



(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 I467944 B

(45)公告日：中華民國 104 (2015) 年 01 月 01 日

(21)申請案號：101120296

(22)申請日：中華民國 101 (2012) 年 06 月 06 日

(51)Int. Cl. : H04B5/00 (2006.01)

H04L9/14 (2006.01)

H04L9/32 (2006.01)

(30)優先權：2011/06/07 美國

61/494,242

2011/06/21 美國

13/165,440

(71)申請人：美國博通公司 (美國) BROADCOM CORPORATION (US)

美國

(72)發明人：啟成 羅伯特 KITCHEN, ROBERT (GB)

(74)代理人：莊志強

(56)參考文獻：

TW I324754

TW 200919354A

TW 200929986A

TW 201026011A

CN 101369306B

CN 201622584U

US 7685429B2

US 2010/0043061A1

Standard ECMA-386, "NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES", 2nd edition, June 2010.

審查人員：陳柏全

申請專利範圍項數：21 項 圖式數：8 共 30 頁

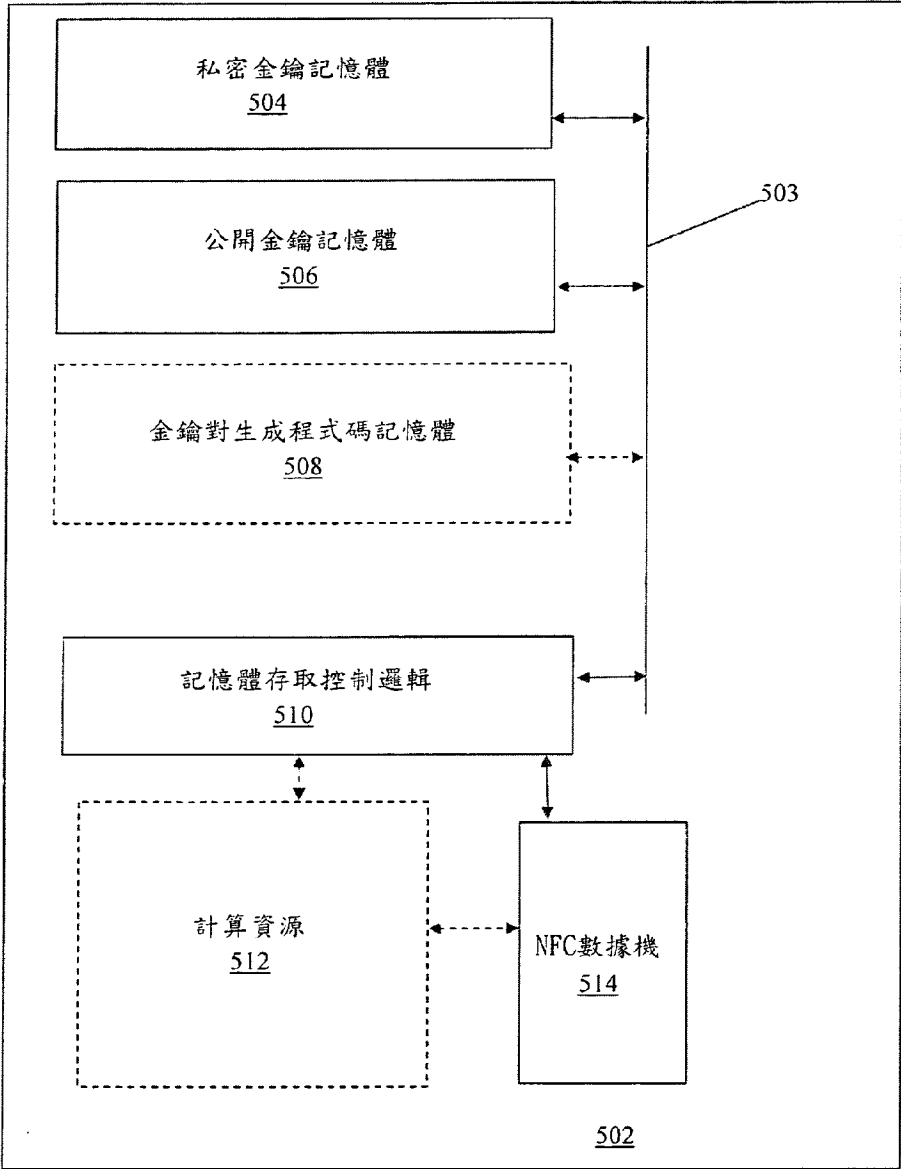
(54)名稱

提供加密通訊的方法、NFC 通訊裝置、及用於加密通訊的系統

NFC COMMUNICATIONS DEVICE FOR SETTING UP ENCRYPTED EMAIL COMMUNICATION

(57)摘要

本發明提供了用於建立加密電子郵件的通訊的 NFC 通訊裝置，其中使用 NFC 通訊來增強加密金鑰和加密處理的安全性。為了加密和解密消息，公開金鑰加密需要使用一對金鑰，即公開金鑰和私密金鑰。本發明的各個實施方式提供加密和/或解密消息的一個或多個方面所需要的資訊的存儲，其中通過 NFC 通訊介面可利用該資訊。啟用 NFC 的裝置與正在執行電子郵件用戶端或以其他方式提供對電子郵件用戶端的訪問的計算平臺物理上接近。一旦啟用 NFC 的裝置和計算平臺在彼此的 NFC 通訊範圍內，則發生建立加密和/或解密處理所需要的資訊的傳輸。由於加密和/或解密金鑰和/或相關的加密處理參數不存儲在計算平臺上，所以提高了該資訊的安全性。



- 502 . . . 啟用 NFC 的裝置
- 503 . . . 匯流排
- 504 . . . 私密金鑰記憶體
- 506 . . . 公開金鑰記憶體
- 508 . . . 金鑰對生成程式碼記憶體
- 510 . . . 記憶體存取控制邏輯
- 512 . . . 計算資源
- 514 . . . NFC 數據機

圖5

發明專利說明書

公告本

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※申請案號：101120296

※申請日：101.6.6

※IPC 分類：H04B 5/00 (2006.01)

H04L 9/14 (2006.01)

H04L 9/32 (2006.01)

一、發明名稱：(中文/英文)

提供加密通訊的方法、NFC 通訊裝置、及用於加密通訊的系統

NFC COMMUNICATIONS DEVICE FOR SETTING UP
ENCRYPTED EMAIL COMMUNICATION

二、中文發明摘要：

本發明提供了用於建立加密電子郵件的通訊的 NFC 通訊裝置，其中使用 NFC 通訊來增強加密金鑰和加密處理的安全性。為了加密和解密消息，公開金鑰加密需要使用一對金鑰，即公開金鑰和私密金鑰。本發明的各個實施方式提供加密和/或解密消息的一個或多個方面所需要的資訊的存儲，其中通過 NFC 通訊介面可利用該資訊。啟用 NFC 的裝置與正在執行電子郵件用戶端或以其他方式提供對電子郵件用戶端的訪問的計算平臺物理上接近。一旦啟用 NFC 的裝置和計算平臺在彼此的 NFC 通訊範圍內，則發生建立加密和/或解密處理所需要的資訊的傳輸。由於加密和/或解密金鑰和/或相關的加密處理參數不存儲在計算平臺上，所以提高了該資訊的安全性。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：圖 5。

(二)本代表圖之元件符號簡單說明：

- 502 啟用 NFC 的裝置
- 503 匯流排
- 504 私密金鑰記憶體
- 506 公開金鑰記憶體
- 508 金鑰對生成程式碼記憶體
- 510 記憶體存取控制邏輯
- 512 計算資源
- 514 NFC 數據機

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

六、發明說明：

【發明所屬之技術領域】

本申請要求於 2011 年 6 月 7 日提交的美國臨時申請第 61/494,242 號、以及於 2011 年 6 月 21 日提交的美國實用申請第 13/165,440 號的權益，其全部內容通過援引加入於本申請中。

