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：96131524

※ 申請日期：96.8.24　　※IPC 分類：H04L 9/00(2006.01)
H04B 7/26(2006.01)

一、發明名稱：（中文/英文）

用於無線通信系統之鑰管理之系統及方法

SYSTEMS AND METHODS FOR KEY MANAGEMENT FOR WIRELESS COMMUNICATIONS SYSTEMS

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商高通公司

QUALCOMM INCORPORATED

代表人：（中文/英文）

湯瑪仕　R　勞斯

ROUSE, THOMAS R.

住居所或營業所地址：（中文/英文）

美國加州聖地牙哥市摩豪斯大道5775號

5775 MOREHOUSE DRIVE SAN DIEGO, CA 92121-1714 U. S. A.

國　籍：（中文/英文）

美國　U.S.A.

三、發明人：(共 4 人)

姓　名：(中文/英文)

1. 威亞　那亞恩
   NARAYANAN, VIDYA
2. 保羅　E　班得
   BENDER, PAUL E.
3. 拉克西米納斯　瑞迪　東迪提
   DONDETI, LAKSHMINATH REDDY
4. 帕拉　亞恩　雅加希
   AGASHE, PARAG ARUN

國　籍：(中文/英文)

1. 印度　INDIA
2. 美國　U.S.A.
3. 印度　INDIA
4. 美國　U.S.A.

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；2006年08月24日；60/840,141

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 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。

五、中文發明摘要：

本發明提供一種用於保護一存取終端機與兩個存取點之間的通信交遞之新穎鑰管理方法。此方法提供一存取終端機與存取點之間的通信的安全交遞，而不存在曝露一用於該存取終端機之主鑰的危險。導出臨時主鑰以用於一新存取點與該存取終端機之間的低潛時交遞及安全鑑認。在一態樣中，提供一分布式鑰管理機制，其中一當前存取點(基於其自身之安全鑰)產生一由一存取終端機與之通信之下一存取點所使用的新安全鑰。在另一態樣中，提供一集中式鑰管理機制，其中一中央鑑認器(基於一與存取終端機相關聯之主安全鑰)保持、產生新安全鑰並將其分配至存取點。

六、英文發明摘要：

A novel key management approach is provided for securing communication handoffs between and access terminal and two access points. This approach provides for securely handing off communications between an access terminal and access point without risking exposure a master key for the access terminal. Temporary master keys are derived for low latency handoffs and secure authentication between a new access point and the access terminal. In one aspect, a distributive key management scheme is provided in which a current access point generates a new security key (based on its own security key) that is used by the next access point with which an access terminal communicates. In another aspect, a centralized key management scheme is provided in which a central authenticator maintains, generates, and distributes new security keys (based on a master security key associated with the access terminal) to access points.

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100	多重存取無線通信系統
102	小區
104	小區
106	小區
110	存取點
112	存取點
114	存取點
116	天線
118a	存取終端機
118b	存取終端機
118c	存取終端機
120	鑑認器
AP	存取點
I-MK	暫時主鑰
I-TSK	暫時暫態會話鑰

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

九、發明說明：

【發明所屬之技術領域】

各種特徵係關於無線通信系統。至少一態樣係關於一種用於以低潛時進行網路存取之鑰管理之系統及方法。

【先前技術】

無線通信網路使得通信設備能夠在移動之同時發射及/或接收資訊。可將此等無線通信網路可通信地耦接至其他公眾或私用網路以使得能夠將資訊轉移至行動存取終端機及自行動存取終端機轉移資訊。此等通信網路通常包括提供至存取終端機(例如，行動通信設備、行動電話、無線使用者終端機)之無線通信鏈路的複數個存取點(例如，基地台)。該等存取點可為靜止的(例如，固定至地面)或行動的(例如，安裝於衛星上，等等)，且經定位以在存取終端機行進跨越不同覆蓋區域時提供寬廣之區域覆蓋。

當一行動存取終端機到處移動時，其與一存取節點之通信鏈路可能會降級。在此情形中，行動節點可切換另一存取點或與另一存取點連接以獲得一更好品質之通信鏈路，同時其第一鏈路仍有效。將建立與另一存取點之通信鏈路的此過程稱作"交遞"。該交遞過程通常面臨在切換存取點的同時保持與無線通信網路之可靠及安全之通信鏈路的問題。軟交遞及硬交遞係兩種通常使用之交遞類型。軟交遞係在終止現有通信鏈路之前建立與新存取點之新通信鏈路的交遞。在硬交遞中，在建立新通信鏈路之前通常終止現有通信鏈路。

在某些通信系統中，當行動存取終端機經由存取點而附接至通信網路時，其執行網路存取鑑認以建立安全主鑰。每次發生一交遞時，可重複此過程。然而，在每次交遞時重複此鑑認過程引入一不可接受之潛時。一種用以減少此潛時之當前解決方案係在存取點中共用主鑰。然而，若一存取點被損害，則此方法產生一嚴重之安全危險，因為主鑰變得不安全且可用於損害使用該主鑰之所有通信。

因此，需要一種提供存取終端機與存取點間之低潛時交遞而不損害安全的方法。

【發明內容】

一特徵提供一用於存取終端機(例如，行動終端機、無線使用者終端機等等)與一或多個存取點(例如，基地台等等)之間的鑰管理的系統及方法。詳言之，提供一用於建立存取終端機與存取點之間的安全通信而不存在曝露用於該存取終端機之主鑰的機制。此方法導出用於一新存取點與該存取終端機之間的低潛時交遞及安全鑑認的臨時主鑰。

在一態樣中，提供一分布式鑰管理機制，其中當前存取點產生一由存取終端機與之通信之下一存取點所使用的新安全鑰。當存取終端機自當前存取點移至一新存取點時，該當前存取點基於其自身之安全鑰及該新存取點之唯一識別符產生一新安全鑰。接著將該新安全鑰發送至該新存取點。存取終端機獨立地產生其可藉以與該新存取點安全地通信之相同新安全鑰。

在另一態樣中，提供一集中式鑰管理機制，其中鑑認器保持、產生新安全鑰且將其分配至存取點。當存取終端機自當前存取點移至一新存取點時，鑑認器基於主安全鑰(與存取終端機相關聯)及該新存取點之唯一識別符產生一新安全鑰。接著將該新安全鑰發送至該新存取點。鑑認器在存取終端機切換至其他存取點時重複此過程。存取終端機獨立地產生其可藉以與新存取點安全地通信之相同新安全鑰。

又一特徵提供一存取終端機，該存取終端機經組態以建立及/或保持其可與之通信的一組有效存取點。由存取終端機保持一組有效鑰，而非在存取終端機移至一新存取點時獲得或協商新鑰(例如，主鑰或暫態會話鑰)。亦即，存取終端機可同時保持或建立與一扇區、區域或地區內之複數個存取點的安全關聯(例如，鑰)。存取終端機可隨後使用預先建立之安全鑰來與其有效組中之存取點通信而無需重新建立一安全關係。可藉由集中式或分布式鑰管理方法獲得此等鑰。

提供包含記憶體及處理器之存取點。該處理器可經組態以：(a)自一主鑰產生一第二臨時鑰；(b)命令將該第二臨時鑰自存取點發射至一第二存取點以允許該第二存取點與一存取終端機通信；(c)在該存取點與該存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於一不同主鑰；及/或(d)自存取終端機接收一請求以將該安全通信自該存取點交遞至第二存取點；其

中用於產生第二臨時鑰之主鑰係至少部分基於不同主鑰。主鑰可為可基於一與存取終端機相關聯之頂層主鑰的成對主鑰。當起始一自存取點至第二存取點與存取終端機之通信交遞時，處理器可自主鑰產生第二臨時鑰。處理器可進一步經組態以：(a)在該存取點與該存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於該主鑰；(b)自存取終端機接收一請求以將該安全通信自該存取點交遞至第二存取點；及/或(c)將通信會話交遞至第二存取點。

處理器可進一步經組態以：(a)自主鑰產生一不同於第二臨時鑰之第三臨時鑰；及(b)命令將第二臨時鑰自存取點發射至一第三存取點以與存取終端機通信。第二臨時鑰亦可基於與第二存取點相關聯之至少一唯一第二存取點識別符，且第三臨時鑰亦係基於與第三存取點相關聯之至少一唯一第三存取點識別符。第二臨時鑰及第三臨時鑰可為暫態會話鑰。第三臨時鑰亦可基於由第二存取點所獲得之至少一偽隨機數。

亦提供一種方法，其用於：(a)在一第一存取點處自一主鑰產生一第二臨時鑰，該主鑰用於第一存取點與一存取終端機之間的通信；(b)將第二臨時鑰自第一存取點發射至一第二存取點以允許該第二存取點與存取終端機通信；(c)在第一存取點與存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於一不同主鑰；(d)自存取終端機接收一請求以將安全通信會話自第一

存取點交遞至第二存取點，其中用於產生第二臨時鑰之主鑰係至少部分基於不同主鑰；(e)在第一存取點與存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於主鑰；(f)自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點；及/或(g)將安全通信交遞至第二存取點。主鑰可為基於一與存取終端機相關聯之頂層主鑰的成對主鑰。可由第一存取點自存取終端機先前與之通信的第三存取點接收不同主鑰。另外，產生第二臨時主鑰可包含當起始與存取終端機之通信自第一存取點至第二存取點之交遞時產生第二臨時鑰。

該方法可進一步包含：(a)自主鑰產生一不同於第二臨時鑰之第三臨時鑰，及將該第三臨時鑰自第一存取點發射至一第三存取點以與存取終端機通信。第二臨時鑰亦可基於與第二存取點相關聯之至少一唯一第二存取點識別符，且第三臨時鑰亦係基於與第三存取點相關聯之至少一唯一第三存取點識別符。第二臨時鑰及第三臨時鑰可為暫態會話鑰。

因此，提供一裝置，其包含：(a)用於在一第一存取點處自一主鑰產生一第二臨時鑰之構件，該主鑰用於第一存取點與一存取終端機之間的通信；(b)用於將第二臨時鑰自第一存取點發射至一第二存取點以允許該第二存取點與存取終端機通信之構件；(c)用於自主鑰產生一不同於第二臨時鑰之第三臨時鑰的構件；(d)用於將第三臨時鑰自第一存取點發射至一第三存取點以與存取終端機通信的構件；(e)用

於起始自第一存取點至第二存取點之通信交遞之構件；(f)用於在第一存取點與存取終端機之間建立一受一第一臨時鑰保護之安全通信的構件，其中該第一臨時鑰係至少部分基於主鑰；(g)用於自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點的構件；及/或(h)用於將該安全通信交遞至第二存取點的構件。

該裝置可進一步包含：(a)用於在第一存取點與存取終端機之間建立一受一第一臨時鑰保護之安全通信的構件，其中該第一臨時鑰係至少部分基於一不同主鑰；及/或(b)用於自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點的構件；其中用於產生第二臨時鑰之主鑰係至少部分基於該不同主鑰。

該裝置亦可包含：(a)用於自主鑰產生一不同於第二臨時鑰之第三臨時鑰及將該第三臨時鑰自第一存取點發射至一第三存取點以與存取終端機通信的構件。第二臨時鑰亦可基於與第二存取點相關聯之至少一唯一第二存取點識別符，且第三臨時鑰亦係基於與第三存取點相關聯之至少一唯一第三存取點識別符。第二臨時鑰及第三臨時鑰可為暫態會話鑰。

一處理器可讀媒體包含可由一或多個處理器所使用之指令，該等指令包含：(a)用於在一第一存取點處自一主鑰產生一第二臨時鑰之指令，該主鑰用於第一存取點與一存取終端機之間的通信；(b)用於將該臨時鑰自第一存取點發射至一第二存取點以允許該第二存取點與存取終端機通信之

指令；(c)用於在第一存取點與存取終端機之間建立一受一第一臨時鑰保護之安全通信的指令，其中該第一臨時鑰係至少部分基於一不同主鑰；(d)用於自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點的指令；其中用於產生第二臨時鑰之主鑰係至少部分基於該不同主鑰；(e)用於在第一存取點與存取終端機之間建立一受一第一臨時鑰保護之安全通信的指令，其中該第一臨時鑰係至少部分基於主鑰；(f)用於自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點的指令；及/或(g)用於將安全通信交遞至第二存取點的指令。

可產生第二臨時鑰以起始自第一存取點至第二存取點之通信交遞。處理器可讀媒體亦可包括用於自主鑰產生一不同於第二臨時鑰之第三臨時鑰及將該第三臨時鑰自第一存取點發射至一第三存取點以與存取終端機通信的指令。

亦提供一包含一處理電路之處理器，該處理電路經組態以：(a)在第一存取點與存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於一不同主鑰；及/或(b)自存取終端機接收一請求以將安全通信會話自第一存取點交遞至第二存取點；其中用於產生第二臨時鑰之主鑰係至少部分基於該不同主鑰。該處理電路亦可經組態以自主鑰產生一不同於第二臨時鑰之第三臨時鑰且將該第三臨時鑰自第一存取點發射至一第三存取點以與存取終端機通信；其中第二臨時鑰亦係基於與第二存取點相關聯之至少一唯一第二存取點識別符，且第三臨時

鑰亦係基於與第三存取點相關聯之至少一唯一第三存取點識別符。在某些實施例中，處理電路亦可經組態以：(a)在第一存取點與存取終端機之間建立一受一第一臨時鑰保護的安全通信，其中該第一臨時鑰係至少部分基於主鑰；(b)自存取終端機接收一請求以將安全通信自第一存取點交遞至第二存取點；及/或(c)將安全通信交遞至第二存取點。

亦提供一存取點，其包含：一記憶體及一與該記憶體耦接之處理器。該處理器可經組態以：(a)自另一存取點接收一第一臨時鑰；(b)命令利用第一臨時鑰來與一存取終端機通信以保護該通信；(c)接收與存取終端機之通信將被交遞至一第二存取點的指示；(d)基於第一臨時鑰產生一第二臨時鑰；及/或(e)將該第二臨時鑰發送至第二存取點。該處理器可進一步經組態以在起始自另一存取點至該存取點之交遞以與存取終端機通信時自該另一存取點接收第一臨時鑰。第一臨時鑰可操作歷時一有限時段，且該處理器進一步經組態以接收一用於保護存取終端機與存取點之間的通信的主鑰並放棄利用第一臨時鑰。

亦提供一種方法，其包含：(a)在一第一存取點處自另一存取點接收一第一臨時鑰；(b)利用第一臨時鑰來與一存取終端機通信以保護該通信；(c)接收一與第一存取終端機之通信將被交遞至一第二存取點之指示；(d)基於第一臨時鑰產生一第二臨時鑰；及/或(e)將該第二臨時鑰發送至第二存取點。

第一臨時鑰可操作歷時一有限時段。該方法可進一步包

含：(a)接收一用於存取終端機與第一存取點之間的通信的主鑰且放棄利用第一臨時鑰；及/或(b)當起始自另一存取點至第一存取點之交遞以與存取終端機通信時，自該另一存取點接收第一臨時鑰。

因此，提供一裝置，其包含：(a)用於在一第一存取點處自另一存取點接收一第一臨時鑰之構件；(b)用於利用第一臨時鑰來與一存取終端機通信以保護該通信之構件；(c)用於接收一用於存取終端機與第一存取點之間的通信之主鑰的構件；(d)用於在起始自另一存取點至第一存取點之交遞以與存取終端機通信時自該另一存取點接收第一臨時鑰之構件；(e)用於接收一與第一存取終端機之通信將被交遞至一第二存取點之指示的構件；(f)用於基於第一臨時鑰產生一第二臨時鑰之構件；(g)用於將該第二臨時鑰發送至第二存取點的構件；及/或(h)用於放棄利用第一臨時鑰之構件。

亦提供一包含可由一或多個處理器使用之指令的處理器可讀媒體，該等指令包含：(a)用於在一第一存取點處自另一存取點接收一第一臨時鑰之指令；(b)用於利用第一臨時鑰來與一存取終端機通信以保護該通信之指令；(c)用於接收一與第一存取終端機之通信將被交遞至一第二存取點之指示的指令；(d)用於基於第一臨時鑰產生一第二臨時鑰之指令；及/或(e)用於將該第二臨時鑰發送至第二存取點的指令。當起始自另一存取點至第一存取點之交遞以與存取終端機通信時，可接收來自該另一存取點之第一臨時鑰。

亦提供一包含一處理電路之處理器，該處理電路經組態以：(a)在一第一存取點處自另一存取點接收一第一臨時鑰；及(b)利用該第一臨時鑰來與一存取終端機通信以保護該通信。第一臨時鑰可操作歷時一有限時段，且該處理電路可進一步經組態以接收一用於存取終端機與第一存取點之間的通信的主鑰且放棄利用第一臨時鑰。在某些實施例中，該處理電路可進一步經組態以在起始自另一存取點至第一存取點之交遞以與存取終端機通信時自該另一存取點接收第一臨時鑰。在其他實施例中，該處理電路亦可經組態以：(a)接收一與第一存取終端機之通信將被交遞至一第二存取點的指示；(b)基於第一臨時鑰產生一第二臨時鑰；及/或(c)將該第二臨時鑰發送至第二存取點。

