I809292

(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 I809292 B**

(45)公告日： 中華民國 112 (2023) 年 07 月 21 日

(21)申請案號：109126454 (22)申請日： 中華民國 109 (2020) 年 08 月 05 日

(51)Int. Cl.： ***H04L9/32*** ***(2006.01)*** ***H04L9/14*** ***(2006.01)***

H04L9/40 ***(2022.01)***

(30)優先權：2019/11/26 中國大陸 201911176393.0

(71)申請人：大陸商中國銀聯股份有限公司 (中國大陸) CHINA UNIONPAY CO., LTD. (CN)
中國大陸

(72)發明人：陳林 (CN) ；許斌 (CN) ；楊森 (CN)

(74)代理人：廖俊龍

(56)參考文獻：

TW	201500955A	CN	108632296A
CN	110414190A	EP	1378092B1
US	2003/0012374A1		

審查人員：林彥廷

申請專利範圍項數：26 項 圖式數：11 共 29 頁

(54)名稱

資料的加解密方法、裝置、存儲介質及加密文件

(57)摘要

本發明提供了一種資料的加解密方法、裝置、存儲介質及加密文件，涉及資料處理技術領域。該資料的加密方法，包括：獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料；獲取第二金鑰，根據第二金鑰，得到混淆運算結果資料的第一簽名；獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文；獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名；生成包括目標密文和第二簽名的加密文件。利用本發明的技術方案能夠提高資料保護的安全性。

指定代表圖：

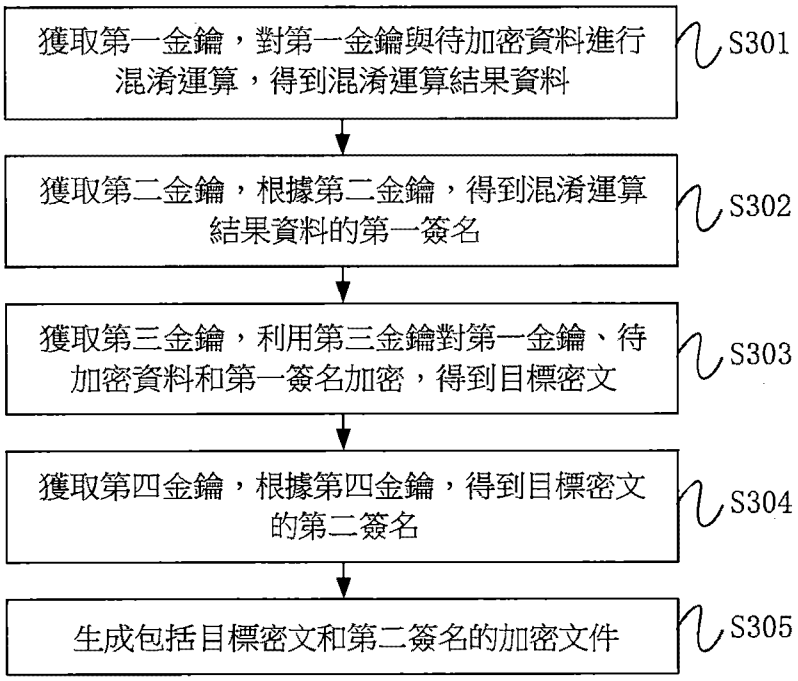

圖 2

符號簡單說明：

S301,S302,S303,S304,S305:步驟

I809292

公告本

發明摘要

【發明名稱】（中文/英文）

資料的加解密方法、裝置、存儲介質及加密文件

【中文】

本發明提供了一種資料的加解密方法、裝置、存儲介質及加密文件，涉及資料處理技術領域。該資料的加密方法，包括：獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料；獲取第二金鑰，根據第二金鑰，得到混淆運算結果資料的第一簽名；獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文；獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名；生成包括目標密文和第二簽名的加密文件。利用本發明的技術方案能夠提高資料保護的安全性。

