



(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 201830291 A

(43)公開日：中華民國 107 (2018) 年 08 月 16 日

(21)申請案號：106138933

(22)申請日：中華民國 106 (2017) 年 11 月 10 日

(51)Int. Cl. : G06K19/06 (2006.01)

G06F21/64 (2013.01)

(30)優先權：2017/02/14 中國大陸

201710078901.6

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)

香港

(72)發明人：郭偉 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：29 項 圖式數：10 共 38 頁

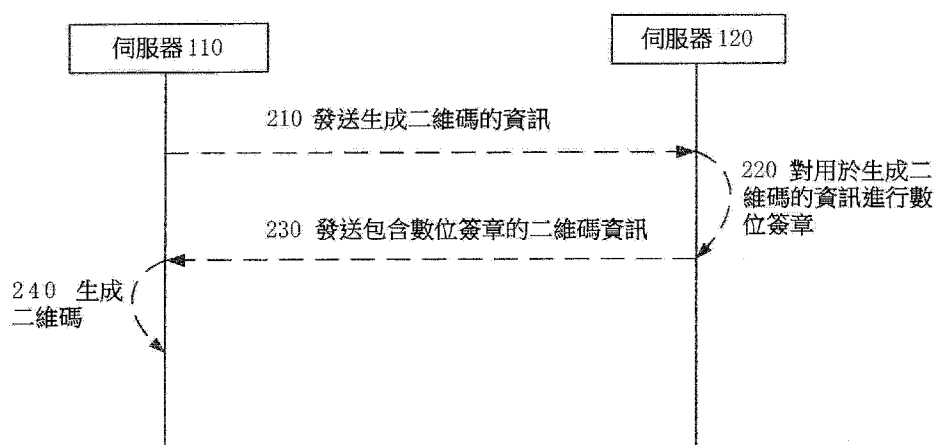
(54)名稱

二維碼生成方法及其設備和二維碼識別方法及其設備

(57)摘要

本申請案公開了一種二維碼生成方法及其設備和二維碼識別方法及其設備。所述方法包括：第一伺服器向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；第二伺服器根據接收到的生成二維碼的請求，對用於生成二維碼的資訊進行數位簽章；將包含有數位簽章的二維碼資訊發送到第一伺服器；第一伺服器利用所述二維碼資訊，生成二維碼。根據本發明的實施例通過一伺服器與另一伺服器之間協同作用產生二維碼，增強了二維碼的安全性和有效性，並且方便在二維碼識別過程中識別出二維碼是否被篡改。

指定代表圖：



符號簡單說明：

110 . . . 伺服器

120 . . . 伺服器

210 . . . 步驟

220 . . . 步驟

圖 2

【發明說明書】

【中文發明名稱】

二維碼生成方法及其設備和二維碼識別方法及其設備

【技術領域】

本申請案涉及圖形圖像技術領域，特別涉及一種二維碼生成方法及其設備和二維碼識別方法及其設備。

【先前技術】

二維碼又稱二維條碼，它通過某種特定幾何圖形按一定規律在平面（二維方向）上分佈形成的條／空相間圖形來記錄資料符號資訊。二維碼具有資訊容量大、編碼範圍廣、容錯力強、解碼可靠性高等特點，同時還具有成本低、易製作等優勢。因此，二維碼在人們生活中得到廣泛應用。

隨著網際網路的發展和行動式終端的普及，生活中的二維碼也隨處可見。例如，商家可將支付二維碼張貼在付款處，使用者可利用應用中的掃描二維碼功能進行掃描。或者商家在對商品進行推廣時，可將app的下載二維碼張貼在人流較多的地方（例如，地鐵、商場等），吸引過往人群掃描二維碼進行應用下載。因此，商家或第三方需要向使用者提供真實有效的二維碼，而使用者需要對這些二維碼進行有效地校驗。

在對現有技術的研究和實踐過程中，本發明的發明人

發現，人們很難從肉眼判斷二維碼的真偽，並且在二維碼識別過程中，手機應用中的掃描單元會在不進行任何驗證的情況下直接對各種二維碼進行識別。由此可以看出，目前存在如下需求：出於保證二維碼真實有效性的考慮而生成二維碼的技術方案，相應地也存在這樣的需求：在識別二維碼時對二維碼進行真偽判定的技術方案。

上述資訊僅作為背景資訊被呈現以說明理解本公開。至於任何上述資訊是否可應用為針對本公開的現有技術，尚未做出決定，也未做出聲明。

【發明內容】

本發明的主要目的在於提供一種二維碼生成方法及其設備和二維碼識別方法及其設備，旨在解決上述問題。

本發明的一方面提供一種二維碼生成方法，包括：第一伺服器向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；第二伺服器根據接收到的生成二維碼的請求，對用於生成二維碼的資訊進行數位簽章；將包含有數位簽章的二維碼資訊發送到第一伺服器；第一伺服器利用所述二維碼資訊，生成二維碼。

