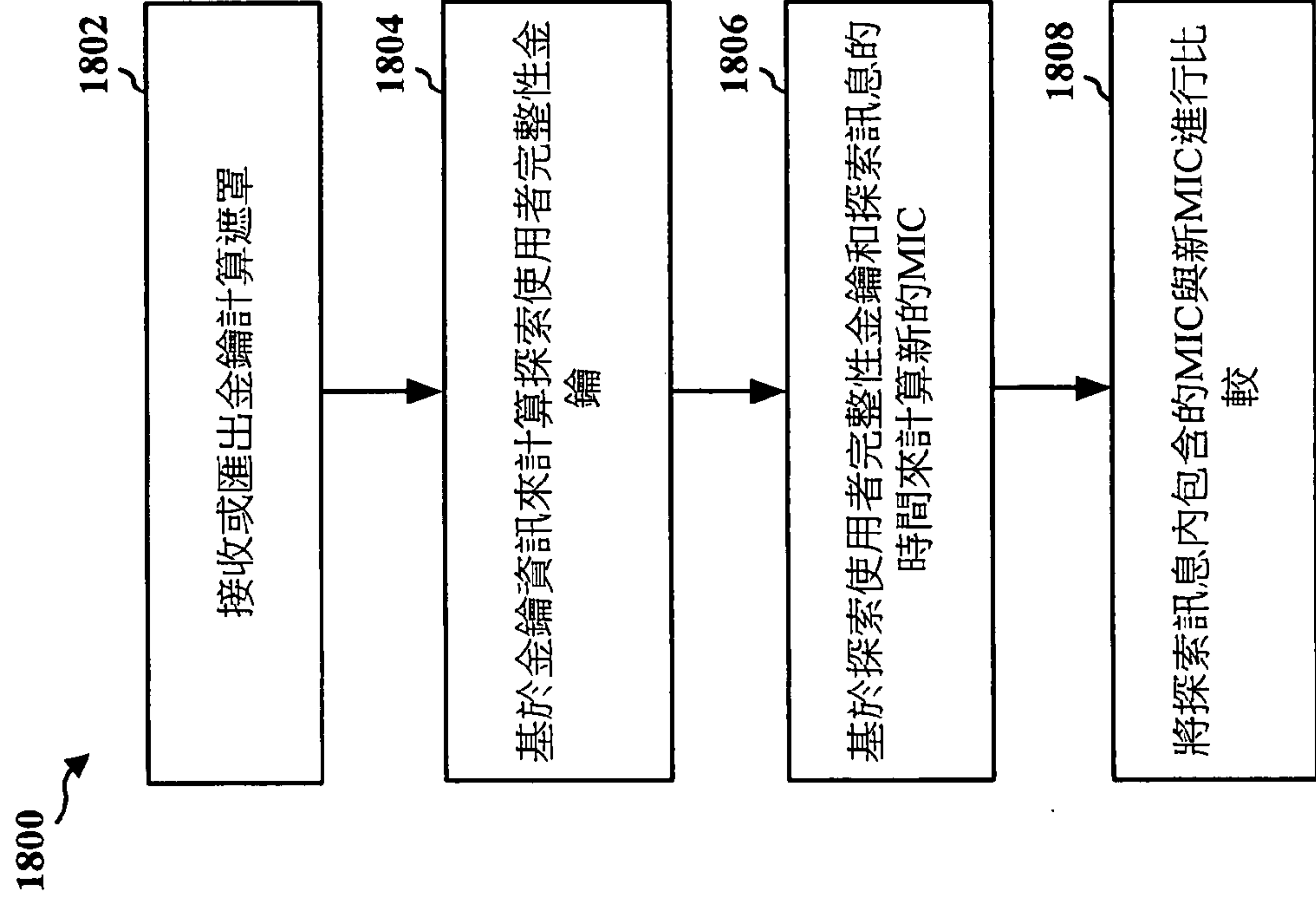


圖18

