



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201002012 A1

(43)公開日：中華民國 99 (2010) 年 01 月 01 日

(21)申請案號：098114894

(22)申請日：中華民國 98 (2009) 年 05 月 05 日

(51)Int. Cl. : **H04L29/06 (2006.01)** **H04L9/30 (2006.01)**

(30)優先權：2008/06/26 美國 12/146,520

(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)

美國

(72)發明人：徐文平史考特 HSU, WEN-PIN SCOTT (US)；書拉米塔瑞克 SOULAMI, TARIK (US)；查戈爾斯基馬克 ZAGORSKI, MARK (US)；曾寧 ZHANG, NING (US)；波爾曼布萊恩 PERLMAN, BRIAN (US)

(74)代理人：蔡坤財；李世章

申請實體審查：無 申請專利範圍項數：20 項 圖式數：10 共 51 頁

(54)名稱

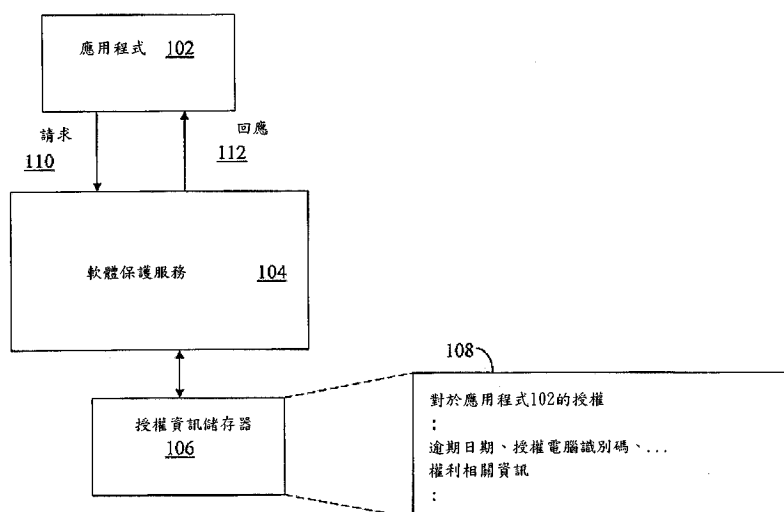
確保通訊之驗證及完備之技術

TECHNIQUES FOR ENSURING AUTHENTICATION AND INTEGRITY OF COMMUNICATIONS

(57)摘要

茲說明多項用於確保所收訊息之資料完備性及驗證的技術。一項技術包含自一第一模組，其將一請求發送至一第二模組，其中該請求含有一第一部分，此部分係一藉一公用金鑰所加密的共享秘密；由該第二模組自一含有用於該第一模組之授權資訊或其他應用程式特定資訊的安全及受信賴資訊儲存器，像是一授權資訊儲存器，獲得一私人金鑰；利用該私人金鑰以解密該第一部分並獲得該共享秘密；自該第二模組將一回應發送至該第一模組，其中該回應含有驗證資料和至少一運用於該共享秘密的資料項目以供決定該驗證資料；以及由該第一模組執行驗證處理程序，藉此驗證包含在該回應中的驗證資料。

100



100：範例圖式

102：應用程式

104：軟體保護服務
(SPS)

106：授權資訊儲存器

108：構件

110：請求

112：回應



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201002012 A1

(43)公開日：中華民國 99 (2010) 年 01 月 01 日

(21)申請案號：098114894

(22)申請日：中華民國 98 (2009) 年 05 月 05 日

(51)Int. Cl. : **H04L29/06 (2006.01)** **H04L9/30 (2006.01)**

(30)優先權：2008/06/26 美國 12/146,520

(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)

美國

(72)發明人：徐文平史考特 HSU, WEN-PIN SCOTT (US)；書拉米塔瑞克 SOULAMI, TARIK (US)；查戈爾斯基馬克 ZAGORSKI, MARK (US)；曾寧 ZHANG, NING (US)；波爾曼布萊恩 PERLMAN, BRIAN (US)

(74)代理人：蔡坤財；李世章

申請實體審查：無 申請專利範圍項數：20 項 圖式數：10 共 51 頁

(54)名稱

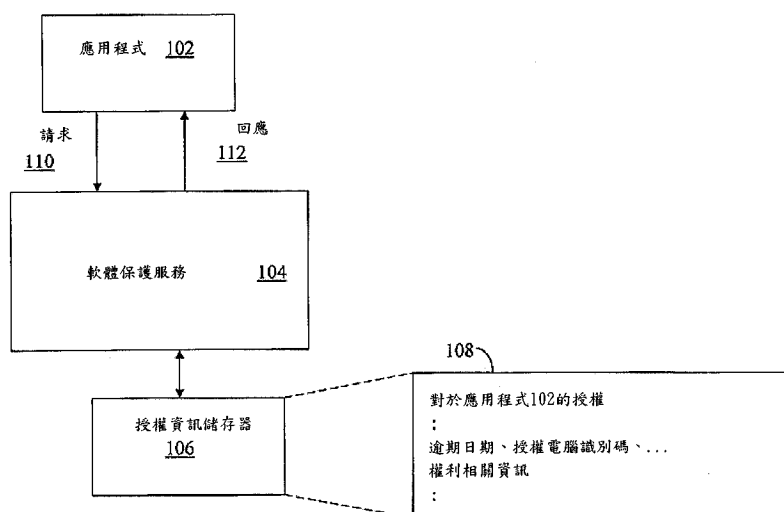
確保通訊之驗證及完備之技術

TECHNIQUES FOR ENSURING AUTHENTICATION AND INTEGRITY OF COMMUNICATIONS

(57)摘要

茲說明多項用於確保所收訊息之資料完備性及驗證的技術。一項技術包含自一第一模組，其將一請求發送至一第二模組，其中該請求含有一第一部分，此部分係一藉一公用金鑰所加密的共享秘密；由該第二模組自一含有用於該第一模組之授權資訊或其他應用程式特定資訊的安全及受信賴資訊儲存器，像是一授權資訊儲存器，獲得一私人金鑰；利用該私人金鑰以解密該第一部分並獲得該共享秘密；自該第二模組將一回應發送至該第一模組，其中該回應含有驗證資料和至少一運用於該共享秘密的資料項目以供決定該驗證資料；以及由該第一模組執行驗證處理程序，藉此驗證包含在該回應中的驗證資料。

100 ↗



100：範例圖式

102：應用程式

104：軟體保護服務
(SPS)

106：授權資訊儲存器

108：構件

110：請求

112：回應

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種確保通訊之驗證及完備之技術

【先前技術】

訊息可於一客戶端、或產生一請求的個體、與一伺服器、或回應於該請求的個體之間傳通。該客戶端可將一請求訊息發送至該伺服器，並且該伺服器可將一回應訊息發送至該客戶端。而該客戶端及該客戶端可為例如下兩台電腦系統、同一電腦系統上的兩個模組等等。然對於在該客戶端與該伺服器間交換之訊息的資料完備性和驗證存在有一項問題。該客戶端及該伺服器其一或兩者對於所交換之訊息的資料完備性和驗證可能會有所疑慮。資料完備性可為與訊息內容相關聯，並確保該所收訊息並非一原始訊息的經修改版本。驗證可為與該發送者的驗證作業相關聯，原因在於一所收訊息可能是由一除所預期之發送者以外的個體所產生。而關於一由一客戶端所收到的回應，一攻擊者可攔截一原先自該伺服器所發送的回應並加以修改。如此，該客戶端收到的是一具有既經修改之內容的回應。或者，不以攔截一原先由該伺服器所發送的回應，一攻擊者亦可引入另一宣稱(purport)為產生該回應的個體。例如，若該攻擊者引入一模組，而此模組取代該伺服器以發送並接收訊息，即出現此後

者。類似地，對於一伺服器所收到的請求而言，一攻擊者可攔截並修改一原始請求，或是該攻擊者可另為引入一模組，而此模組取代該請求者以發送並接收訊息。

【發明內容】

本發明內容係經提供以介紹一種按一較簡化形式，而在後文「實施方式」所進一步描述的概念選擇。本「發明內容」並非為以識別所主張之主題項目的各項關鍵特點或基本特性，亦非為以用於決定所主張主題項目之範圍的輔助。

多項技術係經描述以供確保一由一第一模組自一第二模組所收到之通訊的驗證及資料完備性。根據本發明之一特點，該第一模組利用一非對稱金鑰組對的一公用金鑰對一共享秘密進行加密，並且將該經加密之共享秘密發送至該第二模組。該第二模組從一安全且受信賴的資訊儲存器，像是一授權資訊儲存器，擷取該非對稱金鑰組對的私人金鑰，同時利用該私人金鑰以獲得該共享秘密俾產生用於一自該第二模組發送至該第一模組之訊息的驗證資料。該第一模組利用該共享秘密以執行驗證處理程序。根據本發明之另一特點，該第二模組利用一自該授權資訊儲存器或是其他安全且受信賴資訊儲存器所獲得之非對稱金鑰組對的一私人金鑰來產生一用於一自該第二模組發送至該第一模組之訊息的數位簽章。該第

一模組利用該非對稱金鑰組對的公用金鑰以執行驗證處理程序。

【實施方式】

現參照第 1 圖，該圖說明一其中可實作運用本文揭示技術之具體實施例的適當計算環境之範例。第 1 圖所示之計算環境僅為一適當計算環境的單一範例，而並非為以意指任何對於本文揭示技術之使用範圍或功能性的限制。熟諳本項技藝之人士將能瞭解本文揭示技術可適用於其他一般目的性及特殊性的計算環境與組態。眾知計算系統、環境及/或組態範例包含個人電腦、伺服器電腦、手持式或膝上型裝置、多重處理器系統、微處理器式系統、可程式化消耗性電子裝置、網路 PC、迷你電腦、大型主機電腦、可含有任何前述該等系統或裝置的分散式計算環境等等，然不限於此。

本文揭示所述技術可為按如電腦可執行指令，像是程式模組，而由一或更多電腦或其他裝置所執行的一般情境所說明。一般說來，程式模組包含執行特定任務或是實作出特定抽象資料型態之副程式、程式、物件、元件、資料結構等等。通常，可按如各種具體實施例中所需將程式模組的功能性予以合併或分散。

第 1 圖中含有一電腦 12、一網路 14 及一伺服器 16。該電腦 12 可包含一可用以執行一或更多程式模組的標

準、商購可獲用電腦或是特殊目的性電腦。在後文章節與圖式中所詳細說明者係可由該電腦 12 執行，並有關於利用本文揭示技術以確保一所收通訊之完備性及驗證，的程式模組。該電腦 12 可運作於一網路環境內，並且與其他電腦，像是一伺服器 16，以及第 1 圖中未予顯示的其他項目進行通訊。

熟諳本項技藝之人士將能瞭解該電腦 12 雖在該範例中顯示為在一網路環境中進行通訊，然該電腦 12 確可運用不同通訊媒體以與其他元件進行通訊。例如，該電腦 12 可運用一網路連接，及/或其他業界已知類型的鏈結，像是網際網路、企業內網路或是其他(多個)無線及/或硬接線連接，然不限於此，俾與一或更多元件進行通訊。

即如第 1 圖所示，該電腦 12 可含有一或更多處理單元 20、記憶體 22、儲存裝置 30，以及一用於促成該電腦 12 中多個元件間之通訊的系統匯流排 32，和其他在第 1 圖中未予顯示的元件。

