I577145

(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 I577145 B**

(45)公告日： 中華民國 106 (2017) 年 04 月 01 日

(21)申請案號：104122660 (22)申請日： 中華民國 104 (2015) 年 07 月 13 日

(51)Int. Cl.： ***H04B5/00 (2006.01)*** ***H04L9/28 (2006.01)***

(30)優先權：2014/12/15 中國大陸 201410775282.2

(71)申請人：英華達股份有限公司 (中華民國) INVENTEC APPLIANCES CORP. (TW)
新北市五股區五工五路 37 號

(72)發明人：李森峰 LI, SEN-FENG (CN) ；魏翠紅 WEI, TSUI-HUNG (CN) ；洪智忠 HUNG, CHIH-CHUNG (TW) ；高懿民 KAO, YI-MIN (TW)

(74)代理人：李國光；張仲謙

(56)參考文獻：

CN	101140544B	CN	101261675A
CN	101656960A	CN	103745350A
CN	104025633A		

審查人員：陳奕昌

申請專利範圍項數：8 項 圖式數：4 共 23 頁

(54)名稱

近場通訊設備資料之加密傳輸方法及其系統

METHOD FOR ENCRYPTED DATA TRANSMISSION OF NEAR FIELD COMMUNICATION DEVICE AND SYSTEM THEREOF

(57)摘要

本發明揭露了一種近場通訊設備資料之加密傳輸方法及其系統，該方法是將近場通訊資料劃分為複數段子資料，並分別採用不同之密鑰對該些子資料進行加密，針對不同子資料的作用或者功能，分別將各個加密密鑰告知不同的近場通訊接收設備，進而在不同應用環境進行近場通訊訊息交換時，近場通訊接收設備僅僅能夠利用其所知道的密鑰進行相應子資料的解密，而對其它子資料因為沒有相應之密鑰而無法解密。本發明實現了一個近場通訊發送設備與複數個近場通訊接收設備間進行近場通訊通訊時，能夠保證近場通訊發送設備中資料訊息之安全，實現對近場通訊接收設備所要保密之特定資料訊息的保護。

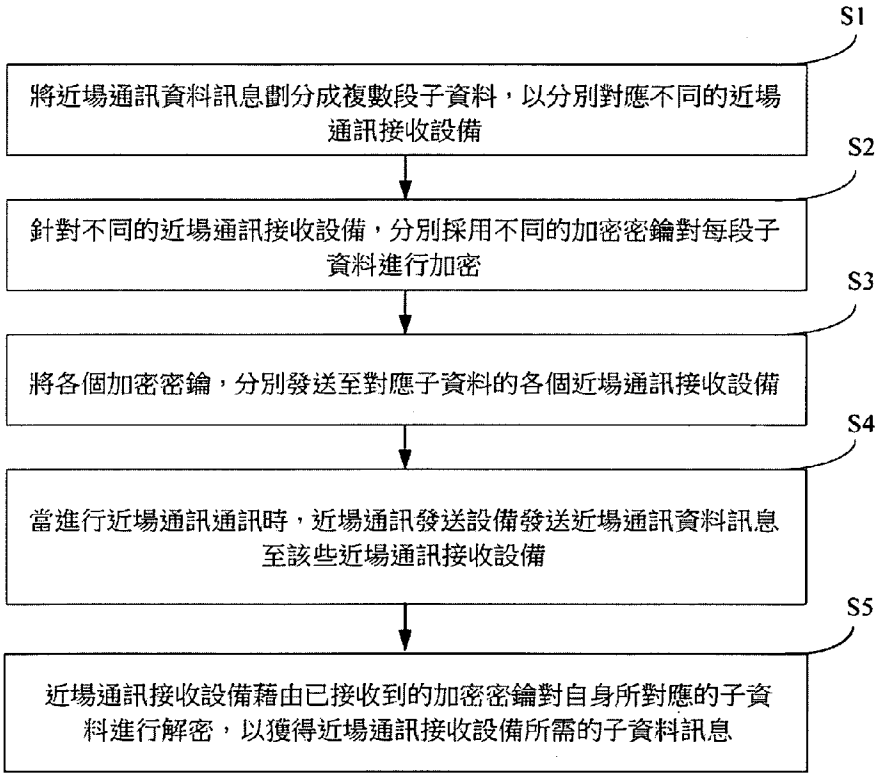
The present invention discloses a method for encrypted data transmission of near field communication device and system thereof. The method is used for dividing near field communication data into a plurality of sub-data and encrypting the sub-data by different keys respectively. The different keys are sent to different near field communication receiving devices respectively according to the different functions of a plurality of sub-data. When the near field communication data is exchanged in different applications, the near field communication receiving devices only use their own keys to decrypt the corresponding sub-data. The near field communication receiving devices can't decrypt other sub-data because they don’t have the keys corresponding to other sub-data. The invention is implemented to ensure the safety of data from the near field communication transmitting device and to protect individual secret information for the near field communication receiving devices when the near field communication is proceeded between a transmitting device and a plurality of near field communication receiving devices.