本發明的一方面提供一種二維碼生成方法，所述方法由第一伺服器執行，包括：向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊；利用所述二維碼資訊，生成二維碼。

本發明的一方面提供二維碼生成設備，包括：發送單元，向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；接收單元，從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊；生成單元，利用所述二維碼資訊，生成二維碼。

本發明的一方面提供一種二維碼生成方法，所述方法由第二伺服器執行，包括：從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊；對用於生成二維碼的資訊進行數位簽章；將包含有數位簽章的二維碼資訊發送到第一伺服器。

本發明的一方面提供一種二維碼生成裝置，包括：接收單元，從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊；處理單元，對用於生成二維碼的資訊進行數位簽章；發送單元，將包含有數位簽章的二維碼資訊發送到第一伺服器。

本發明的一方面提供一種二維碼生成系統，所述系統包括第一伺服器和第二伺服器，第一伺服器包括：發送單元，向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；接收單元，從第二伺服器接收由第一伺服器生成的包含有數位簽章的二維碼資訊；生成單元，利用所述二維碼資訊，生成二維碼；第二伺服器包括：接收單元，從第一伺服器接收所述請求；處理單元，對用於生成二維碼的資訊進行數位簽章；發送單元，將包含有數位簽章的二維碼資訊發送到第一伺服器。

本發明的另一方面提供一種二維碼識別方法，包括：啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用；利用所述應用中的掃描單元掃描所述二維碼；利用公開金鑰對掃描的二維碼進行驗證；若驗證成功，則識別出與掃描的二維碼對應的資訊。

本發明的另一方面提供一種二維碼識別設備，包括：啟動單元，啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用；掃描單元，利用所述應用中的掃描單元掃描所述二維碼；驗證單元，利用公開金鑰對掃描的二維碼進行驗證；識別單元，在驗證單元驗證成功的情況下，識別出與掃描的二維碼對應的資訊。

與現有技術相比，根據本發明的實施例通過一伺服器與另一伺服器之間協同作用產生二維碼，增強了二維碼的安全性和有效性，並且方便在二維碼識別過程中識別出二維碼是否被篡改。此外，根據本發明的另一實施例通過特定應用利用公開金鑰識別出與二維碼對應地資訊，增加了二維碼識別過程中的真偽判定，防止二維碼被篡改。

【圖式簡單說明】

此處所說明的附圖用來提供對本申請案的進一步理解，構成本申請案的一部分，本申請案的示意性實施例及其說明用於解釋本申請案，並不構成對本申請案的不當限定。在附圖中：

圖1是應用根據本發明的實施例的二維碼生成方法的

場景圖；

圖2是圖1中所示出的伺服器110與伺服器120之間的交互處理的示意圖；

圖3是根據本發明的實施例的識別二維碼的示意圖；

圖4是根據本發明的實施例的由第一伺服器執行的二維碼生成方法的流程圖；

圖5是執行如圖4所示的二維碼生成方法的二維碼生成設備的方塊圖；

圖6是根據本發明的實施例的由第二伺服器執行的二維碼生成方法的流程圖；

圖7是執行如圖6所示的二維碼生成方法的二維碼生成設備的方塊圖；

圖8是根據本發明的實施例的二維碼識別方法的流程圖；

圖9是根據本發明的實施例的執行如圖8所述的二維碼識別方法的二維碼識別設備的方塊圖；

圖10是根據本發明的實施例的電子設備的方塊圖。

【實施方式】

為使本申請案的目的、技術方案和優點更加清楚，下面將結合本申請案具體實施例及相應的附圖對本申請案技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本申請案一部分實施例，而不是全部的實施例。基於本申請案中的實施例，本領域普通技術人員在沒有做出進步

性勞動前提下所獲得的所有其他實施例，都屬於本申請案保護的範圍。

在下文中，將參照附圖更詳細地描述實施例。相同的標號始終表示相同的元件。為了更清楚地理解本發明，以下將對本發明所涉及的術語進行解釋。

終端／電子裝置：通常是指網路系統中由使用者使用的並用於與伺服器進行通信的裝置，本發明的實施例提供的二維碼生成方法可由二維碼生成設備執行，並且本發明的實施例提供的二維碼識別方法可由二維碼識別設備執行，而二維碼生成設備和二維碼識別設備可以是終端／電子裝置。根據本發明的終端／電子裝置可包括但不限於具有顯示單元的以下任意設備：個人電腦（PC）、行動式裝置（諸如，蜂巢式電話、個人數位助理（PDA）、數碼相機、可攜式遊戲控制台、MP3播放機、可攜式／個人多媒體播放機（PMP）、手持電子書、平板PC、可攜式膝上型PC和全球定位系統（GPS）導航儀）、智慧TV等。