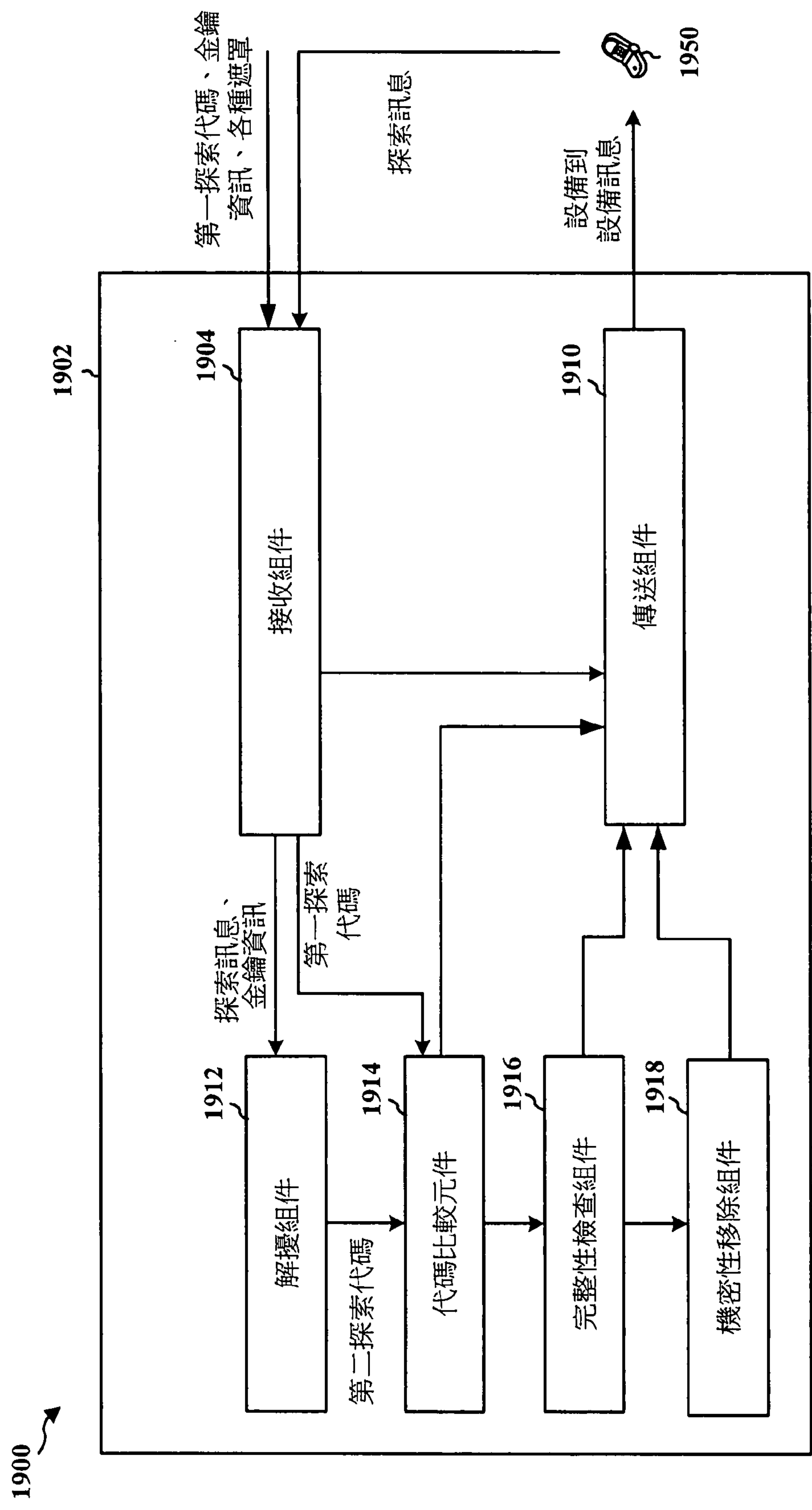


圖19