根據該電腦 12 的組態與類型而定，該記憶體 22 可為揮發性(像是 RAM)、非揮發性(像是 ROM、快閃記憶體等等)，或為此二者的一些組合。此外，該電腦 12 亦可含有額外的儲存裝置(可移除及/或非可移除)，這些包含 USB 裝置、磁性或光學碟片或磁帶，然不限於此。此額外儲存裝置在第 1 圖中是由該儲存裝置 30 所表示。該儲存裝置 30 可包含一或更多可移除及非可移除儲存裝置，此等具備相關的電腦可讀取媒體而可由該電腦 12 加

以運用。在一具體實施例裡，該儲存裝置 30 可包含一硬碟及/或 CD-ROM 碟機。藉由範例，該等記憶體 22 及儲存裝置 30 係電腦可讀取媒體的範例，然不限於此。電腦可讀取媒體包含揮發性及非揮發性、可移除及非可移除媒體，該等可按任何方法或技術所實作，以供儲存像是電腦可讀取指令、資料結構、程式模組或其他資料之資訊。電腦可讀取媒體包含，然不限於此，RAM、ROM、EEPROM、快閃記憶體或其他記憶體技術、CD-ROM、DVD 或其他光學儲存、磁匣、磁帶、磁碟儲存或其他磁性儲存裝置，或者是任何其他可用以儲存所欲資訊並能由該電腦 12 加以存取的媒體。前揭媒體通常具體實作可讀取指令、資料結構、程式模組或其他資料。

在一即如本文揭示所述之具體實施例裡，該電腦 12 可透過一網路，利用連至像是該伺服器 16 之遠端電腦的邏輯連接，藉以於一如第 1 圖所示的網路環境中運作。一或更多軟體模組及/或資料檔案可包含在該電腦 12 的儲存裝置 30 之內。在該電腦 12 的操作過程中，這些經收納在該儲存裝置 30 內之模組的一或更多者亦可常駐於該記憶體 22 的一部分中，例如像是 RAM，以利控制該電腦 12 的操作。

該伺服器 16 可代表一經連接至該網路 14 的伺服器電腦系統。該伺服器電腦系統可包含軟體模組以伺服請求，以及一或更多處理器、儲存裝置等等，即類似於本文揭示中參照於該電腦 12 所述者。本文揭示技術可運用

於一其中該電腦 12 及該伺服器 16 可透過該網路 14 進行通訊的具體實施例。該電腦 12 及該伺服器 16 可執行關聯於處理其間所交換之通訊的操作。例如，該電腦 12 可將一請求發送至該伺服器 16，並且該伺服器 16 可提供一回應。本文揭示技術可運用於確保所收通訊，像是由該電腦 12 自該伺服器 16 所到的回應，或者像是由該伺服器 16 自該電腦 12 收到的請求，的完備性和驗證。資料完備性可為與通訊內容相關聯，並可確保該所收通訊並非一原始通訊的經修改版本。驗證可為與該發送者的驗證作業相關聯，原因在於一所收通訊可能是由一除所預期之發送者以外的個體所產生。

本文揭示技術亦可運用於一與在同一電腦系統上之兩個模組，像是該電腦 12 上之兩個模組，間的通訊相關聯之具體實施例。更一般地，本文揭示技術可運用在關聯於確保自一發送者所收到之訊息的驗證和完備性。本文揭示技術可運用於有關在單一方向上，像是自該伺服器 16 至該電腦 12，所傳送的通訊，並可運用於有關在兩者方向上，像是自該伺服器 16 至該電腦 12 以及自該電腦 12 至該伺服器 16，所傳送的通訊。

為敘述之目的，後文裡詳細陳述其中可利用本文揭示技術來確保一由一第一模組自一第二模組所收到之回應的完備性及驗證俾進行處理的示範性具體實施例，而其中該等第一和第二模組可位於相同電腦上，像是在該電腦 12 上。然即如熟諳本項技藝之人士所將能瞭解並於本

文揭示他處所更廣泛地描述者，該等技術可運用在關於不同電腦系統，而非同一電腦系統，上之個體間所傳送的通訊、由該等第一及第二模組所收到的通訊而非僅由該第一模組所收到者等等。

現參照第 2 圖，其中顯示一可包含在第 1 圖電腦 12 上以供關聯於本文揭示技術而運用之多個模組的範例 100。該範例 100 包含一應用程式 102、軟體保護服務 (SPS) 104 及授權資訊儲存器 106。該應用程式 102 可為該電腦 12 上的一經安裝程式。該授權資訊儲存器 106 可含有對於一或更多經授權以在該電腦上使用之軟體產品的授權資訊。該儲存器 106 可為各種含有該授權資訊之不同資料儲存個體的任一者。例如，該儲存器 106 可為一檔案、資料庫或其他資料容器。構件 108 說明一對於該應用程式 102 之授權資訊的邏輯表示，該者可包含在該授權資訊儲存器 106 內。該 108 的資訊可例如標定逾期日期、識別經授權以執行該應用程式 102 的電腦、識別由該授權所准允的權利等等。該儲存器 106 亦可含有與該授權中所准允之個別權利相關聯的資訊。例如，即如後文中所進一步詳細說明者，一授權可准允一權利以「執行 (run)」該應用程式 102。該授權資訊儲存器 106 亦可將資訊關聯於該執行權利。即如一範例，一非對稱金鑰組對的私人金鑰可經加密並儲存在該 106 內。該私人金鑰可為關聯於該「執行」權利以及該應用程式 102 之授權的其他權利。應注意到該授權資訊儲存器 106 可含有關

聯於按各種不同方式所執行之先前軟體安裝及啟動作業而獲得的授權資料。

即如業界所眾知者，一非對稱金鑰組對係運用在有關於不同的非對稱加密技術，其中利用不同的金鑰以進行加密與解密，像是將一公眾/私人金鑰組對利用於 PKI (「公用金鑰基礎架構」)。除由一擁有該相對應私人金鑰的接收者外，一利用該公用金鑰所加密的訊息是無法獲以解密。後文中將進一步詳細說明將該非對稱金鑰組對運用於執行本文揭示技術之具體實施例的方式。

該 SPS 104 可對該電腦系統上之一或更多軟體產品，像是該應用程式 102，的授權進行管理。該 SPS 104 可執行有關於授權使用的功能，並且透過一 API 以展現(expose)該等功能。該 SPS 104 可執行多項功能，像是獲取授權、儲存並管理授權、保護授權不受侵入、評估一授權的有效性、評估一授權是否正確地限用於一機器(即如該授權表示一軟體產品可在該機器上執行)、評估該授權是否准允對於該軟體產品的一特定權利等等。該應用程式 102 可利用該 API 以將一請求 110 發送至該 SPS 104。而回應於收到該請求 110，該 SPS 104 可將一訊息 112 發送至該應用程式 102。該應用程式 102 可發出該請求 110 以獲得有關對於該應用程式 102 之授權的資訊。例如，一使用者可發出一請求以執行該應用程式 102。「執行」可為與該應用程式相關聯的權利，即表示該使用者有權執行該應用程式。該請求 110 可經發送至該 SPS

104，藉以決定該授權是否表示具備一現存且有效而准允在該電腦上執行該應用程式 102 的授權。回應於收到該請求，該 SPS 104 可執行對於該應用程式 102 之授權與所請求之權利的授權核可與驗證處理。例如，該 SPS 104 可自該授權資訊儲存器 106 擷取對於該應用程式 102 的授權資訊，並且執行處理程序俾決定是否存在一對於該應用程式 102 的有效授權、該授權是否表示該應用程式 102 為正確地限用於該應用程式 102，以及該授權是否表示依如該授權而准允該標定權利。自該 SPS 104 所送返之回應 112 可表示，對於一准允所請求之權利的目前有效授權而言，是否既已為成功地完成前揭核可與驗證處理(即如在本範例中「執行」該應用程式的權利)。

一授權，像是可按一可經儲存在該授權資訊儲存器 106 內之電子形式或文件所表示者，標定在一軟體產品中的權利。一像是該應用程式 102 的呼叫者可利用該 API 以呼叫一「消耗(Consume)」方法，藉此「消耗」一像是該應用程式 102 之軟體產品的權利。在成功地消耗該軟體產品的一權利之後，可自該授權資訊儲存器 106 擷取出與一權利相關聯的額外資料。參照於如前所述的構件 108，在成功地消耗該執行權利之後，即可自該授權資訊儲存器 106 擷取與該執行權利相關聯的私人金鑰。消耗一軟體產品之一權利的特徵可在於執行多項處理步驟，藉以驗證並核可對於該軟體產品的授權和權利，即如前文所述般。該授權，像是按如一包含在該授權資訊儲存

器 106 內之電子文件所表示者，可含有與該消耗處理程序相關聯所運用的資訊。該消耗處理程序可例如包含檢查該軟體產品是否確經授權以在該軟體執行於其上之機器上執行、檢查授權有效性，像是該授權是否既已逾期等等。對於該軟體產品，該授權亦可標定可供與該應用程式相關聯而執行的不同權利。例如，即如前述，「執行」可為一表示該使用者有權執行該軟體產品的權利。該消耗權利 API 可獲叫用以決定目前是否存在一有權執行該軟體產品的有效授權。若確如此，則即已成功地消耗該授權及權利。而在成功地消耗處理程序之後的一後續步驟，可自該應用程式 102 的授權中擷取出與該所消耗權利相關聯的額外資訊，像是該私人金鑰，即如包含在該授權資訊儲存器 106 之內者。Gunyakti 等人於 2003 年 10 月 23 申審，標題為「PROGRAMMING INTERFACE FOR LICENSING」之美國專利公告 2005/009116S A1 ('168 公告案)，美國專利申請案第 10/692,868 號，茲依參考方式併入本案，案文中描述一種示範性軟體授權服務，以及可讓其他模組能夠使用一共同服務之授權管理功能性的 API。前揭 '168 公告之授權管理設施和 API 類似於如前關聯於該 SPS 104 所說明者。

即如後文所詳述，當既已成功地消耗一標定權利之後，可關聯於本文揭示技術以運用自該授權資訊儲存器 106 所擷取的私人金鑰，藉此確保該回應 112 的資料完備性及驗證確如該應用程式 102 自該 SPS 104 所收到者。

與一具體實施例相關者，該應用程式 102 可於該應用程式 102 發出該請求之前，先在該應用程式 102 與該 SPS 104 之間經由交換其他通訊以建立一與該 SPS 104 的會期。與建立該會期相關者，該應用程式 102 可表示一非對稱金鑰組對的一特定公用金鑰，而該應用程式 102 將可關聯於該會期之後續通訊加以運用。該應用程式 102 亦可產生一會期金鑰，其特徵係一對於每個會期為唯一的識別碼。該會期金鑰可為關聯於針對該相關會期而在該應用程式 102 與該 SPS 104 之間所交換的通訊。可利用任何各種確保對於各個會期具備足夠程度唯一性的不同技術來產生該會期金鑰。例如，該會期金鑰的大小可為 16 至 64 個位元組的範圍，並且可為利用一根據該公用金鑰、目前時間等等的隨機數目所產生。該會期金鑰在此可更廣義地稱為一種代表對於各個會期具有一不同數值之識別碼的共享秘密。