本發明總體上關於一種近場通訊（NFC）裝置及其操作與應用。更具體地，本發明關於一種使用 NFC 通訊裝置來建立加密通訊的方法和設備。

【先前技術】

半導體製造技術的進步引起電路封裝密度顯著增大以及運算速度顯著提高。反過來，這些進步使得設計者們能夠創作出以前不實際的許多處理器和通訊功能。在一些情況下，這些功能是被組合在單個高度集成的裝置中的。在其他情況下，這些功能被分佈在兩個以上裝置或晶片中。

數位系統架構的進步和半導體器件速度和密度的進步共同導致大型計算能力的可用性以及成本相對低的數位通訊網路。反過來，這又造成均能夠與其他進行通訊的電腦和其他計算資源具有大的裝機率。普遍存在的計算平臺和網路能夠實現的一種通訊形式為電子郵件，更普遍地稱為電子郵件（email）。

由於越來越多的資訊通過數位通訊網路進行傳遞，所以非指定收件人看到敏感資訊的可能性在逐漸增大。為了保護這種資訊的隱私性，多年來已經開發出各種加密處理（cryptographic process）和技術。

某些加密方案要求寄件者和收件人具有共用的秘密

(secret)，以便寄件者將消息加密並且收件人成功地將資訊解密。例如，資料加密標準使用對稱金鑰對。對稱金鑰對指的是寄件者的加密金鑰與收件人的解密金鑰相同。對稱式金鑰密碼編譯系統的一個缺點在於，兩個金鑰均必須保密，以使得保持寄件者和收件人之間的通訊安全。

克服對稱式金鑰密碼編譯系統的金鑰安全性問題的主要部分的另一種加密系統被稱為公開金鑰加密。公開金鑰加密使用非對稱金鑰對，即，寄件者加密消息所使用的金鑰與收件人解密消息所使用的金鑰不同。在該方案中，用於加密消息的金鑰被稱為公開金鑰，用於解密消息的金鑰被稱為私密金鑰。公開金鑰/私密金鑰對一起生成並且被相關，以使得僅僅使用私密金鑰才可將用公開金鑰加密的消息解密。與對稱式金鑰密碼編譯相比，公開金鑰（即非對稱金鑰）加密的一個重要優點在於僅一個金鑰而非兩個金鑰需要保持保密。實際上，公開金鑰可以廣泛地分佈，這是因為僅僅私密金鑰才可將使用公開金鑰加密的消息解密。

已經開發出各種公開金鑰加密系統，一種眾所周知的市場上可買到的公開金鑰系統稱為 PGP。PGP 為“良好隱私”的首字母縮寫。市場上可買到的 PGP 加密軟體在計算平臺上作用於電子郵件用戶端，以生成用於發送至指定的收件人的加密郵件，並且進一步生成所接收的加密電子郵件的解密版本或明文版本。如上所述，各種金鑰必須可用於公開金鑰加密系統，這種公開金鑰加密系統包括 PGP。由於這些金鑰於諸如個人電腦的計算平臺上的存在會造成安全隱患，這是因為資訊可能會無意地或由於惡意軟體而被

洩漏。

需要提高加密金鑰和加密處理的安全性的方法、設備和系統。

【發明內容】

本發明提供了一種提供加密通訊的方法，包括：將公開金鑰/私密金鑰對的私密金鑰存儲在第一啟用 NFC 的通訊裝置的第一記憶體中；以及通過近場通訊將私密金鑰發送至第二啟用 NFC 的通訊裝置，所述第二啟用 NFC 的通訊裝置被設置為與計算平臺進行通訊；其中，在加密處理中，所述計算平臺執行使用從所述第一啟用 NFC 的通訊裝置中接收到的私密金鑰的程式碼。

【實施方式】

現在，將參照圖式描述本發明。在圖式中，相同的參考標號通常表示相同的、功能上相同的和/或結構上相同的元件。元件第一次出現所在的圖式由參考標號中最左邊的數字表示。

以下的詳細描述參考圖式來說明與本發明一致的示例性實施方式。詳細的描述中所提到的“一個示例性實施方式”、“示意性實施方式”、“示例性實施方式”等表示所描述的示例性實施方式可包括特定的特徵、結構或特性，但並非是每個示例性實施方式必須包括特定的特徵、結構或特性。此外，這種措詞並非必然表示相同的示例性實施方式。而且，當結合示例性實施方式描述特定的特徵、結構或特性時，根據不論是否是明確闡述的其他示例性實施方式來改變這種特徵、結構或特性都在相關領域的普通技術人員的知識範圍之內。

提供本文所描述的示例性實施方式是用於示意性目的的，而不是限制性的。其他示例性實施方式是可行的，並且在本發明的精神和範圍之內，可對這些示例性實施方式進行修改。因此，詳細的描述並不意指限制本發明。相反，本發明的範圍僅根據所附的申請專利範圍及其等同物進行限定。

示例性實施方式的以下詳細描述將完整地揭示本發明的普適性，使得人們為了各種應用，通過應用相關領域的普通技術知識在無需進行過度試驗的情況下，容易地修改和/或調整這種示例性實施方式，這種修改和/或調整是不背離本發明的精神和範圍的。因此，這種調整以及修改意指在基於本文中所給出的這種教導和引導的示例性實施方式的含義以及多個等價物的範圍內。要理解的是，本文中的措辭或術語用於描述而非限制，所以鑒於本文中的教導，相關領域的技術人員能夠理解本說明書的術語或措辭。

術語

術語“金鑰環（keyring）”表示通常以加密形式存儲金鑰的檔。在公開金鑰加密中，公開金鑰和/或私密金鑰可存儲在一個或多個金鑰環上。

術語“密碼短語”表示與密碼相似但是通常比密碼長很多並且由系列單詞構成的字串。

詞語“電子郵件用戶端”表示管理電子郵件使用者的電子郵件消息的電腦程式。

本文中所使用的術語“收發器”表示包括發送器和接收器的電路，使得收發器可用於發送和接收資訊。在本發明的各種實施方式中，收發器可以半雙工模式、全雙工模

式或者兩者進行運作。要注意的是，可在不需要整合在單個裸片上的情況下來實施收發器，並且本發明不限於收發器功能性在任何特定數量的元件之間的任何特定的分佈。在典型的實施方式中，收發器形成在單個裸片上。

術語“晶片”、“裸片”、“積體電路”、“半導體器件”以及“微電子器件”在電子學領域中通常可交叉地使用。當這些術語是領域中通常所理解的時，本發明可應用於上述所有元件中。

對於晶片，通常，電源、地和各種信號可通過物理導電連接而耦接於晶片和其他電路元件之間。這種連接點可稱為輸入、輸出、輸入/輸出（I/O）、端子、線路、管腳、焊盤、埠、介面或類似的變形和組合。雖然通常通過導體來實現兩個以及多個晶片之間的連接，但是本領域的技術人員將理解到，可替換地，可通過光學、機械、磁性、靜電和電磁介面的方式將晶片和其他電路元件耦接。

術語“智慧卡”表示物理基片，例如其中埋有積體電路的信用卡大小的塑膠片。通常，智慧卡用於金融交易或安全進入上鎖的設施內。有源智慧卡是一種包括諸如電池的嵌入式電源的智慧卡。無源智慧卡是一種需要由外部源提供電力的智慧卡。在某些情況下，外部源是無源智慧卡獲得執行其期望的功能所需的能量所借助的能量場。

示意性近場通訊環境

圖 1 為示出了根據本發明的 NFC 環境的框圖。NFC 環境 100 提供彼此足夠接近的第一裝置 102 和第二裝置 104 之間的資訊的無線通訊。該資訊可包括要由第一 NFC 裝置 102 和/或第二 NFC 裝置 104 執行的一個或多個命令、要從