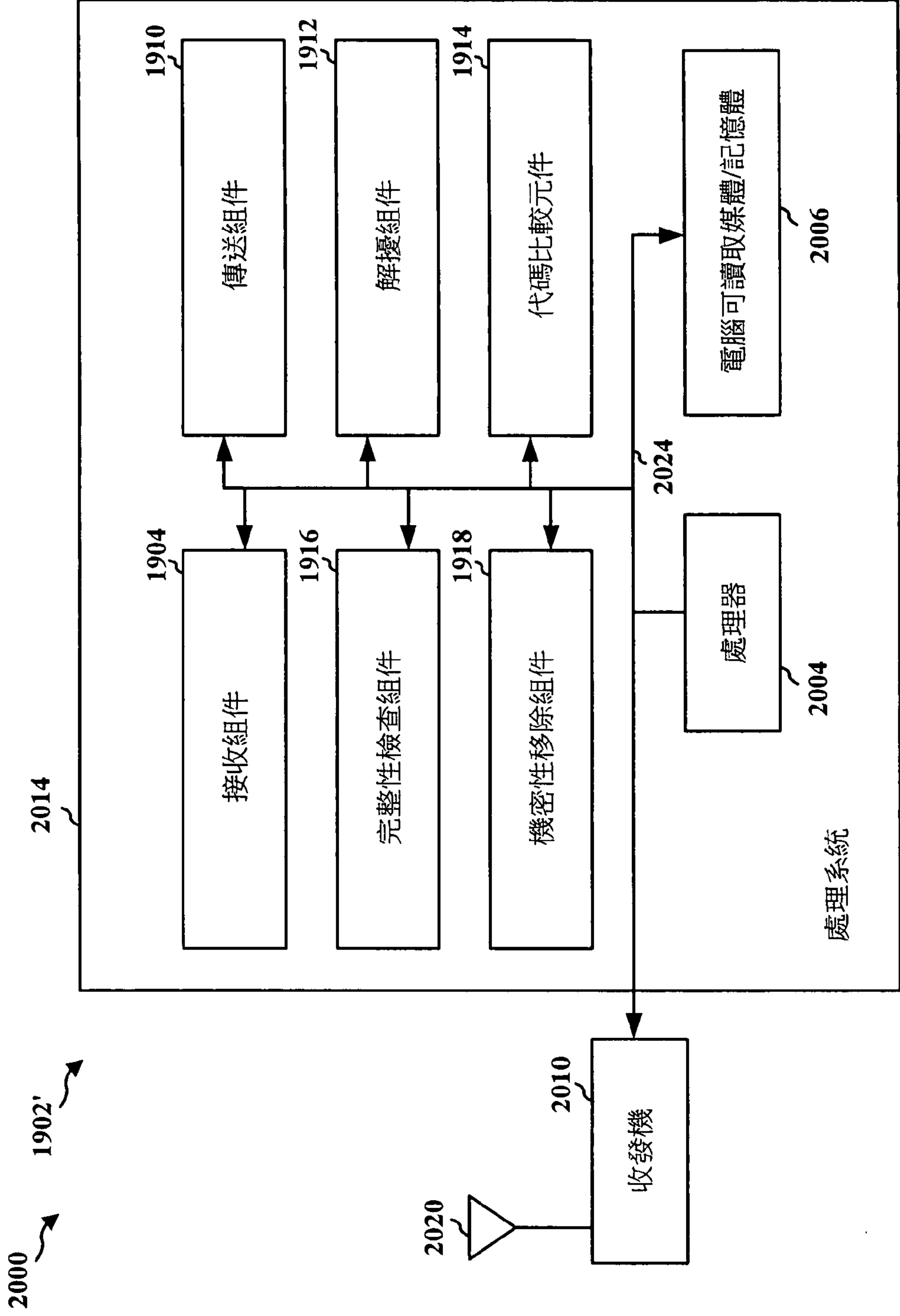


圖20