【英文】

【代表圖】

【本案指定代表圖】：圖2。

【本代表圖之符號簡單說明】：

S301,S302,S303,S304,S305:步驟

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

資料的加解密方法、裝置、存儲介質及加密文件

【技術領域】

【0001】　本發明屬於資料處理技術領域，尤其涉及一種資料的加解密方法、裝置及加密文件。

【先前技術】

【0002】　隨著網路技術的發展，利用網路傳輸資料方便了資訊的傳遞。在資料傳輸過程中，資料有可能洩露或被篡改。在被傳輸的資料中存在敏感性資料，敏感性資料不希望發生洩露或被篡改。因此，包括敏感性資料的資料的傳輸對傳輸安全性的要求較高。

【0003】　現階段，加密裝置會對資料即明文進行加密，將加密後的資料即密文傳輸至解密裝置，解密裝置對密文進行解密，從而得到明文。但是，在密文的傳輸過程中密文有可能被篡改，資料保護的安全性依然較低。

【發明內容】

【0004】　本發明實施例提供了一種資料的加解密方法、裝置、存儲介質及加密文件，能夠提高資料保護的安全性。

【0005】　第一方面，本發明實施例提供一種資料的加密方法，應用於加密裝置，方法包括：獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料；獲取第二金鑰，根據第二金鑰，得到混淆運算結果資料的第一簽名；獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文；獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名；生成包括目標密文和第二簽名的加密文件。

【0006】　第二方面，本發明實施例提供一種資料的解密方法，應用於解密裝置，方法包括：接收包括目標密文和第二簽名的加密文件，第二簽名為加密裝置根據第四金鑰得到的目標密文的簽名；利用預存的與第

三金鑰成對的第五金鑰，對目標密文解密，得到第一金鑰、待加密資料和第一簽名；利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證；對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對得到的混淆運算結果資料和第一簽名進行驗證，第一簽名為加密裝置根據第二金鑰得到的混淆運算結果資料的簽名。

【0007】　第三方面，本發明實施例提供一種加密裝置，包括：混淆運算模組，用於獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果；簽名模組，用於獲取第二金鑰，根據第二金鑰，得到混淆運算結果的第一簽名；加密模組，用於獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文；簽名模組，還用於獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名；加密文件生成模組，用於生成包括目標密文和第二簽名的加密文件。

【0008】　第四方面，本發明實施例提供一種解密裝置，包括：接收模組，用於接收包括目標密文和第二簽名的加密文件，第二簽名為加密裝置根據第四金鑰得到的目標密文的簽名；解密模組，用於利用預存的與第三金鑰對應的第五金鑰，對目標密文解密，得到第一金鑰、待加密資料和第一簽名；第一驗證模組，用於利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證；第二驗證模組，用於對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對混淆運算結果資料和第一簽名進行驗證，第一簽名為加密裝置根據第二金鑰得到的混淆運算結果資料的簽名。

【0009】　第五方面，本發明實施例提供一種加密裝置，包括處理器、記憶體及存儲在記憶體上並可在處理器上運行的電腦程式，電腦程式被處理器執行時實現第一方面的技術方案中的資料的加密方法。

【0010】　第六方面，本發明實施例提供一種解密裝置，包括處理器、記憶體及存儲在記憶體上並可在處理器上運行的電腦程式，電腦程式被處理器執行時實現第二方面的技術方案中的資料的解密方法。

【0011】　第七方面，本發明實施例提供一種電腦可讀存儲介質，電腦可讀存儲介質上存儲電腦程式，電腦程式被處理器執行時實現第一方面的技術方案中的資料的加密方法或第二方面的技術方案中的資料的解密方法。