應用（app）：可由使用者直接在電腦作業系統（OS）或行動式OS上執行的軟體，應用可包括儲存在終端的儲存單元中的嵌入式應用或第三方應用。嵌入式應用是指預先安裝在終端中的應用。例如，嵌入式應用可以是瀏覽器、電子郵件、即時通等。第三方應用非常多樣化，並且是指如下所述從線上市場下載以安裝在終端上的應用，例如，支付應用、購物應用、娛樂應用等。

圖1是應用根據本發明的實施例的二維碼生成方法的

場景圖。

如圖1所示，伺服器110與伺服器120以有線或無線方式進行連接，應理解，在本發明的各個實施例中，無線連接可以是一對一的無線連接，例如，藍牙、近距離無線通訊（NFC）等，在安全性有保障的場景中，也可以使用無線局域網（WiFi）。

伺服器110是用於生成二維碼的伺服器，例如，伺服器110可以是應用伺服器、網站伺服器等。舉例來說，伺服器110是支付應用伺服器，則應用伺服器110可回應於使用者輸入來生成關於某一商品的二維碼。或者伺服器110是網站伺服器，則可在顯示器上顯示由伺服器110根據需求生成的各種二維碼。伺服器120是第三方伺服器並且是具有權威認證的第三方伺服器（例如，支付寶伺服器）。

應注意，伺服器110和伺服器120均是提供計算服務的電子裝置，可以回應於伺服器請求並進行處理，並且這兩個伺服器的架構與通用電腦的架構類似，在本發明中，伺服器110和伺服器120提供不同的服務。

參照圖1，伺服器110與伺服器120進行交互處理，隨後伺服器110根據伺服器提供的資訊生成二維碼，這將在以下參照圖2進行詳細描述，因此省略對其的描述。

隨後，伺服器110可將二維碼顯示在顯示器上，或者直接利用輸出設備（例如，印表機等）進行輸出。然後，使用者可利用行動式終端中的掃描單元對二維碼進行掃描。

以下將參照圖2詳細說明伺服器110與伺服器120之間的交互處理。

如圖2所示，在步驟210，伺服器110向伺服器120發送生成二維碼的請求，所述請求可包括用於生成二維碼的資訊（以下簡稱二維碼資訊），例如，所述二維碼資訊可包括收款人帳號資訊，或者所述二維碼資訊可包括網址資訊。

可選地，伺服器110執行步驟210之前預先向伺服器120提出註冊請求，所述註冊請求中可包含與本次註冊相關的所有資訊，例如，伺服器110可向伺服器120提供自身的各類資質證明，例如，經營許可證、商品明細等。隨後，伺服器120在對伺服器110提供的資訊校驗通過後，完成對伺服器110的註冊。並將伺服器110提供的這些資質證明儲存在伺服器120的記憶體中。可選地，可將這些資質證明儲存在遠端記憶體中，這樣，在需要調用這些資質證明時，通過遠端記憶體的地址調用這些資質證明。

如此，在伺服器110向伺服器120發送二維碼生成請求之後，伺服器120對伺服器110進行驗證來確定伺服器110是否已在伺服器120中註冊，若否，則伺服器120不提供接下來的服務，並提示伺服器110進行註冊，具體來說，伺服器120可拒絕伺服器110的二維碼生成請求，並向伺服器110發出註冊邀請。若伺服器110已在伺服器120中註冊，則進行接下來的步驟。

通過以上的註冊步驟，伺服器120可對所有通過驗證

的裝置提供服務，從而能夠保證由伺服器120協同生成的二維碼的合法性。並在與伺服器110的商家產生糾紛時留有證據。

在步驟220，伺服器120可基於非對稱加密演算法對所述二維碼資訊進行數位簽章。具體來說，伺服器120可基於非對稱加密演算法，利用預先生成的私密金鑰（儲存在伺服器120中），對步驟210中的二維碼生成請求中的二維碼資訊進行數位簽章。如此一來，在識別二維碼的過程中，若利用公開金鑰掃描成功，則表明該二維碼為伺服器110利用伺服器120生成的二維碼，若掃描不成功，則表明該二維碼很可能是偽造二維碼或者僅由伺服器110生成未利用伺服器120進行處理的二維碼。