亦可提供一存取終端機，其包含：一記憶體及一與該記憶體耦接之處理器。該處理器可經組態以：(a)自一主鑰產生一用於一第一存取點與存取終端機之間的通信的第一臨時鑰；(b)命令在一第二存取點與存取終端機之間利用第一臨時鑰來通信；(c)命令一鑑認伺服器提供另一主鑰用於與第二存取點通信且停止使用第一臨時鑰；及/或(d)提供與第二存取點之通信將被交遞至一第三存取點之指示。主鑰可為一用於一第一存取點與存取終端機之間的通信之第二臨時鑰。

處理器亦可經組態以：(a)自第一臨時鑰產生一用於第二存取點與存取終端機之間的通信之第二臨時鑰；及/或(b)命令在一第三存取點與存取終端機之間利用第二臨時鑰來

通信。

該處理器亦可經組態以：(a)自主鑰產生一第二臨時鑰；及/或(b)命令在一第三存取點與存取終端機之間利用該第二臨時鑰來通信。

在存取終端機之某些實施例中，該處理器可進一步經組態以：(a)掃描存取點；(b)將被識別之存取點添加至一組有效存取點；及/或(c)在將每一存取點添加至有效組時建立一與每一存取點之安全鑰。在一分布式鑰管理系統中，該處理器進一步經組態以在將每一存取點添加至有效組時產生一用於該每一存取點之暫態會話鑰，其中該暫態會話鑰係基於一與該有效組中之另一存取點相關聯之暫時主鑰。在一集中式鑰管理系統中，處理器可進一步經組態以在將每一存取點添加至有效組時產生一用於該每一存取點之暫態會話鑰，其中該暫態會話鑰係基於一主暫態鑰及該存取點之唯一存取點識別符。

亦提供一種可對一存取終端機進行操作之方法，其包含：(a)利用一主鑰來與一第一存取點通信；(b)自該主鑰產生一第一臨時鑰；(c)利用該第一臨時鑰來與一第二存取點通信；(d)命令一鑑認伺服器提供另一主鑰用於與第二存取點通信且停止使用第一臨時鑰；(e)提供一與第二存取點之通信將被交遞至一第三存取點之指示。主鑰可為一用於保護一第一存取點與存取終端機之間的通信之第二臨時鑰。主鑰可為與一鑑認伺服器共用之成對主鑰。

在某些實施例中，該方法亦可包含：(a)自第一臨時鑰產

生一用於第二存取點與存取終端機之間的通信之第二臨時鑰；及/或(b)命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信。

在其他實施例中，該方法亦可包含：(a)自主鑰產生一第二臨時鑰；及/或(b)命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信。

在其他實施例中，該方法可進一步包含：(a)掃描存取點；(b)將被識別之存取點添加至一組有效存取點；及/或(c)在將每一存取點添加至有效組時建立一與每一存取點之安全鑰。在一分布式鑰管理系統中，該方法可進一步包含當將每一存取點添加至有效組時產生一用於每一存取點之暫態會話鑰，其中該暫態會話鑰係基於一與該有效組中之另一存取點相關聯之暫時主鑰。在一集中式鑰管理系統中，該方法可進一步包含當將每一存取點添加至有效組時產生一用於每一存取點之暫態會話鑰，其中該暫態會話鑰係基於一主暫態鑰及該存取點之唯一存取點識別符。

因此，亦提供一存取終端機，其包含：(a)用於利用一主鑰來與一第一存取點通信之構件；(b)用於自主鑰產生一第一臨時鑰之構件；(c)用於利用該第一臨時鑰來與一第二存取點通信之構件；(d)用於命令一鑑認伺服器提供另一主鑰用於與第二存取點通信且停止使用第一臨時鑰之構件；及/或(e)用於提供一與第二存取點之通信將被交遞至一第三存取點之指示的構件。主鑰係一用於保護一第一存取點與存取終端機之間的通信之第二臨時鑰。

在某些實施例中，存取終端機可進一步包括：(a)用於自第一臨時鑰產生一用於第二存取點與存取終端機之間的通信之第二臨時鑰的構件；及/或(b)用於命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信之構件。

在某些實施例中，存取終端機可進一步包括：(a)用於自主鑰產生一第二臨時鑰之構件；及/或(b)用於命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信之構件。

亦提供一包含可由一或多個處理器使用之指令的處理器可讀媒體，該等指令包含：(a)用於利用一主鑰來自一存取終端機與一第一存取點通信之指令；(b)用於自主鑰產生一第一臨時鑰之指令；(c)用於利用該第一臨時鑰來與一第二存取點通信之指令；(d)用於提供一與第二存取點之通信將被交遞至一第三存取點之指示的指令。

在某些實施例中，處理器可讀媒體可進一步包括：(a)用於自第一臨時鑰產生一用於第二存取點與存取終端機之間的通信之第二臨時鑰的指令；及/或(b)用於命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信之指令。

在其他實施例中，處理器可讀媒體可進一步包括：(a)用於自主鑰產生一第二臨時鑰之指令；及/或(b)用於命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信之指令。

亦提供一包含一處理電路之處理器，該處理電路經組態以：(a)利用一主鑰來與一第一存取點通信；(b)自該主鑰

產生一第一臨時鑰；及/或(c)利用該第一臨時鑰來與一第二存取點通信。主鑰可為一用於保護一第一存取點與存取終端機之間的通信之第二臨時鑰。該處理電路亦可進一步經組態以命令一鑑認伺服器提供另一主鑰用於與第二存取點通信且停止使用第一臨時鑰。在某些實施例中，該處理電路亦可經組態以：(a)自第一臨時鑰產生一用於第二存取點與存取終端機之間的通信的第二臨時鑰；及/或(b)命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信。在另一實施例中，該處理電路亦可經組態以：(a)自主鑰產生一第二臨時鑰；(b)命令在一第三存取點與存取終端機之間利用第二臨時鑰來通信。在某些實施例中，該處理電路進一步經組態以：(a)掃描存取點；(b)將被識別之存取點添加至一組有效存取點；及(c)當將每一存取點添加至有效組時建立一與每一存取點之安全鑰。

【實施方式】

在以下描述中，將給出特定細節以提供對實施例之詳盡理解。然而，一般熟習此項技術者將理解，可在無此等特定細節之情況下實踐該等實施例。舉例而言，可在方塊圖中展示電路以便不會在不必要之細節方面混淆該等實施例。在其他例子中，可詳細展示熟知之電路、結構及技術以便不會混淆該等實施例。

又，應注意，可將該等實施例描述為描繪為流程圖、結構圖或方塊圖之過程。儘管一流程圖可將操作描述為連續過程，但可並行或同時執行該等操作中之許多者。另外，

可重新排列該等操作之次序。當完成一過程之操作時，終止該過程。一過程可對應於方法、函數、程序、子例程、子程式等等。當一過程對應於一函數時，其之終止對應於該函數返回至調用函數或主函數。

此外，儲存媒體可表示用於儲存資料之一或多個設備，其包括唯讀記憶體(ROM)、隨機存取記憶體(RAM)、磁碟儲存媒體、光學儲存媒體、快閃記憶體設備及/或用於儲存資訊之其他機器可讀媒體。術語"機器可讀媒體"包括(但不限於)攜帶型或固定儲存設備、光學儲存設備、無線通道及能夠儲存、容納或承載(一或多個)指令及/或資料之各種其他媒體。

此外，實施例可由硬體、軟體、韌體、中間體、微碼或其任何組合來實施。當以軟體、韌體、中間體或微碼來實施時，可將用以執行必要任務之程式碼或碼段儲存於機器可讀媒體(諸如儲存媒體或其他儲存器)中。處理器可執行該等必要任務。碼段可表示程序、函數、子程式、程式、例程、子例程、模組、軟體封裝、類別或者指令、資料結構或程式語句之任何組合。可藉由傳遞及/或接收資訊、資料、引數、參數或記憶體內容而將碼段耦接至另一碼段或硬體電路。可經由任何合適之方式(包括記憶體共用、訊息傳遞、符記傳遞、網路發射等等)來傳遞、轉發或發射資訊、引數、參數、資料等等。

一特徵提供一用於存取終端機(例如，行動終端機、無線使用者終端機等等)與一或多個存取點(例如，基地台等

等)之間的鑰管理的系統及方法。詳言之，提供一用於建立存取終端機與存取點之間的安全通信而不存在曝露用於該存取終端機之主鑰之危險的機制。此方法導出用於一新存取點與該存取終端機之間的低潛時交遞及安全鑑認之臨時主鑰。

在一態樣中，提供一分布式管理機制，其中一當前存取點產生一由一存取終端機與之通信之下一存取點所使用的新安全鑰。當存取終端機自當前存取點移至一新存取點時，該當前存取點基於其自身之安全鑰及該新存取點之唯一識別符產生一新安全鑰。接著將該新安全鑰發送至該新存取點。存取終端機獨立地產生其可藉以與該新存取點安全地通信之相同新安全鑰。

在另一態樣中，提供一集中式鑰管理機制，其中一鑑認器保持、產生新安全鑰並將其分配給存取點。當存取終端機自一當前存取點移至一新存取點時，鑑認器基於一主安全鑰(與存取終端機相關聯)及該新存取點之唯一識別符產生一新安全鑰。接著將該新安全鑰發送至該新存取點。當存取終端機切換至其他存取點時，鑑認器重複此過程。存取終端機獨立地產生其可藉以與新存取點安全地通信之相同新安全鑰。

又一特徵提供一存取終端機，該存取終端機經組態以建立及/或保持其可與之通信之一組有效存取點。由存取終端機保持一組有效鑰，而非在存取終端機移至一新存取點時獲得或協商新鑰。亦即，存取終端機可同時保持或建立

與一扇區、區域或地區內之複數個存取點的安全關聯(例如，鑰)。存取終端機可隨後使用預先建立之安全鑰來與其有效組中之存取點通信而無需重新建立一安全關係。可藉由集中式或分布式鑰管理方法而獲得此等鑰。

圖1說明一具有促進安全、低潛時通信會話交遞之分布式鑰管理的無線通信系統。多重存取無線通信系統100可包括多個小區(例如，小區102、104及106)。每一小區102、104及106可包括一提供至該小區內之多個扇區之覆蓋的存取點110、112及114。每一存取點110、112及114可包括跨越一小區中之多個扇區而提供至行動終端機(例如，使用者終端機)之網路覆蓋的一或多個天線116。舉例而言，在小區102中，存取點110包括一群天線116，其中每一天線提供至小區102內之一不同扇區的網路覆蓋。類似地，在小區104及106中，存取點112及114可包括若干群天線，其中每一天線提供至一小區內之一不同扇區的網路覆蓋。

每一小區102、104及106內之存取點110、112及114可將網路連接服務提供至一或多個存取終端機。舉例而言，當存取終端機118移動跨越不同小區102、104、106時，其可與存取點110、112及114通信。於本文中使用時，將自存取點至存取終端機之發射稱作前向鏈路或下行鏈路，而將自存取終端機至存取點之發射稱作反向鏈路或上行鏈路。

一鑑認器120可用於管理存取點110、112及114之操作及/或鑑認存取終端機。在某些應用中，鑑認器120可保持

與由網路100所服務之存取終端機唯一地相關聯之頂層主鑰。可將主鑰(master key, MK)保持於鑑認器120與其所服務之存取終端機之間。舉例而言，一第一頂層主鑰MK已為鑑認器120及存取終端機118所知，且與該存取終端機唯一地相關聯。在實施一可擴展鑑認協定(extensible authentication protocol, EAP)之情況下，通常將此頂層主鑰(MK)稱作一主會話鑰(master session key, MSK)。應理解，無論在什麼情況下使用術語"主鑰"，其皆可包括用於EAP實施之此MSK。

在各種應用中，鑑認器120可為遠離存取點110、112及114的網路控制器、基地台控制器或存取點控制器之部分，或其可與該等存取點中之一者共處在一地。

在某些態樣中，每一存取終端機可與一或多個小區之兩個或兩個以上扇區通信。可完成此以便在一存取終端機移動或行進時為獲得恰當容量管理及/或為了其他原因而允許在不同扇區或小區之間進行交遞。

於本文中使用時，存取點可為用於與存取終端機通信之固定台，且亦可被稱作基地台、節點B或某一其他術語且包括基地台、節點B或該某一其他術語之一些或所有功能性。存取終端機亦可被稱作使用者裝備(UE)、無線通信設備、終端機、行動終端機、行動台或某一其他術語且包括使用者裝備(UE)、無線通信設備、終端機、行動終端機、行動台或該某一其他術語之一些或所有功能性。

本文中所描述之發射技術亦可用於各種無線通信系統

(諸如，CDMA系統、TDMA系統、FDMA系統、正交分頻多重存取(OFDMA)系統、單載波FDMA(SC-FDMA)系統等等)。OFDMA系統利用正交分頻多工(OFDM)，該OFDM係一將整個系統頻寬分割為多個(K)正交副載波之調變技術。此等副載波亦稱為載頻調、子載波(bin)等等。就OFDM而言，每一副載波可使用資料來獨立調變。SC-FDMA系統可利用交錯FDMA(IFDMA)以在跨越系統頻寬而分布之副載波上進行發射、可利用區域化FDMA(LFDMA)以在一鄰近副載波區塊上進行發射或可利用增強型FDMA(EFDMA)以在多個鄰近副載波區塊上進行發射。通常，在頻域中使用OFDM且在時域中使用SC-FDMA來發射調變符號。

本文中所描述之實例中之一些係關於在存取點及存取終端機處提供成對主鑰MK之可擴展鑑認協定(EAP)。可經由充當鑑認器之存取點來在存取終端機與鑑認伺服器之間(例如，在網路控制器、AAA伺服器等等中)完成EAP鑑認；在某些狀況下，鑑認器自身可充當鑑認伺服器。在某些例子中，鑑認器可與一或多個存取點共處在一地。

在存取點與存取終端機之間建立及保持一暫態會話鑰(Transient Session Key, TSK)。可計算(例如，基於主鑰MK或用於EAP應用之MSK)TSK以保護存取終端機與存取點之間的通信。舉例而言，可如下計算TSK：TSKn=PRF(MKn, Data)，其中PRF係一偽隨機函數(諸如，HMAC-SHA-256或AES-128-CMAC)或另一鑰導出函數，且Data可為參數

(如存取點識別符(AP_ID)、存取終端機識別符(AT_ID)、由某一方產生之隨機數或甚至一靜態串)。Data參數可根據系統設計而知曉或可在會話期間加以傳達。在此方法中，在TSK導出中不使用動態變數，且因此除用於TSK之EAP或EAP重新鑑認之外不需要鑰交換。

通常，存取點與存取終端機之間的通信會話使用某一類型之加密以在發射期間保護資料(例如，使用一鑰加密機制)。然而，在將通信自當前存取點交遞至一新存取點期間，存在如何藉由經由無線電來發射存取點之間的鑰或其他加密產生值而繼續與新存取點之受保護通信而不損害通信會話的問題。由於應與新存取點建立一新暫態會話鑰(TSK)，所以應首先在該新存取點與存取終端機之間建立一新主鑰(MK)。另外，較佳避免在存取點中共用會話鑰，因為此引入了一弱點：一存取點之損害導致與該被損害之存取點進行鑰共用的存取點受到損害。然而，協商交遞之關鍵路徑中之新暫態會話鑰增加了交遞潛時。因此，需要提供一用於每一存取點及存取終端機對之安全、低潛時會話鑰。

根據一特徵，提供一分布式鑰管理機制，其中一當前存取點產生一由下一存取點用以在交遞之後與一行動終端機通信之暫時主會話鑰(interim master session key, I-MK)。舉例而言，存取終端機118a可使用一受保護之第一暫時主鑰I-MK1來保護與其當前存取點110之通信。該第一暫時主鑰I-MK1可基於頂層主鑰Mko(已為鑑認器120及存取終端

機118所知，且與存取終端機118唯一地相關聯)。當存取終端機118b移至一不同扇區或小區時，其通信會話可能會被交遞至一新存取點112。為在交遞之後立即保護存取終端機118b與新存取點112之間的通信，當前存取點110基於其受保護之第一暫時主鑰I-MK1產生一第二暫時主鑰I-MK2且將此新主鑰I-MK2提供至新存取點112。該新存取點112接著使用第二頂層主鑰I-MK2用於其與存取終端機118b之通信會話。可使用第二暫時主鑰I-MK2歷時一延長之時段或直至獲得另一暫時主鑰以保護通信會話。儘管第二暫時主鑰I-MK2可基於第一暫時主鑰I-MK1而產生，但其並非一頂層主鑰。因此，並不經由無線電或經由有線鏈路來發射與存取終端機118相關聯之頂層主鑰Mko。一旦已在存取點與存取終端機之間建立暫時主鑰，便可使用該暫時主鑰來導出一暫時暫態會話鑰(interim transient session key, I-TSK)。

圖2(包含圖2A及圖2B)係一流程圖，其說明一具有促進安全、低潛時交遞之分布式鑰管理的無線通信系統之操作。在此實例中，為說明之目的而使用圖1之鑑認器120、存取點A 110、存取終端機118及存取點B 112。鑑認器120與存取終端機118可各自儲存一與存取終端機118唯一地相關聯之頂層主鑰MKo 202及204。存取終端機118亦可保持一用於使一存取點與一唯一序列號相關聯之序列號清單206。