一個或多個資料存儲裝置傳送給第一 NFC 裝置 102 和/或第二 NFC 裝置 104 的資料或其任意組合。資料存儲裝置可包括一個或多個非接觸式轉發器 (transponder)、一個或多個非接觸式標籤、一個或多個非接觸式智慧卡、不背離本發明的精神和範圍的情況下對本領域普通技術人員顯而易見的任何其他機器可讀媒體或其任意組合。其他機器可讀媒體可包括非暫時性存儲媒體，例如但不限於易失性記憶體 (隨機存取記憶體 (RAM))；非易失性記憶體，例如唯讀記憶體 (ROM)、快閃記憶體、磁片存儲媒體和光學存儲媒體。另外一些機器可讀媒體可包括諸如作為一些示例所提供的載波、紅外線信號以及數位信號的傳播信號的電、光、聲或其他形式。

圖 2 為示出了用於將寄件者的文檔加密並且將收件人的文檔解密的基於公開金鑰的處理的高層框圖。在安全通訊領域中也建立公開金鑰加密系統。在基於公開金鑰的加密系統內，生成一對金鑰，並且該對金鑰被稱為公開金鑰/私密金鑰對。在公開金鑰加密中，加密/解密演算法和公開金鑰是已知的，並且僅私密金鑰為保密的。在生成公開金鑰/私密金鑰對並且公佈或發佈公開金鑰之後，寄件者可使用一個金鑰加密消息 (明文)，以生成加密的消息 (密文)，收件人可使用另一個金鑰解密該密文，以再現明文。公眾中任何人可使用公開金鑰加密消息並且將該消息發送給私密金鑰的持有人 (即，收件人)。僅私密金鑰可解密該密文。然後，使用私密金鑰解密該密文，以生成所需要的消息。由於金鑰對的公開金鑰和私密金鑰不同，所以公開金鑰加密被稱為非對稱金鑰系統。將理解到，通過用於發送消息

的任何合適方法和設備可實現將密文發送給收件人。作為示例而非限制性地，加密電子郵件消息通常通過網際網路發送給收件人。

圖 3 為示出了用於對寄件者的文檔進行數位簽章並且在收件人系統證實文檔已經由假設的寄件者系統實際簽名的基於公開金鑰的處理的高層框圖。在這種情況下，使用寄件者系統的私密金鑰對明文進行簽名（即，加密），並且將簽名的消息發送至收件人系統。在收件人系統，通過用公開金鑰/私密金鑰對的公開金鑰進行解密處理，來驗證所簽名的文檔。由於僅僅公開金鑰/私密金鑰對的公開金鑰可解密所簽名的文檔，所以文檔的成功解密就證實了所簽名的消息是由公開金鑰/私密金鑰對的私密金鑰持有人發送的。將要理解到，通過用於發送消息的任何合適的方法和設備可實現將簽名的消息發送至收件人系統。作為示例而非限制性地，簽名的電子郵件消息通常通過網際網路發送至收件人系統。

圖 4 為示出了用於對寄件者的文檔進行數位簽章並且證實文檔已經由假設的寄件者簽名的另一基於公開金鑰的處理的高層框圖。在這種情況下，明文要經過散列處理以生成“消息摘要”。該消息摘要對於被散列的明文是唯一的。然後，使用寄件者的私密金鑰對消息摘要進行簽名（即，加密）。然後，將一份明文以及所簽名的消息摘要一起發送給收件人。然後，收件人：(a) 對所接收的明文進行相同的散列處理，以生成新版消息摘要；(b) 使用公開金鑰驗證所簽名的消息摘要，從而生成寄件者消息摘要的明文版本；(c) 將最新生成的消息摘要與寄件者消息摘要

的明文版本比較；以及（d）如果最新生成的消息摘要和寄件者消息摘要的明文版本匹配，那麼收件人意識到明文實際上來自於寄件者而非冒名頂替者，並且還意識到明文消息尚未被篡改。

上面給出的公開金鑰加密的所有示例需要使用保密的私密金鑰以及公佈或以其他方式發佈給潛在接收者的公開金鑰。要注意的是，公開金鑰加密適於應用於數位資訊，而不管內容的意義。換言之，明文是表示電子郵件、文字處理文檔還是隨機資訊，對於加密處理而言並不重要。

用於安全電子郵件的啟用 NFC 的裝置的概述

如上所述，製造技術和數位架構的進步已經使得產生了大量之前不實際的或者不能實施的產品和產品類別。近場通訊（NFC）電路、系統和應用領域的新興發展使得新產品和產品類別成為可能。結合有 NFC 通訊能力的產品在該領域有時被稱為啟用的 NFC。比如，包括 NFC 通訊能力的行動電話、智慧卡或其他電子產品被稱為啟用的 NFC。NFC 通訊允許兩個裝配相似的裝置在短距離內彼此交換資料。雖然在該領域中短距離範圍的嚴格定義並不一致，但是通常認為 NFC 的短距離小於 4cm，或者在所選通訊頻率的一個波長內。

本發明的各個實施方式有利地使用 NFC 通訊來提供用於增強式加密金鑰和加密處理的安全性的方法、設備和系統。

對於消息的加密和解密，公開金鑰加密需要使用金鑰對，即公開金鑰和私密金鑰。本發明的各個實施方式提供加密和/或解密消息的一個或多個方面所需的資訊的存儲，

其中通過 NFC 通訊介面可使用該資訊。在具體的示例性實施方式中，啟用 NFC 的裝置與正在執行或以其他方式提供對電子郵件用戶端的訪問的計算平臺物理靠近。一旦啟用 NFC 的裝置和計算平臺在彼此的 NFC 通訊範圍內，則發生建立加密和/或解密處理所需要的資訊的交換。根據本發明，由於加密/解密金鑰和/或相關的加密處理參數不存儲在其進行（有意的或無意的）公開的計算平臺上，所以提高了該資訊的安全性。

在本發明的典型實施方式中，加密處理為公開金鑰處理。在一些實施方式中，使用 PGP 公開金鑰加密/解密。在各個實施方式中，啟用 NFC 的裝置提供用於建立加密通訊的資訊和/或指令。在這些實施方式的某些中，加密通訊為加密電子郵件。在一些實施方式中，加密通訊為 PGP 加密電子郵件。

圖 5 為示出了根據本發明的啟用 NFC 的裝置 502 的框圖，該框圖示出了裝置 502 中與加密電子郵件的使用相關的部分。啟用 NFC 的裝置 502 包括私密金鑰記憶體 504、公開金鑰記憶體 506、可選的金鑰對生成程式碼記憶體 508、記憶體存取控制邏輯 510、可選的計算資源 512 以及 NFC 數據機 514。啟用 NFC 的裝置 502 還包括匯流排 503，私密金鑰記憶體 504、公開金鑰記憶體 506、可選的金鑰對生成程式碼記憶體 508 以及記憶體存取控制邏輯 510 通過該匯流排能夠進行通訊。要注意的是，根據本發明也可實施其中各塊經由專用的路徑而非經由公共匯流排進行通訊的可替換裝置。

可使用任何適當類型的記憶體電路來實施存儲塊

504、506 和 508。在典型的實施方式中，存儲塊 504、506 以及 508（如果存在的話）為非易失性記憶體。非易失性存儲器具有即使未向這些記憶體供電時也能夠將存儲的內容保持於其中的特性。存在多種不同類型的非易失性記憶體，包括但不限於快閃記憶體、唯讀記憶體（ROM）、一次性可程式設計記憶體、熔絲式可程式設計記憶體、反熔絲式可程式設計記憶體、鐳射可程式設計記憶體、電可讀寫唯讀記憶體等。

在該示意性實施方式中，NFC 數據機 514 包括發送器和接收器電路。要理解的是，在本發明的各個實施方式中，NFC 數據機 514 可進一步包括用於一種或多種控制功能的電路，諸如但不限於 NFC 通訊協議和握手序列。