應注意，伺服器120根據二維碼資訊的不同生成不同的數位簽章，也就是說，伺服器120可根據二維碼資訊的不同提供不同的私密金鑰，隨後利用各個私密金鑰對各個二維碼資訊進行數位簽章。因此，即使是同一網站發送的關於不同商品的不同的連結資訊，也使用不同的私密金鑰對不同的連結資訊進行數位簽章。

以上所述的非對稱加密演算法可稱為公開金鑰加密演算法，在該演算法中，利用公開金鑰對資料進行加密，而利用對應的私密金鑰才能解密，或者利用私密金鑰對資料進行加密，而利用對應的公開金鑰進行解密。根據示例性實施例，非對稱加密演算法可包括RSA公開金鑰加密演算法、Elgamal加密演算法、背包演算法、橢圓曲線加密演

算法（ECC）加密演算法。由於本發明的發明目的在於保證二維碼真實有效性，較佳地，可選擇RSA公開金鑰加密演算法對生成的交易資料進行加密。

由於利用非對稱加密演算法對資料進行數位簽章是本領域常見的技術手段，在此將省略對其的詳細描述。應注意，雖然以上示出了非對稱加密演算法的示例，但本領域技術人員應理解，所有能夠生成數位簽章的非對稱加密演算法都可應用於此。

隨後，在步驟130，伺服器120將包含數位簽章的二維碼資訊發送到伺服器110。伺服器110在接收到包含數位簽章的二維碼資訊之後，在步驟140，利用包含數位簽章的二維碼資訊生成二維碼。具體來說，可基於二維碼生成演算法，利用二維碼資訊和數位簽章生成二維碼。較佳的，二維碼生成演算法包括快速反應碼（Quickresponse code，QRcode）演算法。

由於利用二維碼生成演算法生成二維碼是本領域常見的技術手段，在此將省略對其的詳細描述。本領域技術人員應理解，所有能夠生成二維碼的二維碼生成演算法都可應用於此。

接下來將參照圖3詳細描述對二維碼進行驗證的示意圖。

如圖3所示，使用者可利用行動式終端對顯示器上顯示的電子二維碼或經由輸出設備輸出的二維碼進行驗證。

使用者啟動與伺服器120對應的應用，例如，使用者

可在行動式終端中啟動與支付寶伺服器對應的支付寶應用。隨後，使用者利用所述應用中的掃描單元對顯示在顯示器上的二維碼或列印出來的二維碼進行掃描。

應注意，使用者在進行二維碼識別過程中，必須利用與伺服器120對應的應用中的掃描單元。這是由於在與伺服器120對應的應用包含或可獲取與二維碼對應的公開金鑰。

可選地，在利用所述應用中的掃描單元對二維碼進行掃描之後，可向伺服器120或儲存有公開金鑰的遠端記憶體獲取公開金鑰。隨後，利用所述公開金鑰對掃描的二維碼進行驗證，若驗證成功，則可成功識別出二維碼以進行下一步操作。也就是說，可根據二維碼識別結果，在行動式終端的顯示介面上顯示與所述二維碼對應的操作介面，例如，如果二維碼的識別結果是關於支付寶的連結，則行動式終端調用支付寶應用，從而在顯示單元上顯示關於支付寶的操作介面，如果二維碼的識別結果是關於微信的連結，則行動式終端調用微信應用，從而在顯示單元上顯示關於微信的操作介面。如果二維碼的識別結果是關於網址的連結，則行動式終端調用瀏覽器應用，從而在顯示單元上顯示關於瀏覽器的操作介面。

若驗證不成功，則說明二維碼被篡改。此外，還存在這種情況：篡改二維碼的操作者同樣在伺服器120上註冊，並且用於篡改原始二維碼的二維碼同樣是在伺服器120的協同下生成。例如，商家乙將商家甲張貼在外的二

維碼撕掉，張貼他自己的二維碼。在這種情況下，利用與伺服器120對應的應用中的掃描單元能夠成功識別商家乙的二維碼。為了解決這種情況，可記錄以上所述的掃描過程。這樣可根據掃描記錄確定篡改二維碼的操作者，並根據操作者在註冊階段提供的資訊來確定操作者的身份。

圖4是根據本發明的實施例的由第一伺服器執行的二維碼生成方法的流程圖。

在步驟S410，向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊。

在步驟S420，從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊。

在步驟S430，利用所述二維碼資訊，生成二維碼。

在可替換實施例中，向第二伺服器發送生成二維碼的請求之前還包括：向第二伺服器發送註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