TW I577145 B

指定代表圖：

符號簡單說明：

S1~S5・・・步驟



【第1圖】

I577145
專利案號：104122660

公告本

105年 08月 18日 修正替換頁

申請日：104.7.13

IPC分類：H04B 5/00 (2006.01)
H04L 9/28 (2006.01)

【發明摘要】

【中文發明名稱】近場通訊設備資料之加密傳輸方法及其系統

【英文發明名稱】METHOD FOR ENCRYPTED DATA TRANSMISSION OF NEAR FIELD COMMUNICATION DEVICE AND SYSTEM THEREOF

【中文】

本發明揭露了一種近場通訊設備資料之加密傳輸方法及其系統，該方法是將近場通訊資料劃分為複數段子資料，並分別採用不同之密鑰對該些子資料進行加密，針對不同子資料的作用或者功能，分別將各個加密密鑰告知不同的近場通訊接收設備，進而在不同應用環境進行近場通訊訊息交換時，近場通訊接收設備僅僅能夠利用其所知道的密鑰進行相應子資料的解密，而對其它子資料因為沒有相應之密鑰而無法解密。本發明實現了一個近場通訊發送設備與複數個近場通訊接收設備間進行近場通訊通訊時，能夠保證近場通訊發送設備中資料訊息之安全，實現對近場通訊接收設備所要保密之特定資料訊息的保護。

【英文】

The present invention discloses a method for encrypted data transmission of near field communication device and system thereof. The method is used for dividing near field communication data into a plurality of sub-data and encrypting the sub-data by different keys respectively. The different keys are sent to different near field

communication receiving devices respectively according to the different functions of a plurality of sub-data. When the near field communication data is exchanged in different applications, the near field communication receiving devices only use their own keys to decrypt the corresponding sub-data. The near field communication receiving devices can't decrypt other sub-data because they don't have the keys corresponding to other sub-data. The invention is implemented to ensure the safety of data from the near field communication transmitting device and to protect individual secret information for the near field communication receiving devices when the near field communication is proceeded between a transmitting device and a plurality of near field communication receiving devices.

【指定代表圖】第（1）圖。

【代表圖之符號簡單說明】

S1~S5：步驟

【特徵化學式】

無

105年 08月 18日 修正替換頁

【發明說明書】

【中文發明名稱】近場通訊設備資料之加密傳輸方法及其系統

【英文發明名稱】METHOD FOR ENCRYPTED DATA TRANSMISSION OF NEAR FIELD COMMUNICATION DEVICE AND SYSTEM THEREOF

【技術領域】

【0001】 本發明關於訊息安全領域，特別是關於一種基於近場通訊設備之資料加密傳輸方法及其系統。

【先前技術】

【0002】 隨著網際網路技術的發展，資料訊息的安全越發重要。資料認證設備，例如硬體數位證書載體 USB KEY 等，具有個人身份認證以及資料加密解密等功能，已經被廣泛應用於網路銀行、電子政務等領域的各種業務中。

【0003】 習知技術中，資料認證設備主要藉由 USB 介面與個人電腦終端相連，以完成資料的認證過程。但是，隨著移動網際網路的發展，移動終端設備（例如手機，尤其是智慧型手機）已經逐漸應用到個人辦公、網路銀行支付等領域，而移動終端設備中的大部分不支持藉由 USB 介面與資料認證設備進行通訊，因此，對於移動終端而言，資料訊息的安全保障是一項亟待解決的問題。

【0004】 NFC（Near Field Communication，近場通訊技術）技術

是由 RFID（Radio Frequency Identification，無線射頻識別）技術演變而來，可實現應用於移動終端設備，進而在移動終端（例如智慧型手機）中逐漸地得到了越來越高的關注和越來越廣泛的應用。

【0005】 近場通訊手機，是在手機中加入近場通訊模組，進而實現近距離無線通訊，該技術由於具有近距離無線通訊之特點，因此可以設計很多手機應用，例如身份認證、音視訊傳輸、訊息瀏覽、手機支付等。近場通訊技術之一個特性是近場通訊設備在進行資料傳輸時，只能一次傳輸近場通訊模組內的所有資料。因此，目前的近場通訊發送設備（例如近場通訊手機）在傳輸資料時，都只能一次性地傳送其近場通訊模組內的全部資料，進而導致所有被近場通訊發送設備所接觸之近場通訊接收設備所接收到的資料和訊息都是相同，即所有被近場通訊發送設備所接觸之近場通訊接收設備所接收到之資料和訊息都與該近場通訊發送設備所發出之資料一致。這些一致的資料，整體上要麼都是未加密資料，要麼都是採用同一種加密方式進行加密處理後之資料。

【0006】 目前近場通訊設備存在的一個缺點，對於近場通訊設備用戶來說，用戶對所接觸之不同近場通訊接收設備進行資料傳輸時，不能自主地選擇傳輸不同內容之資料訊息，只能同樣地傳輸近場通訊模組中之全部資料和訊息，無法針對不同近場通訊接收設備傳輸不同內容之資料訊息，不便於對某些近場通訊接收設備所要保密之特定資料訊息進行保留和保護，因而難以做到資料訊息之安全保護。