啟用 NFC 的裝置 502 可以是但不限於智慧卡、行動電話、智慧型電話、電子金鑰卡、無金鑰安全接入卡、平板電腦等產品。

圖 6 為示出了根據本發明的另一示意性啟用 NFC 的裝置 602 的框圖，該框圖示出了裝置 602 中與加密電子郵件的使用相關的部分。圖 6 中的啟用 NFC 的裝置 602 與啟用 NFC 的裝置 502 相似，除了在該圖中不包括用於金鑰對生成的可選程式碼和可選計算資源而添加了能量獲取電路 604 之外。各種能量獲取電路在本領域中是已知的，並且通常結合 RFID 裝置一起使用。本發明的實施方式可配置有一個或多個能量獲取電路。在其他可替換的實施方式中，多個能量獲取電路中的各個電路可由不同的電路、不同的電路技術、不同的功率輸出特性和/或不同的能量源構成。能量源可包括但不限於電磁場、磁場以及熱梯度（使用熱電

發電材料)。

依然參照圖 6，要注意的是，能量獲取電路 604 通過由導電材料形成的路徑(未示出)耦接至啟用 NFC 的裝置 602 的其他塊 504、506、510 和 514。

圖 7 為示出了根據本發明的另一示意性啟用 NFC 的裝置 702 的框圖，該框圖示出了裝置 702 中與加密電子郵件的使用相關的部分。啟用 NFC 的裝置 702 包括私密金鑰記憶體 504、記憶體存取控制邏輯 510、NFC 數據機 514 以及能量獲取電路 604。能量獲取電路 604 通過電源匯流排 704 向私密金鑰記憶體 504、記憶體存取控制邏輯 510 以及 NFC 數據機 514 提供電力。要理解的是，電源匯流排 704 可包括多條導電互連線路，其中這些線路中的每條線路耦接至一個電源節點。作為示例而非限制性的，電源匯流排可包括接電線和正電壓供給線。在可替換的配置中，能量獲取電路 604 可產生多個輸出電源電壓，以適應啟用 NFC 的裝置 702 的各個其他電路塊的需求。在這種可替換的配置中，電源匯流排 704 包括相應數量的電壓供給線，以將電壓供給節點與需要特定電壓供給的一個或多個塊耦接。

圖 8 為示意性系統 800 的框圖，該框圖示出了其中具有金鑰存儲和能量獲取電路的第一啟用 NFC 的裝置 802 以及具有能量場發生器並且耦接至其上存儲有 PGP 加密程式碼的存儲媒體 806 以及進一步耦接至其上存儲有電子郵件用戶端程式碼的存儲媒體 808 的啟用 NFC 的計算平臺 804。啟用 NFC 的裝置 802 可為智慧卡、智慧型電話、行動電話、平板電腦等的一部分，但不限於此。啟用 NFC 的計算平臺 804 可為個人電腦、智慧型電話、行動電話、平

板電腦、電子郵件資訊站 (kiosk) 等，但不限於此。要理解的是，PGP 加密為市場上可買到的公開金鑰加密產品，並且本發明並不限於使用這種特定的公開金鑰加密產品。在本發明的各個實施方式中，裝置 802 和計算平臺 804 之間的 NFC 通訊在發送或通訊與加密相關的資訊之前，可包括各種與協定相關的步驟。

要注意的是，除了存儲一個或多個私密金鑰之外，啟用 NFC 的裝置 802 還可存儲一個或多個公開金鑰、一個或多個散列演算法規範或識別、一個或多個密碼短語以及包括但不限於金鑰尺寸的一個或多個加密參數，並且可為計算平臺 804 使用。這樣，啟用 NFC 的裝置 802 能夠提供實現使加密處理在計算平臺 804 上運行所需的所有資訊，而不需要將那些金鑰和其他參數存儲在計算平臺 804 中或有線連接到計算平臺 804。同樣，這些金鑰和其他參數不再經由它們可能被攔截的 RF 遠場載體 (carrier)。當這些金鑰和/或其他參數與計算平臺 804 進行通訊時，僅僅使用與遠場發送相比不易受攔截的近場通訊，並且僅在執行特定加密任務所需要的時間段內是可利用的。

在一些實施方式中，預定的時間量之後，啟用 NFC 的裝置 802 中斷金鑰或加密參數的通訊。在其他實施方式中，發送預定的資料量之後，中斷該通訊。在另外一些實施方式中，在啟用 NFC 的裝置 802 將參與與加密相關的資訊的另一交換之前，必須逝去預定的時間量。

在本發明的一個示意性實施方式中，提供加密通訊的方法包括將公開金鑰/私密金鑰對的私密金鑰存儲在第一啟用 NFC 的通訊裝置的第一記憶體內，並且通過近場通訊將

私密金鑰發送給第二啟用 NFC 的通訊裝置，第二啟用 NFC 的通訊裝置被設置為與計算平臺進行通訊，其中在加密處理中，計算平臺執行使用從第一啟用 NFC 的通訊裝置接收到的私密金鑰的程式碼。在一些實施方式中，加密處理為 PGP 公開金鑰加密。在各個實施方式中，第一記憶體可為非易失性記憶體，計算平臺可為個人電腦、智慧型電話、平板電腦或可用於發送或接收電子郵件的類似裝置。在另一實施方式中，提供加密通訊的方法包括在發送之前，從能量場中獲取能量。在其他實施方式中，第二啟用 NFC 的通訊裝置被設置為與計算平臺進行有線通訊，並且可設置在計算平臺內。在另外一些實施方式中，計算平臺執行程式碼，以提供電子郵件用戶端的功能，而在其他實施方式中，計算平臺執行程式碼，以提供對電子郵件用戶端的訪問。

在本發明的另一個示意性實施方式中，提供加密通訊的方法包括在啟用 NFC 的計算平臺上通過近場通訊接收私密金鑰；在計算平臺上執行提供電子郵件用戶端的程式碼；以及在計算平臺上，在加密處理中，執行使用私密金鑰的程式碼。在一些實施方式中，加密處理使用私密金鑰對加密的電子郵件消息進行解密，以生成加密電子郵件消息的明文版本。在其他實施方式中，加密處理使用私密金鑰對明文電子郵件消息進行簽名，以生成明文電子郵件消息的密文版本。

在本發明的一個實施方式中，NFC 通訊裝置包括第一記憶體，第一記憶體內存儲有至少一個私密金鑰；第二記憶體，第二記憶體內存儲有至少一個公開金鑰；第三記憶

體，第三記憶體內存儲有至少一個密碼短語；記憶體存取控制器，耦接至第一記憶體、第二記憶體以及第三記憶體；以及 NFC 數據機，耦接至記憶體存取控制器。第一記憶體、第二記憶體和第三記憶體通常為非易失性記憶體。第一記憶體、第二記憶體和第三記憶體可整合在單個晶片上、不同的晶片上或者以任何合適的方式進行分佈。可使用相同或不同的製造技術來實現第一記憶體、第二記憶體和第三記憶體。第一記憶體、第二記憶體和第三記憶體可為邏輯上鄰近的記憶體陣列的可定址區域。其他實施方式進一步包括耦接至 NFC 數據機的至少一個能量獲取電路。另外一些實施方式包括第四記憶體，第四記憶體存儲有這樣的程式碼，即，當該程式碼被計算資源執行時，會使計算資源生成私密金鑰/公開金鑰對。

在本發明的一個實施方式中，用於加密通訊的系統包括第一 NFC 通訊裝置，該裝置包括第一記憶體，第一記憶體內存儲有至少一個私密金鑰，記憶體存取控制器耦接至第一記憶體；以及第一 NFC 數據機，耦接至記憶體存取控制器；以及計算平臺，被配置成執行程式碼，該計算平臺包括機器可讀存儲媒體，該機器可讀存儲媒體上存儲有當被執行時會使計算平臺提供電子郵件用戶端的程式碼，並且計算平臺進一步包括第二 NFC 通訊裝置；其中第一 NFC 通訊裝置以及計算平臺的第二 NFC 通訊裝置必須設置為彼此具有預定的空間關係，以使得能夠實現第一 NFC 通訊裝置和第二 NFC 通訊裝置之間的近場通訊。在一些實施方式中，第一 NFC 通訊裝置進一步包括能量獲取電路，該能量獲取電路耦接至第一記憶體、記憶體存取控制器和第一