該應用程式 102 可利用該非對稱金鑰組對的公用金鑰，即如當建立與該 SPS 104 的會期時所標定者，以對該共享秘密進行加密。該應用程式 102 建構該請求 110，此請求中含有該經加密之共享秘密以及對於該特定請求的任何其他資料。此等其他資料可例如識別一為其而發出該請求 110 的權利。即如前述，該請求 110 可為一查詢，此查詢係針對，於一表示准允在該電腦 12 上執行該應用程式 102 的有效授權中，是否准允該請求內所含的一權利，像是該「執行」權利。

應注意到該共享秘密可為對於該應用程式 102 所「共享」，並為按如經加密之形式而傳通至該 SPS 104。

現參照第 3 圖，其中顯示一可自該應用程式 102 發送至該 SPS 104 之請求 110 的範例表示。該請求 602 包含請求資料 604、經加密之共享秘密 606，以及選擇性地對於該請求的其他資訊 608。該請求資料 604 可例如識別一待予藉由切換電源供應器 104 而執行的特定操作、識別一或更多權利、識別該應用程式 102 等等。構件 606 可表示運用各種不同非對稱加密技術之任一者，像是 RSA，而利用與該目前會期相關聯之公用金鑰，所加密的共享秘密。

該 SPS 104 收到該請求 110 並執行處理，藉此針對於該應用程式 102 的授權以消耗該請求中的所標定權利。即如前述，權利的消耗可包含，根據包含在該授權資訊儲存器 106 內之資訊，針對該應用程式 102 的授權和所標定權利來執行核可與驗證處理程序。例如，該 SPS 104 可自該儲存器 106 擷取對於該應用程式 102 的授權資訊以決定該授權是否既已逾期、該授權是否表示該應用程式 102 係經授權以於該特定電腦 12 上執行、在該請求 110 中所標定的權利在該授權中是否既獲准允等等。若處理程序決定該標定權利係經關聯於一有效授權而獲准允運用於該電腦 12 上，則該權利既經成功地消耗。當成功地消耗一權利時，即可自該儲存器 106 內的授權中後續地擷取出與該權利相關聯的額外資訊。關聯於一根據

本文揭示技術的具體實施例，一私人金鑰可為關聯於該所標定之經消耗權利，並可為自該儲存器 106 所擷取出。該私人金鑰可對應於由該電腦 12 所使用之非對稱私有/公用金鑰組對的公用金鑰以供加密該共享秘密。當針對該請求 110 而成功地消耗該標定權利時，該 SPS 104 自該授權資訊儲存器 106 擷取該私人金鑰，並且解密包含在來自該應用程式 102 之請求內的經加密共享秘密 606。該 SPS 亦可執行關聯於該請求的其他處理程序。

應注意到該 SPS 104 可執行處理程序以決定一自該授權資訊儲存器 106 所擷取的私人金鑰是否為當建立該會期時所標定之公用金鑰的所匹配非對稱金鑰。例如，該授權資訊儲存器 106 可包含該私人金鑰以及該非對稱組對的相對應公用金鑰兩者，並且可自該 106 所取得此二者。該 SPS 104 可決定自該儲存器 106 所擷取的公用金鑰是否匹配於當建立該會期時所標定的公用金鑰。若該等公用金鑰並不匹配，則該 SPS 104 可採取適當步驟，像是終止處理程序並在回應中送返一適當狀態。同時，當成功地消耗時可擷取多個私人金鑰，並且該 SPS 可藉由比對等公用金鑰以執行處理程序俾選定適當的私人金鑰。

現參照第 4 圖，此圖顯示一範例，而其中說明可供執行以決定包含在待予發送至該應用程式 102 之回應 112 內的資料之處理程序。該回應 704 可含有一版本號碼 702a、選擇性的回應資料 702b、一選擇性的臨時資料

(Nonce) 702c 以及驗證資料 702d。即如後文所述，該版本號碼 702a，以及選擇性地該回應資料 702b 及/或該臨時資料 702c，可用來作為一輸入以供產生該驗證資料 702d。臨時資料 (Nonce) 可稱為「使用一次的號碼」，此者係隨各個經驗證訊息而改變，即如後文中關聯於構件 702 所詳細說明者。

該版本號碼 702a 可為一關聯於該 SPS 104 的版本號碼。該版本號碼 702a 可為由該 SPS 104 按各種不同方式所獲得。例如，該版本號碼可為在該模組 SPS 104 內所編碼，自該授權資訊儲存器 106 或該電腦 12 上的其他預定位位置所擷取得。一具體實施例可對於該版本號碼 702a 選定一適當大小。例如，一具體實施例可利用一具有最大 4 個位元組大小的版本號碼 702a。該回應資料 702b 可為選擇性，例如若該特定請求 110 並不具有任何經送返至該呼叫者的資訊。該臨時資料 702c 之特徵為一對於各次回應通訊具有唯一性的號碼或是其他符號。例如，該臨時資料 702c 可為一由該 SPS 104 所產生的隨機或虛似隨機號碼。該臨時資料 702c 可運用在一具體實施例中以協助防止重播攻擊。一重播攻擊之特徵為一種其中可攔截一有效資料傳輸然後再予以複播或重傳的攻擊。此一重播攻擊可獲防止，因為會將不同的臨時資料 702c 納入在各回應內，從而使得該訊息資料 702 以及所產生的驗證資料 702d 亦能對於各次回應而有所改變。

即如所示，該待予驗證的訊息資料 702 可含有 702a，

並且亦可含有 702b 及 / 或 702c。該訊息資料 702 可為藉由接合 702a 以及選擇性地 702b 及 / 或 702c 所構成。該訊息資料 702 係對於一封包函數 712 的第一輸入，此功能在決定該驗證資料 702d 會利用該共享秘密 710。在一具體實施例裡，該封包函數 712 可為經執行以決定一 HMAC (金鑰雜湊訊息驗證碼) 值來作為該驗證資料 702d 的處理程序。可利用一加密雜湊函數以及一金鑰，此者在本範例中為該共享秘密 710，的組合來計算一 HMAC 值。即如前述，可藉由利用自該授權儲存器 106 所取得的私人金鑰對該請求之一部分進行解密以獲取該共享秘密 710。該 HMAC 值可用來作為該驗證資料 702d，藉以驗證用於產生該 HMAC 值之訊息資料 702 的資料完備性及驗證兩者。該 HMAC 可為按如下式所定義：

$$\text{HMAC}_{\text{KEY}}(\text{M}) = \text{h}((\text{KEY XOR opad} \parallel \text{h}((\text{KEY XOR ipad}) \parallel \text{m}))) \quad \text{等式 1}$$

其中 h 為一所選定的加密雜湊函數。KEY 為一金鑰，像是藉由解密該請求之一部分所獲得的共享秘密，在此該 KEY 係對於該雜湊函數，h，之特定區塊大小而經填入以額外零值，M 為待予驗證的訊息 702。應注意到「||」是表示接合、XOR 表示邏輯斥 OR 運算，並且外部填入「opad」係一十六進位常數 0x5c5c5c...5c5c，而內部填入「ipad」亦為一十六進位常數 0x363636...3636。在此範例裡，M 可表示為按如藉由接合該版本號碼 702a、該

回應資料 702b 及 / 或該臨時資料 702c 之結果所構成的 702。在前述的 HMAC 表示式中，可運用任何各種不同的加密雜湊函數，像是 SHA-1 或 MD-5，來作為該雜湊函數。該 HMAC 值的加密強度可為根據該底層雜湊函數、該金鑰的大小和品質，以及該雜湊輸出長度依位元而計的大小所決定。

而關聯於 HMAC，該 KEY 係用以構成由該雜湊演算法 h 所雜湊的內容。一替代方式為，不利用等式 1 (HMAC) 以決定驗證資料來作為該封包函數，一具體實施例可利用一對稱加密技術，像是 AES (先進加密標準)，來作為該封包函數，而這是利用該共享秘密以作為該對稱金鑰。換言之，不以利用一根據一雜湊函數之金鑰雜湊演算法的封包函數 712 以產生一 HMAC 值作為該驗證資料，而是一具體實施例可另外利用一根據對稱加密技術，像是 AHS，的金鑰雜湊函數以作為該封包函數 712，藉此產生該驗證資料 702d。關聯於像是 AES 的對稱加密技術，該金鑰可用來作為一第一輸入，而構成該訊息的內容則為一第二輸入。應注意到一對稱加密技術是利用相同的金鑰以進行加密和解密運算。

熟諳本項技藝之人士將能瞭解該封包函數可更概略地為任何依據包含該訊息及金鑰在內之輸入以產生驗證資料的演算法。本文揭示所述之 HMAC 演算法和對稱加密技術係可運用在一具體實施例中的封包函數範例。

該臨時資料 702c 可為按各種不同方式所決定，並且按

各種方式而令由該應用程式 102 及該 SPS 104 二者所獲知。例如，該 SPS 104 可利用一依時間為基礎的數值、隨機號碼產生器等等來產生一數值以作為該臨時資料。自該 SPS 發送至該應用程式的回應 112 可含有此臨時資料，或者一數值而該應用程式可自此值決定/導算出該臨時資料。即如另一範例，該應用程式可決定該臨時資料，或是用以導算出該臨時資料的數值，並且可將其納入在發送至該 SPS 的請求之內。接著，SPS 可利用此臨時資料以構成在決定該 HMAC 值過程中所使用的訊息 702。更一般說來，一利用一臨時資料 702c 的具體實施例可按照該 SPS 及該應用程式所能瞭解的任何方式來產生該臨時資料。

一旦既已決定該驗證資料 702d 後，該 SPS 104 可如所述建構該回應 704，並且將該回應 704 傳送至該應用程式 102。應注意到，在一具體實施例裡，可對該回應資料 702b 以及該回應的其他部分選擇性地進行加密。例如，若該回應資料 702b 中包含有價內容，或是該 SPS 104 並不希望按一可讀取形式所傳送的內容，則一具體實施例可選定對該回應資料 702b 進行加密。

而當收到該回應後，例如若該 SPS 104 既已加密該回應資料 702b，則該應用程式 102 可執行任何必要的解密作業。接著該應用程式 102 執行驗證處理程序。更確切地說，該應用程式 102 會按與該 SPS 104 計算包含在該回應內之驗證資料相同的方式來計算其本身的驗證資料

拷貝。該應用程式 102 利用該共享秘密，此者係該應用程式 102 所已知，以及包含在該所收回應裡的版本號碼 702a 和回應資料 702b 及/或臨時資料 702c，若確存在，來計算其本身的驗證資料拷貝。該應用程式 102 執行為以決定一 HMAC 值或其他封包函數 712 的處理程序，即如可在一具體實施例用以決定驗證資料。該應用程式 102 將其本身算出的驗證資料拷貝比較於包含在該回應內的驗證資料 702d。若二者相符，則驗證處理程序成功。若否，則驗證處理程序失敗。

應注意到一具體實施例亦可執行有關於驗證處理程序的額外步驟。例如，該應用程式 102 亦可執行一關聯於在該回應中所收到之版本號碼 702a 的額外檢查。該應用程式 102 可擷取該版本號碼的一預期數值，並且將該預期數值比較於包含在該回應之內的版本號碼 702a。該應用程式 102 可按各種不同方式獲得該預期版本號碼，像是在本文揭示他處關聯於該 SPS 104 所描述者。