【發明內容】

【0007】 有鑑於此，本發明提供一種近場通訊設備資料之加密傳輸方法及其系統，以保證一個近場通訊發送設備向複數個近場通訊接收設

備發送的資料訊息的安全，實現對近場通訊接收設備所要保密的特定資料訊息的保護。

【0008】 本發明之技術方案是這樣實現的：

【0009】 一種近場通訊設備資料之加密傳輸方法，其包括下列步驟：

【0010】 將一近場通訊資料訊息劃分為複數段子資料；

【0011】 分別採用不同之加密密鑰對該些子資料進行加密；

【0012】 將該些加密密鑰，分別發送至對應該些子資料之複數個近場通訊接收設備；

【0013】 發送近場通訊資料至近場通訊接收設備；

【0014】 近場通訊接收設備藉由已接收到之加密密鑰對其自身所對應之子資料進行解密，以獲得該近場通訊接收設備所需之子資料訊息。

【0015】 進一步，將該些加密密鑰分別發送至對應該些子資料之該些近場通訊接收設備之步驟中，更包括下列步驟：

藉由簡訊或者電子郵件方式，將該些加密密鑰分別發送至該些近場通訊接收設備。

【0016】 進一步，發送近場通訊資料至近場通訊接收設備之步驟，更包含下列步驟：

將該些子資料之位置分別告知對應之該些近場通訊接收設備。

【0017】 進一步，近場通訊接收設備係具有近場通訊模組之手機、具有近場通訊模組之手環、具有近場通訊模組之門禁設備或具有近場通訊模組之支付設備。

【0018】 一種近場通訊設備資料之加密傳輸系統，包括近場通訊發送設備和複數個近場通訊接收設備， 近場通訊發送設備包括：

【0019】 管理模組，用以將近場通訊發送設備中的近場通訊資料劃分為複數段子資料，並分別採用不同之加密密鑰對該些子資料進行加密；

【0020】 通訊模組，用以將該些加密密鑰分別發送至對應該些子資料之複數個近場通訊接收設備；以及

【0021】 近場通訊模組，用以儲存加密後之近場通訊資料，並當與該些近場通訊接收設備通訊連接時，將所儲存之該近場通訊資料發送至近場通訊接收設備；

【0022】 其中，近場通訊接收設備接收並儲存由通訊模組發送來之該些加密密鑰，當與近場通訊發送設備通訊連接時，在接收近場通訊模組發送來之近場通訊資料後，藉由已接收到之加密密鑰對其自身所對應之子資料進行解密，以獲得該近場通訊接收設備所需之子資料訊息。

【0023】 進一步，近場通訊模組更包括訊息處理子模組，通訊連接近場通訊接收設備，用以將該些近場通訊接收設備對應之子資料之位置告知所對應之該些近場通訊接收設備。

【0024】 進一步，近場通訊發送設備具有近場通訊模組之手機、具有近場通訊模組之手環、具有近場通訊模組之門禁設備或具有近場通訊模組之支付設備。

【0025】 進一步，近場通訊接收設備具有近場通訊功能之手機、具有近場通訊功能之手環、具有近場通訊功能之門禁設備、具有近場通訊功能之支付設備。

【0026】 從上述方案可以看出，本發明所提供之近場通訊設備資料

系統，將近場通訊設備中之近場通訊資料劃分為複數段子資料，並分別採用不同之加密密鑰對複數個子資料進行加密，針對不同子資料之作用或者功能，分別將複數個子資料之加密密鑰告知不同的近場通訊接收設備，進而在不同應用環境進行近場通訊訊息交互時，近場通訊接收設備僅僅能夠利用其所知道的加密密鑰進行相應子資料的解密，而對其它子資料因為沒有相應之加密密鑰而無法解密。本發明之近場通訊設備資料之加密傳輸方法及其系統實現了在進行一個近場通訊發送設備與複數個近場通訊接收設備間進行近場通訊通訊時，能夠保證近場通訊發送設備中資料訊息之安全，實現對近場通訊接收設備所要保密之特定資料訊息的保護。

【圖式簡單說明】

【0027】 第 1 圖為本發明之近場通訊設備資料之加密傳輸方法之流程圖；

第 2 圖為本發明之近場通訊設備資料之加密傳輸方法中的加密過程實施例示意圖；

第 3 圖為本發明之近場通訊設備資料之加密傳輸方法中的解密過程實施例之示意圖；

第 4 圖為本發明之近場通訊設備資料之加密傳輸系統的實施例結構之示意圖。

【實施方式】

【0028】 為了使本發明的目的、技術方案及優點更加清楚明白，以

下參照圖式並舉實施例，對本發明作進一步詳細說明。

【0029】 如第 1 圖所示，本發明之近場通訊設備資料之加密傳輸方法，包括：

【0030】 步驟 S1、將一近場通訊資料劃分成複數段子資料，以分別對應不同的近場通訊接收設備；

【0031】 步驟 S2、針對不同的近場通訊接收設備，分別採用不同的加密密鑰對該些子資料進行加密；

【0032】 步驟 S3、將該些加密密鑰，分別發送至對應該些子資料的複數個近場通訊接收設備；

【0033】 步驟 S4、發送近場通訊資料至近場通訊接收設備；

【0034】 步驟 S5、近場通訊接收設備藉由已接收到的加密密鑰對其自身所對應的子資料進行解密，以獲得該近場通訊接收設備所需的子資料訊息。

【0035】 本發明的上述方法中，近場通訊發送設備例如具有近場通訊模組的手機，其能夠實現手機的電子支付、身份認證等功能，其中電子支付中可應用於消費、交通卡刷卡等，身份認證可應用於公司、家庭門禁系統的認證以及個人名片訊息等。近場通訊發送設備更可以為具有近場通訊模組的手環、具有近場通訊模組的門禁設備、具有近場通訊模組的支付設備等。對應於近場通訊發送設備，近場通訊接收設備可包括複數種設備，例如具有近場通訊模組的手機、具有近場通訊模組的手環、具有近場通訊模組的門禁設備、具有近場通訊模組的支付設備等。