NFC 數據機。在這些實施方式中的一些實施方式中，第一 NFC 通訊裝置設置在智慧卡內。在其他實施方式中，第一 NFC 通訊裝置設置在例如但不限於行動電話、智慧型電話、平板電腦的產品內，或者設置在包括電源的其他產品內，該電源包括但不限於電池。在各個實施方式中，第一 NFC 通訊裝置進一步包括第二記憶體，第二記憶體內存儲有至少一個公開金鑰。要注意的是，本發明的各個實施方式適合於進行加密的電子郵件通訊，其中使用公開金鑰加密處理將加密的電子郵件加密。在這些實施方式的一些實施方式中，公開金鑰加密處理為 PGP。

在各個實施方式中，NFC 通訊裝置可包括其自身內設置的計算資源。作為示例但非限制性地，NFC 通訊裝置可被實施成包括處理器內核（即計算資源）的積體電路晶片。在其他實施方式中，計算資源可物理地設置於 NFC 通訊裝置的外部，但是以可通訊的方式耦接至該裝置。可替換地，計算資源既可設置在 NFC 通訊裝置內，也可物理地設置在 NFC 通訊裝置的外部/以可通訊的方式耦接至 NFC 通訊裝置。另外一些實施方式可包括一個或多個記憶體，用於存儲一個或多個對稱金鑰，其中對稱金鑰適用於對稱式金鑰密碼編譯處理。

要注意的是，諸如本文中所描述的那些啟用 NFC 的裝置還可包括其他加密資訊，例如但不限於用於可替換加密方案的一個或多個金鑰。例如，一個或多個對稱金鑰可存儲在啟用 NFC 的裝置內，以用於例如但不限於 DES 的對稱金鑰演算法。諸如密文回饋、密碼分組連結以及三重 DES 的基本的 DES 演算法的變形已經用於擴展該對稱金鑰演算

法的能行性。

結論

要理解的是，詳細描述的部分而非本公開的摘要意指用於解釋申請專利範圍。本公開的摘要可闡述本發明的一個或多個示例性實施方式，但並非是所有的示例性實施方式，因此，不意指以任何方式限制本發明和所附申請專利範圍。

上面已經借助於示出了特定功能及其關係的實施的功能性構建塊描述了本發明。為了便於進行描述，本文任意地定義了這些功能性構建塊的界限。可以定義可替換的界限，只要特定的功能和其關係能夠被適當地執行即可。

對本領域普通技術人員顯而易見的是，在不背離本發明的精神和範圍的前提下，可在其內進行形式和細節上的各種變化。因此，本發明不應受到上述示例性實施方式中的任一個的限定，而僅由所附申請專利範圍及其等同物來限定。

【圖式簡單說明】

圖 1 為示出了根據本發明的近場通訊（NFC）環境的框圖。

圖 2 為示出了用於將寄件者的文檔加密並且將收件人的文檔解密的基於公開金鑰的處理的高層（high-level）框圖。

圖 3 為示出了用於對寄件者的文檔進行數位簽章並且證實文檔已經由假設的寄件者簽名的基於公開金鑰的處理的高層框圖。

圖 4 為示出了用於對寄件者的文檔進行數位簽章並且

證實文檔已經由假設的寄件者簽名的另一基於公開金鑰的處理的高層框圖。

圖 5 為示出了根據本發明的啟用 NFC (NFC-enabled) 的裝置的框圖，該框圖示出了裝置中與加密電子郵件的使用相關的部分。

圖 6 為示出了根據本發明的另一啟用 NFC 的裝置的框圖，該框圖示出了裝置中與加密電子郵件的使用相關的部分。

圖 7 為示出了根據本發明的另一啟用 NFC 的裝置的框圖，該框圖示出了裝置中與加密電子郵件的使用相關的部分。

圖 8 為示意性系統的框圖，該框圖示出了其中具有金鑰存儲和能量獲取電路的第一啟用 NFC 的裝置以及具有能量場發生器並且進一步耦接至其上存儲有各種程式碼的存儲媒體的啟用 NFC 的計算平臺。

【主要元件符號說明】

- 100 NFC 環境
- 102 第一裝置
- 104 第二裝置
- 152 近場通訊裝置
- 154 近場通訊裝置
- 502 啟用 NFC 的裝置
- 503 匯流排
- 504 私密金鑰記憶體
- 506 公開金鑰記憶體
- 508 金鑰對生成程式碼記憶體

- 510 記憶體存取控制邏輯
- 512 計算資源
- 514 NFC 數據機
- 602 啟用 NFC 的裝置
- 604 能量獲取電路
- 702 啟用 NFC 的裝置
- 704 私密金鑰記憶體
- 800 系統
- 802 啟用 NFC 的裝置
- 804 啟用 NFC 的計算平臺
- 806 PGP 加密程式碼的存儲媒體
- 808 電子郵件用戶端程式碼的存儲媒體

七、申請專利範圍：

1. 一種提供加密通訊的方法，包括：

藉由設置於第一啟用 NFC 的通訊裝置中的計算資源產生
私密金鑰/公開金鑰對；

將所述公開金鑰/私密金鑰對的私密金鑰存儲在所述第
一啟用 NFC 的通訊裝置的第一記憶體中；以及

通過近場通訊將所述私密金鑰發送至第二啟用 NFC 的通
訊裝置，所述第二啟用 NFC 的通訊裝置被設置為與一計算
平臺進行通訊；

其中，在加密處理中，所述計算平臺執行使用從所述第
一啟用 NFC 的通訊裝置中接收到的私密金鑰的程式碼。

2. 如申請專利範圍第 1 項之方法，進一步包括：

在進行發送之前，從能量場獲取能量。

3. 如申請專利範圍第 1 項之方法，其中，所述第二啟用 NFC 的通訊裝置被設置為與所述計算平臺進行有線通訊。

4. 如申請專利範圍第 3 項之方法，其中，所述第二啟用 NFC 的通訊裝置設置在所述計算平臺內。

5. 如申請專利範圍第 1 項之方法，其中，所述計算平臺進一 步執行用於提供電子郵件用戶端的功能的程式碼。

6. 如申請專利範圍第 1 項之方法，其中，所述計算平臺進一 步執行用於提供對電子郵件用戶端的訪問(Access)的程式 碼。

7. 如申請專利範圍第 5 項之方法，其中，所述加密處理將加 密電子郵件消息解密，以生成加密電子郵件消息的明文版 本。

8. 如申請專利範圍第 5 項之方法，其中，所述加密處理對明

文電子郵件消息進行簽名，以生成所述明文電子郵件消息的密文版本。

9. 一種啟用的 NFC 通訊裝置，包括：

第一記憶體，所述第一記憶體內存儲有至少一個私密金鑰；

第二記憶體，所述第二記憶體內存儲有至少一個公開金鑰；

第三記憶體，所述第三記憶體內存儲有至少一個密碼短語；

第四記憶體，所述第四記憶體儲存被計算資源執行之程式碼，以產生私密金鑰/公開金鑰對；

記憶體存取控制器，耦接至所述第一記憶體、所述第二記憶體、所述第三記憶體和所述第四記憶體；以及

NFC 數據機，耦接至所述記憶體存取控制器。

10. 如申請專利範圍第 9 項之啟用的 NFC 通訊裝置，進一步包括：

能量獲取電路，耦接至所述 NFC 數據機。

11. 如申請專利範圍第 9 項之啟用的 NFC 通訊裝置，其中，所述計算資源設置在所述 NFC 通訊裝置內。

12. 如申請專利範圍第 9 項之啟用的 NFC 通訊裝置，其中，所述計算資源物理上設置在所述 NFC 通訊裝置的外部，並且以能夠進行通訊的耦接方式與所述 NFC 通訊裝置進行通訊。