關聯於前述之示範性具體實施例，該應用程式希望能夠確保該所收回應確為由該 SPS 104，而非由另一宣稱 (purport) 為該 SPS 104 的個體，所發送。該應用程式 102 也希望能夠確保該所收回應未經修改。為確保該所收回應的驗證和資料完備性，該應用程式 102 產生一質疑，此為該共享秘密，藉該公用金鑰以將該質疑加密，並且將該經加密質疑發送至該 SPS 104。然後，該 SPS 104 執行處理程序以證明該者確擁有關聯於該應用程式 102

之授權資訊所儲存的私人金鑰。該 SPS 104 藉由將該質疑(即如共享秘密)解密，並且利用該經解密數值以構成該驗證資料，來證明該者確擁有該私人金鑰。該應用程式 102 藉由計算所預期的驗證資料，並且將該回應中的所收驗證資料比較於該所預期驗證資料，來驗證該回應。

現參照第 5 及 6 圖，其中顯示在一根據本文揭示技術之具體實施例中可予執行的處理程序步驟之流程圖。第 5 及 6 圖的步驟彙總如前文所述的處理程序。在步驟 302，該應用程式建立一與 SPS 的會期，並且表示在該會期過程中應予使用的公用金鑰。該 SPS 將利用此公用金鑰以決定待自於後續處理程序中所儲存之授權裡擷取的匹配非對稱私人金鑰。即如前述，該會期可為藉由例如該應用程式與該 SPS 之間所交換的一或更多通訊而建立。在步驟 304，該應用程式產生該共享秘密，並且藉由在步驟 302 中與該會期相關聯的公用金鑰來加密該共享秘密。在步驟 306，該應用程式按如該請求的一部份將該經加密共享秘密發送至該 SPS。在步驟 308，該 SPS 接收該請求。在步驟 310，該 SPS 執行處理程序以消耗一標定權利，即如可在該請求中對於該應用程式的授權所表示者。在步驟 310，對於該消耗處理程序是否成功作出一決定。若否，則控制前進到步驟 314，在此可執行與不成功消耗處理程序相關聯的步驟。此步驟 314 可包含該 SPS 送返一表示步驟 310 處理程序之狀態的數碼。若步驟 312 評估為是，則控制前進到步驟 316，在

此該 SPS 獲得該非對稱金鑰組對中對於該步驟 302 之公用金鑰的私人金鑰。該步驟 316 可包含該 SPS 自含有對於該應用程式之授權資訊的授權資訊儲存器擷取該私人金鑰。自第 5 圖的步驟 316，控制前進到第 6 圖的步驟 402，在此該 SPS 利用該私人金鑰以解密該請求的資料並獲得該共享秘密。在步驟 404，該 SPS 利用該版本號碼、臨時資料(選擇性)及回應資料(選擇性)以構成一訊息，而對此可利用該共享秘密作為金鑰俾決定驗證資料。該 SPS 建構一回應，此者含有該版本號碼、臨時資料(選擇性)、回應資料(選擇性)及驗證資料。該 SPS 的一具體實施例亦可選擇性地加密該回應資料及/或包含在該回應之內的其他資訊。在步驟 406，該 SPS 將該回應發送至該應用程式。該應用程式若有必要可對該回應進行解密，並且計算驗證資料。該應用程式藉由將該所算得驗證資料比較於在該回應中所到的驗證資料以執行驗證處理程序。一具體實施例亦可執行與驗證處理程序相關聯的其他比較作業，例如像是將在該回應中的所收版本號碼比較於一所預期版本號碼。在步驟 408，對於步驟 406 的驗證資料值是否相符作出一決定。該步驟 408 亦可包含決定其他資料值，像是所預期及所收到的版本號碼，之間的比較是否表示一相符。若步驟 408 評估為是，則該應用程式決定驗證處理程序為成功。否則，若步驟 408 評估為否，則該應用程式決定驗證處理程序為失敗。成功的驗證處理程序可向該應用程式確保對於該所收回應

的驗證及資料完備性。

現將說明另一利用本文揭示技術的具體實施例，其中該 SPS 利用自該授權資訊儲存器所擷取的私人金鑰來產生該驗證資料，而此驗證資料係一利用一非對稱加密技術，像是 RSA，的數位簽章。可利用自該授權所擷取的私人金鑰來構成該數位簽章。該應用程式可接收含有該驗證資料(數位簽章)的回應，然後關聯於驗證處理程序以利用該公用金鑰。關聯於驗證處理程序，該應用程式接收即為該數位簽章的經加密雜湊值，計算一由該應用程式所新近產生的雜湊值，並且利用該公用金鑰以將該新近產生雜湊值與該數位簽章驗證比對。在此具體實施例裡，由該 SPS 利用來產生該雜湊值然後再利用該私人金鑰以對其進行加密(由該 SPS 作為「簽章」)的「訊息」可包含下列經接合為一的項目：模組版本號碼、回應資料(若有的話)及/或臨時資料(若有的話)。該臨時資料可為類似於前述者按各種不同方式所決定並獲為該 SPS 及該應用程式所知曉。關聯於此一利用數位簽章的後者具體實施例，該請求中無須含有一共享秘密。相反地，該應用程式可例如在當初始地建立該會期時標定所應使用的公用金鑰。該 SPS 可擷取該私人金鑰，而此者係對應於經使用以構成該回應中之數位簽章的公用金鑰。接著，該應用程式可在接受該回應為有效之前先利用該公用金鑰以執行驗證處理程序。

現將進一步詳細說明該等請求及回應的表示，以及可

運用於一如前所述利用數位簽章之具體實施例內的處理步驟流程圖。

現參照第 7 圖，此圖顯示一可運用於其中該驗證資料為一數位簽章之一具體實施例內的請求之範例。該請求 1002 包含請求資料 1004 以及選擇性的其他資訊 1006。相比於第 3 圖的請求，在此一後者具體實施例裡該經加密共享秘密係自該請求中所省略。而該請求的其他部分則為類似於前文關聯於第 3 圖所述者。

現參照第 8 圖，此圖顯示一範例，而其中說明可供執行以決定包含在經發送至該應用程式 102 之回應 1130 內的資料之處理程序。該回應 1130 可含有一版本號碼 1102a、選擇性的回應資料 1102b、一選擇性的臨時資料 1102c 以及驗證資料 1102d。該等構件 1102a、1102b 及 1102c 可為如前文關聯於第 4 圖所述。該回應 1130 亦含有驗證資料 1102d，然在本具體實施例裡該驗證資料 1102d 為該數位簽章，此係不同於第 4 圖的驗證資料 702d。在本範例 1100 裡，可將該訊息資料 1102 輸入至一加密雜湊函數 1104，此函數產生一雜湊值 1106，然後再以利用該私人金鑰 1112 的加密處理程序 1110 來進行加密，藉此獲得該數位簽章 1102d 俾作為該驗證資料 1102d。關聯於此具體實施例，該 1120 中所包含的元件可構成概如前文所述，並例如由第 4 圖所示，由該封包函數所執行的處理程序。

現參照第 9 及 10 圖，其中顯示可關聯於利用本文揭示

技術之另一具體實施例所執行的處理程序步驟之流程圖。第 9 及 10 圖彙總在一其中該驗證資料係一數位簽章之具體實施例裡所敘述的處理程序。關聯於第 9 及 10 圖之步驟，將能瞭解一些處理步驟是類似於前文中關聯於第 5 及 6 圖所說明者。在步驟 802，該應用程式建立一與 SPS 的會期，並且表示在該會期過程中應予使用的公用金鑰。該步驟 802 類似於第 5 圖的步驟 302。在步驟 804，該應用程式構成該請求並予發送至該 SPS。此一請求之一範例為如第 7 圖所示。在步驟 806，該 SPS 接收該請求，並在步驟 808 執行消耗處理程序。在步驟 810，對於該消耗處理程序是否成功作出一決定。若否，則控制前進到步驟 812。若是，則控制前進到步驟 814，在此該 SPS 自該授權資訊儲存器擷取該私人金鑰。該等步驟 808、810、812 及 814 分別地類似於第 5 圖的步驟 310、312、314 及 316。

在步驟 902，該 SPS 決定該數位簽章作為驗證資料。該版本號碼以及選擇性地該回應資料和該臨時資料係用以構成該訊息資料，而為此訊息資料決定出一雜湊值。然後利用該私人金鑰以將該雜湊值加密，並且所獲經加密資料即為包含在該回應之內以作為該驗證資料的數位簽章。在步驟 904，該 SPS 建構含有該版本號碼、回應資料(選擇性)、臨時資料(選擇性)及驗證資料的回應。該回應資料及/或該回應內的其他資訊可為選擇性地加密，即如關聯於第 6 圖步驟 404 所述者。在步驟 906，

將該回應發送至該應用程式並由其接收。該應用程式解密該回應資料，或視需要該回應的其他部分。在步驟 908，該應用程式藉由計算該訊息之一雜湊值，並且利用該公用金鑰以依據該數位簽章來驗證該所算得雜湊值，藉此驗證該數位簽章。在步驟 910，對於該驗證處理程序是否成功作出一決定。若是，則驗證處理程序為成功並且控制前進到步驟 912。否則，驗證處理程序為失敗並且控制前進到步驟 914。即如關聯於第 6 圖步驟 406 所述，該步驟 908 亦可包含比較其他數值，像是所收及所預期版本號碼，以作為該驗證處理程序的一部份。在此一情況下，該步驟 910 可包含決定該等版本號碼是否相符。可根據驗證資料、版本號碼以及其他在一具體實施例中能夠執行的比較結果來決定成功的驗證處理程序。

即如前述，像是關聯於一利用一數位簽章作為驗證資料的具體實施例，可藉由首先利用一雜湊函數產生一加密雜湊值以決定對於該訊息內容之雜湊值的方式來數位地簽署一訊息。一雜湊函數係一演算法，這可按具一標準長度之「雜湊值」或「雜湊結果」的形式產生一數位表示或「指紋」。當使用相同的雜湊函數時，對於該訊息內容所進行的任何變動都會產生不同的雜湊結果。然後將對該訊息內容所計算的雜湊值予以加密。經發送至另一方之訊息可包含該訊息內容以及該經加密雜湊值而作為簽署的一部份。該經加密雜湊值亦可稱為數位簽章。在

一具體實施例中可運用業界所眾知的任何各種不同雜湊函數及加密技術。接著，該訊息的接收者可利用與該發送者相同的雜湊演算法來計算一對於該訊息內容的新雜湊值，並且利用該公用金鑰依據該數位簽章來執行該新雜湊值的驗證處理程序。

本文揭示所述之示範性具體實施例可為關聯於防止軟體剽竊而運用。即如一範例，一應用程式 102 的未經授權拷貝可能被安裝在一電腦上以供使用。而當一使用者嘗試執行該應用程式的未經授權拷貝時，一攻擊者可例如以另一模組來取代該應用程式 102 所與其相通訊的 SPS 104，即如本文揭示所述者。一攻擊者亦可攔截一由該 SPS 104 所發送的回應並加以修改。一具體實施例可利用本文揭示技術，因而該應用程式 102 能夠與該 SPS 進行通訊來決定該授權是否為有效，並且准允必要權利以供執行所請求操作。可運用本文揭示技術來確保由該應用程式 102 所收到之回應的完備性和驗證，所以該應用程式 102 能夠偵測出一既經一攻擊者所駭解的所收通訊，即如前文所述。