【0036】 以下對本發明之近場通訊設備資料之加密傳輸方法進行具體說明。

【0037】 步驟 S1、將近場通訊資料劃分成複數段子資料，以分別對應不同的近場通訊接收設備。

【0038】 如第 2 圖所示，本發明之步驟 1 中例如將近場通訊發送設備中的近場通訊模組所儲存的近場通訊資料訊息劃分為 n 段子資料，其中 n 為大於等於 1 之整數。各段子資料分別對應不同的近場通訊接收設備，例如，第 1 子資料對應第 1 近場通訊接收設備，第 2 子資料對應第 2 近場通訊接收設備……第 n 子資料對應第 n 近場通訊接收設備。各段子資料依據用戶的需求定制，例如當用戶具有三方面近場通訊應用需求（例如，個人名片訊息用於發送給他人的近場通訊設備，公司門禁訊息用於進入公司使用，以及住宅門禁訊息用戶回家使用）時，其近場通訊資料訊息可劃分為 3 段子資料（分別儲存個人名片訊息、公司門禁訊息和住宅門禁訊息）。

【0039】 步驟 S2、針對不同的近場通訊接收設備，分別採用不同的加密密鑰對該些子資料進行加密。

【0040】 繼續參照第 2 圖所示，本發明之步驟 2 中，例如，針對第 1 近場通訊接收設備，採用第 1 密鑰對第 1 子資料進行加密，針對第 2 近場通訊接收設備，採用第 2 密鑰對第 2 子資料進行加密……針對第 n 近場通訊接收設備，採用第 n 密鑰對第 n 子資料進行加密，其中，第 1 密鑰至第 n 密鑰各不相同。

【0041】 步驟 S3、將該些加密密鑰，分別發送至對應該些子資料的複數個近場通訊接收設備。

【0042】 本發明之步驟 S3 中，例如，將第 1 密鑰發送至第 1 近場通訊接收設備，將第 2 密鑰發送至第 2 近場通訊接收設備……將第 n 密鑰發送至第 n 近場通訊接收設備。各個近場通訊接收設備不知道除了自

身以外之其它近場通訊接收設備之加密密鑰。每個加密密鑰只針對整個近場通訊資料中其所加密之子資料。

【0043】 本發明之近場通訊設備資料之加密傳輸方法實施例中，近場通訊發送設備可為具有近場通訊模組的手機，因此本發明之步驟 3 中，近場通訊發送設備可藉由簡訊或者電子郵件（email）等方式，也可採用口頭告知方式，如語音方式，將加密密鑰分別發送給各個近場通訊接收設備，便於將具有近場通訊模組的手環、具有近場通訊模組的門禁設備、具有近場通訊模組的支付設備等近場通訊發送設備之加密密鑰告知相應的近場通訊接收設備。

【0044】 至此，便完成了近場通訊發送設備中之資料加密。

【0045】 步驟 S4、當進行近場通訊通訊時，近場通訊發送設備發送近場通訊資料訊息至該些近場通訊接收設備。

【0046】 本發明之步驟 S4 中，進行近場通訊通訊是指近場通訊發送設備向近場通訊接收設備發送其中的近場通訊模組中所保存的近場通訊資料訊息，例如具有近場通訊模組的手機進行電子支付或者門禁刷卡、優遊卡刷卡等操作，其過程可參照第 3 圖所示。

【0047】 步驟 S5、該些近場通訊接收設備藉由已接收到的加密密鑰對其自身所對應的子資料進行解密，以獲得該近場通訊接收設備所需的子資料訊息。

【0048】 例如在近場通訊發送設備之近場通訊模組中將近場通訊資料訊息劃分為 n 段子資料，並且透過前序步驟 1 至步驟 3 對每段子資料進行加密，並將各段子資料之加密密鑰藉由簡訊或電子郵件等方式告知了各段子資料所對應的各個近場通訊接收設備（第 1 近場通訊接收設備與第 1 子資料、第 1 密鑰相對應並且已經接收到了第 1 密鑰，第 2 近場

通訊接收設備與第 2 子資料、第 2 密鑰相對應並且已經接收到了第 2 密鑰……第 n 近場通訊接收設備與第 n 子資料、第 n 密鑰相對應並且已經接收到了第 n 密鑰），則本發明之步驟 5 中，在近場通訊發送設備與第 1 近場通訊接收設備到第 n 近場通訊接收設備中的第 i 近場通訊接收設備（第 i 近場通訊接收設備與第 i 子資料、第 i 密鑰相對應並且已經接收到了第 i 密鑰）之間進行近場通訊時，由於近場通訊資料傳輸特性，近場通訊發送設備必須將所儲存的整個近場通訊資料發送至第 i 近場通訊接收設備，因此第 i 近場通訊接收設備接收到了近場通訊發送設備所儲存的整個近場通訊資料，但是，整個近場通訊資料此時全部處於加密狀態，而第 i 近場通訊接收設備僅僅具有用於解密其中第 i 子資料之第 i 密鑰，沒有解密其它子資料之密鑰，因此除了第 i 子資料以外，其它子資料對於第 i 近場通訊接收設備來說仍然處於加密狀態，這些加密狀態之子資料無法被第 i 近場通訊接收設備所解密，因此，這些加密狀態之子資料對於第 i 近場通訊接收設備來說是安全的，而對於近場通訊發送設備來說，第 i 近場通訊接收設備則無法破解其他子資料。本發明之加密傳輸方法能夠保證一個近場通訊發送設備向複數個近場通訊接收設備發送之近場通訊資料的安全，實現對近場通訊接收設備所要保密之特定資料訊息的保護。