【0012】　本發明實施例提供一種資料的加解密方法、裝置、存儲介質及加密文件，對第一金鑰與待加密資料進行混淆運算，對混淆運算後的第一金鑰與待加密資料進行簽名，得到第一簽名。利用第三金鑰，將第一金鑰、待加密資料和得到的第一簽名進行加密，對加密後的第一金鑰、待加密資料和第一簽名進行簽名，得到第二簽名，從而得到了包括第二簽名和加密後的第一金鑰、待加密資料和第一簽名的加密文件。解密裝置接收到的加密文件包括目標密文和第二簽名，利用與第三金鑰成對的第五金鑰對目標密文解密，得到第一金鑰、待加密資料和第一簽名。利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證。對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，利用與第二金鑰成對的第七金鑰，對混淆運算後的解密得到的第一金鑰與待加密資料，和第一簽名進行驗證，完成解密和驗證的全過程。加密裝置通過混淆、簽名、加密和再簽名四重防護手段，對待加密資料進行了處理。若加密文件中的內容被篡改，則解密裝置可通過驗證檢測得到，從而提高了資料保護的安全性。

【圖式簡單說明】

【0013】

從下面結合圖式對本發明的具體實施方式的描述中可以更好地理解本發明，其中，相同或相似的圖式標記表示相同或相似的特徵。

圖 1 為本發明實施例提供的一種資料的加解密方法應用的場景示意圖；

圖 2 為本發明一實施例提供的一種資料的加密方法的流程圖；

圖 3 為本發明實施例提供的一種使用者可見的加密文件結構示意圖；

圖 4 為本發明實施例提供的與圖 3 所示的加密文件結構對應的明文結構的示意圖；

圖 5 為本發明實施例提供的一種加密文件生成形式的示意圖；

圖 6 為本發明一實施例提供的一種資料的解密方法的流程圖；

圖 7 為本發明一實施例提供的一種加密裝置的結構示意圖；

圖 8 為本發明另一實施例提供的一種加密裝置的結構示意圖；

圖 9 為本發明一實施例提供的一種解密裝置的結構示意圖；

圖 10 為本發明另一實施例提供的一種解密裝置的結構示意圖；

圖 11 為本發明實施例提供的一種加密裝置的結構示意圖。

【實施方式】

【0014】 下面將詳細描述本發明的各個方面的特徵和示例性實施例。在下面的詳細描述中，提出了許多具體細節，以便提供對本發明的全面理解。但是，對於本領域技術人員來說很明顯的是，本發明可以在不需要這些具體細節中的一些細節的情況下實施。下面對實施例的描述僅僅是為了通過示出本發明的示例來提供對本發明的更好的理解。本發明絕不限於下面所提出的任何具體配置和演算法，而是在不脫離本發明的精神的前提下覆蓋了元素、部件和演算法的任何修改、替換和改進。在圖式和下面的描述中，沒有示出公知的結構和技術，以便避免對本發明造成不必要的模糊。

【0015】 本發明提供一種資料的加解密方法、裝置及加密文件，可應用於對資料進行加密，以便於安全傳輸的場景中。圖 1 為本發明實施例提供的一種資料的加解密方法應用的場景示意圖。如圖 1 所示，資料的加解密方法可應用於加密裝置 10 和解密裝置 20。其中，加密裝置 10 用於執行本發明實施例中資料的加密方法。解密裝置 20 用於執行本發明實施例中資料的解密方法。

【0016】 在本發明中，加密裝置可對待加密資料即明文進行混淆、簽名、加密和再簽名四層防護處理，從而使得在資料的傳輸過程中，資料難以被篡改，或者，若資料被篡改，解密裝置在解密即驗證過程中，可及時準確地發現資料被篡改的問題，從而提高了資料的安全性。

【0017】　圖 2 為本發明一實施例提供的一種資料的加密方法的流程圖。該資料的加密方法可應用於加密裝置。如圖 2 所示，該資料的加密方法可包括步驟 S301 至步驟 S305。