存取終端機118可收聽識別局部存取點之廣播(208)。在

一實例中，存取終端機可基於其與附近任何其他存取點相比之信號強度而選擇一存取點A 110。存取終端機118使存取點A 110之存取點識別符AP_ID_A與一唯一序列號SQN-A相關聯。存取終端機118接著使用識別符AP_ID_A及SQN-A而請求與存取點A 110之通信鏈路(212)。鑑認器120及存取終端機118皆可至少部分基於頂層主鑰Mko及所指派之序列號SQN-A產生一暫時主鑰I-MK1(214及216)。注意，由於在分布式鑰管理模型中，每一I-MKn係基於一不同之先前I-MK(n-1)，所以序列號SQN-A無需在所有I-MK之導出中係唯一的。鑑認器120接著將其暫時主鑰I-MK1發送至存取點A(218)。存取點A 110及存取終端機118接著根據暫時主鑰I-MK1及(可能之)其他資料產生一暫時暫態會話鑰(I-TSK1)(220及222)。舉例而言，在某些實施例中，此其他資料可包括一由存取終端機118及/或當前存取點A 110產生及/或供應之隨機數。因而，可在存取點及/或存取終端機之間實施一協定以在導出I-TSK1之前(或同時)導出、產生及/或交換此隨機數。可接著使用會話鑰I-TSK1而在存取點A 110與存取終端機118之間安全地建立通信(224)。

存取終端機118可繼續收聽來自局部存取終端機之廣播(226)以判定是否應發生與一新存取點B之交遞(228)。亦即，當存取終端機118漫遊或移至一不同扇區或小區中時，或自另一存取點偵測到一較強信號時，可能需要至新存取點之交遞。若存取終端機118決定自當前存取點A 110

至新存取點112進行交遞，則其使一序列號SQN-B與新存取點識別符AP_ID_B相關聯(230)。亦即，與新存取點B 112相關聯之序列號SQN-B與當前存取點A 100相關聯之序列號SQN-A係連續的。此等序列號之使用允許當前存取點A 110及存取終端機118獨立或分別地產生新暫時主鑰I-MK2。

存取終端機118接著請求使用識別符AP_ID_B及SQN-B而將一通信會話交遞至新存取點B 112(232)。在某些實施例中，鑑認器120可回應於該交遞請求而將指示當前通信會話將被交遞至新存取點B 112之訊息發送至當前存取點A 110(234)。當前存取點A 110及存取終端機118皆可至少部分基於當前暫時主鑰I-MK1及與新存取點B相關聯之序列號SQN-B產生一新暫時主鑰I-MK2(236及238)。當前存取點110接著將該新暫時主鑰I-MK2發送至新存取點B(240)。

新存取點B 112及存取終端機118接著根據新暫時主鑰I-MK2及(可能之)其他資料產生一新暫時暫態會話鑰(I-TSK2)(242及244)。舉例而言，在某些實施例中，此其他資料可包括由存取終端機118、當前存取點A 110或新存取點B 112產生及/或供應之隨機數。因而，可在存取點及/或存取終端機之間實施一協定以在I-TSK2之導出之前(或同時)導出、產生及/或交換此隨機數。可接著使用新暫時會話鑰I-TSK2來在存取點B 112與存取終端機118之間繼續安全通信會話(246)。因此，存取終端機118與存取點A 110之間的通信被終止(248)。

可多次重複將一通信會話自一存取點安全地交遞至另一存取點之過程。舉例而言，在圖1中，存取終端機118可自當前小區104漫遊或移至一新小區106且試圖將一會話自當前存取點B 112交遞至一新存取點C 114。存取終端機118使一序列號SQN-C與新存取點C 114相關聯，且將該SQN-C提供至當前存取點B 112。當前存取點B 112接著基於當前暫時主鑰I-MK2及SQN-C產生一新暫時主鑰I-MK3，且將該新暫時主鑰I-MK3發送至新存取點C 114。存取終端機118可獨立地產生其自身型式之新暫時主鑰I-MK3。存取終端機118及新存取點C 114可接著產生一可用於繼續其間之安全通信會話的新暫時暫態會話鑰I-TSK3。

圖3說明可用於在交遞期間及/或之後保護存取終端機與新存取點之間的通信會話的安全鑰之分布式模型。當一存取終端機想要附接至一新存取點時，當前存取點APn產生一用於新存取點AP(n+1)之新暫時主鑰I-MK(n+1)。根據一態樣，新暫時主鑰I-MK(n+1)可根據當前暫時主鑰I-MKn及可能之其他參數(諸如新存取點識別符(AP_ID)、存取終端機識別符(AT-ID)、由某一方所產生之隨機數、由存取終端機所提供之序列號SQN-n及/或甚至一靜態串)而產生。新存取點AP(n+1)及存取終端機可接著使用新暫時主鑰I-MK(n+1)來產生及/或協商一用於保護其間之通信的暫態會話鑰。在重新建鑰之後，存取終端機停止使用其先前鑰I-MKn及I-TSKn。

新暫時主鑰I-MK(n+1)可精確地用作新存取點AP(n+1)與

存取終端機之間的頂層主鑰(MKo)，但其限於一特定存取終端機與存取點對。可在一通信會話交遞之後立即使用新暫時主鑰I-MK(n+1)。此在保護此通信會話之同時提供現有通信會話之低潛時交遞。在各種實施例中，可在交遞之後在一較短時間內使用新暫時主鑰I-MK(n+1)，或可無限期地使用新暫時主鑰I-MK(n+1)以保護存取終端機與新存取點AP(n+1)之間的通信。在某些應用中，可隨後經由存取點執行對存取終端機之EAP鑑認或重新鑑認以便降低損害通信會話之可能性。或者，新暫時主鑰I-MK(n+1)可作為一頂層主鑰(在新存取點AP(n+1)內)而操作，且在需要通信會話之進一步交遞的情況下用於產生用於其他存取點之額外暫時主鑰。因此，在如何將暫時主鑰I-MK與頂層主鑰MK用於保護通信之間可能無差別。

在先前技術方法中，可在所有存取點中共用一存取終端機之相同頂層主鑰(MKo)以保護與該存取終端機之通信會話。若頂層主鑰MKo在該等存取點中之任一者處受到損害，則其將損害該存取終端機與所有其他存取點之間的所有通信會話。使用暫時主鑰I-MK之一優勢在於，在一暫時主鑰I-MKn在一存取點處受到損害之情況下，其他存取點之暫時主鑰I-MK1...I-MKn-1或MKo並未受到損害。此係因為每一暫時主鑰對於一特定存取終端機與存取點對而言係唯一的。

於圖1至圖3及本文描述中使用時，暫時主鑰(I-MK)及暫時暫態會話鑰(I-TSK)亦可被稱作臨時鑰，因為其對於一

特定存取點/存取終端機對而言係特定的，及/或其僅在一通信會話被交遞之後的一有限時間量內使用。在某些實施例中，亦可在一延長之時段內使用此等臨時鑰，直至通信會話被交遞至另一存取點或通信會話結束。

圖4說明一具有促進安全、低潛時交遞之集中式鑰管理的無線通信系統。與圖1、圖2及圖3中所描述之分布式鑰管理方法相比，由集中式實體來執行鑰管理。多重存取無線通信系統400可包括多個小區(例如，小區402、404及406)。每一小區402、404及406可包括一提供至該小區內之多個扇區之覆蓋的存取點410、412及414。每一小區402、404及406內之存取點410、412及414可將網路連接服務提供至一或多個存取終端機。舉例而言，當一存取終端機418移動跨越不同小區402、404、406時，其可與存取點410、412及414通信。一鑑認器420可用於管理存取點410、412及414之操作及/或管理對存取終端機之鑰鑑認。在某些應用中，鑑認器420可保持與由網路400服務之存取終端機唯一地相關聯之頂層主鑰。舉例而言，一第一頂層主鑰MKo已為鑑認器420及存取終端機418所知，且與存取終端機418唯一地相關聯。在各種應用中，鑑認器420可為遠離存取點410、412及414的網路控制器之部分，或其可與該等存取點中之一者共處在一起。每一存取終端機可與一或多個小區之兩個或兩個以上扇區通信。此可為了獲得恰當之容量管理及/或為了其他原因而在一存取終端機418移動或行進時允許在不同扇區或小區之間交遞通信會話。

為將一通信會話自第一存取點安全地交遞至第二存取點，鑑認器420經組態以與存取終端機418協商一主暫態鑰(master transient key, MTK)。舉例而言，當初次建立一通信會話時，鑑認器420及存取終端機418可使用頂層主鑰MKo來建立主暫態鑰(MTK)。鑑認器420可接著(至少部分)基於主暫態鑰(MTK)、存取終端機識別符(AT_ID)及/或存取點識別符(AP_ID)產生用於存取點410、412及414之暫態會話鑰(TSK)。該等暫態會話鑰(TSK)可由鑑認器420一起產生及/或分配或當需要該等暫態會話鑰(TSK)來將一會話交遞至一新存取點時而加以產生及/或分配。存取終端機418可在每次其將一會話交遞至一新存取點時類似地產生一新暫態會話鑰。

圖5(包含圖5A及圖5B)係一流程圖，其說明一具有促進安全、低潛時交遞之集中式鑰管理的無線通信系統之操作。在此實例中，為說明之目的而使用圖4之鑑認器420、存取點A 410、存取終端機418及存取點B 412。鑑認器420及存取終端機418可各自儲存一與存取終端機418唯一地相關聯之頂層主鑰MKo 502及504。鑑認器420及存取終端機418亦可經由一3向鑰交換而協商一主暫態鑰(MTK)(及可能之MTK識別符MTK_ID)。該MTK可(至少部分)基於頂層主鑰MKo及/或存取終端機識別符(AT_ID)(506)。可藉由鑑認器420及存取終端機418來安全地保持MTK。

在某些實施例中，MTK導出亦可包括一由存取終端機418及/或鑑認器420產生及/或供應之隨機數。因而，可在

鑑認器420及/或存取終端機418之間實施一協定以在MTK導出之前(或同時)導出、產生及/或交換此隨機數。

存取終端機418可收聽識別局部存取點之廣播(508)。在一實例中，存取終端機418可基於其與附近任何其他存取點相比之信號強度而選擇一存取點A 410。存取終端機418請求使用識別符AP_ID_A來建立與存取點A 410之通信會話(510)。鑑認器420及存取終端機418皆可至少部分基於主暫態鑰MTK及可能之存取點識別符AP_ID_A、存取終端機識別符(AT_ID)及/或其他資料來產生一暫態會話鑰TSK1(514及516)。可使用一偽隨機函數(PRF)或其他合適之鑰導出函數來產生一暫態會話鑰TSKn。由於暫態會話鑰TSK係使用一共同MTK而產生，所以至少AP_ID或每一TSK之導出中所使用之資料對於一特定存取點與存取終端機對而言係唯一的。鑑認器420接著將暫態會話鑰TSK1發送至存取點A(518)。可接著使用會話鑰TSK1而在存取點A 410與存取終端機418之間安全地建立一通信會話(520)。

在某些實施例中，TSK導出亦可包括額外資料，諸如由存取終端機418及/或鑑認器420產生及/或供應之隨機數。因而，可在鑑認器420、存取點410及/或存取終端機418之間實施一協定以在TSK導出之前(或同時)導出、產生及/或交換此隨機數。

存取終端機418可繼續收聽來自局部存取終端機之廣播(526)以判定是否應發生與一新存取點B之交遞(528)。亦即，當存取終端機418漫遊或移至一不同扇區或小區中或

自另一存取點偵測到一較強信號時，可能需要至一新存取點B 412之交遞。若存取終端機418決定自當前存取點A 410至新存取點B 412進行交遞，則其請求使用一存取點識別符AP_ID_B來將通信會話交遞至新存取點B 412(532)。鑑認器420及存取終端機418皆可至少部分基於當前主暫態鑰MTK及/或存取點識別符AP_ID_B而獨立地產生一新暫態會話鑰TSK2(536及538)。鑑認器420接著將新暫態會話鑰TSK2發送至新存取點B(540)。可接著使用新會話鑰TSK2而在存取點B 412與存取終端機418之間繼續安全通信會話(542)。因此，存取終端機418與存取點A 410之間的通信被終止(544)。

可多次重複將一通信會話自一存取點安全地交遞至另一存取點之過程。舉例而言，在圖4中，存取終端機418可自當前小區404漫遊或移至一新小區406且試圖將通信會話自當前存取點B 412交遞至一新存取點C 414。存取終端機418可請求至與存取點識別符AP_ID_C相關聯之新存取點的交遞。鑑認器420接著(至少部分)基於主暫態鑰MTK產生一新暫態會話鑰TSK3，且將該暫態會話鑰TSK3發送至新存取點C 414。存取終端機418可獨立地產生其自身型式之新暫態會話鑰TSK3。存取終端機418及新存取點C 414可接著使用新暫態會話鑰TSK3來繼續其間之安全通信會話。

圖6說明一用於在交遞期間及/或之後保護存取終端機與新存取點之間的通信會話的安全鑰之一集中式模型。在此

集中式模型中，鑑認器(例如，網路控制器、鑑認伺服器等等)及存取終端機(至少部分)基於一與該存取終端機唯一地相關聯之頂層主鑰MKo而協商一主暫態鑰(MTK)。鑑認器產生、管理暫態會話鑰及/或將其分配給每一存取點。因為僅協商暫態主鑰MTK一次(例如，當存取終端機及鑑認器初次起始通信時)，所以此加速了產生會話鑰之過程。又，即使暫態主鑰MTK被損害，其並不會損害頂層主鑰MKo。此外，由於頂層主鑰MKo或主暫態鑰MTK皆未分配給存取點(例如，僅暫態會話鑰被分配)，所以其降低了在一存取點被損害之情況下損害安全之危險。

此集中式鑰管理提供現有通信會話之低潛時交遞，因為由於頂層主鑰MKo或主暫態鑰MTK皆未分配給存取點，所以在保護通信會話的同時由鑑認器產生並提供暫態會話鑰。

在各種實施例中，可在交遞之後在一較短時間內使用新暫態會話鑰TSKt或可無限期地使用新暫態會話鑰TSKt以保護存取終端機與新存取點AP-t之間的通信。在某些應用中，可隨後經由存取點執行對存取終端機EAP鑑認或重新鑑認(例如，以更新MTK)，以便降低損害通信會話之可能性。

於圖4至圖6及本文描述中使用時，主暫態鑰(MTK)及暫態會話鑰(TSK)亦可被稱作臨時鑰，因為其對於一特定存取點/存取終端機對而言係特定的。在鑑認器(其亦可為一存取點)與存取終端機之間使用MTK。在存取點與存取終

端機之間使用TSK。在某些實施例中，亦可使用此等臨時鑰歷時一較短時段(直至在存取終端機與存取點之間協商一安全鑰)或歷時一延長之時段(例如，直至通信會話被交遞至另一存取點或通信會話結束)。

儘管圖1至圖6中所說明之實例通常係關於在將通信自當前存取點交遞至一新存取點之上下文中實施分布式及集中式鑰管理機制，但此等鑰管理方法皆可在其他上下文中加以實施。在一實例中，由一存取終端機保持一組有效鑰，而非在該存取終端機移至一新存取點時獲得或協商新鑰。亦即，存取終端機可同時建立與扇區、區域或地區內之複數個存取點的安全關聯(例如，鑰)。存取終端機與之保持此等同時安全關聯(例如，鑰)之存取點被稱作存取點之"有效組"。每次將一新存取點添加至存取終端機之有效組時，該存取終端機與該新存取點可建立一安全鑰。舉例而言，存取終端機與新存取點可建立一暫時主鑰(I-MK)(在分布式鑰管理方法之狀況下)或一暫態會話鑰(TSK)(在集中式鑰管理方法之狀況下)。

在於一組有效存取點之上下文中實施分布式鑰管理方法之情況下，用於一新存取點之暫時主鑰(I-MKn)可基於用於被添加至有效組之先前存取點之先前主鑰(I-MK(n-1))。在此組態中，存取終端機可請求先前存取點將其IMK(n-1)發送或提供至新存取點。

在於一組有效存取點之上下文中實施集中式鑰管理方法之情況下，存取終端機可針對新存取點而藉由鑑認器來簡

單地導出一新暫態會話鑰(TSK)，且使鑑認器將其提供至該新存取點。

在分布式鑰管理方法(說明於圖1至圖3中)或集中式鑰管理方法(說明於圖4至圖6中)中使用一組有效存取點使得存取終端機能夠快速地切換與其有效組中之存取點的通信。

圖7係一方塊圖，其說明一經組態以執行低潛時安全通信會話交遞之存取終端機。存取終端機702可包括一耦接至無線通信介面706以經由無線網路而通信之處理電路704，及一用以儲存一唯一頂層主鑰MKo(與存取終端機相關聯)及與所識別之存取點相關聯之一序列號清單的儲存設備708。處理電路704可經組態以安全地交遞一正在進行之通信會話而無該通信會話之明顯中斷。處理電路704(例如，處理器、處理模組等等)可包括一經組態以產生可用於保護一通信會話之一或多個鑰的鑰產生器模組。

圖8係一流程圖，其說明一可使用分布式鑰管理方法在一存取終端機中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。起初，可使用至少一頂層主鑰(與存取終端機相關聯)及一與第一存取點相關聯以產生藉以獲得第一暫態會話鑰之第一暫時主鑰的第一序列號來建立與該第一存取點之安全通信會話(802)。第一暫時主鑰對於特定存取終端機與第一存取點組合而言可為唯一的。存取終端機可接著收聽來自局部存取點之廣播(804)。若一第二存取點被識別，則存取終端機判定是否應將現有通信會話自第一存取點交遞至第二存取點(806)。此可藉由在信號