【0049】 本發明之步驟 S4 中，近場通訊發送設備發送近場通訊資料至近場通訊接收設備的同時，進一步地更將近場通訊接收設備對應之子資料在近場通訊資料中之位置告知近場通訊接收設備，這樣更便於近場通訊接收設備解密其所需要之資料訊息。關於加密密鑰所加密之子資料在整個近場通訊資料中之位置確定可採用複數種方法，例如在近場通訊資料之 n 段子資料中，將第 i 子資料經過第 i 密鑰加密後，在該子資料之頭部和尾部增加標識，以表明標識間之子資料為第 i 密鑰所加密之子

資料，並將該標識告知第 i 近場通訊接收設備後，第 i 近場通訊接收設備便可依據該標識獲知所要解密之子資料在近場通訊資料中之位置。

【0050】 作為本發明之近場通訊設備資料之加密傳輸方法的實際使用實例，例如，在具有近場通訊模組的手機（即近場通訊發送設備）中，藉由例如手機應用軟體，將近場通訊模組儲存的近場通訊資料劃分為 3 段子資料，第 1 子資料用於個人名片訊息，第 2 子資料用於公司門禁密碼訊息，第 3 子資料用於家庭門禁密碼訊息；之後，將個人名片訊息、公司門禁密碼訊息和家庭門禁密碼訊息分別利用第 1 密鑰、第 2 密鑰、第 3 密鑰進行加密，其中，第 1 密鑰、第 2 密鑰、第 3 密鑰各不相同；之後，將第 1 密鑰藉由簡訊、電子郵件或者例如口頭（如語音）等方式告知相關近場通訊接收設備，例如同事、客戶等其他人的具有近場通訊模組的手機；將第 2 密鑰藉由簡訊、電子郵件或者例如手動輸入等方式告知相關近場通訊接收設備，例如公司門禁系統的具有近場通訊模組的刷卡器；將第 3 密鑰藉由簡訊、電子郵件或者例如手動輸入等方式告知相關近場通訊接收設備，例如家庭門禁系統的具有近場通訊模組的刷卡器；對於第 1 子資料的個人名片訊息來說，當進行近場通訊設備之間的通訊時，例如具有近場通訊模組手機的使用者與其他持有近場通訊模組手機的使用者進行名片訊息交換時，具有近場通訊模組手機的使用者將手機靠近其他具有近場通訊模組的手機，則該使用者的手機將其中近場通訊模組所儲存的整個近場通訊資料發送給對方具有近場通訊模組的手機，同時將對方手機所需要解密之第 1 子資料告知對方手機，對方手機接收到整個近場通訊資料後，利用第 1 密鑰對接收到的近場通訊資料中的第 1 子資料進行解密，以獲得該使用者的個人名片訊息；對於第 2 資料訊息區段的公司門禁密碼訊息來說，當進行近場通訊設備間之通訊時，例如具有近場通訊模組手機的使用者在公司進行門禁刷卡時，具有

近場通訊模組手機的使用者將手機靠近公司門禁系統具有近場通訊模組之刷卡器，該使用者的手機將其中近場通訊模組所儲存的整個近場通訊資料發送給該刷卡器，同時將該刷卡器所需要解密之第 2 子資料告知該刷卡器，該刷卡器接收到整個近場通訊資料後，利用第 2 密鑰對接收到之第 2 子資料進行解密，之後公司門禁系統藉由該密碼訊息的驗證，進而觸發開門；對於第 3 子資料的家庭門禁密碼訊息來說，當進行近場通訊設備間之通訊時，例如具有近場通訊模組手機的使用者在家中進行門禁刷卡時，具有近場通訊模組手機的使用者將手機靠近家中門禁系統具有近場通訊模組之刷卡器，該使用者的手機將其中近場通訊模組所儲存的整個近場通訊資料發送給該刷卡器，同時將該刷卡器所需要解密之第 3 子資料告知刷卡器，刷卡器接收到整個近場通訊資料後，利用第 3 密鑰對接收到之第 3 子資料進行解密，之後家中門禁系統藉由該密碼訊息的驗證，進而觸發開門。

【0051】 本發明實施例同時提供了一種近場通訊設備資料之加密傳輸系統，如第 4 圖所示，其包括近場通訊發送設備 10 和複數個近場通訊接收設備 20；其中，近場通訊發送設備包括管理模組 11、近場通訊模組 12 和通訊模組 13；

【0052】 管理模組 11，用以將近場通訊發送設備 10 中的近場通訊資料劃分為複數段子資料，以分別對應不同的近場通訊接收設備 20，並分別採用不同的加密密鑰對該些子資料進行加密；

【0053】 通訊模組 13，用以將該些加密密鑰，分別發送至對應該些子資料的複數個近場通訊接收設備 20；

【0054】 近場通訊模組 12，用以儲存加密的近場通訊資料，並在進行近場通訊通訊時，將所儲存的近場通訊資料發送至近場通訊接收設備

20；

【0055】 近場通訊接收設備 20 接受並儲存由通訊模組 13 發送來的該些加密密鑰，當與近場通訊發送設備通訊連接時，在接收到近場通訊模組 12 發送來的近場通訊資料後，藉由已接收到的加密密鑰對其自身所對應的子資料進行解密，以獲得該近場通訊接收設備 20 所需要的子資料訊息。

【0056】 進一步地，近場通訊模組 12 更包括訊息處理子模組 121，通訊連接近場通訊接收設備 20，用以將該些子資料的位置告知所對應之該些近場通訊接收設備 20。