【0018】　在步驟 S301 中，獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料。

【0019】　待加密資料可為不希望洩露及不希望被篡改的資料，比如，待加密資料可為敏感性資料。在此對待加密資料的種類、數量和大小並不限定。

【0020】　混淆運算結果資料即為第一金鑰與待加密資料混淆運算的結果資料。混淆運算所涉及的混淆演算法可由加密裝置和解密裝置預先約定，該混淆演算法可為非公開的混淆演算法，也就是說，該混淆演算法只有加密裝置和解密裝置可知，並不對外公開。在一些示例中，每次混淆運算可對應隨機產生混淆因子，混淆因子會影響混淆演算法中的區域變數，使得每次混淆運算均會有所不同，攻擊者無法準確地獲取每次混淆運算的混淆演算法，因此難以獲得待加密資料，或篡改待加密資料，從而進一步提高了資料保護的安全性。在另一些示例中，混淆運算中的混淆因子可包括第一金鑰，也就是說，可將第一金鑰作為混淆因子參與混淆運算，在此並不限定。

【0021】　在一些示例中，第一金鑰可以為公開金鑰。

【0022】　在步驟 S302 中，獲取第二金鑰，根據第二金鑰，得到混淆運算結果資料的第一簽名。

【0023】　根據第二金鑰，對混淆運算結果資料進行簽名，得到第一簽名。具體地，在一些示例中，第一金鑰為公開金鑰，第二金鑰可為與第一金鑰對應的私密金鑰，即第一金鑰與第二金鑰為一對公私密金鑰。

【0024】　在步驟 S303 中，獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文。

【0025】　在這裡進行一次加密，利用第三金鑰對第一金鑰、待加密資料和第一簽名的整體進行加密。加密後的第一金鑰、待加密資料和第

一簽名即為目標密文。其中，第三金鑰可為公開金鑰或對稱金鑰，在此並不限定。

【0026】　在步驟 S304 中，獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名。

【0027】　第二簽名是針對目標密文的簽名。具體地，在一些示例中，第一金鑰為公開金鑰，第四金鑰可為與第一金鑰對應的私密金鑰，即第一金鑰與第四金鑰為一對公私密金鑰。更進一步地，第二金鑰與第四金鑰可為相同的金鑰。

【0028】　在步驟 S305 中，生成包括目標密文和第二簽名的加密文件。

【0029】　利用目標密文和第二簽名生成加密文件，該加密文件包括目標密文和第二簽名。需要說明的是，加密文件中還可包括不進行混淆、簽名、加密的可公開的資料，在此並不限定。

【0030】　比如，圖 3 為本發明實施例提供的一種使用者可見的加密文件結構示意圖。如圖 3 所示，加密文件被打開後，在不經過解密處理的情況下，使用者可見的是可公開的資料如可公開的內容說明資訊等、目標密文和第二簽名。圖 4 為本發明實施例提供的與圖 3 所示的加密文件結構對應的明文結構的示意圖。如圖 4 所示，假設待加密資料包括敏感性資料 1、敏感性資料 2 和敏感性資料 3，則與加密文件結構對應的明文結構具體包括可公開的資料如可公開的內容說明資訊等、第一金鑰、敏感性資料 1、敏感性資料 2、敏感性資料 3、第一簽名和第二簽名。

【0031】　為了便於更直觀地說明上述實施例中的混淆、簽名、加密和再簽名四層防護處理。圖 5 為本發明實施例提供的一種加密文件生成形式的示意圖。如圖 5 所示，對第一金鑰和待加密資料進行混淆運算；對混淆運算後的第一金鑰和待加密資料進行簽名，得到簽名 1；對第一金鑰、待加密資料和簽名 1 進行加密，對加密後的第一金鑰、待加密資料和簽名 1 進行簽名，得到簽名 2；最終得到加密文件。