13. 如申請專利範圍第 9 項之啟用的 NFC 通訊裝置，進一步包括用於存儲一個或多個對稱金鑰的記憶體，所述對稱金鑰適用於對稱式金鑰密碼編譯處理。

14. 一種用於加密通訊的系統，包括：

第一 NFC 通訊裝置，包括

第一記憶體，所述第一記憶體內存儲有至少一個私密金鑰；

記憶體存取控制器，耦接至所述第一記憶體；以及

第一 NFC 數據機，耦接至所述記憶體存取控制器；以及

計算平臺，被配置成執行程式碼，所述計算平臺包括機器可讀存儲媒體，所述機器可讀存儲媒體上存儲有當被執行時使所述計算平臺提供電子郵件用戶端的程式碼，並且所述計算平臺進一步包括第二 NFC 通訊裝置；

其中，所述第一 NFC 通訊裝置以及所述計算平臺的所述第二 NFC 通訊裝置必須設置成彼此具有預定的空間關係，以使得所述第一 NFC 通訊裝置和所述第二 NFC 通訊裝置之間能夠進行近場通訊。

15. 如申請專利範圍第 14 項之系統，其中，所述第一 NFC 通訊裝置進一步包括能量獲取電路，所述能量獲取電路耦接至所述第一記憶體、所述記憶體存取控制器以及所述第一 NFC 數據機。

16. 如申請專利範圍第 15 項之系統，其中，所述第一 NFC 通訊裝置設置在智慧卡內。

17. 如申請專利範圍第 14 項之系統，其中，所述第一 NFC 通訊裝置設置在行動電話內。

18. 如申請專利範圍第 14 項之系統，其中，所述第一 NFC 通訊裝置進一步包括第二記憶體，所述第二記憶體內存儲有至少一個公開金鑰。

19. 如申請專利範圍第 14 項之系統，其中，所述加密通訊為

加密電子郵件。

20. 如申請專利範圍第 19 項之系統，其中，使用公開金鑰執行加密處理將一待加密電子郵件加密。
21. 如申請專利範圍第 20 項之系統，其中，所述公開金鑰加密處理為 PGP。