【0057】 其中，近場通訊發送設備 10 為具有近場通訊模組的手機、具有近場通訊模組的手環、具有近場通訊模組的門禁設備、具有近場通訊模組的支付設備等。作為具有近場通訊模組的手機來說，管理模組 11 可藉由手機所提供之硬體結合所開發之相應軟體實現，而通訊模組 13 可藉由手機中已有功能模組實現，例如利用簡訊收發功能模組以及手機上網功能模組實現。近場通訊接收設備可包括具有近場通訊功能的手機、具有近場通訊功能的手環、具有近場通訊功能的門禁設備、具有近場通訊功能的支付設備等。

【0058】 本發明之近場通訊設備資料之加密傳輸方法及其系統，將近場通訊設備中之近場通訊資料劃分為複數段子資料，並分別採用不同之加密密鑰對複數段子資料進行加密，針對不同子資料的作用或者功能，分別將各個子資料的加密密鑰告知不同的近場通訊接收設備，進而在不同應用環境進行近場通訊訊息交換時，近場通訊接收設備僅僅能夠利用其所知道的密鑰進行相應子資料的解密，而對其它子資料因為沒有相應之密鑰而無法解密，本發明之近場通訊設備資料之加密傳輸方法及

其系統實現了一個近場通訊發送設備與複數個近場通訊接收設備間進行近場通訊通訊時，能夠保證近場通訊發送設備中資料訊息之安全，實現對近場通訊接收設備所要保密之特定資料訊息的保護。

【0059】 以上所述僅為本發明的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

【符號說明】

【0060】 S1~S5：步驟

10：近場通訊發送設備

11：管理模組

12：近場通訊模組

121：訊息處理子模組

13：通訊模組

20：近場通訊接收設備

【發明申請專利範圍】

【第1項】 一種近場通訊設備資料之加密傳輸方法，其包括下列步驟：

將一近場通訊資料劃分為複數段子資料；

分別採用不同之一未加密之加密密鑰對該些子資料進行加密；

將該些未加密之加密密鑰分別發送至對應該些子資料之複數個近場通訊接收設備；

發送該近場通訊資料至該些近場通訊接收設備；以及

該些近場通訊接收設備藉由已接收到之該未加密之加密密鑰直接對其自身所對應之該子資料進行解密，以獲得該近場通訊接收設備所需之該子資料訊息。

【第2項】 如申請專利範圍第 1 項所述之近場通訊設備資料之加密傳輸方法，其中將該些加密密鑰分別發送至對應該些子資料之該些近場通訊接收設備之步驟，更包括下列步驟：

藉由一簡訊或者一電子郵件方式，將該些加密密鑰分別發送至該些近場通訊接收設備。

【第3項】 如申請專利範圍第 1 項所述之近場通訊設備資料之加密傳輸方法，其中發送該近場通訊資料至該近場通訊接收設備之步驟，更包括下列步驟：

將該些子資料之一位置分別告知所對應之該些近場通訊接收設備。

【第4項】 如申請專利範圍第 1 項所述之近場通訊設備資料之加

密傳輸方法，其中該些近場通訊接收設備係具有近場通訊模組之一手機、具有近場通訊模組之一手環、具有近場通訊模組之一門禁設備或具有近場通訊模組之一支付設備。

【第5項】 一種近場通訊設備資料之加密傳輸系統，包括一近場通訊發送設備和複數個近場通訊接收設備，該近場通訊發送設備包括：

一管理模組，用以將該近場通訊發送設備中的一近場通訊資料劃分為複數段子資料，並分別採用不同之一未加密之加密密鑰對該些子資料進行加密；

一通訊模組，用以將該些未加密之加密密鑰分別發送至對應該些子資料之該複數個近場通訊接收設備；以及

一近場通訊模組，用以儲存加密後之該近場通訊資料，並當與該些近場通訊接收設備通訊連接時，將所儲存之該近場通訊資料發送至該近場通訊接收設備；

其中，該些近場通訊接收設備接收並儲存由該通訊模組發送來之該些未加密之加密密鑰，當與該近場通訊發送設備通訊連接時，在接收該近場通訊模組發送之該近場通訊資料後，藉由已接收到之該未加密之加密密鑰直接對其自身所對應之該子資料進行解密，以獲得該近場通訊接收設備所需之該子資料訊息。