強度及/或品質方面來比較第一存取點與第二存取點來判定。存取終端機可判定繼續與第一存取點之通信會話(808)。另外，存取終端機可選擇起始現有通信會話至第二存取點之交遞(810)。一第二序列號可與第二存取點相關聯且可被發送至第一存取點(812)。存取終端機基於第一暫時主鑰及第二序列號來產生一第二暫時主鑰，且獲得一第二暫態會話鑰(814)。存取終端機接著將安全通信會話自第一存取點交遞至第二存取點，且使用第二暫態會話鑰對其加以保護(816)。可多次重複此交遞過程，其中每一當前存取點產生用於下一存取點之新暫時主鑰。

圖9係一流程圖，其說明一可使用集中式鑰管理方法在一存取終端機中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。起初，可藉由一鑑認器來基於與存取終端機相關聯之至少一頂層主鑰來安全地建立一主暫態鑰(902)。可使用基於主暫態鑰所產生之至少一唯一第一暫態會話鑰及一與第一存取點相關聯之第一存取點識別符來建立與第一存取點之安全通信會話(904)。存取終端機可接著收聽來自局部存取點之廣播(906)。若第二存取點被識別，則存取終端機判定是否應將現有通信會話自第一存取點交遞至第二存取點(908)。此可藉由在信號強度及/或品質方面來比較第一存取點與第二存取點來判定。存取終端機可判定繼續與第一存取點之通信會話(910)。另外，存取終端機可選擇起始現有通信會話至第二存取點之交遞(912)。可基於一與第二存取點相關聯之第二存取點識別符

及主暫態鑰產生一第二暫態會話鑰(914)。存取終端機接著將安全通信會話自第一存取點交遞至第二存取點，且使用第二暫態會話鑰對其加以保護(916)。可藉由使用主暫態鑰及一用以產生下一暫態會話鑰之新存取點識別符來多次重複此交遞過程。

圖10係一方塊圖，其說明一經組態以促進低潛時安全通信會話交遞之鑑認器。鑑認器1002可包括一耦接至一通信介面1006以經由一網路進行通信之處理電路1004，及一用以儲存一唯一頂層主鑰MKo(與一存取終端機相關聯)之儲存設備1008。處理電路1004可經組態以促進一正在進行之通信會話自一存取點至一存取終端機之安全交遞而無該通信會話之明顯中斷。處理電路1004(例如，處理器、處理模組等等)可包括一經組態以產生可用於保護一通信會話之一或多個鑰的鑰產生器模組。在各種應用中，鑑認器1002可定位於一網路控制器處，或者其可與一或多個存取點共處在一地。

圖11係一流程圖，其說明一可使用一分布式鑰管理方法在一鑑認器中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。鑑認器自一存取終端機接收一請求以建立與第一存取點之安全通信會話(1102)。其接著基於一與該存取終端機相關聯之頂層主鑰及一與該第一存取點相關聯之第一序列號(例如，自存取終端機接收)產生一第一暫時主鑰(1104)。鑑認器接著將第一暫時主鑰發送至第一存取點(1106)。隨後，可自存取終端機接收另一請求

以將通信會話自第一存取點交遞至第二存取點(1108)。鑑認器可向第一存取點指示其應基於第一暫時主鑰及一與第二存取點相關聯之第二序列號(例如，自存取終端機接收)產生一第二暫時主鑰(1110)。

圖12係一流程圖，其說明一可使用集中式鑰管理方法在一鑑認器中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。鑑認器自一存取終端機接收一請求以建立與第一存取點之安全通信會話(1202)。鑑認器基於一與存取終端機相關聯之頂層主鑰產生一主暫態鑰(1204)。由鑑認器至少基於主暫態鑰及一第一存取點識別符產生一第一暫態會話鑰(1206)。由鑑認器將第一暫態會話鑰發送至第一存取點(1208)。隨後，可由鑑認器接收來自存取終端機之另一請求以將安全通信會話自第一存取點交遞至第二存取點(1210)。至少基於主暫態鑰及一第二存取點識別符產生一第二暫態會話鑰(1212)。鑑認器接著將第一暫態會話鑰發送至第一存取點(1214)。

圖13係一方塊圖，其說明一經組態以促進低潛時安全通信會話交遞之存取點。存取點1302可包括一耦接至一無線通信介面1306以與一或多個存取終端機通信之處理電路1304、一用以與鑑認器及/或其他存取點通信之通信介面1310及一用以儲存一唯一頂層主鑰MKo(與存取終端機相關聯)之儲存設備1308。處理電路1304可經組態以促進一正在進行之通信會話自存取點1302至存取終端機之安全交遞而無該通信會話之明顯中斷。處理電路1304(例如，處

理器、處理模組等等)可包括一經組態以產生可用於保護一通信會話之一或多個鑰的鑰產生器模組。

圖14係一方塊圖，其說明一具有一整合式鑑認器之存取點1402之一替代性實施例。存取點1402可包括許多與圖13中之存取點1302相同之組件，但並非經由其通信介面1310與鑑認器通信，鑑認器1412與存取點1402共處在一地。鑑認器1412及存取點1402可如圖1至圖12及圖15至圖17中所說明而操作。

圖15係一流程圖，其說明一可使用一分布式鑰管理方法在第一存取點中操作以促進自該第一存取點至一第二存取點之安全通信會話交遞的方法。在建立一安全通信會話的過程中，第一存取點可自鑑認器接收第一暫時主鑰，其中該第一暫時主鑰係基於一與存取終端機相關聯之頂層主鑰及一與第一存取點相關聯之唯一第一序列號(1502)。第一存取點基於第一暫時主鑰產生一第一暫態會話鑰(1504)。其接著使用該第一暫態會話鑰建立與存取終端機之安全通信會話(1506)。隨後，第一存取點可接收通信會話將被交遞至一第二存取點的一指示連同一與第二存取點相關聯之唯一第二序列號(1508)。第一存取點基於第一暫時主鑰及第二序列號產生一第二暫時主鑰(1510)，且將該第二暫時主鑰發送至第二存取點(1512)。其可接著將通信會話交遞至第二存取點(1514)。可多次重複此交遞過程，其中每一當前存取點基於當前暫時主鑰來產生用於下一存取點之新暫時主鑰。新存取點可接著使用新暫時主鑰來產生一新暫

態會話鑰。

圖16係一流程圖，其說明一可使用集中式鑰管理方法在第一存取點中操作以促進自該第一存取點至一第二存取點之安全通信會話交遞的方法。第一存取點自存取終端機接收一請求以建立與第一存取點之安全通信會話(1602)。其接著自一鑑認器獲得一第一暫態會話鑰(1604)。第一存取點可接著使用第一暫態會話鑰來建立與存取終端機之安全通信會話(1606)。隨後，第一存取點可自存取終端機接收一請求以將安全通信會話交遞至一第二存取點(1608)。此導致第一存取點向鑑認器指示通信會話將被交遞至第二存取點(1610)。可接著將通信會話交遞至第二存取點(1612)。

圖17係一流程圖，其說明一可在一存取終端機中操作以獲得及/或建立一組有效存取點之方法。存取終端機可掃描存取點(1702)。當一新存取點被識別時，存取終端機將其添加至其存取點之有效組(1704)。當將每一存取點添加至該有效組時，存取終端機可建立一與每一存取點之安全鑰(1706)。

在分布式鑰管理方法中，用於每一存取點之安全鑰可包括基於一與有效組中之另一存取點相關聯之暫時主鑰產生一暫態會話鑰(1708)。舉例而言，此暫時主鑰可已如圖1至3及/或圖8中所說明而產生。

在集中式鑰管理方法中，用於每一存取點之安全鑰可包括基於一主暫態鑰及有效組中之存取點之唯一存取點識別

符產生一暫態會話鑰(1710)。舉例而言，此主暫態鑰可已如圖4至6及/或圖9中所說明而產生。

存取終端機可起始與有效組中之第一存取點的通信會話，其中使用一與第一存取點相關聯之第一安全鑰來保護該通信會話(1712)。存取點可隨後將通信會話切換至有效組中之第二存取點，其中使用一與第二存取點相關聯之第二安全鑰來保護該通信會話(1714)。甚至在存取終端機自第一存取點切換至第二存取點之後，若存取終端機切換回與第一存取終端機通信，則仍可在隨後重新使用第一安全鑰。

可重新配置圖1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16及/或17中所說明之組件、步驟及/或函數中之一或多者及/或將其組合為單一組件、步驟或函數或體現於若干組件、步驟或函數中，而不會影響偽隨機數產生之操作。亦可添加額外元件、組件、步驟及/或函數而不背離本發明。圖1、4、7、10、13及/或14中所說明之裝置、設備及/或組件可經組態以執行圖2、3、5、6、8、9、11、12、15、16及/或17中所描述之方法、特徵或步驟中之一或多者。可以軟體及/或嵌入式硬體來有效地實施本文中所描述之新穎演算法。

熟習此項技術者將進一步瞭解，可將結合本文所揭示之實施例而描述的各種說明性邏輯區塊、模組、電路及演算法步驟實施為電子硬體、電腦軟體或兩者之組合。為清楚地說明硬體與軟體之此互換性，各種說明性組件、區塊、

模組、電路及步驟已在上文就其功能性加以一般性地描述。將此功能性實施為硬體還是軟體視特定應用及外加於整個系統之設計約束而定。

可在不同系統中實施本文中所描述之本發明之各種特徵而不背離本發明。舉例而言，可使用移動或靜態通信設備(例如，存取終端機)及複數個行動或靜態基地台(例如，存取點)來執行本發明之某些實施例。

應注意，上述實施例僅為實例且並不應解釋為限制本發明。對該等實施例之描述意欲為說明性的，且並不意欲限制申請專利範圍之範疇。因而，可輕易地將本發明之教示應用於其他類型之裝置，且熟習此項技術者將易瞭解許多替代例、修改及變化。

【圖式簡單說明】

圖1說明一具有促進安全、低潛時通信會話交遞之分布式鑰管理的無線通信系統。

圖2(包含圖2A及圖2B)係一流程圖，其說明一具有促進安全、低潛時交遞之分布式鑰管理的無線通信系統之操作。

圖3說明安全鑰之一分布式模型，其可用於在交遞期間及/或之後保護一存取終端機與一新存取點之間的通信會話。

圖4說明一具有促進安全、低潛時交遞之集中式鑰管理的無線通信系統。

圖5(包含圖5A及圖5B)係一流程圖，其說明一具有促進

安全、低潛時交遞之集中式鑰管理的無線通信系統之操作。

圖6說明安全鑰之一集中式模型，其可用於在交遞期間及/或之後保護一存取終端機與一新存取點之間的通信會話。

圖7係一方塊圖，其說明一經組態以執行低潛時安全通信會話交遞之存取終端機。

圖8係一流程圖，其說明一可使用分布式鑰管理方法在存取終端機中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。

圖9係一流程圖，其說明一可使用集中式鑰管理方法在存取終端機中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。

圖10係一方塊圖，其說明一經組態以促進低潛時安全通信會話交遞之鑑認器。

圖11係一流程圖，其說明一可使用分布式鑰管理方法在鑑認器中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。

圖12係一流程圖，其說明一可使用集中式鑰管理方法在鑑認器中操作以促進自第一存取點至一新存取點之安全通信會話交遞的方法。

圖13係一方塊圖，其說明一經組態以促進低潛時安全通信會話交遞之存取點。

圖14係一方塊圖，其說明一具有一整合式鑑認器之存取

點之一替代性實施例。

圖15係一流程圖，其說明一可使用分布式鑰管理方法在第一存取點中操作以促進自該第一存取點至一第二存取點之安全通信會話交遞的方法。

圖16係一流程圖，其說明一可使用集中式鑰管理方法在一第一存取點中操作以促進自該第一存取點至一第二存取點之安全通信會話交遞的方法。

圖17係一流程圖，其說明一可在一存取終端機中操作以獲得及/或建立一組有效存取點之方法。

【主要元件符號說明】

100	多重存取無線通信系統
102	小區
104	小區
106	小區
110	存取點
112	存取點
114	存取點
116	天線
118	存取終端機
118a	存取終端機
118b	存取終端機
118c	存取終端機
120	鑑認器
202	頂層主鑰

204	頂層主鑰
206	序列號清單
400	多重存取無線通信系統
402	小區
404	小區
406	小區
410	存取點
412	存取點
414	存取點
418	存取終端機
420	鑑認器
502	頂層主鑰
504	頂層主鑰
702	存取終端機
704	處理電路
706	無線通信介面
708	儲存設備
1002	鑑認器
1004	處理電路
1006	通信介面
1008	儲存設備
1302	存取點
1304	處理電路
1306	無線通信介面

1308	儲存設備
1310	通信介面
1402	存取點
1412	鑑認器
AP	存取點
I-MK	暫時主鑰
I-TSK	暫時暫態會話鑰
MKo	頂層主鑰
MTK	主暫態鑰
TSK	暫態會話鑰

十、申請專利範圍：

1. 一種用於安全交遞之方法，其包含：

一存取終端機，其利用一第一暫態會話鑰以安全地與一第一存取點通信，其中基於一第一暫時主鑰以產生該第一暫態會話鑰，且其中基於一頂層主鑰及與該第一存取點相關聯之一第一序列號以產生該第一暫時主鑰；

該存取終端機使一第二序列號與一第二存取點相關聯；

該存取終端機起始自該第一存取點至該第二存取點之一安全交遞，其中轉發該第二序列號至該第一存取點；

該存取終端機基於該第一暫時主鑰及該第二序列號以產生一第二暫時主鑰；

該存取終端機基於該第二暫時主鑰以產生一第二暫態會話鑰；及

該存取終端機利用該第二暫態會話鑰以安全地與該第二存取點通信。

2. 如請求項1之用於安全交遞之方法，其中該存取終端機基於該第二暫時主鑰以產生一第二暫態會話鑰包含該存取終端機基於一隨機數及該第二暫時主鑰以產生該第二暫態會話鑰。

3. 如請求項2之用於安全交遞之方法，其中該隨機數係由該存取終端機所產生。

4. 如請求項2之用於安全交遞之方法，其中該隨機數係來自該第一存取點。

5. 如請求項2之用於安全交遞之方法，其中該隨機數係來自該第二存取點。

6. 如請求項1之用於安全交遞之方法，其進一步包含：

該存取終端機保持用於使每一存取點與一唯一序列號相關聯之一序列號清單。

7. 如請求項1之用於安全交遞之方法，其進一步包含：

該存取終端機使一第三序列號與一第三存取點相關聯；

該存取終端機起始自該第二存取點至該第三存取點之一安全交遞，其中該第三序列號被轉發至該第二存取點；

該存取終端機基於該第二暫時主鑰及該第三序列號以產生一第三暫時主鑰；

該存取終端機基於該第三暫時主鑰以產生一第三暫態會話鑰；及

該存取終端機利用該第三暫態會話鑰以安全地與該第三存取點通信。

8. 如請求項7之用於安全交遞之方法，其中該存取終端機基於該第三暫時主鑰以產生一第三暫態會話鑰包含該存取終端機基於一第二隨機數及該第三暫時主鑰以產生該第三暫態會話鑰。

9. 一種存取終端機，其包含：

一記憶體；及

與該記憶體耦接之一處理器，該處理器經組態以：

利用一第一暫態會話鑰以安全地與一第一存取點通信，其中基於一第一暫時主鑰以產生該第一暫態會話鑰，且其中基於一頂層主鑰及與該第一存取點相關聯之一第一序列號以產生該第一暫時主鑰；

使一第二序列號與一第二存取點相關聯；

起始自該第一存取點至該第二存取點之一安全交遞，其中該第二序列號被轉發至該第一存取點；

基於該第一暫時主鑰及該第二序列號以產生一第二暫時主鑰；

基於該第二暫時主鑰以產生一第二暫態會話鑰；及

利用該第二暫態會話鑰以安全地與該第二存取點通信。

10. 如請求項9之存取終端機，其中基於該第二暫時主鑰以產生一第二暫態會話鑰包含基於一隨機數及該第二暫時主鑰以產生該第二暫態會話鑰。

11. 如請求項10之存取終端機，其中該處理器進一步經組態以：產生該隨機數。

12. 如請求項9之存取終端機，其中該處理器進一步經組態以：

保持用於使每一存取點與一唯一序列號相關聯之一序列號清單。

13. 如請求項9之存取終端機，其中該處理器進一步經組態以：

使一第三序列號與一第三存取點相關聯；

起始自該第二存取點至該第三存取點之一安全交遞，其中該第三序列號被轉發至該第二存取點；

基於該第二暫時主鑰及該第三序列號以產生一第三暫時主鑰；

基於該第三暫時主鑰以產生一第三暫態會話鑰；及

利用該第三暫態會話鑰以安全地與該第三存取點通信。

14. 如請求項13之存取終端機，其中基於該第三暫時主鑰以產生一第三暫態會話鑰包含基於一第二隨機數及該第三暫時主鑰以產生該第三暫態會話鑰。

15. 一種用於安全交遞之裝置，其包含：

用於利用一第一暫態會話鑰以安全地與一第一存取點通信之構件，其中基於一第一暫時主鑰以產生該第一暫態會話鑰，且其中基於一頂層主鑰及與該第一存取點相關聯之一第一序列號以產生該第一暫時主鑰；