關聯於本文揭示所述之示範性具體實施例，該私人金鑰可為關聯於與一特定軟體應用程式相關的授權資訊而儲存。例如，即如前述，該私人金鑰可經納入作為與一應用程式相關聯之授權資訊的一部份，同時該授權資訊可為包含在一授權資訊儲存器內。熟諳本項技藝之人士將能瞭解一應用程式的授權資訊是一種具有特別類型的

應用程式特定資訊。除授權資訊外，其他利用本文揭示技術之具體實施例可關聯於其他類型的應用程式特定資訊來儲存並關聯該私人金鑰。並且，除一授權資訊儲存器以外，可將與一應用程式相關聯的私人金鑰及應用程式特定資訊儲存在其他類型的貯庫或資料儲存器裡。更一般地，可將該應用程式特定資訊，包含該私人金鑰在內，儲存在任何類型的安全與受信賴資訊儲存器中。該安全與受信賴資訊儲存器可為一用以儲存一或更多不同類型之應用程式特定資訊，包含該私人金鑰在內，的資料儲存器。同時，即如關聯於授權資訊所述，除非消耗處理程序成功，否則可不擷取該私人金鑰，其中該消耗處理程序包含例如決定對於該應用程式是否存在一有效授權，以及該授權是否准允該等標定權利。如此，該授權資訊儲存器可提供關聯於該私人金鑰的安全及存取控制，原因在於除非消耗處理程序成功，否則是無法獲得該私人金鑰。而在一其中使用一不同類型的安全與受信賴之資訊儲存器，然非該授權資訊儲存器，的具體實施例裡，除該消耗處理程序以外，可在提供存取至該私人金鑰之前，先要求成功地執行其他的驗證及/或核可(validation)處理程序。此等驗證及/或核可處理程序可隨具體實施例而變，並且可包含例如驗證嘗試獲得該私人金鑰的應用程式或其他模組提供必要資料、驗證及/或核可其他包含在該應用程式特定資訊內的資料、驗證關於硬體及/或軟體資訊，例如像是該應用程式係經執行於一

利用一特定作業系統的特定電腦系統上等等。

前文僅敘述說明本文揭示技術之使用方式的兩項範例。熟諳本項技藝之人士將能瞭解確可關聯於在相同或不同的電腦系統上自任何發送者傳送至任何接收者之通訊以更廣泛地運用本文揭示技術。此外，該等技術可為關聯於針對兩個模組或其他個體而在一單一方向上所發送的通訊，或是在兩者方向上所發送的通訊，而運用。對於本文揭示範例而言，該等技術係關聯於在一自該 SPS 104 至該應用程式 102 之單一方向上所發送的通訊所述。然本文揭示技術亦可為單獨地，或是合併於利用本文揭示技術而關聯於自該 SPS 至該應用程式的通訊，關聯於自該應用程式 102 發送至該 SPS 104 的通訊所運用。

雖既已按照特定於結構特性及/或方法動作之語言來描述主題項目，然應瞭解在後載申請專利範圍中所定義主題項目並非必然地受限於前述各項特定特性或動作。相反地，上述各項特定特性及動作係按如實作該申請專利範圍之範例形式所揭示。

【圖式簡單說明】

自所述之本發明示範性具體實施例的詳細說明，且併同於隨附圖式，將更能顯知本發明的特性與優點，其中：

第 1 圖係一可運用於有關本文揭示所述技術之一具體

實施例的環境之範例；

第 2 圖係一可包含在一具體實施例內並且關聯於執行本文揭示技術而運用之多項元件的範例；

第 3 圖係一可運用於執行本文揭示技術之一具體實施例中的請求之範例表示；

第 4 圖係一回應以及在一運用本文揭示技術之具體實施例中可如何地決定包含在該回應內的驗證資料之範例表示；

第 5 及 6 圖為在一運用本文揭示技術之具體實施例中可予執行的處理程序步驟之流程圖；

第 7 圖係一可運用於執行本文揭示技術之一具體實施例中的另一請求之範例表示；

第 8 圖係一另一回應以及在一運用本文揭示技術之具體實施例中可如何地決定包含在該回應內的驗證資料之範例表示；以及

第 9 及 10 圖為在另一運用本文揭示技術之具體實施例中可予執行的處理程序步驟之流程圖。

【主要元件符號說明】

10	範例圖式
12	電腦
14	網路
16	伺服器

20	處理單元
22	記憶體
30	儲存裝置
32	系統匯流排
100	範例圖式
102	應用程式
104	軟體保護服務 (SPS)
106	授權資訊儲存器
108	構件
110	請求
112	回應
600	範例圖式
602	請求
604	請求資料
606	經加密共享秘密
608	其他資訊
700	範例圖式
702	構件
702a	版本號碼
702b	回應資料
702c	臨時資料 (Nonce)
702d	驗證資料
704	回應
710	共享秘密

- 712 封包函數
- 1000 範例圖式
- 1002 請求
- 1004 請求資料
- 1006 其他資訊
- 1100 範例圖式
- 1102 訊息資料
 - 1102a 版本號碼
 - 1102b 回應資料
 - 1102c 臨時資料
 - 1102d 驗證資料/數位簽章
- 1104 加密雜湊函數
- 1106 雜湊值
- 1110 加密處理程序
- 1112 私人金鑰
- 1120 多個元件
- 1130 回應

發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫)

※ 申請案號：98114894

※ 申請日期：2009 年 5 月 5 日

※IPC 分類：H04L 29/06 (2006.01)
H04L 9/70 (2006.01)

一、發明名稱：(中文/英文)

確保通訊之驗證及完備之技術

TECHNIQUES FOR ENSURING AUTHENTICATION AND INTEGRITY OF COMMUNICATIONS

二、中文發明摘要：

茲說明多項用於確保所收訊息之資料完備性及驗證的技術。一項技術包含自一第一模組，其將一請求發送至一第二模組，其中該請求含有一第一部分，此部分係一藉一公用金鑰所加密的共享秘密；由該第二模組自一含有用於該第一模組之授權資訊或其他應用程式特定資訊的安全及受信賴資訊儲存器，像是一授權資訊儲存器，獲得一私人金鑰；利用該私人金鑰以解密該第一部分並獲得該共享秘密；自該第二模組將一回應發送至該第一模組，其中該回應含有驗證資料和至少一運用於該共享秘密的資料項目以供決定該驗證資料；以及由該第一模組執行驗證處理程序，藉此驗證包含在該回應中的驗證資料。

三、英文發明摘要：

Techniques are described for ensuring data integrity and authentication of received messages. One technique includes sending a request from a first module to a second module in which the request includes a first portion that is a shared

secret encrypted with a public key, obtaining by the second module a private key from a secure and trusted information store, such as a license information store, including license information or other application specific information for the first module, using the private key to decrypt the first portion and obtain the shared secret, sending a response from the second module to the first module in which the response includes authentication data and at least one data item used with the shared secret to determine the authentication data, and performing by the first module verification processing to verify the authentication data included in the response.

七、申請專利範圍：

1. 一種電腦實作之通訊方法，包含以下步驟：

將一請求自一第一模組發送至一第二模組，該請求包含一第一部分，此部分為藉一非對稱金鑰組對之公用金鑰所加密的一共享秘密；

由該第二模組自一含有用於該第一模組之應用程式特定資訊的安全且受信賴資訊儲存器，獲得該非對稱金鑰組對的一私人金鑰；

由該第二模組利用該私人金鑰來解密該第一部分以獲得該共享秘密；

將一回應自該第二模組發送至該第一模組，該回應含有用於該共享秘密的驗證資料及至少一資料項目以供決定該驗證資料；以及

由該第一模組利用該共享秘密以執行驗證處理程序，藉此對包含在該回應內的驗證資料進行驗證。

2. 如申請專利範圍第 1 項所述之方法，其中該共享秘密係一與該第一模組和該第二模組間之一通訊會期相關聯的會期金鑰，並且該第一模組對於各個通訊會期產生一不同的會期金鑰。

3. 如申請專利範圍第 1 項所述之方法，進一步包含以下步驟：

由該第二模組執行驗證處理程序以決定是否提供包含在用於該第一模組之應用程式特性資訊內的私人金鑰，而僅在成功地執行有關該私人金鑰的驗證處理程序之後，方才自該安全及受信賴資訊儲存器擷取該私人金鑰並予提供至該第二模組。

4. 如申請專利範圍第 1 項所述之方法，其中該第二模組執行處理程序以利用一含有一版本號碼的訊息決定該驗證資料。

5. 如申請專利範圍第 4 項所述之方法，其中該訊息包含回應資料或一臨時資料的至少一者。

6. 如申請專利範圍第 5 項所述之方法，其中該回應包含用於構成該訊息的資料項目。

7. 如申請專利範圍第 1 項所述之方法，其中該驗證處理程序包含：該第一模組計算第一驗證資料，並且將該第一驗證資料與包含在該回應內的驗證資料比較。

8. 如申請專利範圍第 7 項所述之方法，其中該第一驗證資料係利用包含在該回應之內的至少一其他資料項目所算得。

9. 如申請專利範圍第 8 項所述之方法，其中包含在該回應之內的至少一其他資料項目係一版本號碼。

10. 如申請專利範圍第 1 項所述之方法，其中該驗證資料係利用一運用該共享秘密作為一金鑰的封包函數所決定。

11. 如申請專利範圍第 10 項所述之方法，其中該驗證資料係利用依據一雜湊函數之一金鑰雜湊演算法以及該共享秘密作為一金鑰所決定。

12. 如申請專利範圍第 10 項所述之方法，其中該驗證資料係利用運用該共享秘密作為一對稱金鑰的一對稱加密技術所決定。

13. 一種電腦實作之通訊方法，其中包含以下步驟：

將一請求自一第一模組發送至一第二模組；

由該第二模組自一含有授權資訊之授權資訊儲存器，獲得一非對稱金鑰組對的私人金鑰；

將一回應自該第二模組發送至該第一模組，該回應含有利用該私人金鑰及至少一資料項目所構成的一數位簽章；以及

由該第一模組利用該非對稱金鑰組對的公用金鑰執行驗證處理程序，以驗證該回應內的數位簽章。

14. 如申請專利範圍第 13 項所述之方法，其中該第二模組決定對於一含有該至少一資料之訊息的一雜湊值，利用該私人金鑰對該雜湊值進行加密，以及將該雜湊值納入在該回應內以作為該回應的數位簽章。

15. 如申請專利範圍第 13 項所述之方法，其中該驗證處理程序包含：利用該至少一資料項目並利用該非對稱金鑰組對的公用金鑰以計算一新雜湊值，藉此將該新雜湊值與該回應的數位簽章驗證比對，並且其中該私人金鑰係僅在根據由一有效授權所准允的一或更多標定權利，而成功地執行決定該第一模組之有效授權的處理程序之後，方能自該授權資訊儲存器獲得。