八、圖式：

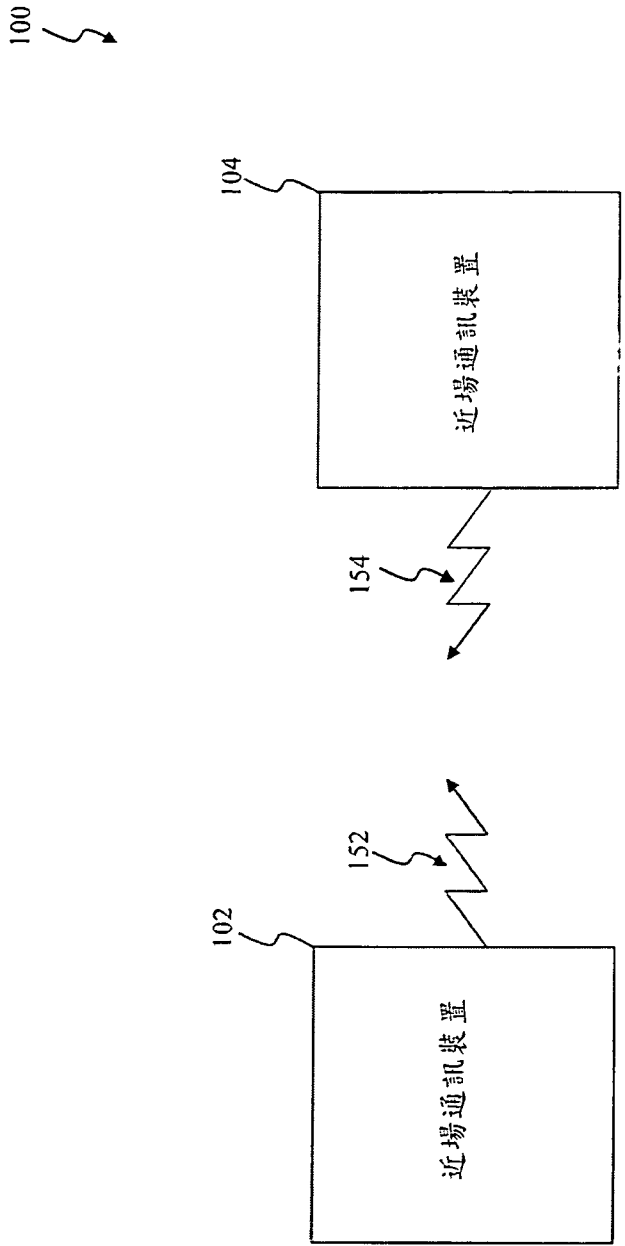


圖1

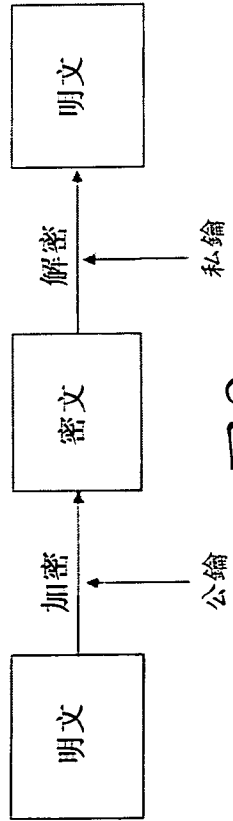


圖2

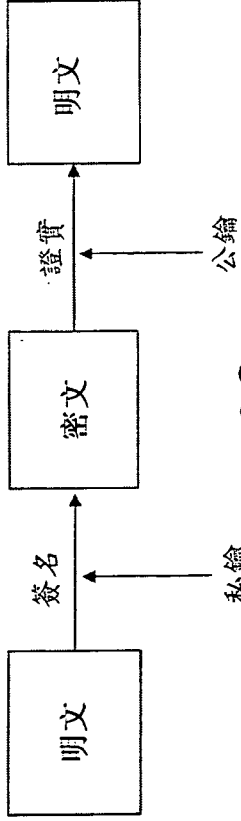


圖3

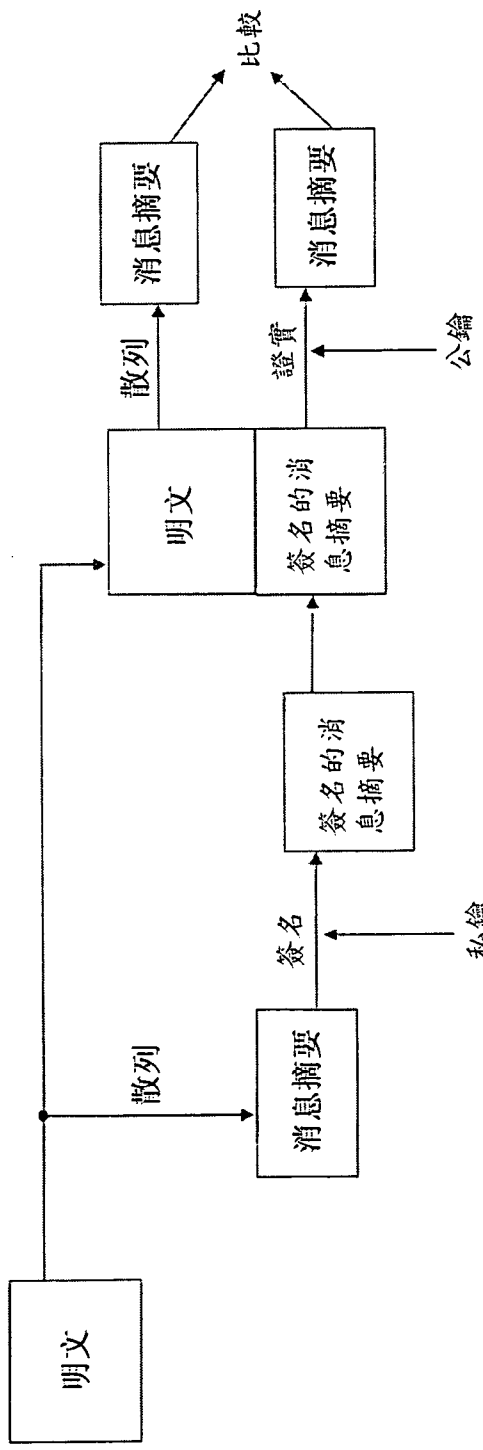