用於使一第二序列號與一第二存取點相關聯之構件；

用於起始自該第一存取點至該第二存取點之一安全交遞之構件，其中轉發該第二序列號至該第一存取點；

用於基於該第一暫時主鑰及該第二序列號以產生一第二暫時主鑰之構件；

用於基於該第二暫時主鑰以產生一第二暫態會話鑰之構件；及

用於利用該第二暫態會話鑰以安全地與該第二存取點通信之構件。

16. 如請求項15之用於安全交遞之裝置，其中用於基於該第二暫時主鑰以產生一第二暫態會話鑰之該構件包含用於基於一隨機數及該第二暫時主鑰以產生該第二暫態會話鑰之構件。

17. 如請求項16之用於安全交遞之裝置，其進一步包含：

用於產生該隨機數之構件。

18. 如請求項15之用於安全交遞之裝置，其進一步包含：

用於保持用於使每一存取點與一唯一序列號相關聯之一序列號清單之構件。

19. 如請求項15之用於安全交遞之裝置，其進一步包含：

用於使一第三序列號與一第三存取點相關聯之構件；

用於起始自該第二存取點至該第三存取點之一安全交遞之構件，其中該第三序列號被轉發至該第二存取點；

用於基於該第二暫時主鑰及該第三序列號以產生一第三暫時主鑰之構件；

用於基於該第三暫時主鑰以產生一第三暫態會話鑰之構件；及

用於利用該第三暫態會話鑰以安全地與該第三存取點通信之構件。

20. 如請求項19之用於安全交遞之裝置，其中用於基於該第三暫時主鑰以產生一第三暫態會話鑰之該構件包含用於基於一第二隨機數及該第三暫時主鑰以產生該第三暫態會話鑰之構件。

21. 一種包含可由一或多個處理器使用之若干指令的處理器

可讀媒體，該等指令包含：

用於利用一第一暫態會話鑰以安全地與一第一存取點通信之若干指令，其中基於一第一暫時主鑰以產生該第一暫態會話鑰，且其中基於一頂層主鑰及與該第一存取點相關聯之一第一序列號以產生該第一暫時主鑰；

用於使一第二序列號與一第二存取點相關聯之若干指令；

用於起始自該第一存取點至該第二存取點之一安全交遞之若干指令，其中轉發該第二序列號至該第一存取點；

用於基於該第一暫時主鑰及該第二序列號以產生一第二暫時主鑰之若干指令；

用於基於該第二暫時主鑰以產生一第二暫態會話鑰之若干指令；及

用於利用該第二暫態會話鑰以安全地與該第二存取點通信之若干指令。

22. 如請求項21之處理器可讀媒體，其進一步包含：

用於基於一隨機數及該第二暫時主鑰以產生該第二暫態會話鑰之若干指令。

23. 如請求項22之處理器可讀媒體，其進一步包含：

用於產生該隨機數之若干指令。

24. 如請求項21之處理器可讀媒體，其進一步包含：

用於保持用於使每一存取點與一唯一序列號相關聯之一序列號清單之若干指令。

25. 如請求項21之處理器可讀媒體，其進一步包含：

用於使一第三序列號與一第三存取點相關聯之若干指令；

用於起始自該第二存取點至該第三存取點之一安全交遞之若干指令，其中該第三序列號被轉發至該第二存取點；

用於基於該第二暫時主鑰及該第三序列號以產生一第三暫時主鑰之若干指令；

用於基於該第三暫時主鑰以產生一第三暫態會話鑰之若干指令；及

用於利用該第三暫態會話鑰以安全地與該第三存取點通信之若干指令。

26. 如請求項25之處理器可讀媒體，其進一步包含：

用於基於一第二隨機數及該第三暫時主鑰以產生該第三暫態會話鑰之若干指令。

十一、圖式：

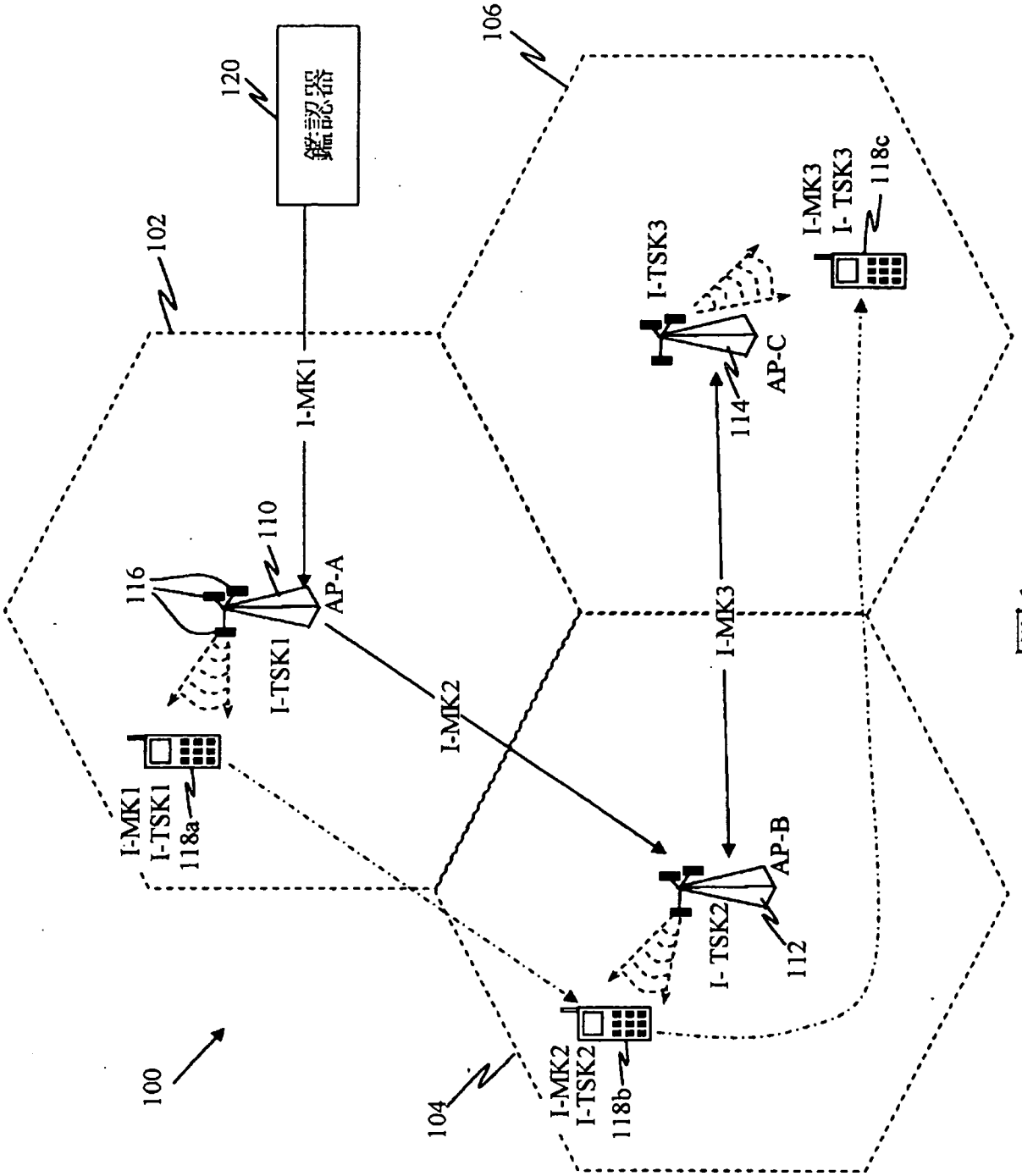
120
鑑認器
106
102
I-MK1
I-TSK3
I-MK3
I- TSK3
118c
AP-C
114
110
AP-A
116
I-TSK1
I-MK3
I-MK2
I-MK1
I-TSK1
118a
AP-B
I- TSK2
112
100
104
I-MK2
I-TSK2
118b

圖1

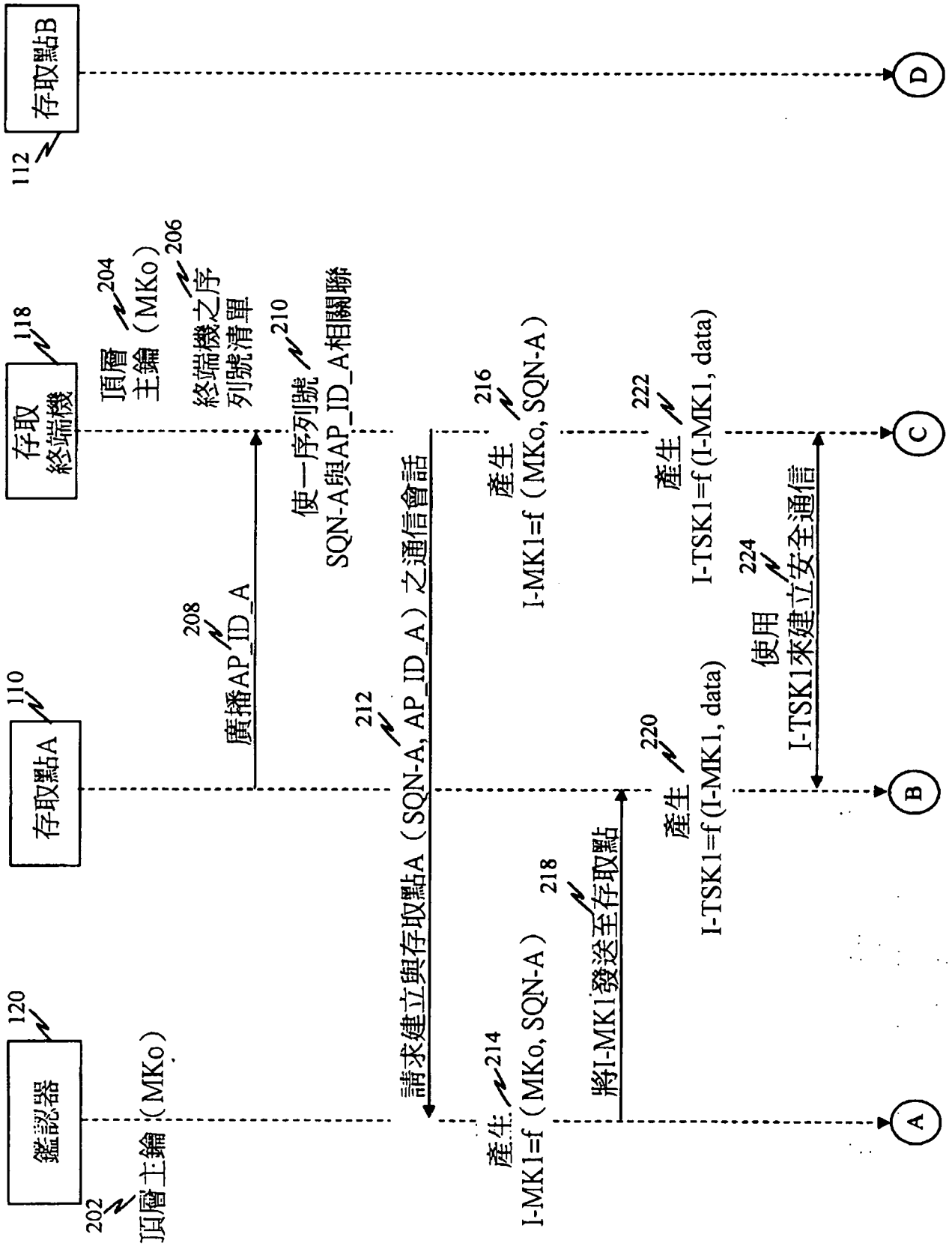
鑑認器
120
存取點A
110
存取終端機
118
存取點B
112
頂層主鑰（MKo）
202
頂層主鑰（MKo）
204
終端機之序列號清單
206
廣播AP_ID_A
208
使一序列號SQN-A與AP_ID_A相關聯
210
請求建立與存取點A（SQN-A, AP_ID_A）之通信會話
212
產生I-MK1=f（MKo, SQN-A）
214
將I-MK1發送至存取點
218
產生I-MK1=f（MKo, SQN-A）
216
產生I-TSK1=f（I-MK1, data）
220
使用I-TSK1來建立安全通信
224
產生I-TSK1=f（I-MK1, data）
222
A
B
C
D

圖2A

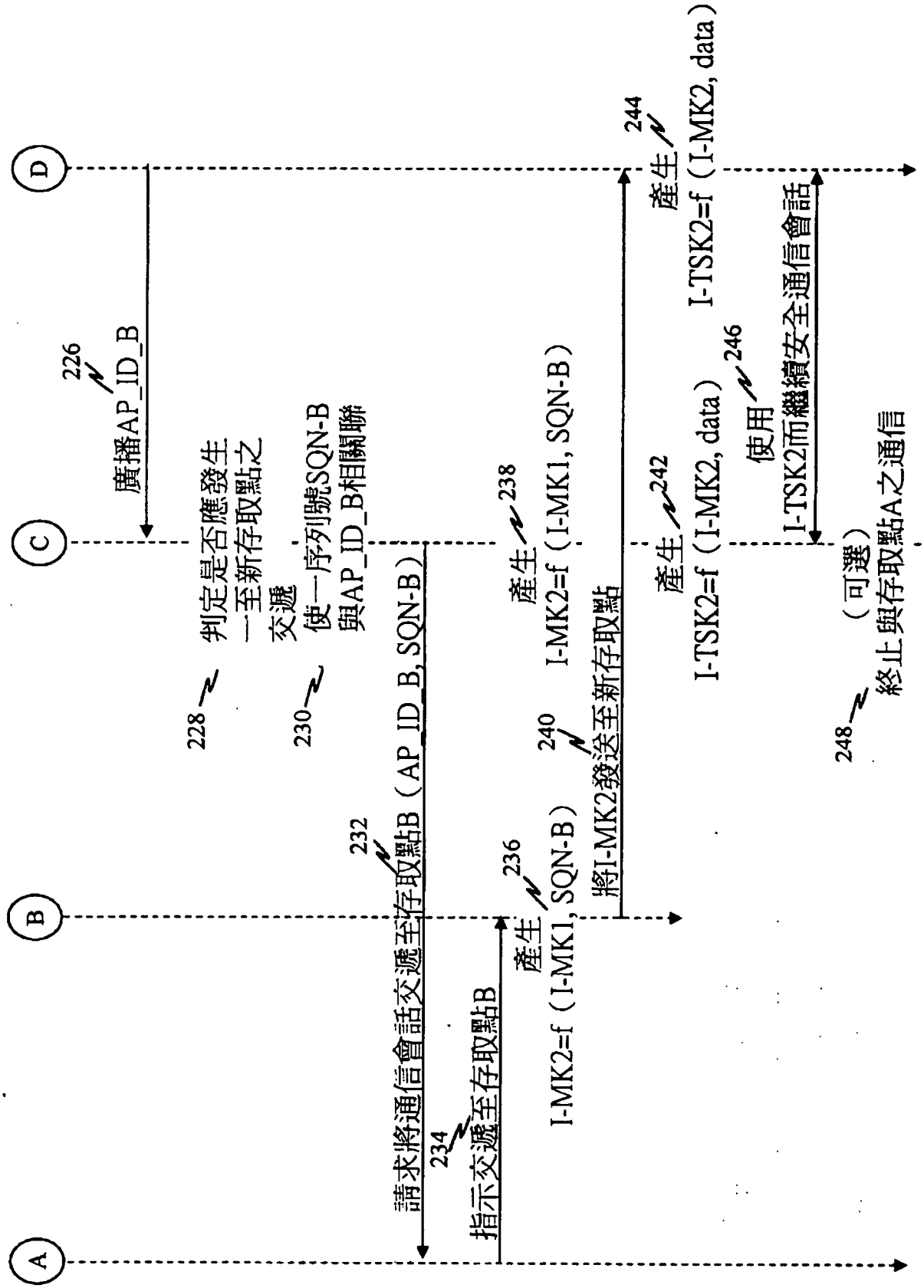
A
B
C
D
廣播AP_ID_B
226
判定是否應發生
一至新存取點之
交遞
228
使一序列號SQN-B
與AP_ID_B相關聯
230
請求將通信會話交遞至存取點B（AP_ID_B, SQN-B）
232
指示交遞至存取點B
234
產生
I-MK2=f（I-MK1, SQN-B）
236
產生
I-MK2=f（I-MK1, SQN-B）
238
將I-MK2發送至新存取點
240
產生
I-TSK2=f（I-MK2, data）
242
使用
I-TSK2而繼續安全通信會話
246
產生
I-TSK2=f（I-MK2, data）
244
（可選）
終止與存取點A之通信
248

圖2B

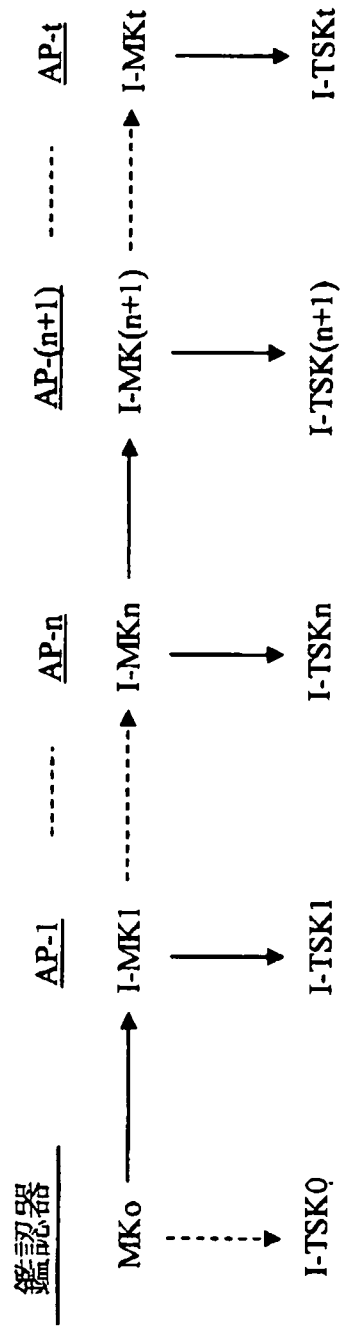
鑑認器
AP-1
AP-n
AP-(n+1)
AP-t
MKo
I-MK1
I-MKn
I-MK(n+1)
I-MKt
I-TSK0
I-TSK1
I-TSKn
I-TSK(n+1)
I-TSKt