圖5是執行如圖4所示的二維碼生成方法的二維碼生成設備（即，第一伺服器）的方塊圖。

本領域技術人員將理解，圖5中示出的二維碼生成設備的結構並不構成對本發明的電子裝置的限定，可包括比圖示更多或更少的部件，或組合某些部件，或不同的部件佈置。

如圖5所示，二維碼生成設備可包括發送單元510、接收單元520和生成單元530。

發送單元510可向第二伺服器發送生成二維碼的請

求，所述請求包括用於生成二維碼的資訊。

接收單元520可從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊；

生成單元530可利用所述二維碼資訊，生成二維碼。

在可替換實施例中，發送單元510在向第一伺服器發送生成二維碼的請求之前，向第一伺服器發送註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

圖6是根據本發明的實施例的由第二伺服器執行的二維碼生成方法的流程圖。

在步驟S610，從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

在步驟S620，對用於生成二維碼的資訊進行數位簽章；

在步驟S630，將包含有數位簽章的二維碼資訊發送到第一伺服器。

在可選實施例中，在從第一伺服器接收生成二維碼的請求之前還包括：從第一伺服器接收註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。並且，在從第一伺服器接收到註冊請求之後，所述二維碼生成方法還可包括：根據所述註冊請求，完成對第一伺服器的註冊。

圖7是執行如圖6所示的二維碼生成方法的二維碼生成設備（即，第二伺服器）的方塊圖。

本領域技術人員將理解，圖7中示出的二維碼生成設備的結構並不構成對本發明的電子裝置的限定，可包括比

圖示更多或更少的部件，或組合某些部件，或不同的部件佈置。

所述二維碼生成設備可包括接收單元710、處理單元720和發送單元730。

接收單元710從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊。在可替換實施例中，接收單元還從第一伺服器接收註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

在可替換實施例中，所述二維碼生成設備可包括註冊單元，所述註冊單元根據所述註冊請求，完成對第一伺服器的註冊。

處理單元720對用於生成二維碼的資訊進行數位簽章。可選地，處理單元720可基於非對稱加密演算法，利用私密金鑰對用於生成二維碼的資訊進行數位簽章。

發送單元730將包含有數位簽章的二維碼資訊發送到第一伺服器。

在可替換實施例中，所述二維碼生成設備還包括確定單元，所述確定單元確定第一伺服器是否在第二伺服器中註冊；若是，則根據接收到的生成二維碼的請求對用於生成二維碼的資訊進行數位簽章；若否，則不執行對用於生成二維碼的資訊進行數位簽章並向第一伺服器發送註冊邀請。

在可替換的實施例中，根據生成二維碼的資訊的不同，在對用於生成二維碼的資訊進行數位簽章的步驟中使

用的私密金鑰不同。

在另一示例性實施例中，可提供一種二維碼生成系統，所述系統包括如圖5中的二維碼生成設備和如圖7所述的二維碼生成設備。

如上所述，根據本發明的實施例提供的二維碼生成方法及其設備通過一伺服器與另一伺服器之間協同作用產生二維碼，增強了二維碼的安全性和有效性，並且方便在二維碼識別過程中識別出二維碼是否被篡改。

圖8是根據本發明的實施例的二維碼識別方法的流程圖。

在步驟S810，啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用。

在步驟S820，利用所述應用中的掃描單元掃描所述二維碼。

在步驟S830，利用公開金鑰對掃描的二維碼進行驗證。

在步驟S840，若驗證成功，則識別出與掃描的二維碼對應的資訊。

在可替換實施例中，所述公開金鑰是從所述伺服器或遠端存放裝置獲得的。此外，所述方法還可包括儲存所述驗證步驟中相關的資訊。

圖9是根據本發明的實施例的執行如圖8所述的二維碼識別方法的二維碼識別設備的方塊圖。

本領域技術人員將理解，圖9中示出的二維碼識別設

備的結構並不構成對本發明的電子裝置的限定，可包括比圖示更多或更少的部件，或組合某些部件，或不同的部件佈置。

所述二維碼識別設備可包括啟動單元910、掃描單元920、驗證單元930和識別單元940。

啟動單元910可啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用。

掃描單元920可利用所述應用中的掃描單元掃描所述二維碼；

驗證單元930可利用公開金鑰對掃描的二維碼進行驗證；

識別單元940可在驗證單元驗證成功的情況下，識別出與掃描的二維碼對應的資訊。

在可替換實施例中，所述公開金鑰是從所述伺服器或遠端存放裝置獲得的。

在可替換實施例中，所述二維碼識別設備還包括儲存單元，所述儲存單元儲存所述驗證步驟中相關的資訊。

圖10是執行根據本發明的實施例的二維碼生成方法或二維碼識別方法的電子設備的方塊圖。參考圖10，在硬體層面，該電子設備包括處理器、內部匯流排、網路介面、記憶體以及非易失性記憶體，當然還可能包括其他業務所需要的硬體。處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成的網頁截圖裝置。當然，除了軟體實現方式之外，本申請案並不排除