16. 如申請專利範圍第 14 項所述之方法，其中該訊息包含一版本號碼，以及一臨時資料和一回應資料的至少一者。

17. 一種電腦可讀取媒體，而於其上儲存有可執程式碼以確保一自一第二模組發送至一第一模組之通訊的驗證和資料完備性，該電腦可讀取媒體其上儲存有程式碼以供：

由一第二模組自一第一模組接收一第一通訊，該第一通訊包含一第一部分，此部分為經一非對稱金鑰組對之

公用金鑰所加密的一共享秘密；

由該第二模組根據一授權及標定權利執行消耗處理程序；

當成功地執行消耗處理程序時，由該第二模組自一儲存用於該第一模組之授權資訊的授權資訊儲存器擷取非對稱金鑰組對之私人金鑰；

由該第二模組利用該私人金鑰來解密該第一部分以獲得該共享秘密；

由該第二模組利用該共享秘密及至少一資料項目決定驗證資料；以及

將一第二通訊自該第二模組發送至該第一模組，該第二通訊含有該驗證資料及該至少一資料項目。

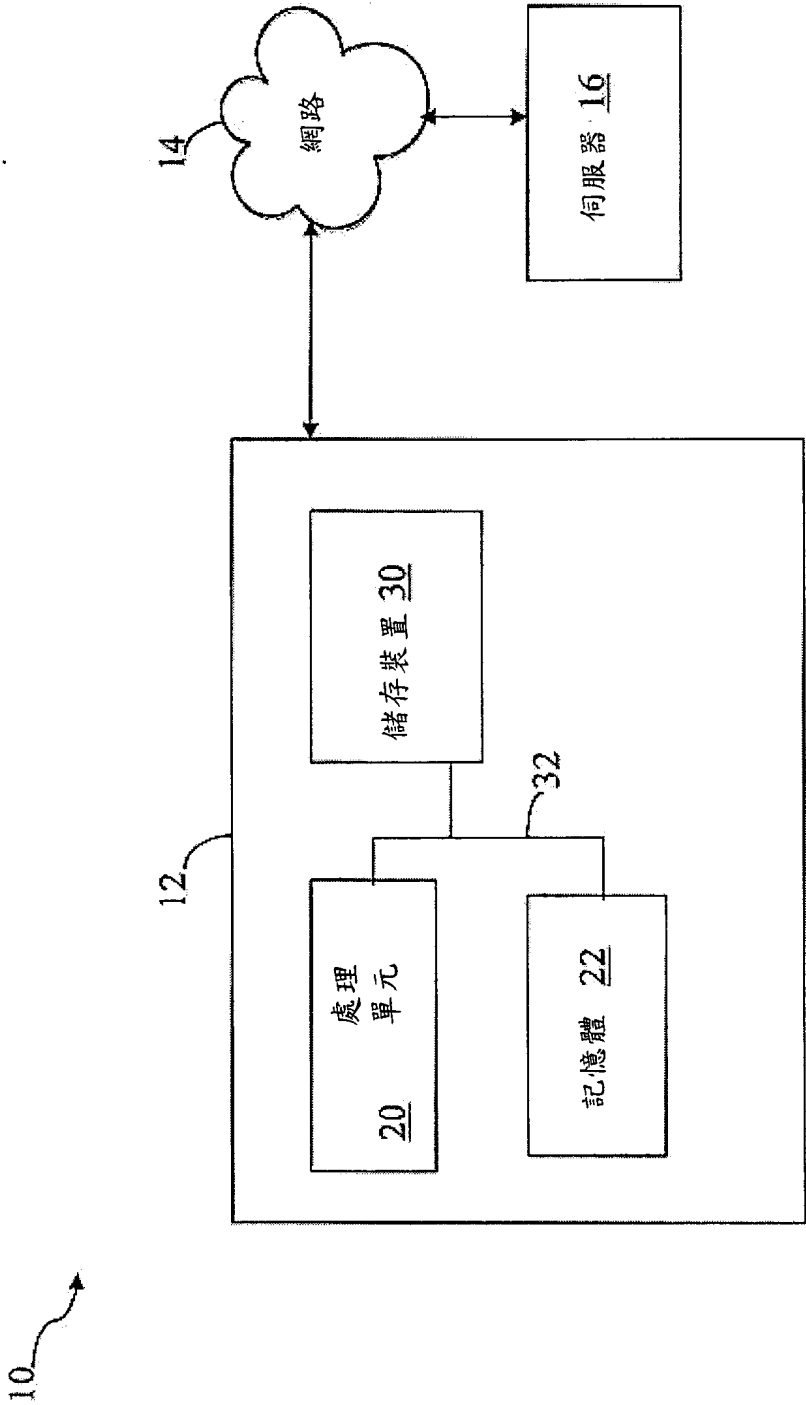
18. 如申請專利範圍第 17 項所述之電腦可讀取媒體，進一步包含其上儲存有可執行程式碼以供：

由該第一模組利用該共享秘密以執行驗證處理程序，藉此對包含在該第二通訊內的驗證資料進行驗證。

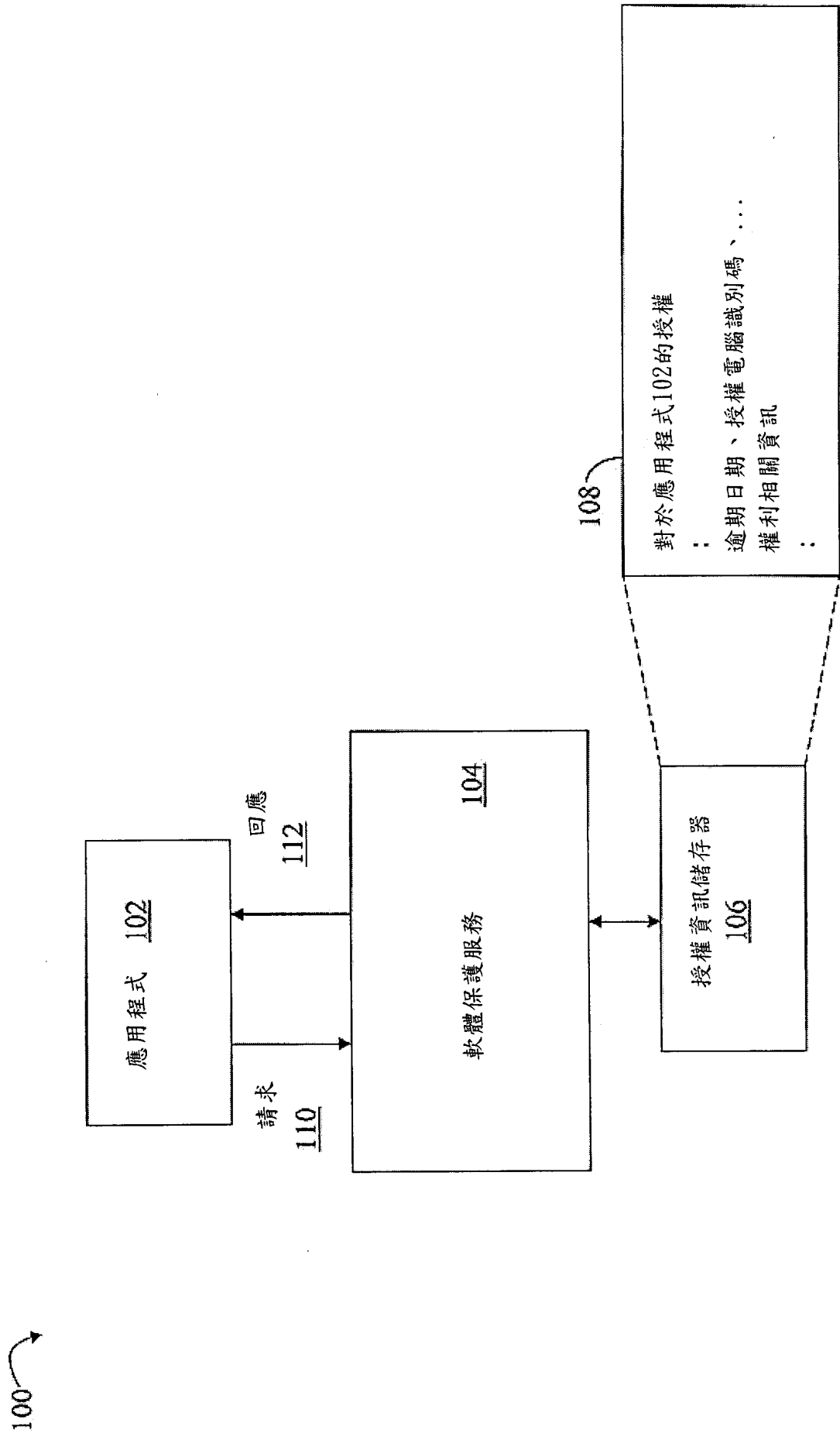
19. 如申請專利範圍第 18 項所述之電腦可讀取媒體，其中該至少一資料項目含有一版本號碼，並且該驗證處理程序包含將該回應之版本號碼與一所預期版本號碼比較，而其中該消耗處理程序包含決定是否存在用於該第一模組的一有效授權，以及該等所標定權利在該有效授權中是否獲准允，且僅在成功地決定一有效授權以及該

有效授權中准允該等標定權利之後，方能自該授權資訊儲存器擷取該私人金鑰。

20. 如申請專利範圍第 17 項所述之電腦可讀取媒體，其中該驗證資料係利用運用該共享秘密作為一對稱金鑰之一對稱加密技術，或者根據運用該共享秘密作為一金鑰之一雜湊函數的一金鑰雜湊演算法，所決定。