【第6項】 如申請專利範圍第 5 項所述之近場通訊設備資料之加

密傳輸系統，其中該近場通訊模組更包括：

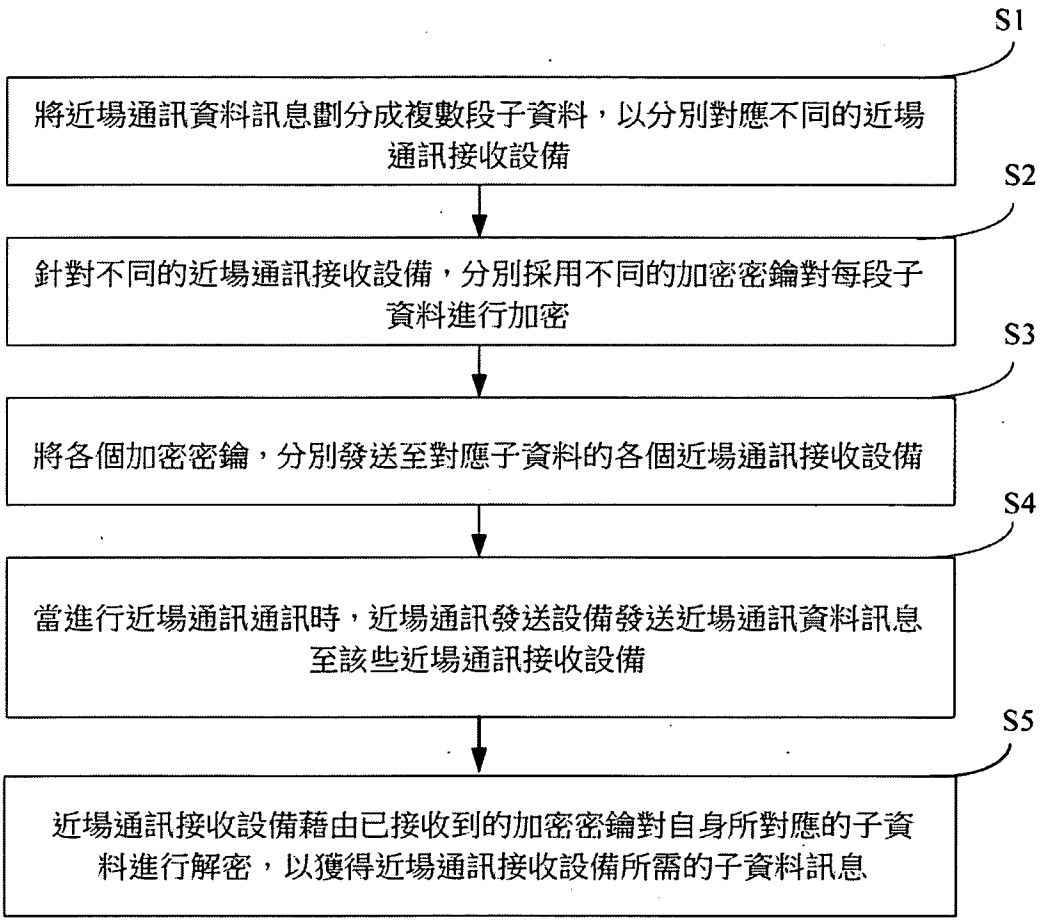
一訊息處理模組，通訊連接該近場通訊接收設備，用以將該些子資料之一位置告知所對應之該些近場通訊接收設備。

【第7項】 如申請專利範圍第 5 項所述之近場通訊設備資料之加密傳輸系統，其中該近場通訊發送設備係具有該近場通訊模組之一手機、具有該近場通訊模組之一手環、具有該近場通訊模組之一門禁設備或具有該近場通訊模組之一支付設備。

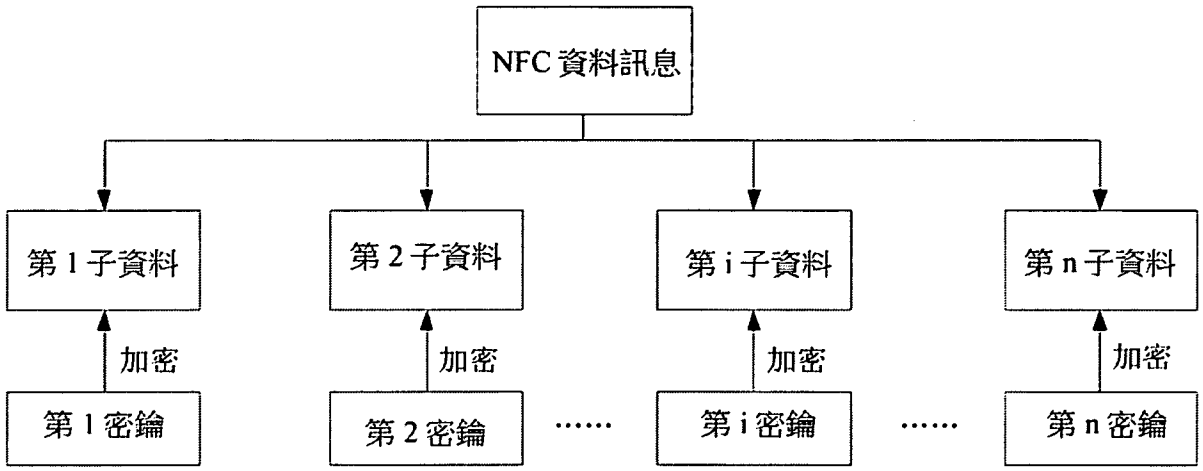
【第8項】 如申請專利範圍第 5 項所述之近場通訊設備資料之加密傳輸系統，其中該近場通訊接收設備係具有近場通訊功能之一手機、具有近場通訊功能之一手環、具有近場通訊功能之一門禁設備或具有近場通訊功能之一支付設備。