其他實現方式，比如邏輯裝置抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯裝置。

根據本發明的實施例提供的二維碼識別方法及其設備通過特定應用利用公開金鑰識別出與二維碼對應地資訊，增加了二維碼識別過程中的真偽判定，防止二維碼被篡改。

在20世紀90年代，對於一個技術的改進可以很明顯地區分是硬體上的改進（例如，對二極體、電晶體、開關等電路結構的改進）還是軟體上的改進（對於方法流程的改進）。然而，隨著技術的發展，當今的很多方法流程的改進已經可以視為硬體電路結構的直接改進。設計人員幾乎都通過將改進的方法流程程式設計到硬體電路中來得到相應的硬體電路結構。因此，不能說一個方法流程的改進就不能用硬體實體模組來實現。例如，可程式設計邏輯裝置（**Programmable Logic Device, PLD**）（例如場可程式設計閘陣列（**Field Programmable Gate Array, FPGA**））就是這樣一種積體電路，其邏輯功能由使用者對裝置程式設計來確定。由設計人員自行程式設計來把一個數位系統“集成”在一片PLD上，而不需要請晶片製造廠商來設計和製作專用的積體電路晶片。而且，如今，取代手工地製作積體電路晶片，這種程式設計也多半改用“邏輯編譯器（**logic compiler**）”軟體來實現，它與程式開發撰寫時所用的軟體編譯器相類似，而要編譯之前的原始代碼也得用

特定的程式設計語言來撰寫，此稱之為硬體描述語言（Hardware Description Language，HDL），而HDL也並非僅有一種，而是有許多種，如ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）與Verilog。本領域技術人員也應該清楚，只需要將方法流程用上述幾種硬體描述語言稍作邏輯程式設計並程式設計到積體電路中，就可以很容易得到實現該邏輯方法流程的硬體電路。

控制器可以按任何適當的方式實現，例如，控制器可以採取例如微處理器或處理器以及儲存可由該（微）處理器執行的電腦可讀程式碼（例如軟體或韌體）的電腦可讀媒體、邏輯閘、開關、專用積體電路（Application Specific Integrated Circuit，ASIC）、可程式設計邏輯控制器和嵌入微控制器的形式，控制器的例子包括但不限於以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320，記憶體控制器還可以被實現為記憶體的邏輯控制的一部分。本領域技術人員也知道，除了以純電腦可讀程式碼方式實現控制器

以外，完全可以通過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積體電路、可程式設計邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內包括的用於實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦。具體的，電腦例如可以為個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件設備、遊戲控制台、平板電腦、可穿戴設備或者這些設備中的任何設備的組合。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本申請案時可以把各單元的功能在同一個或多個軟體和／或硬體中實現。

本領域內的技術人員應明白，本申請案的實施例可提供為方法、系統、或電腦程式產品。因此，本申請案可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本申請案可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（包括但不限於磁碟記憶體、**CD-ROM**、光學記憶體等）上實施的電腦程式產品的形式。

本申請案是參照根據本申請案實施例的方法、設備（系統）、和電腦程式產品的流程圖和／或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和／或方塊圖中的每一流程和／或方塊、以及流程圖和／或方塊圖中的流程和／或方塊的結合。可提供這些電腦程式指令到通用電腦、專用電腦、嵌入式處理機或其他可程式設計資料處理設備的處理器以產生一個機器，使得通過電腦或其他可程式設計資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的裝置。

這些電腦程式指令也可儲存在能引導電腦或其他可程式設計資料處理設備以特定方式工作的電腦可讀記憶體中，使得儲存在該電腦可讀記憶體中的指令產生包括指令裝置的製造品，該指令裝置實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦或其他可程式設計設備上執行的指令提供用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的步驟。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入／輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，

隨機存取記憶體（RAM）和／或非易失性記憶體等形式，如唯讀記憶體（ROM）或快閃記憶體（flash RAM）。記憶體是電腦可讀媒體的示例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體（PRAM）、靜態隨機存取記憶體（SRAM）、動態隨機存取記憶體（DRAM）、其他類型的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電可擦除可程式設計唯讀記憶體（EEPROM）、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體（CD-ROM）、數位多功能光碟（DVD）或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置或任何其他非傳輸媒體，可用於儲存可以被計算設備存取的資訊。按照本文中的界定，電腦可讀媒體不包括暫存電腦可讀媒體（transitory media），如調製的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還