圖3

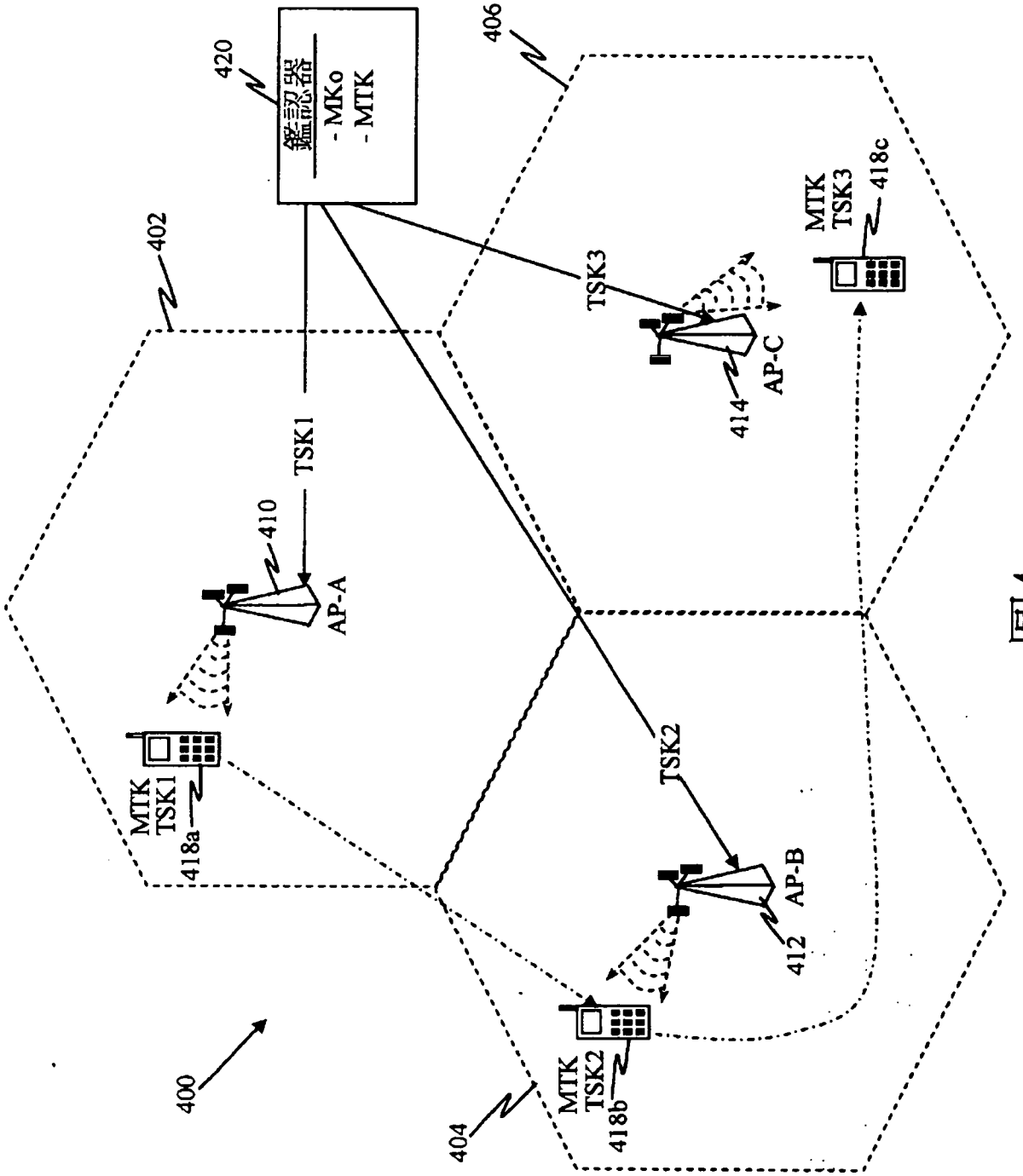
400
402
404
406
420
鑑認伺服器
- MKo
- MTK
TSK1
TSK2
TSK3
410
AP-A
412
AP-B
414
AP-C
MTK
TSK1
418a
MTK
TSK2
418b
MTK
TSK3
418c

圖4

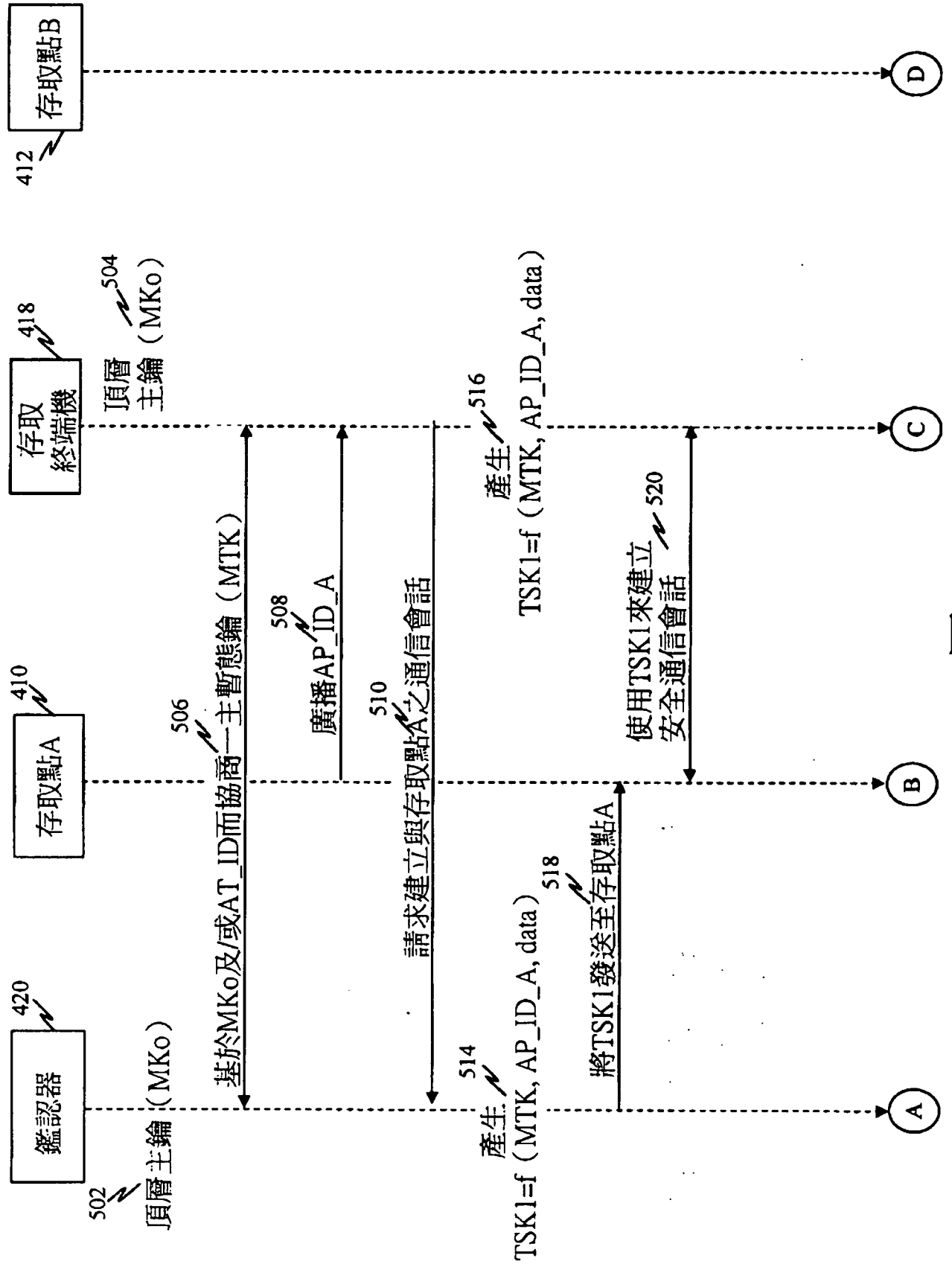
鑑認器
420
存取點A
410
存取終端機
418
存取點B
412
502
頂層主鑰（MKo）
506
基於MKo及/或AT_ID而協商一主暫態鑰（MTK）
508
廣播AP_ID_A
510
請求建立與存取點A之通信會話
514
產生TSK1=f（MTK, AP_ID_A, data）
518
將TSK1發送至存取點A
520
使用TSK1來建立安全通信會話
516
產生TSK1=f（MTK, AP_ID_A, data）
504
頂層主鑰（MKo）
A
B
C
D

圖5A

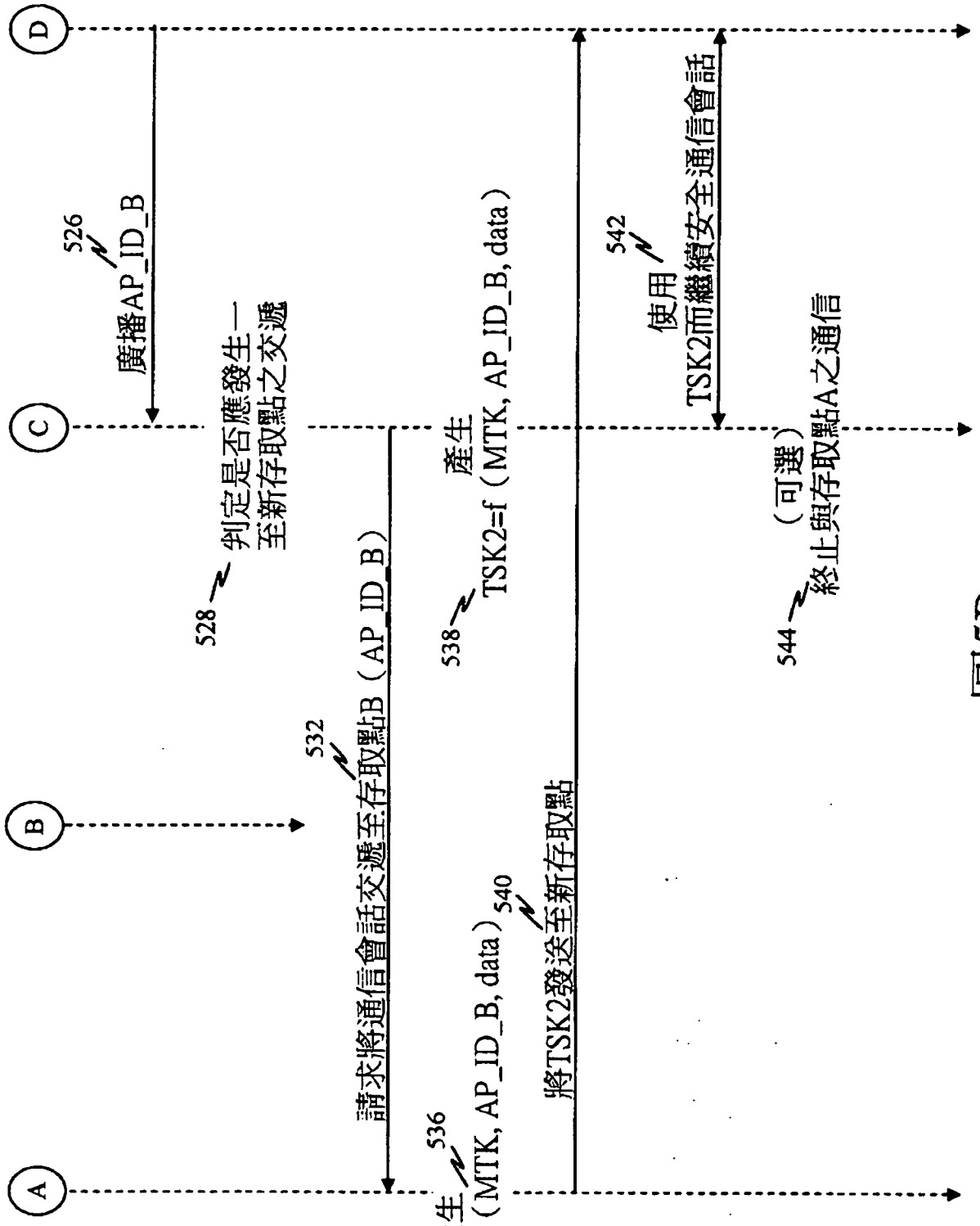
A
B
C
D
526
廣播AP_ID_B
528
判定是否應發生一至新存取點之交遞
532
請求將通信會話交遞至存取點B（AP_ID_B）
536
產生TSK2=f（MTK, AP_ID_B, data）
538
產生TSK2=f（MTK, AP_ID_B, data）
540
將TSK2發送至新存取點
542
使用TSK2而繼續安全通信會話
544
（可選）終止與存取點A之通信

圖5B

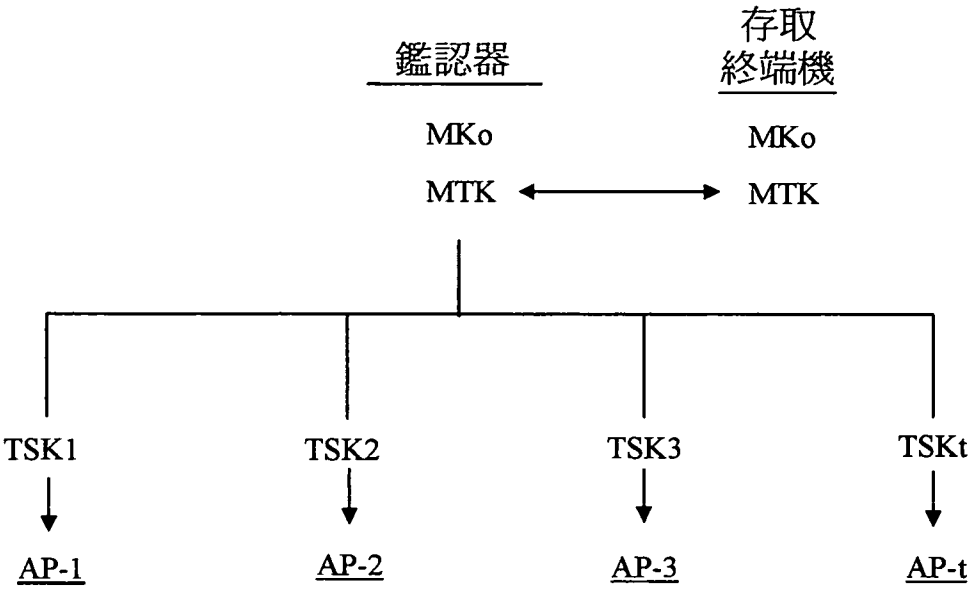
鑑認器
存取
終端機
MKo
MTK
MKo
MTK
TSK1
TSK2
TSK3
TSKt
AP-1
AP-2
AP-3
AP-t

圖6

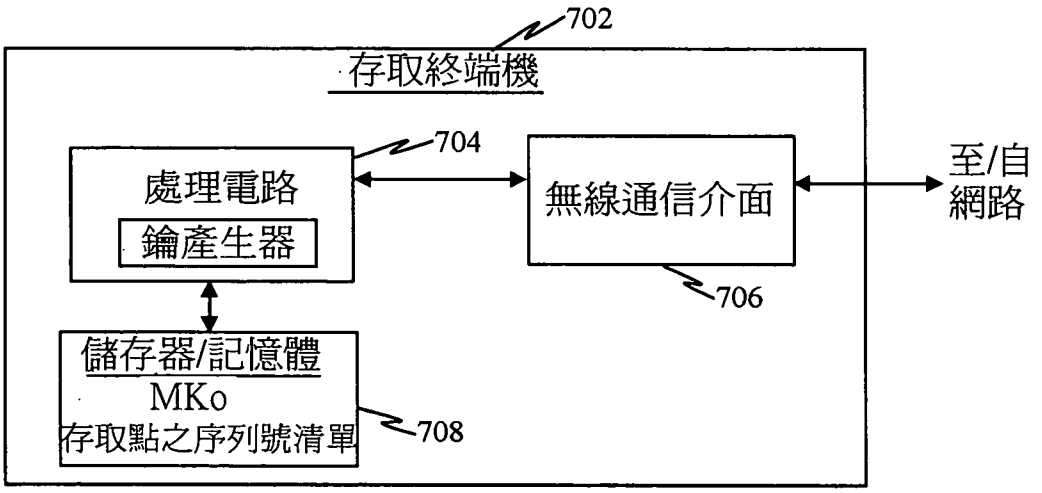
702
存取終端機
704
處理電路
鑰產生器
無線通信介面
至/自
網路
706
儲存器/記憶體
MKo
存取點之序列號清單
708