105年 08月 18日 修正替換頁

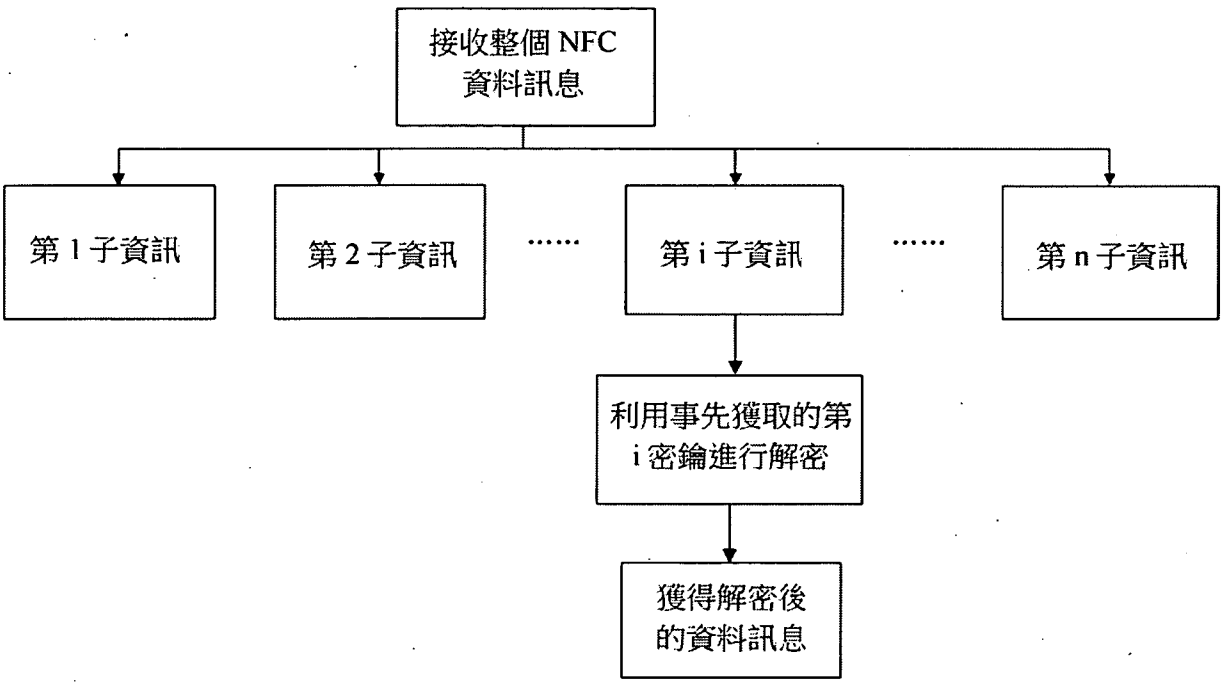
【發明圖式】



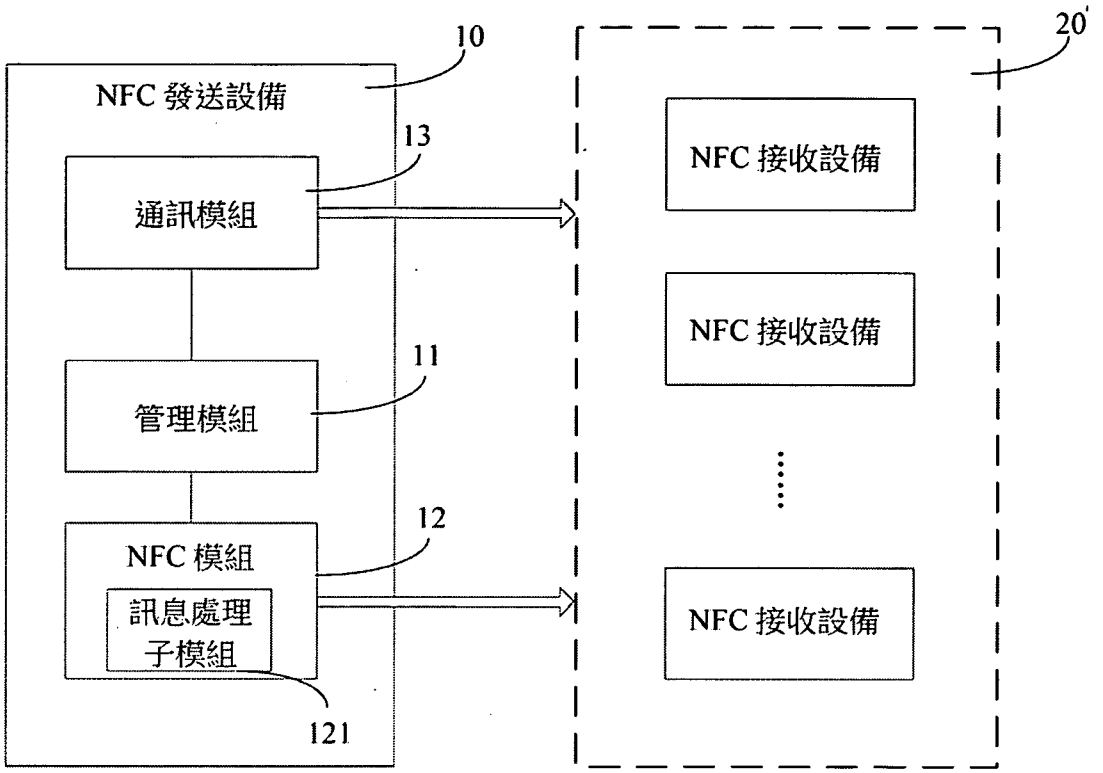
【第1圖】


NFC 資料訊息
第 1 子資料
第 2 子資料
第 i 子資料
第 n 子資料
加密
加密
加密
加密
第 1 密鑰
第 2 密鑰
第 i 密鑰
第 n 密鑰
.....
.....

【第2圖】


接收整個 NFC 資料訊息
第 1 子資訊
第 2 子資訊
.....
第 i 子資訊
.....
第 n 子資訊
利用事先獲取的第 i 密鑰進行解密
獲得解密後的資料訊息

【第3圖】


10
NFC 發送設備
13
通訊模組
11
管理模組
12
NFC 模組
訊息處理
子模組
121
20
NFC 接收設備
NFC 接收設備
NFC 接收設備

【第4圖】