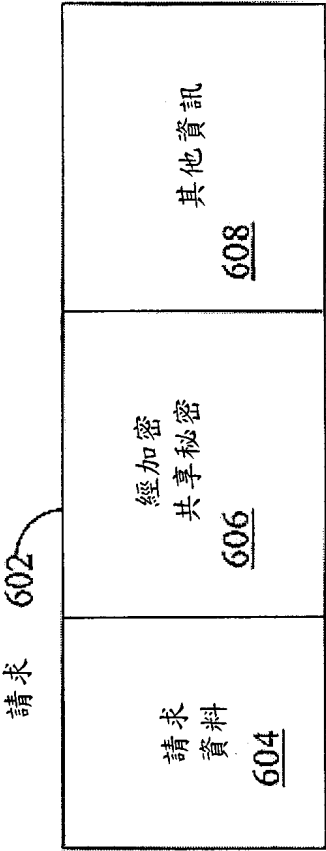


第 1 圖

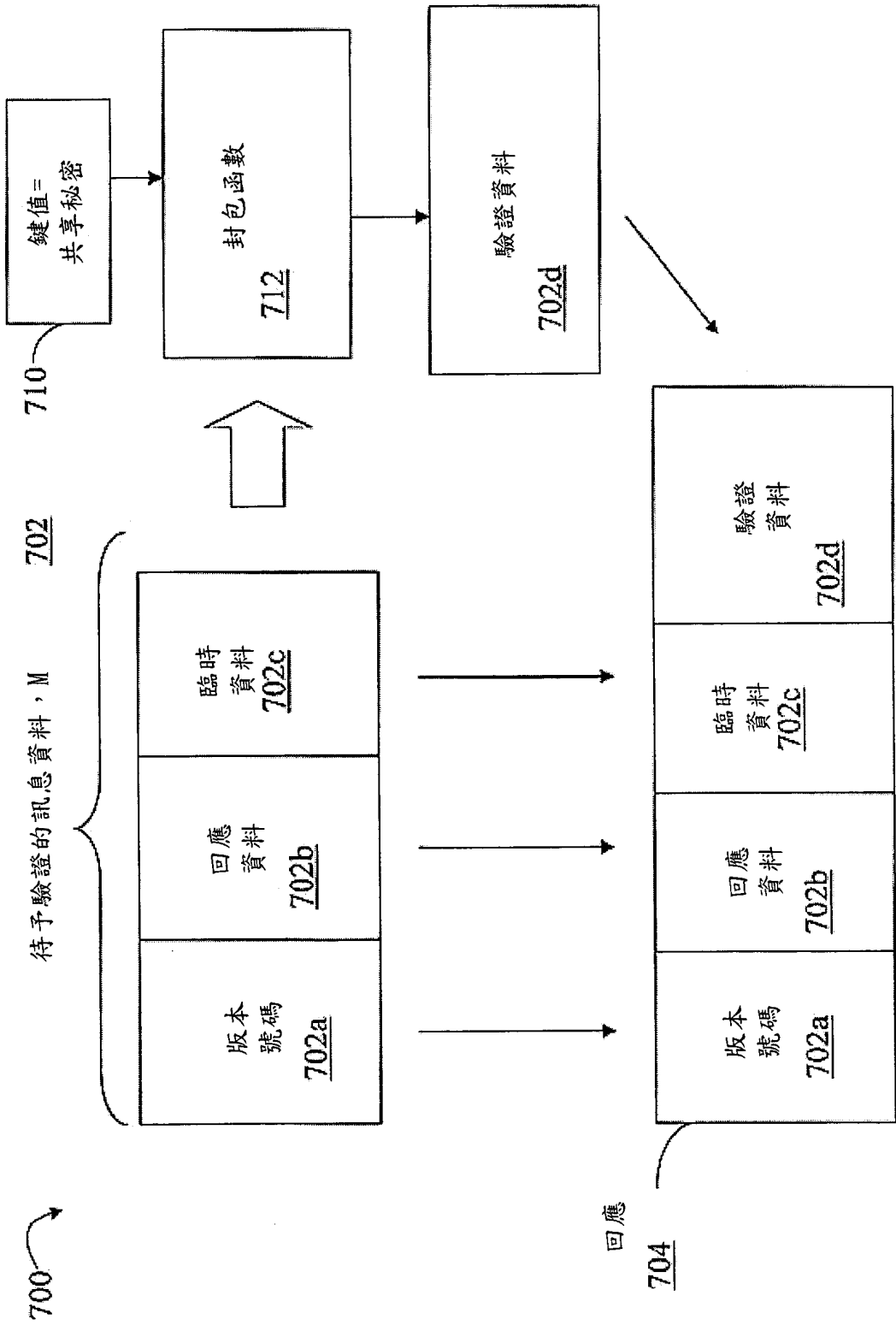


第 2 圖

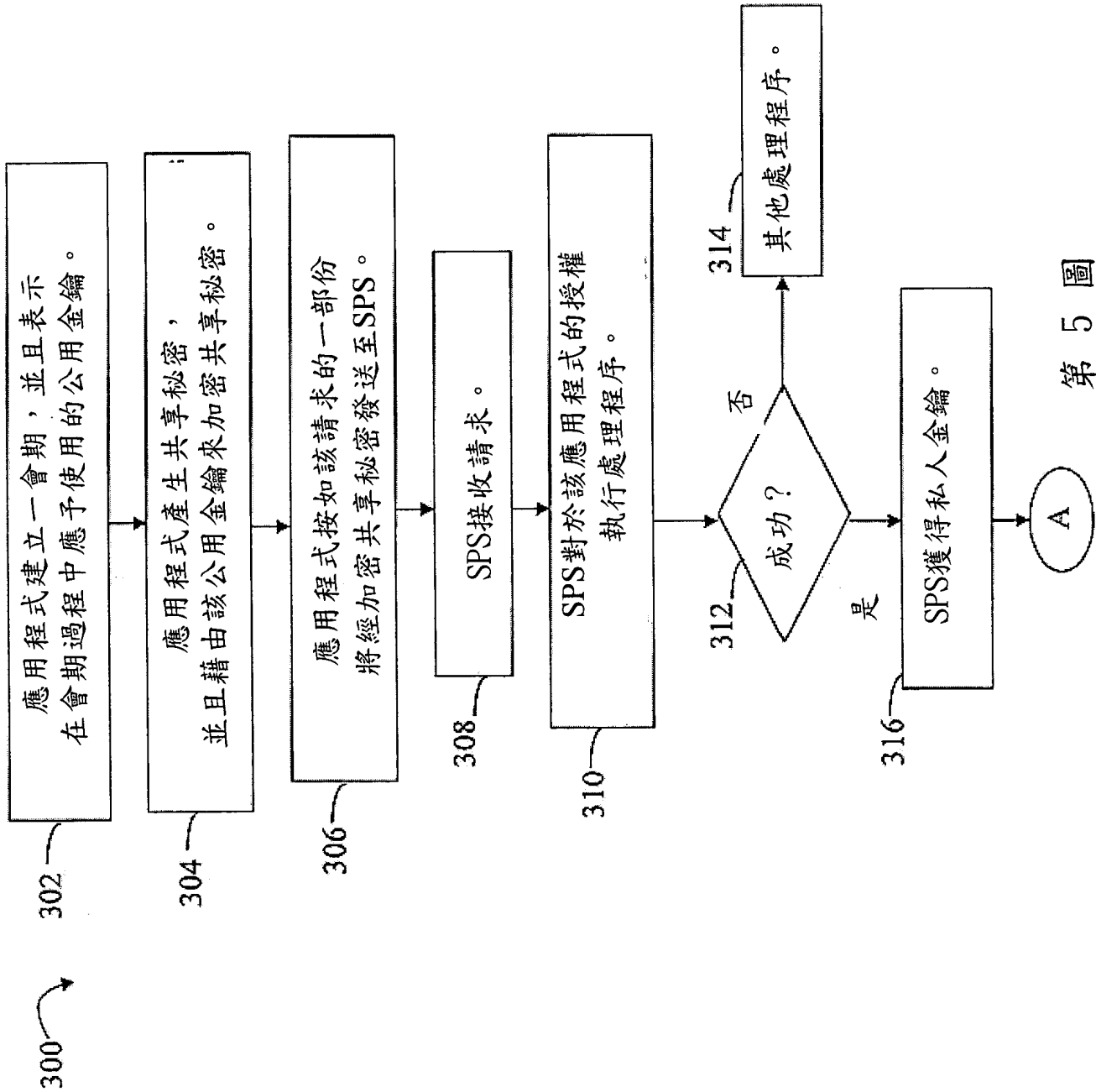
600 ↗



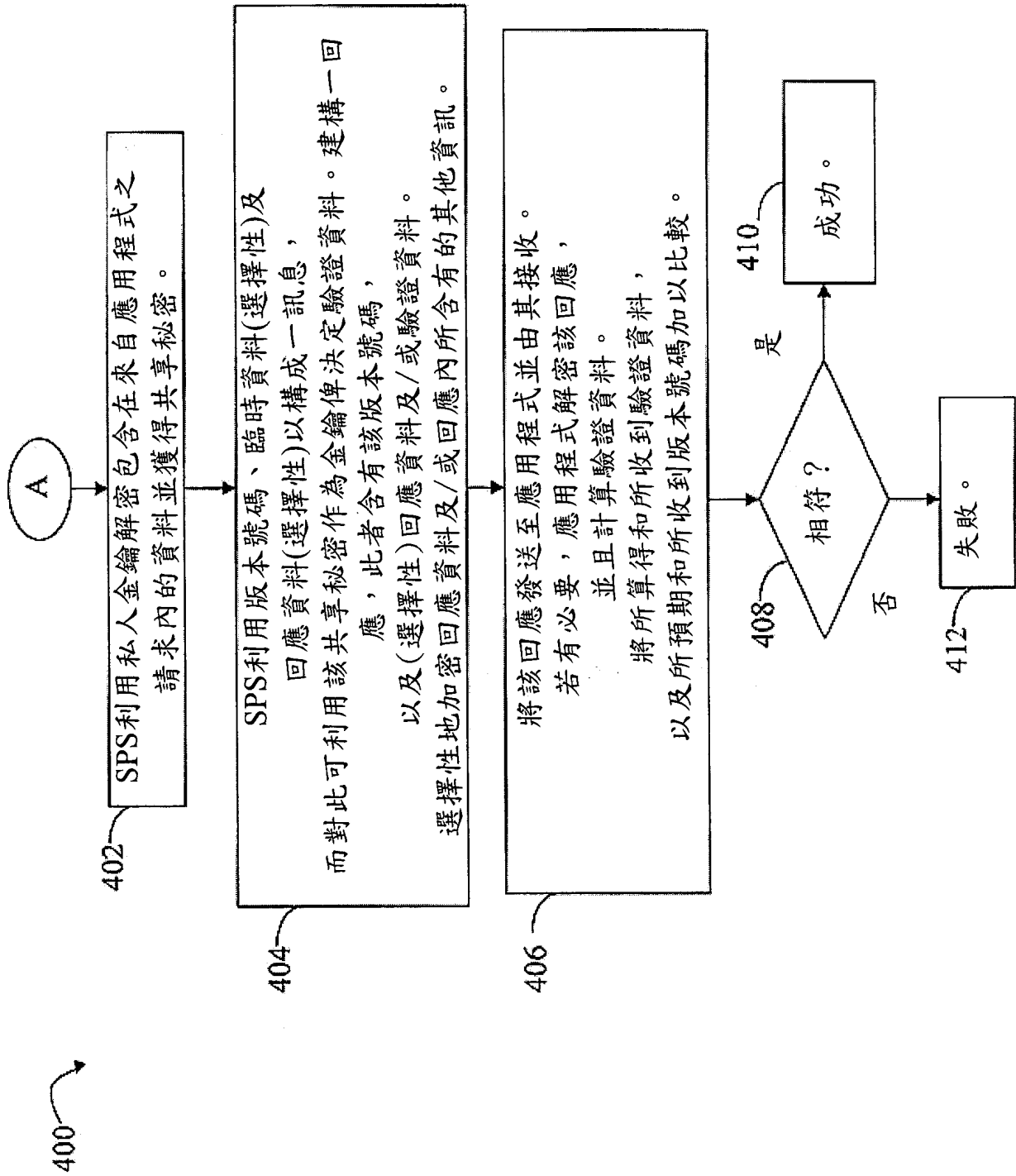
第 3 圖



第 4 圖

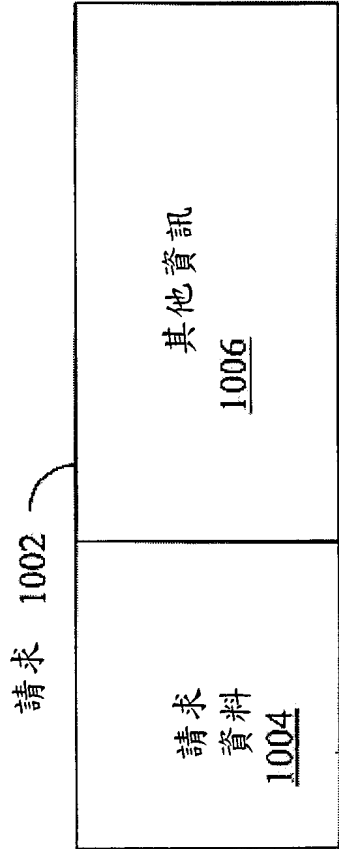


第 5 圖

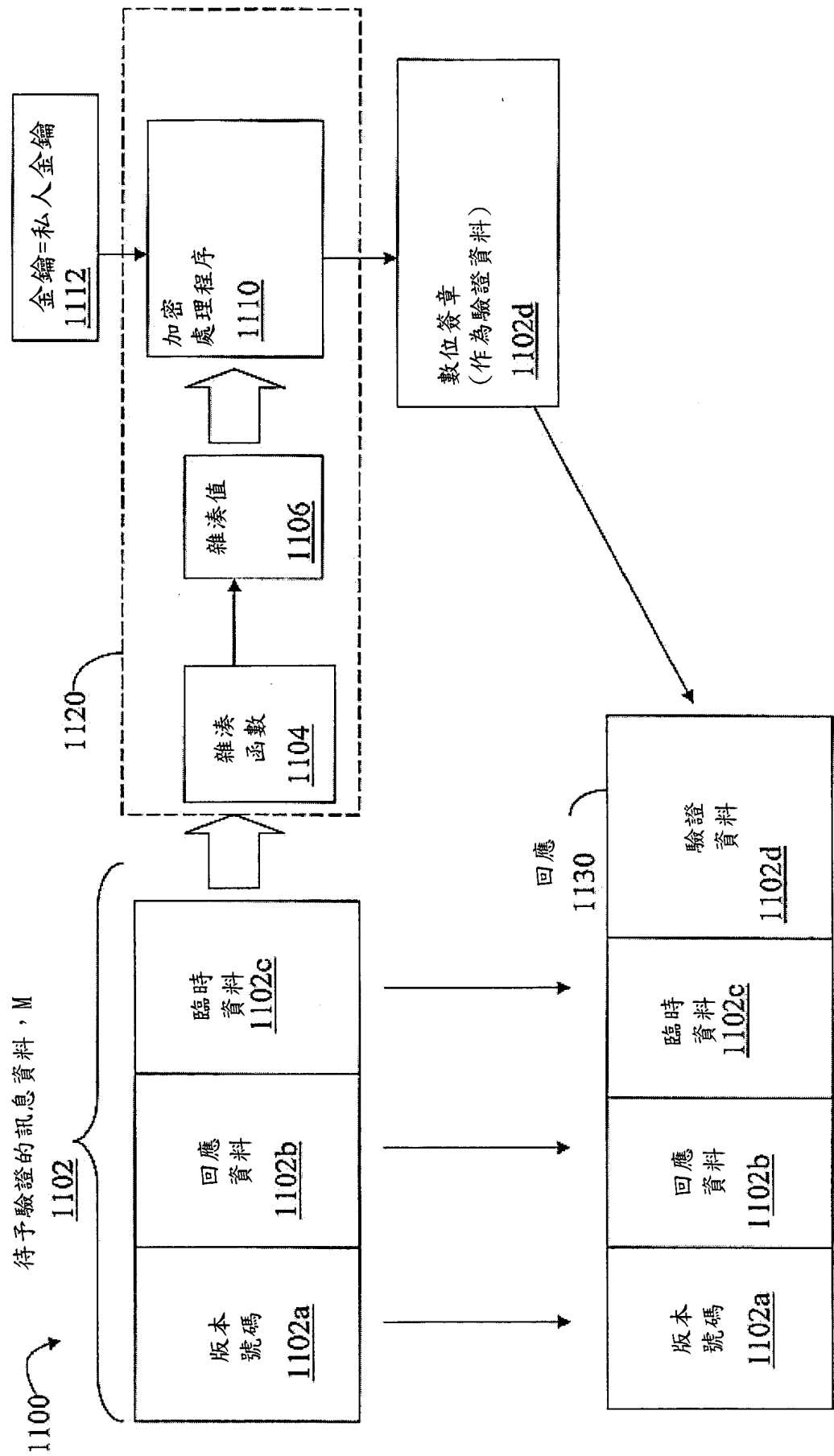


第 6 圖