存在另外的相同要素。

本領域技術人員應明白，本申請案的實施例可提供為方法、系統或電腦程式產品。因此，本申請案可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本申請案可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（包括但不限於磁碟記憶體、**CD-ROM**、光學記憶體等）上實施的電腦程式產品形式。

本申請案可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定任務或實現特定抽象資料類型的常式、程式、物件、組件、資料結構等等。也可以在分散式運算環境中實踐本申請案，在這些分散式運算環境中，由通過通信網路而被連接的遠端處理設備來執行任務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦儲存媒體中。

本說明書中的各個實施例均採用遞進的方式描述，各個實施例之間相同相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。尤其，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

以上所述僅為本申請案的實施例而已，並不用於限制本申請案。對於本領域技術人員來說，本申請案可以有各種更改和變化。凡在本申請案的精神和原理之內所作的任

何修改、等同替換、改進等，均應包含在本申請案的申請專利範圍之內。

【符號說明】

110：伺服器

120：伺服器

510：發送單元

520：接收單元

530：生成單元

710：接收單元

720：處理單元

730：發送單元

910：啟動單元

920：掃描單元

930：驗證單元

940：識別單元



201830291

【發明摘要】

【中文發明名稱】

二維碼生成方法及其設備和二維碼識別方法及其設備

【中文】

本申請案公開了一種二維碼生成方法及其設備和二維碼識別方法及其設備。所述方法包括：第一伺服器向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；第二伺服器根據接收到的生成二維碼的請求，對用於生成二維碼的資訊進行數位簽章；將包含有數位簽章的二維碼資訊發送到第一伺服器；第一伺服器利用所述二維碼資訊，生成二維碼。根據本發明的實施例通過一伺服器與另一伺服器之間協同作用產生二維碼，增強了二維碼的安全性和有效性，並且方便在二維碼識別過程中識別出二維碼是否被篡改。

【指定代表圖】第(2)圖。

【代表圖之符號簡單說明】

110：伺服器

120：伺服器

210：步驟

220：步驟

【特徵化學式】無

【發明申請專利範圍】

【第1項】

一種二維碼生成方法，其特徵在於，包括：

第一伺服器向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

第二伺服器根據接收到的生成二維碼的請求，對用於生成二維碼的資訊進行數位簽章；

將包含有數位簽章的二維碼資訊發送到第一伺服器；

第一伺服器利用所述二維碼資訊，生成二維碼。

【第2項】

如申請專利範圍第1項所述的方法，其中，第一伺服器向第二伺服器發送生成二維碼的請求之前還包括：第一伺服器向第二伺服器發送註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

【第3項】

如申請專利範圍第2項所述的方法，其中，在第一伺服器向第二伺服器發送註冊請求之後還包括：第二伺服器根據所述註冊請求，完成對第一伺服器的註冊。

【第4項】

如申請專利範圍第3項所述的方法，其中，第二伺服器根據接收到的生成二維碼的請求對用於生成二維碼的資訊進行數位簽章之前還包括：

確定第一伺服器是否向第二伺服器註冊；

若是，則第二伺服器根據接收到的生成二維碼的請求

對用於生成二維碼的資訊進行數位簽章；

若否，則第二伺服器不執行對用於生成二維碼的資訊進行數位簽章並向第一伺服器發送註冊邀請。

【第5項】

如申請專利範圍第1至4項中的任一項所述的方法，其中，第二伺服器根據接收到的生成二維碼的請求對用於生成二維碼的資訊進行數位簽章的步驟包括：第二伺服器在接收到生成二維碼的請求之後，基於非對稱加密演算法，利用私密金鑰對用於生成二維碼的資訊進行數位簽章。

【第6項】

如申請專利範圍第5項所述的方法，其中，根據生成二維碼的資訊的不同，在對用於生成二維碼的資訊進行數位簽章的步驟中使用的私密金鑰不同。

【第7項】

一種二維碼生成方法，所述方法由第一伺服器執行，其特徵在於，包括：

向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊；

利用所述二維碼資訊，生成二維碼。

【第8項】

如申請專利範圍第7項所述的方法，其中，向第二伺服器發送生成二維碼的請求之前還包括：向第二伺服器發

送註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

【第9項】

一種二維碼生成設備，其特徵在於，包括：

發送單元，向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

接收單元，從第二伺服器接收由第二伺服器生成的包含有數位簽章的二維碼資訊；

生成單元，利用所述二維碼資訊，生成二維碼。

【第10項】

如申請專利範圍第9項所述的設備，其中，其特徵在，發送單元在向第一伺服器發送生成二維碼的請求之前，向第一伺服器發送註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