【0032】　在本發明實施例中，對第一金鑰與待加密資料進行混淆

運算，對混淆運算後的第一金鑰與待加密資料進行簽名，得到第一簽名。利用第三金鑰，將第一金鑰、待加密資料和得到的第一簽名進行加密，對加密後的第一金鑰、待加密資料和第一簽名進行簽名，得到第二簽名，從而得到了包括第二簽名和加密後的第一金鑰、待加密資料和第一簽名的加密文件。通過混淆、簽名、加密和再簽名四重防護手段，對待加密資料進行了處理，從而提高了資料保護的安全性。

【0033】　比如，若目標密文被替換，則在後續解密過程中，會發生解密失敗或得到錯誤資料，在發生解密失敗或得到錯誤資料的情況下，對第二簽名驗證是不會成功的。同理，若第二簽名被替換，則對第二簽名的驗證是不會成功的。若在加密文件案傳輸的過程中發生了金鑰的洩露導致待加密資料被篡改，由於第一簽名是針對混淆後的第一金鑰與待加密資料簽名得到的，且混淆演算法不對外公開，因此，在後續的解密過程中，被篡改後的待加密資料與第一簽名的驗證是不會成功的，提高了資料的安全性。

【0034】　在一些示例中，上述資料的加密方法還可包括接收解密裝置生成並發送的第三金鑰。即第三金鑰為解密裝置生成的。第一金鑰、第二金鑰和第四金鑰均可為加密裝置生成的。也就是說，本發明實施例中的資料的加密方法最少可只依賴解密裝置提供的一個金鑰即可實現混淆、簽名、加密和再簽名的過程，降低瞭解密裝置需要承擔的開發工作量，提高了對加密裝置、待加密資料和解密裝置的保護的安全性。第二金鑰和第四金鑰可為相同的金鑰，第一金鑰與第二金鑰可為成對的公私密金鑰，則加密裝置生成一對公私密金鑰即可實現上述實施例中的第一金鑰、第二金鑰和第四金鑰。

【0035】　本發明實施例還可提供一種加密文件，該加密文件包括目標密文和第二簽名。

【0036】　目標密文為利用第三金鑰對第一金鑰、待加密資料和第一簽名加密得到的密文。其中，所述第一簽名為根據第二金鑰得到的混淆運算結果資料的簽名。所述混淆運算結果資料為對所述第一金鑰與所述待

加密資料進行混淆運算得到的資料。

【0037】 第二簽名為根據第四金鑰得到的所述目標密文的簽名。

【0038】 加密文件的結構及生成形式可參見上述實施例中的圖 3、圖 4 和圖 5，其中，關於加密文件、目標密文、第二簽名等的具體內容可參見上述實施例中的相關說明，在此不再贅述。

【0039】 在一些示例中，第一金鑰為公開金鑰。

【0040】 在一些示例中，第三金鑰為公開金鑰或對稱金鑰。

【0041】 在一些示例中，第二金鑰與第四金鑰為私密金鑰。

【0042】 進一步地，第一金鑰為公開金鑰，第二金鑰和/或第四金鑰為與第一金鑰對應的私密金鑰。

【0043】 在一些示例中，第二金鑰與第四金鑰相同。

【0044】 在一些示例中，上述混淆運算中的混淆因子包括第一金鑰。

【0045】 圖 6 為本發明一實施例提供的一種資料的解密方法的流程圖。該資料的解密方法可應用於解密裝置。如圖 6 所示，該資料的解密方法可包括步驟 S401 至步驟 S404。

【0046】 在步驟 S401 中，接收包括目標密文和第二簽名的加密文件。

【0047】 為了便於與上述實施例中的資料的加密方法對應，本發明實施例中的資料的解密方法中涉及到的名稱與上述資料的加密方法涉及到的名稱對應。

【0048】 其中，第二簽名為加密裝置根據第四金鑰得到的目標密文的簽名。目標密文是加密裝置利用第三金鑰，對第一金鑰、待加密資料和第一簽名加密得到的密文。需要說明的是，本發明實施例中的加密文件已經過傳輸，在傳輸過程中，目標密文和第二簽名有可能被篡改。