圖7

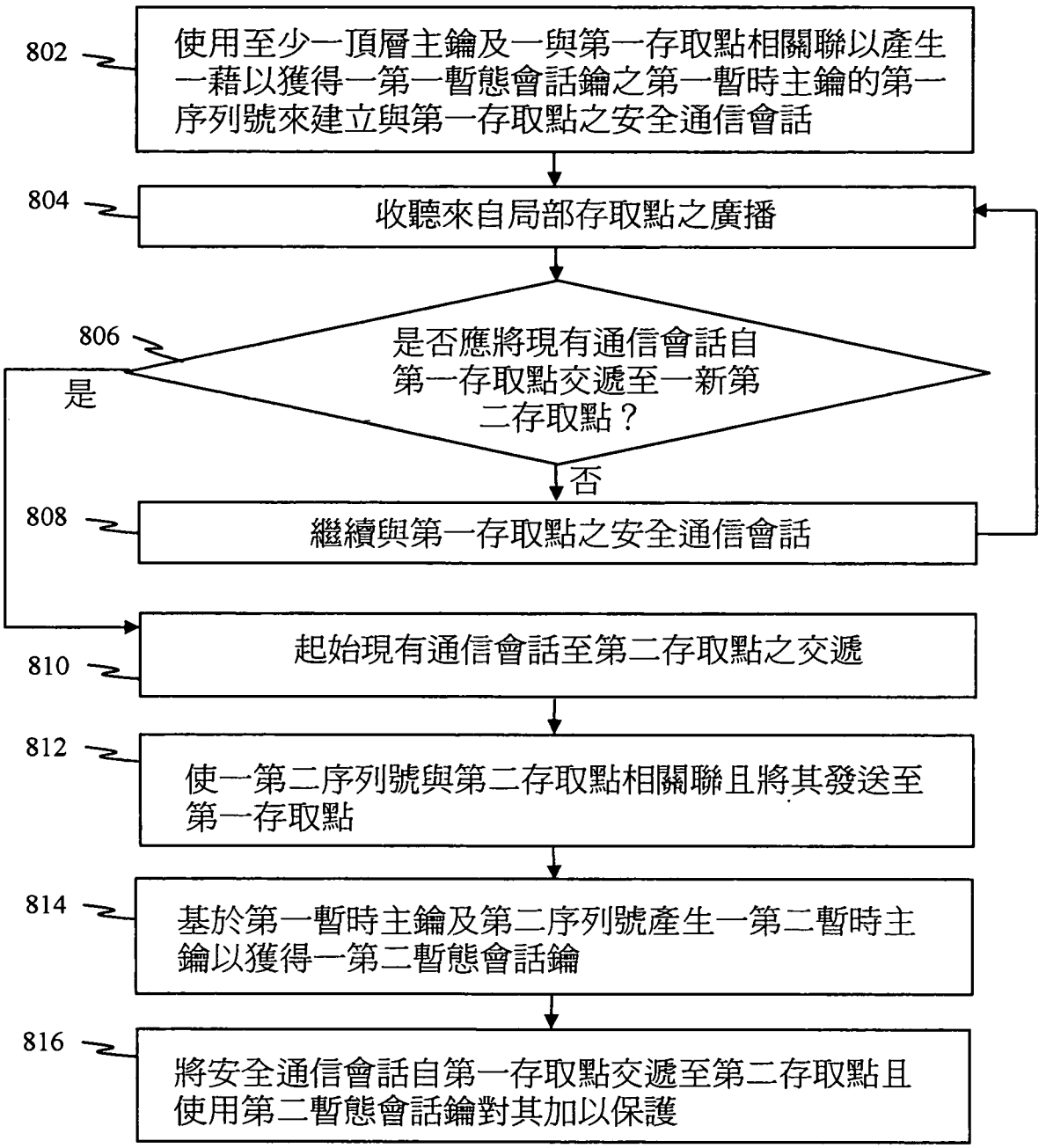
802
使用至少一頂層主鑰及一與第一存取點相關聯以產生一藉以獲得一第一暫態會話鑰之第一暫時主鑰的第一序列號來建立與第一存取點之安全通信會話
804
收聽來自局部存取點之廣播
806
是否應將現有通信會話自第一存取點交遞至一新第二存取點？
是
否
808
繼續與第一存取點之安全通信會話
810
起始現有通信會話至第二存取點之交遞
812
使一第二序列號與第二存取點相關聯且將其發送至第一存取點
814
基於第一暫時主鑰及第二序列號產生一第二暫時主鑰以獲得一第二暫態會話鑰
816
將安全通信會話自第一存取點交遞至第二存取點且使用第二暫態會話鑰對其加以保護

圖8

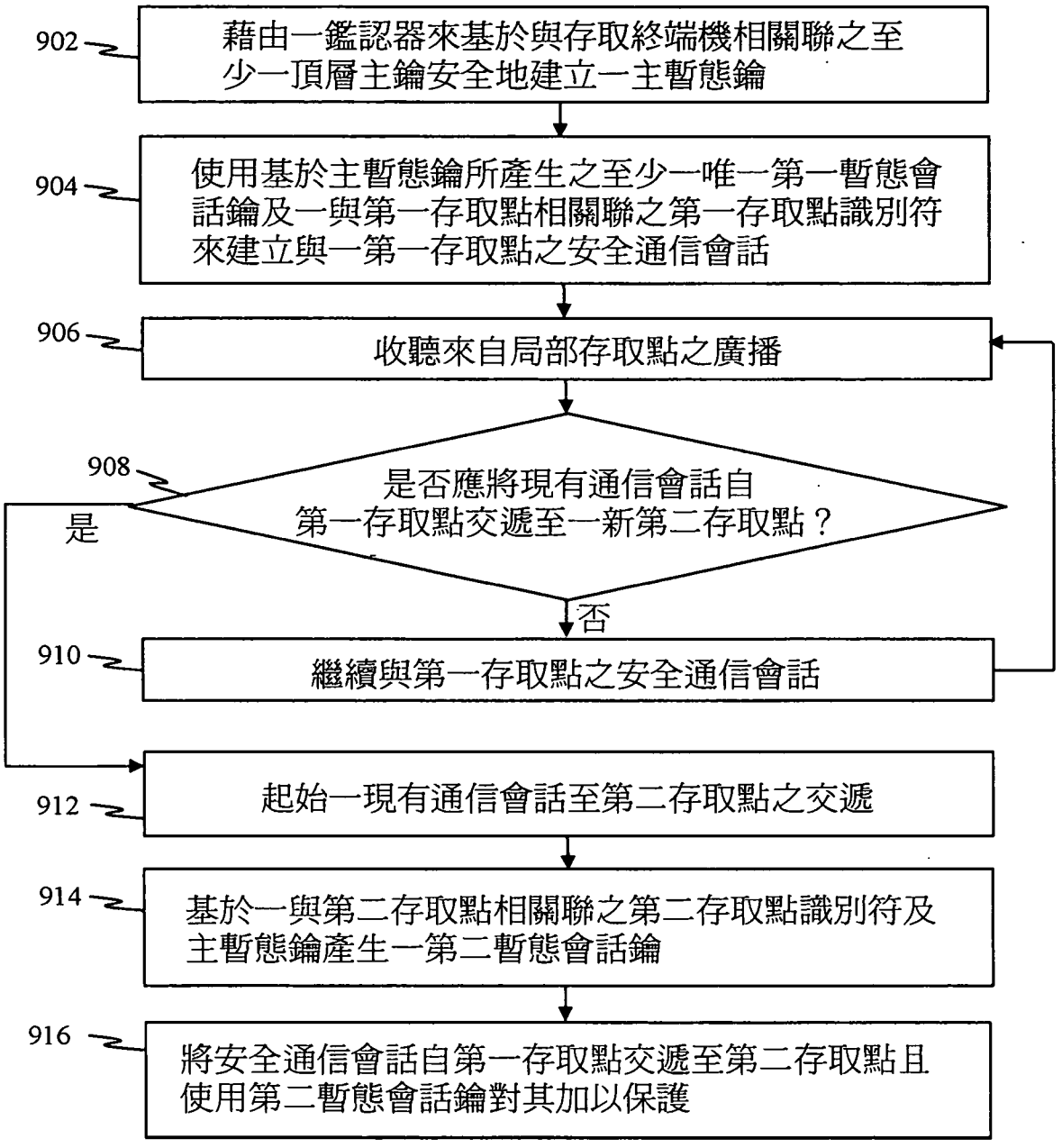
902
藉由一鑑認器來基於與存取終端機相關聯之至少一頂層主鑰安全地建立一主暫態鑰
904
使用基於主暫態鑰所產生之至少一唯一第一暫態會話鑰及一與第一存取點相關聯之第一存取點識別符來建立與一第一存取點之安全通信會話
906
收聽來自局部存取點之廣播
908
是否應將現有通信會話自第一存取點交遞至一新第二存取點？
是
否
910
繼續與第一存取點之安全通信會話
912
起始一現有通信會話至第二存取點之交遞
914
基於一與第二存取點相關聯之第二存取點識別符及主暫態鑰產生一第二暫態會話鑰
916
將安全通信會話自第一存取點交遞至第二存取點且使用第二暫態會話鑰對其加以保護

圖9

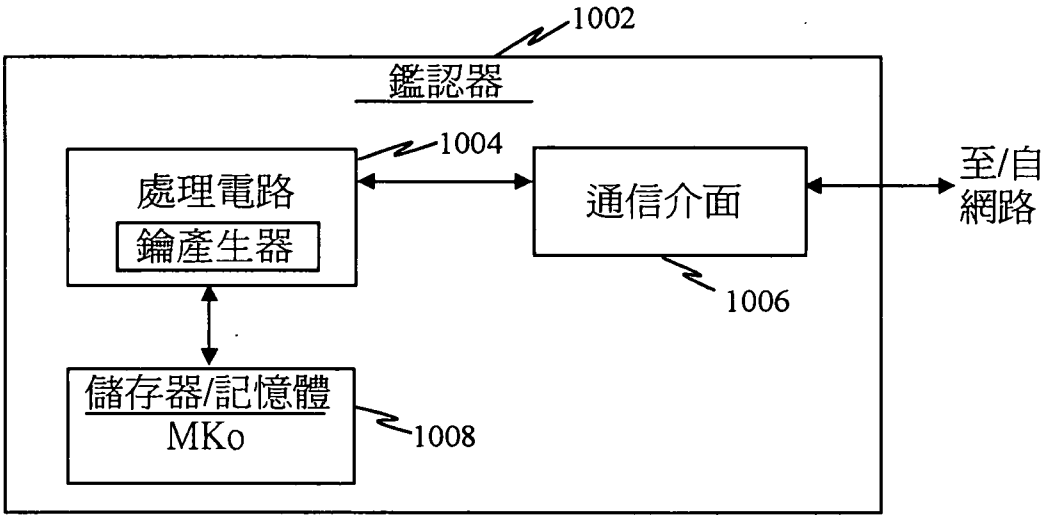

圖10

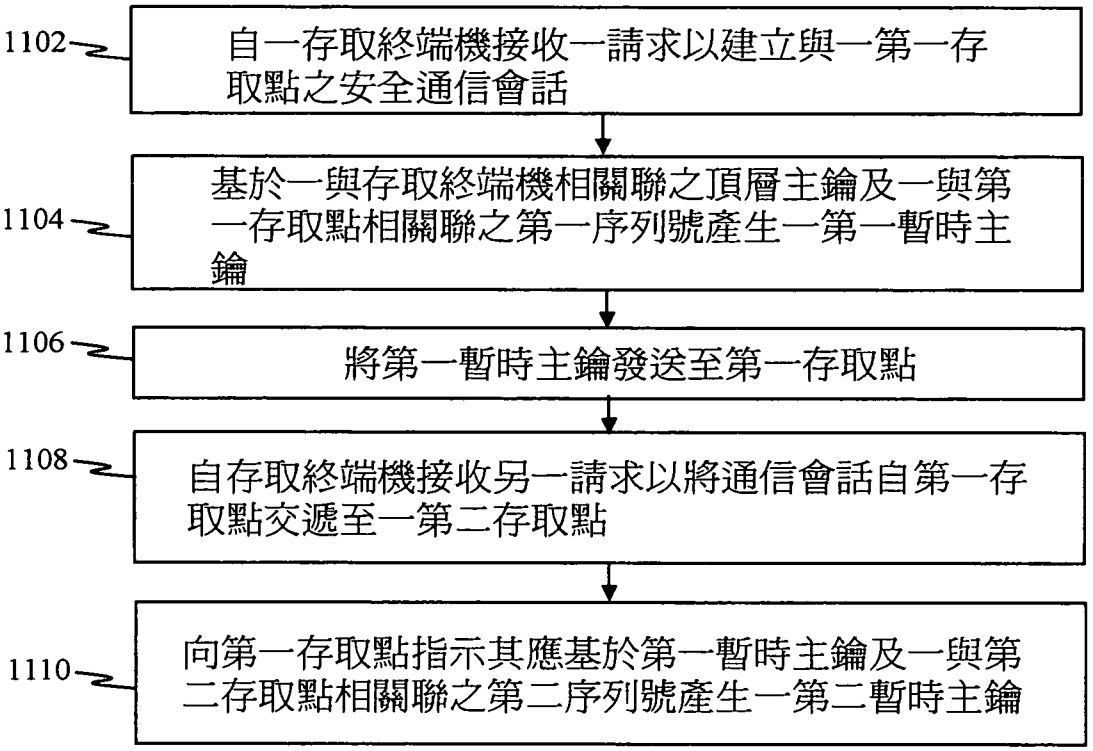
1102
自一存取終端機接收一請求以建立與一第一存取點之安全通信會話
1104
基於一與存取終端機相關聯之頂層主鑰及一與第一存取點相關聯之第一序列號產生一第一暫時主鑰
1106
將第一暫時主鑰發送至第一存取點
1108
自存取終端機接收另一請求以將通信會話自第一存取點交遞至一第二存取點
1110
向第一存取點指示其應基於第一暫時主鑰及一與第二存取點相關聯之第二序列號產生一第二暫時主鑰

圖11

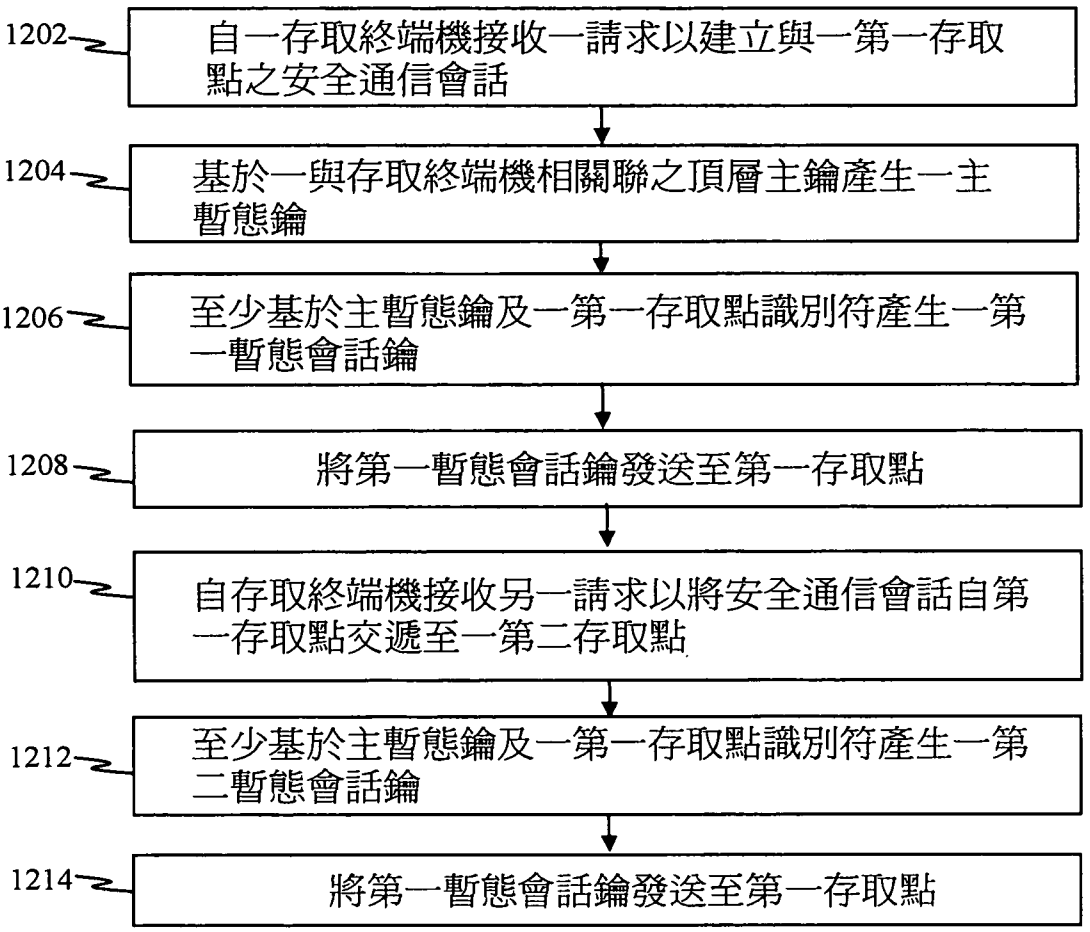
1202
自一存取終端機接收一請求以建立與一第一存取點之安全通信會話
1204
基於一與存取終端機相關聯之頂層主鑰產生一主暫態鑰
1206
至少基於主暫態鑰及一第一存取點識別符產生一第一暫態會話鑰
1208
將第一暫態會話鑰發送至第一存取點
1210
自存取終端機接收另一請求以將安全通信會話自第一存取點交遞至一第二存取點
1212
至少基於主暫態鑰及一第一存取點識別符產生一第二暫態會話鑰
1214
將第一暫態會話鑰發送至第一存取點