圖4

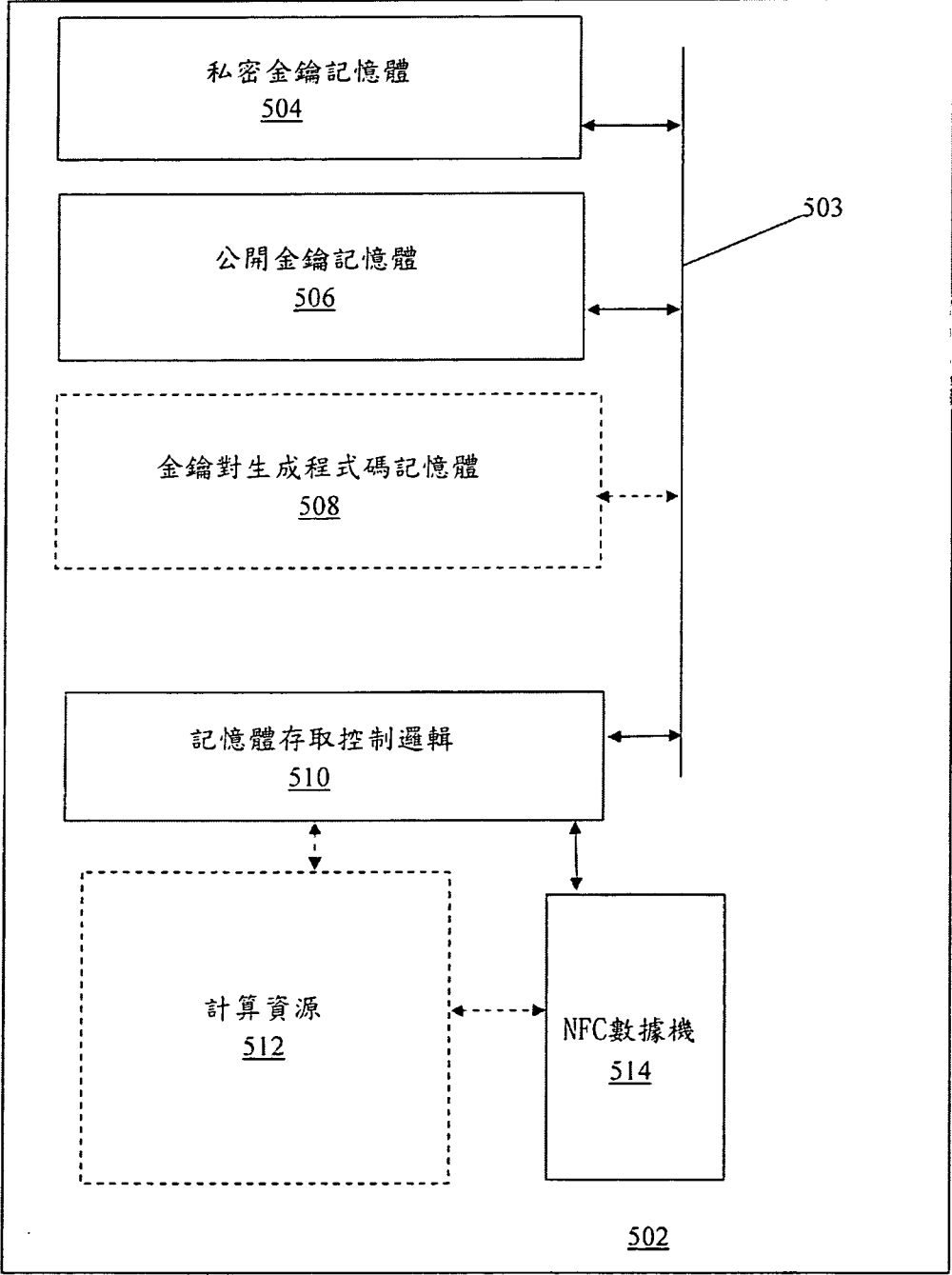


圖5

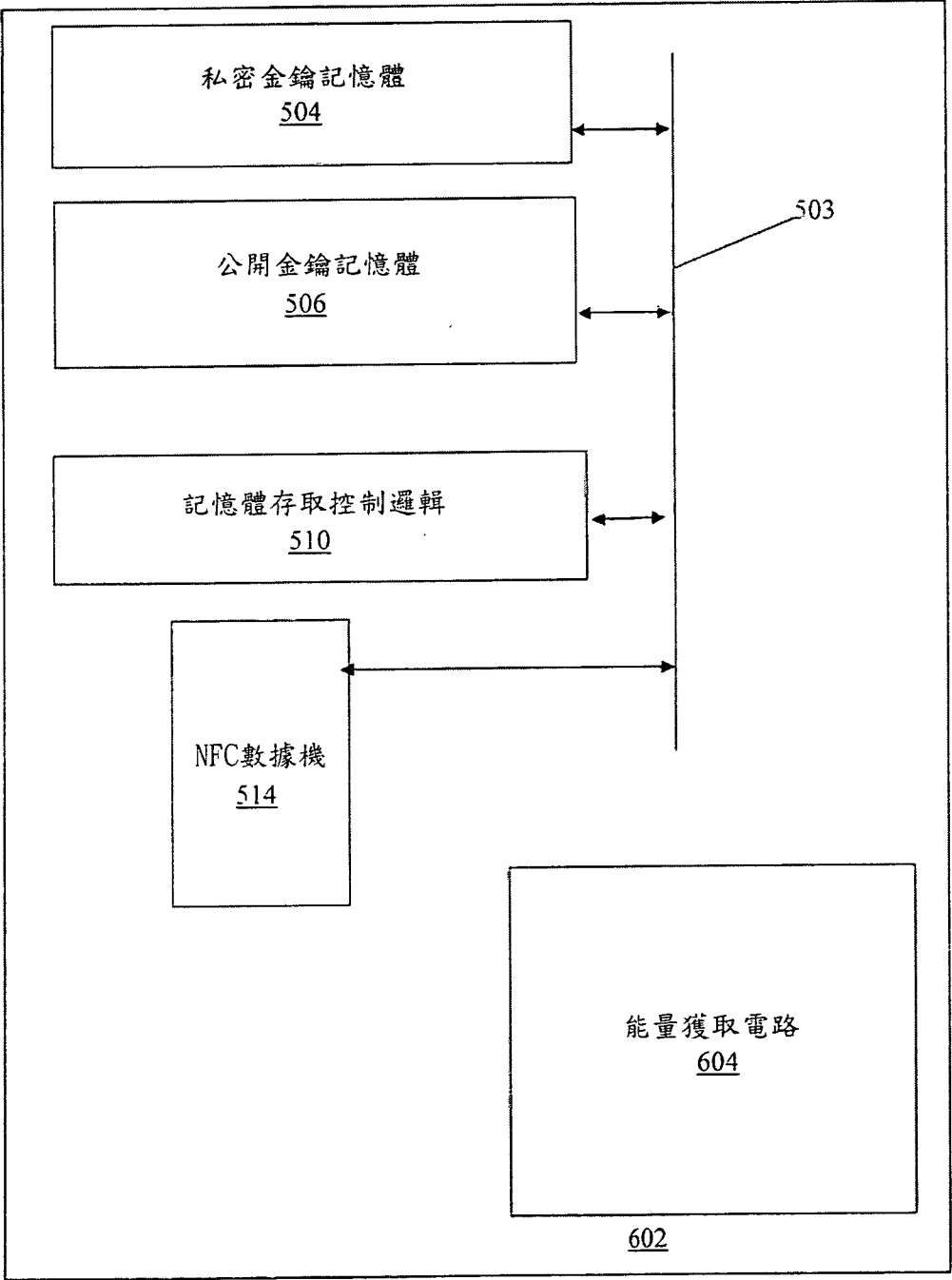


圖6

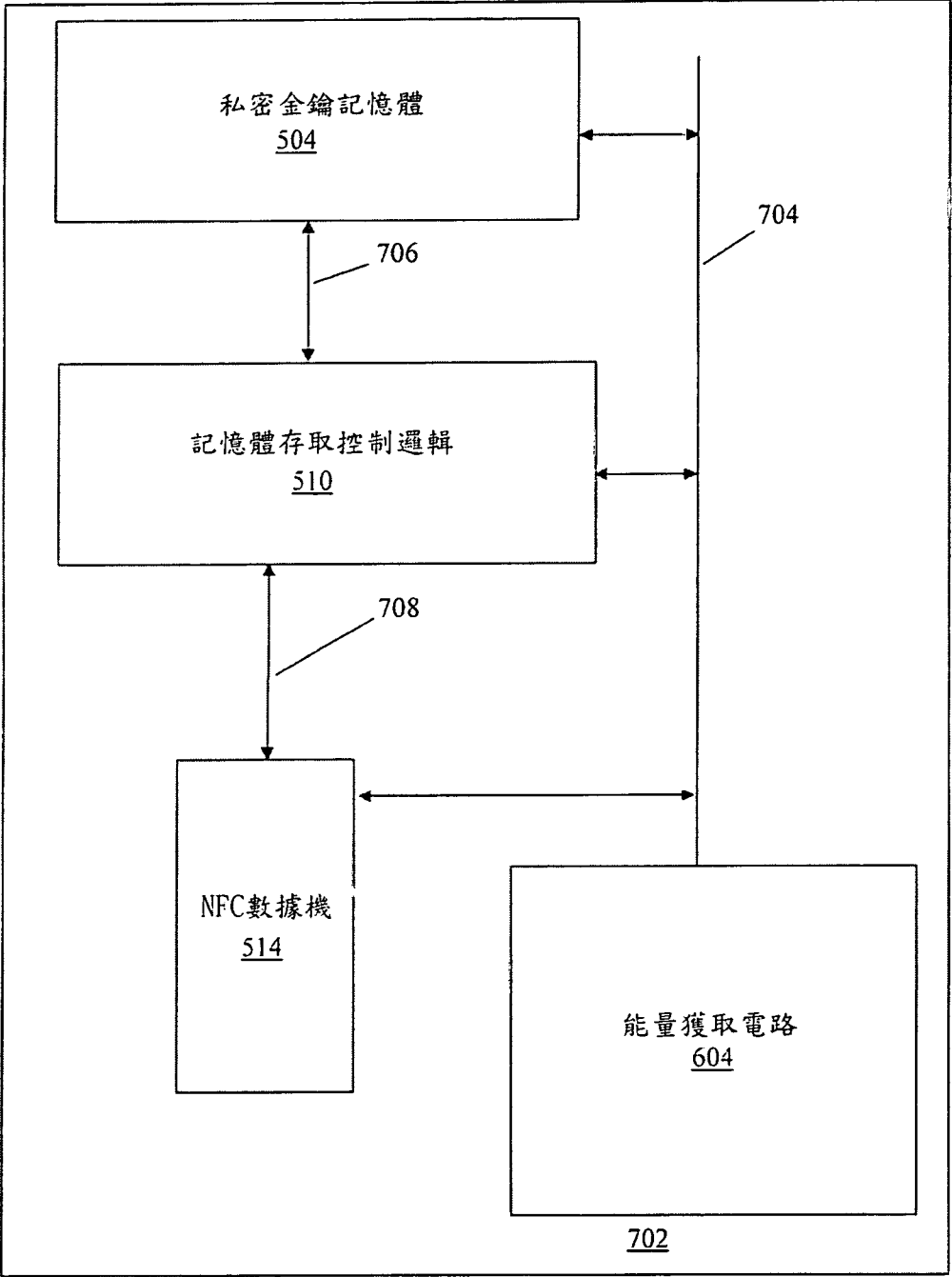


圖 7

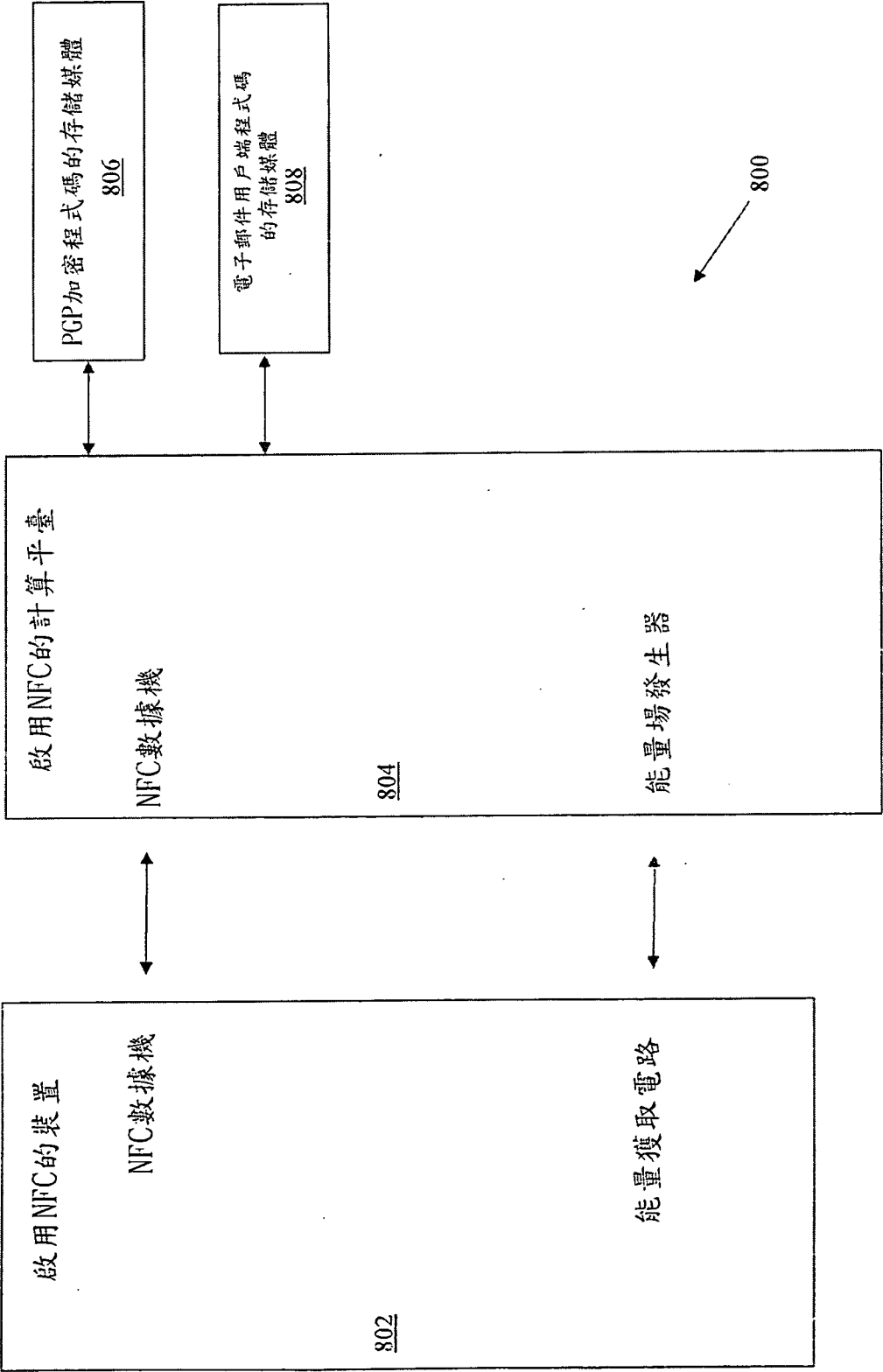


圖8