【0049】 在一些示例中，加密文件還可包括其他資料，比如可公開的資料等。

【0050】 在步驟 S402 中，利用預存的與第三金鑰成對的第五金鑰，

對目標密文解密，得到第一金鑰、待加密資料和第一簽名。

【0051】　在一些示例中，第三金鑰和第五金鑰可為解密裝置生成對稱金鑰或成對的公私密金鑰，由解密裝置將第三金鑰發送給加密裝置，以使得加密裝置利用第三金鑰對第一金鑰、待加密資料和第一簽名加密。解密裝置利用與第三金鑰成對的第五金鑰可對目標密文解密，解密後的目標密文包括第一金鑰、待加密資料和第一簽名。

【0052】　在一些示例中，第一金鑰為公開金鑰。第三金鑰可為公開金鑰或對稱金鑰。若第三金鑰為公開金鑰，則第五金鑰為與第三金鑰成對的私密金鑰。若第三金鑰為對稱金鑰，則第五金鑰與第三金鑰為相同的金鑰。

【0053】　在步驟 S403 中，利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證。

【0054】　解密裝置可對目標密文和第二簽名進行驗證。若目標密文和第二簽名驗證成功，表示目標密文和第二簽名未被篡改。

【0055】　在一些示例中，第四金鑰為私密金鑰，第六金鑰即為與第四金鑰成對的公開金鑰。進一步地，在第一金鑰為公開金鑰且第四金鑰為與第一金鑰對應的私密金鑰的情況下，第六金鑰即為對目標密文解密後得到的第一金鑰。解密裝置可在對目標密文解密的過程中獲取得到第六金鑰即第一金鑰，不需在自身存儲第六金鑰，一方面可避免第六金鑰由解密裝置洩露，另一方面也便於對第六金鑰的管理，即第六金鑰是隨目標密文而更新的。進一步提高了加、解密的安全性。

【0056】　在步驟 S404 中，對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對得到的混淆運算結果資料和第一簽名進行驗證。

【0057】　其中，第一簽名為加密裝置根據第二金鑰得到的混淆運算結果資料的簽名。解密裝置可對得到的混淆運算結果資料和第一簽名進行驗證，若得到的混淆運算結果資料和第一簽名的驗證成功，表示待加密資料、第一金鑰和第一簽名未被篡改。

【0058】　在一些示例中，第二金鑰為私密金鑰，第七金鑰即為與第二金鑰成對的公開金鑰。進一步地，在第一金鑰為公開金鑰且第二金鑰為與第一金鑰對應的私密金鑰的情況下，第七金鑰即為對目標密文解密後得到的第一金鑰。解密裝置可在對目標密文解密的過程中獲取得到第七金鑰即第一金鑰，不需在自身存儲第七金鑰，一方面可避免第七金鑰由解密裝置洩露，另一方面也便於對第七金鑰的管理，即第七金鑰是隨目標密文而更新的。進一步提高了加、解密的安全性。

【0059】　在一些示例中，上述混淆運算中的混淆因子包括第一金鑰。

【0060】　在本發明實施例中，解密裝置接收到的加密文件包括目標密文和第二簽名，利用與第三金鑰成對的第五金鑰對目標密文解密，得到第一金鑰、待加密資料和第一簽名。利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證。對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對混淆運算結果資料和第一簽名進行驗證，完成解密和驗證的全過程。若加密文件中的內容被篡改，則可通過驗證檢測得到，提高了資料保護的安全性。

【0061】　具體地，在上述實施例中，若對目標密文和第二簽名的驗證成功，且對得到混淆運算結果資料和第一簽名的驗證成功，確定加密文件未被篡改。

【0062】　在一些示例中，第三金鑰可為解密裝置生成的，對應地，上述實施例中的資料的解密方法還可包括生成並向加密裝置發送第三金鑰的步驟。

【0063】　在一些示例中，上述實施例中的第一金鑰、第二金鑰和第四金鑰可為加密裝置生成的金鑰。也就是說，最少可只依賴解密裝置提供的一個金鑰即可實現加密裝置執行的資料的加密方法中混淆、簽名、加密和再簽名的過程，降低瞭解密裝置需要承擔的開發工作量，提高了對加密裝置、待加密資料和解密裝置的保護的安全性。