圖12

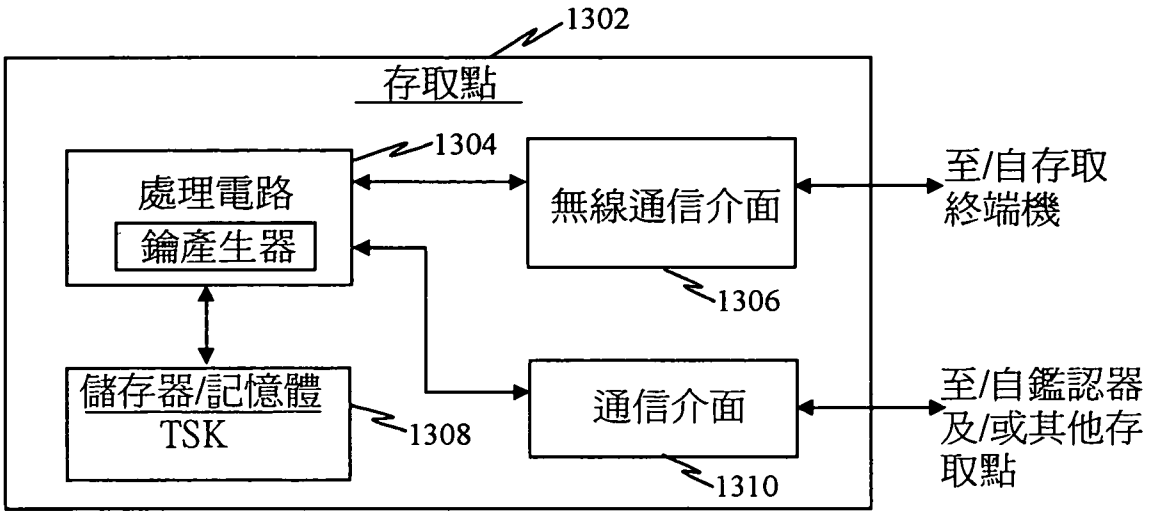
1302
存取點
1304
處理電路
鑰產生器
無線通信介面
至/自存取
終端機
1306
儲存器/記憶體
TSK
1308
通信介面
至/自鑑認器
及/或其他存
取點
1310

圖13

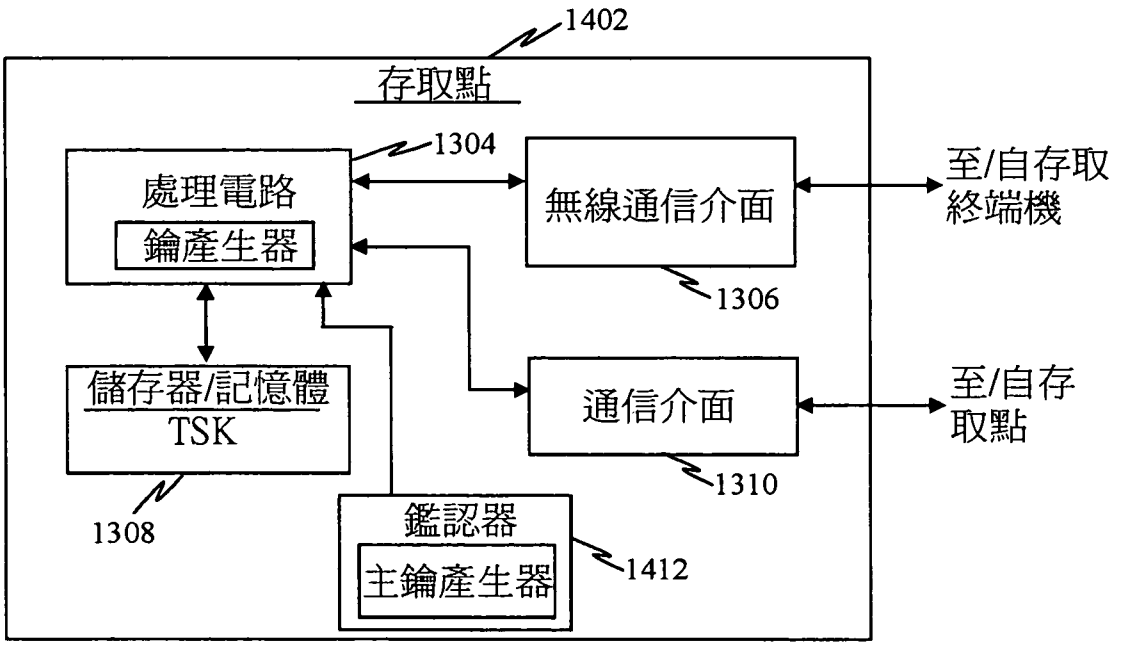
1402
存取點
1304
處理電路
鑰產生器
無線通信介面
至/自存取
終端機
1306
儲存器/記憶體
TSK
通信介面
至/自存
取點
1310
1308
鑑認器
主鑰產生器
1412

圖14

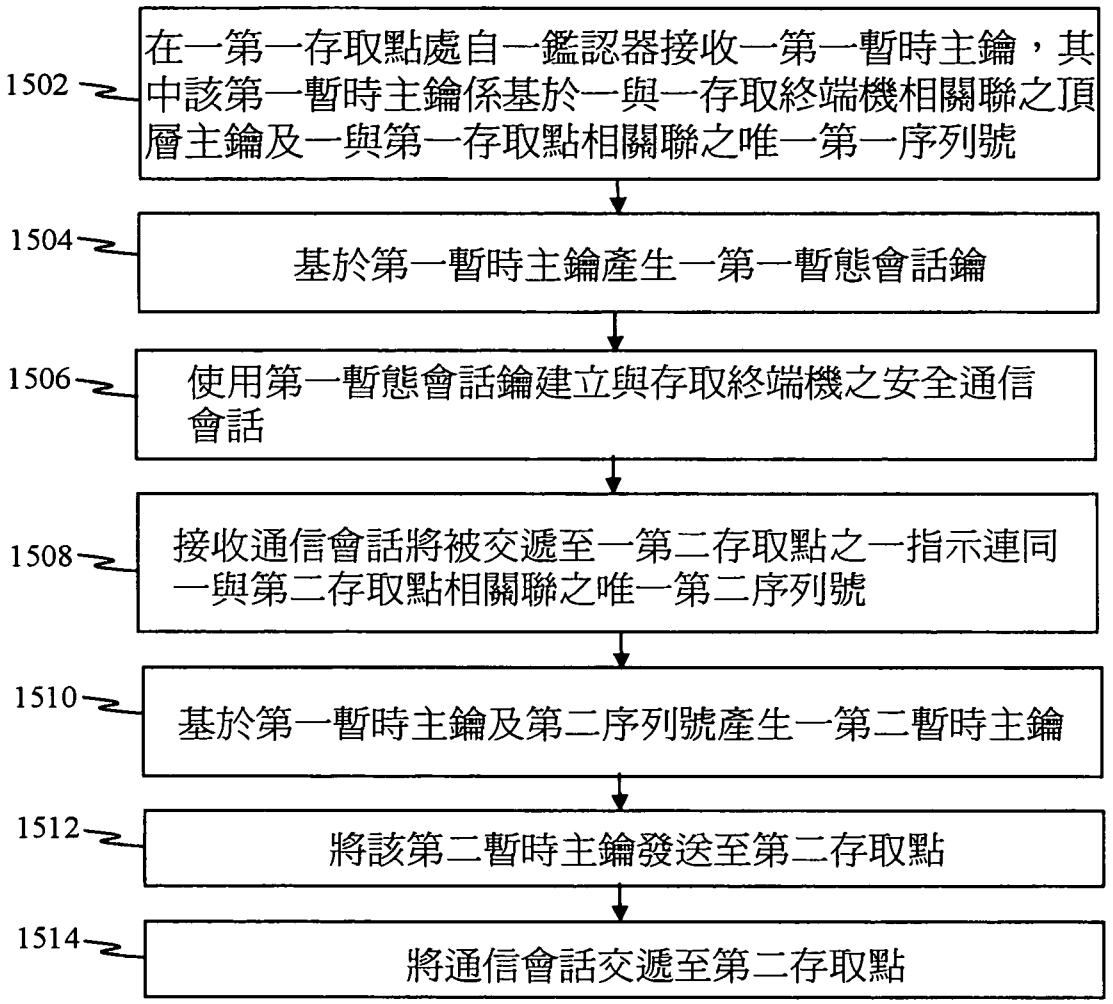
1502
在一第一存取點處自一鑑認器接收一第一暫時主鑰，其中該第一暫時主鑰係基於一與一存取終端機相關聯之頂層主鑰及一與第一存取點相關聯之唯一第一序列號
1504
基於第一暫時主鑰產生一第一暫態會話鑰
1506
使用第一暫態會話鑰建立與存取終端機之安全通信會話
1508
接收通信會話將被交遞至一第二存取點之一指示連同一與第二存取點相關聯之唯一第二序列號
1510
基於第一暫時主鑰及第二序列號產生一第二暫時主鑰
1512
將該第二暫時主鑰發送至第二存取點
1514
將通信會話交遞至第二存取點

圖15

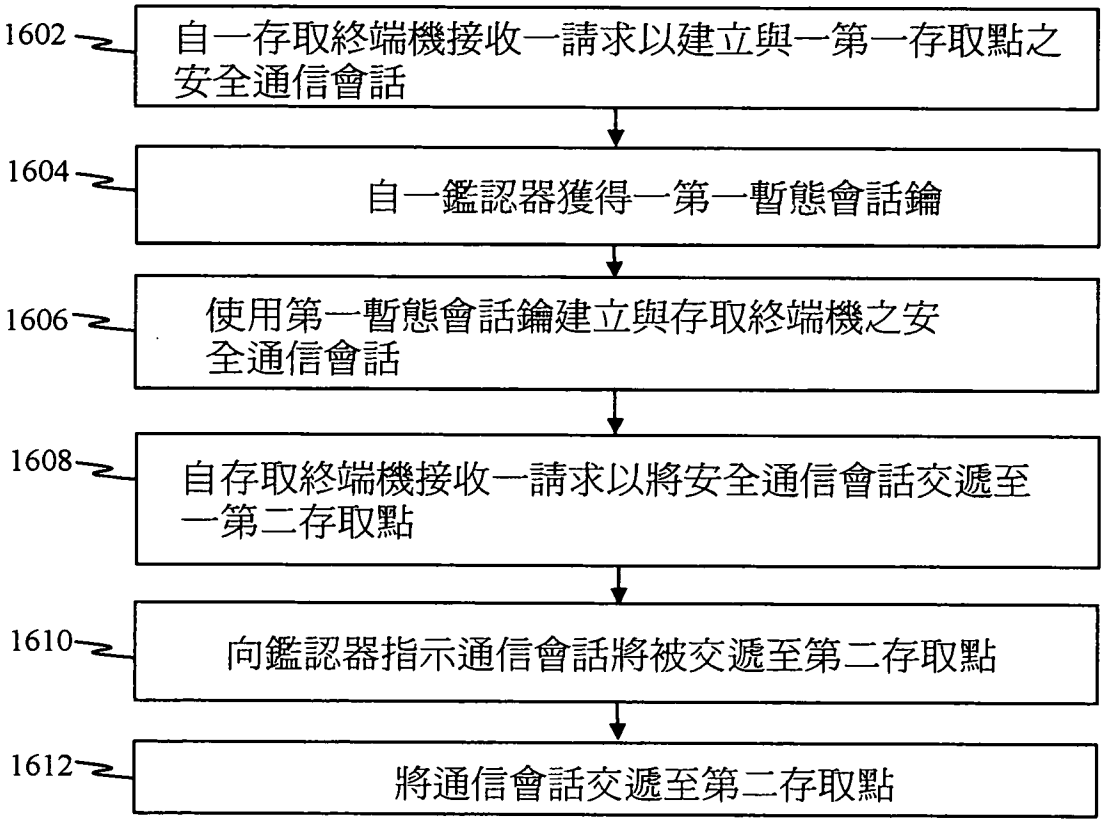
1602
自一存取終端機接收一請求以建立與一第一存取點之安全通信會話
1604
自一鑑認器獲得一第一暫態會話鑰
1606
使用第一暫態會話鑰建立與存取終端機之安全通信會話
1608
自存取終端機接收一請求以將安全通信會話交遞至一第二存取點
1610
向鑑認器指示通信會話將被交遞至第二存取點
1612
將通信會話交遞至第二存取點

圖16

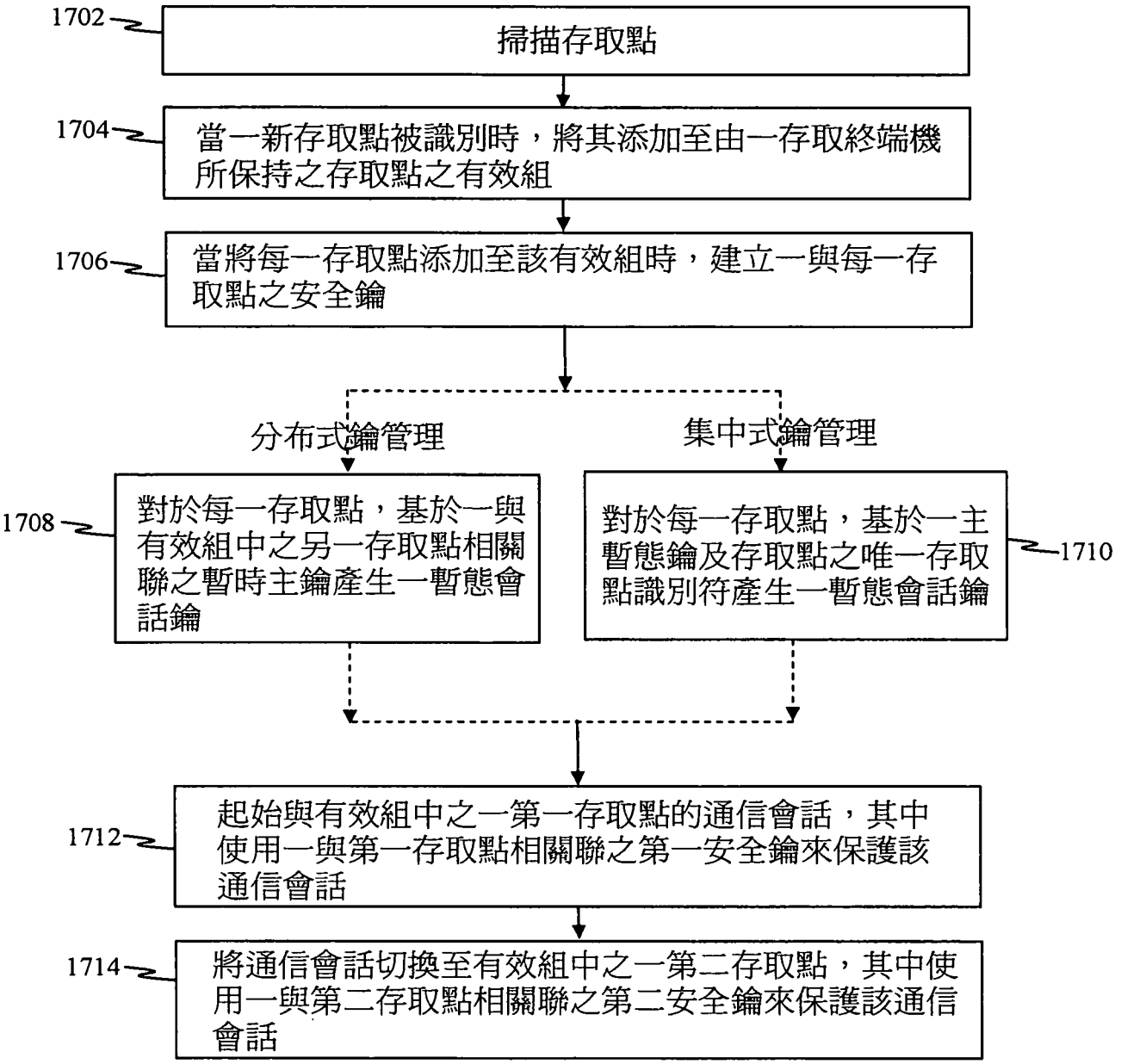
1702
掃描存取點
1704
當一新存取點被識別時，將其添加至由一存取終端機所保持之存取點之有效組
1706
當將每一存取點添加至該有效組時，建立一與每一存取點之安全鑰
分布式鑰管理
集中式鑰管理
1708
對於每一存取點，基於一與有效組中之另一存取點相關聯之暫時主鑰產生一暫態會話鑰
對於每一存取點，基於一主暫態鑰及存取點之唯一存取點識別符產生一暫態會話鑰
1710
1712
起始與有效組中之一第一存取點的通信會話，其中使用一與第一存取點相關聯之第一安全鑰來保護該通信會話
1714
將通信會話切換至有效組中之一第二存取點，其中使用一與第二存取點相關聯之第二安全鑰來保護該通信會話

圖17