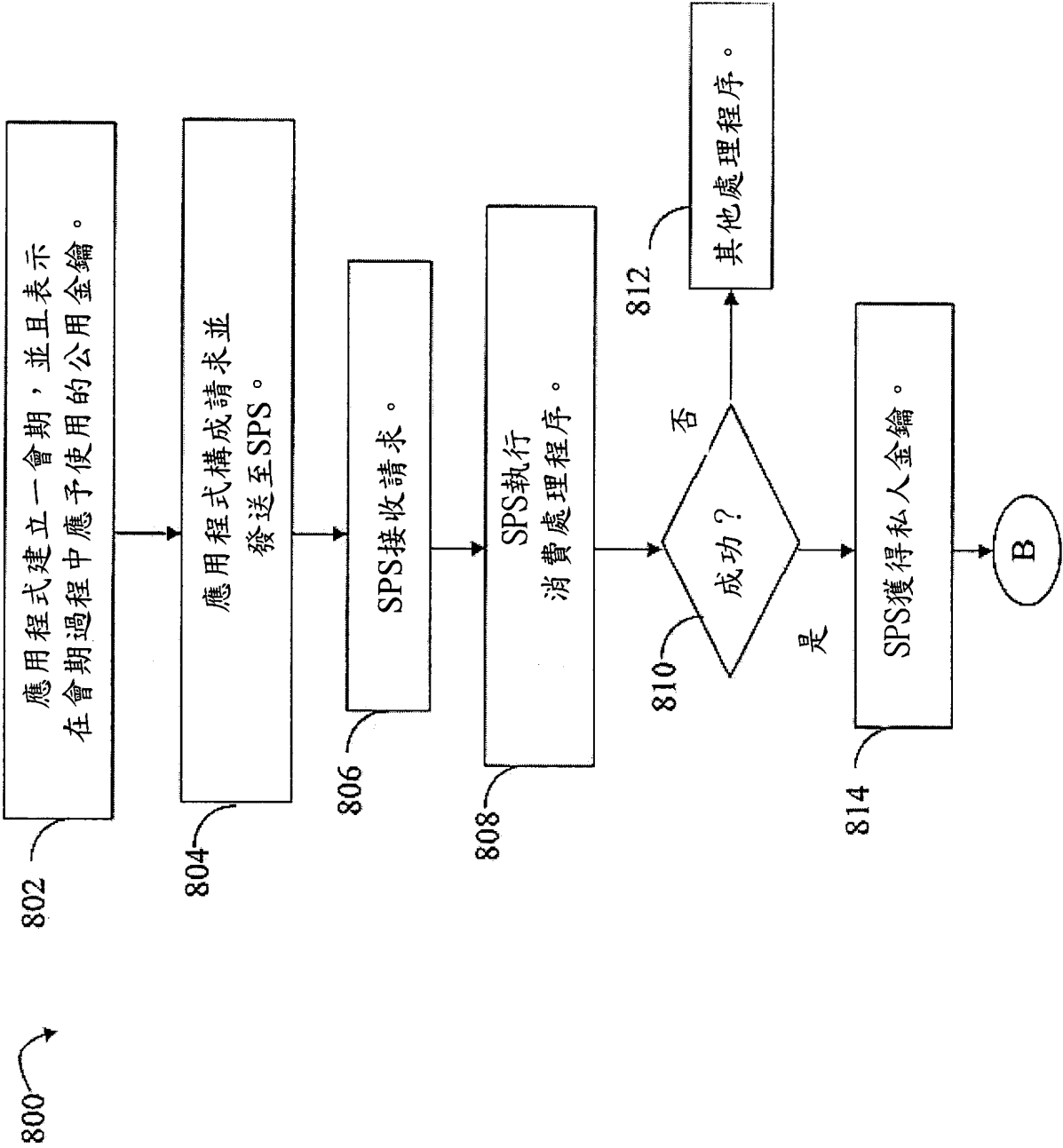
1000 ↗



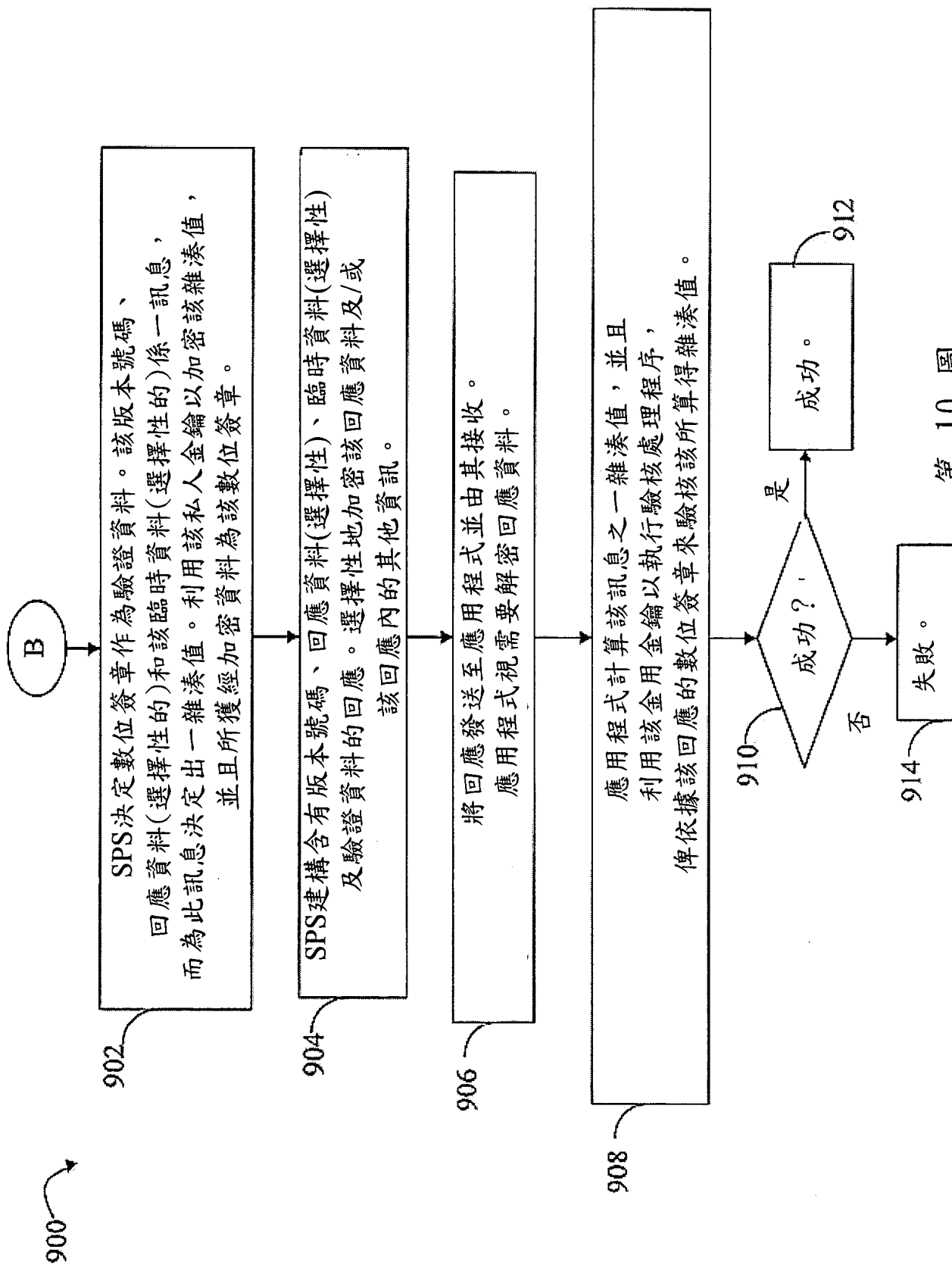
第 7 圖



第 8 圖



第 9 圖



第 10 圖

四、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

- 100 範例圖式
- 102 應用程式
- 104 軟體保護服務(SPS)
- 106 授權資訊儲存器
- 108 構件
- 110 請求
- 112 回應

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：