【第11項】

一種二維碼生成方法，所述方法由第二伺服器執行，其特徵在於，包括：

從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

對用於生成二維碼的資訊進行數位簽章；

將包含有數位簽章的二維碼資訊發送到第一伺服器。

【第12項】

如申請專利範圍第11項所述的方法，其中，在從第一伺服器接收生成二維碼的請求之前還包括：從第一伺服器

接收註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

【第13項】

如申請專利範圍第12項所述的方法，其中，在從第一伺服器接收到註冊請求之後，還包括：根據所述註冊請求，完成對第一伺服器的註冊。

【第14項】

如申請專利範圍第13項所述的方法，其中，在對用於生成二維碼的資訊進行數位簽章之前還包括：

確定第一伺服器是否在第二伺服器中註冊：

若是，則根據接收到的生成二維碼的請求對用於生成二維碼的資訊進行數位簽章；

若否，則不執行對用於生成二維碼的資訊進行數位簽章並向第一伺服器發送註冊邀請。

【第15項】

如申請專利範圍第11至14項中的任一項所述的方法，其中，對用於生成二維碼的資訊進行數位簽章的步驟包括：基於非對稱加密演算法，利用私密金鑰對用於生成二維碼的資訊進行數位簽章。

【第16項】

如申請專利範圍第15項所述的方法，其中，根據生成二維碼的資訊的不同，在對用於生成二維碼的資訊進行數位簽章的步驟中使用的私密金鑰不同。

【第17項】

一種二維碼生成裝置，其特徵在於，包括：

接收單元，從第一伺服器接收生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

處理單元，對用於生成二維碼的資訊進行數位簽章；

發送單元，將包含有數位簽章的二維碼資訊發送到第一伺服器。

【第18項】

如申請專利範圍第17項所述的裝置，其中，接收單元還從第一伺服器接收註冊請求，所述註冊請求包括與本次註冊相關的所有資訊。

【第19項】

如申請專利範圍第18項所述的裝置，其中，還包括：註冊單元，根據所述註冊請求，完成對第一伺服器的註冊。

【第20項】

如申請專利範圍第19項所述的裝置，其中，還包括：確定單元確定第一伺服器是否在第二伺服器中註冊：

若是，則根據接收到的生成二維碼的請求對用於生成二維碼的資訊進行數位簽章；

若否，則不執行對用於生成二維碼的資訊進行數位簽章並向第一伺服器發送註冊邀請。

【第21項】

如申請專利範圍第17至20項中的任一項所述的裝置，其中，處理單元基於非對稱加密演算法，利用私密金鑰對

用於生成二維碼的資訊進行數位簽章。

【第22項】

如申請專利範圍第21項所述的裝置，其中，根據生成二維碼的資訊的不同，在對用於生成二維碼的資訊進行數位簽章的步驟中使用的私密金鑰不同。

【第23項】

一種二維碼生成系統，其特徵在於，所述系統包括第一伺服器和第二伺服器，第一伺服器包括：

發送單元，向第二伺服器發送生成二維碼的請求，所述請求包括用於生成二維碼的資訊；

接收單元，從第二伺服器接收由第一伺服器生成的包含有數位簽章的二維碼資訊；

生成單元，利用所述二維碼資訊，生成二維碼，
第二伺服器包括：

接收單元，從第一伺服器接收所述請求；

處理單元，對用於生成二維碼的資訊進行數位簽章；

發送單元，將包含有數位簽章的二維碼資訊發送到第一伺服器。

【第24項】

一種二維碼識別方法，其特徵在於，包括：

啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用；

利用所述應用中的掃描單元掃描所述二維碼；

利用公開金鑰對掃描的二維碼進行驗證；

若驗證成功，則識別出與掃描的二維碼對應的資訊。

【第25項】

如申請專利範圍第24項所述的方法，其中，所述公開金鑰是從所述伺服器或遠端儲存裝置獲得的。

【第26項】

如申請專利範圍第24項所述的方法，其中，還包括：
儲存所述驗證步驟中相關的資訊。

【第27項】

一種二維碼識別設備，其特徵在於，包括：

啟動單元，啟動與對用於生成二維碼的資訊進行數位簽章的伺服器對應的應用；

掃描單元，利用所述應用中的掃描單元掃描所述二維碼；

驗證單元，利用公開金鑰對掃描的二維碼進行驗證；

識別單元，在驗證單元驗證成功的情況下，識別出與掃描的二維碼對應的資訊。

【第28項】

如申請專利範圍第27項所述的設備，其中，所述公開金鑰是從所述伺服器或遠端存放裝置獲得的。

【第29項】

如申請專利範圍第28項所述的設備，其中，還包括：
儲存單元，儲存所述驗證步驟中相關的資訊。