【0064】 圖 7 為本發明一實施例提供的一種加密裝置的結構示意圖。如圖 7 所示，該加密裝置 10 可包括混淆運算模組 101、簽名模組 102、加密模組 103 和加密文件生成模組 104。

【0065】 混淆運算模組 101，用於獲取第一金鑰，對所述第一金鑰與待加密資料進行混淆運算，得到混淆運算結果。

【0066】 簽名模組 102，用於獲取第二金鑰，根據所述第二金鑰，得到所述混淆運算結果的第一簽名。

【0067】 加密模組 103，用於獲取第三金鑰，利用所述第三金鑰對所述第一金鑰、所述待加密資料和所述第一簽名加密，得到目標密文。

【0068】 所述簽名模組 102，還用於獲取第四金鑰，根據所述第四金鑰，得到所述目標密文的第二簽名。

【0069】 加密文件生成模組 104，用於生成包括所述目標密文和所述第二簽名的加密文件。

【0070】 在本發明實施例中，對第一金鑰與待加密資料進行混淆運算，對混淆運算後的第一金鑰與待加密資料進行簽名，得到第一簽名。利用第三金鑰，將第一金鑰、待加密資料和得到的第一簽名進行加密，對加密後的第一金鑰、待加密資料和第一簽名進行簽名，得到第二簽名，從而得到了包括第二簽名和加密後的第一金鑰、待加密資料和第一簽名的加密文件。通過混淆、簽名、加密和再簽名四重防護手段，對待加密資料進行了處理，從而提高了資料保護的安全性。

【0071】 圖 8 為本發明另一實施例提供的一種加密裝置的結構示意圖。圖 8 與圖 7 的不同之處在於，圖 8 所示的加密裝置 10 還包括接收模組 105 和第一金鑰生成模組 106。

【0072】 接收模組 105，用於接收解密裝置生成並發送的第三金鑰。

【0073】 在一些示例中，第三金鑰為公開金鑰或對稱金鑰。

【0074】 第一金鑰生成模組 106，用於生成第一金鑰、第二金鑰與第四金鑰。

【0075】　在一些示例中，第一金鑰為公開金鑰。

【0076】　在一些示例中，第二金鑰與第四金鑰為私密金鑰。

【0077】　進一步地，第一金鑰為公開金鑰，第二金鑰和/或第四金鑰為與第一金鑰對應的私密金鑰。

【0078】　在一些示例中，第二金鑰與第四金鑰相同。

【0079】　在一些示例中，上述混淆運算中的混淆因子包括第一金鑰。

【0080】　圖 9 為本發明一實施例提供的一種解密裝置的結構示意圖。如圖 9 所示，該解密裝置 20 可包括接收模組 201、解密模組 202、第一驗證模組 203 和第二驗證模組 204。

【0081】　接收模組 201，用於接收包括目標密文和第二簽名的加密文件，第二簽名為加密裝置根據第四金鑰得到的目標密文的簽名；

【0082】　解密模組 202，用於利用預存的與第三金鑰成對的第五金鑰，對目標密文解密，得到第一金鑰、待加密資料和第一簽名；

【0083】　第一驗證模組 203，用於利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證；

【0084】　第二驗證模組 204，用於對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對混淆運算結果資料和第一簽名進行驗證，第一簽名為加密裝置根據第二金鑰得到的混淆運算結果資料的簽名。

【0085】　在本發明實施例中，解密裝置接收到的加密文件包括目標密文和第二簽名，利用與第三金鑰成對的第五金鑰對目標密文解密，得到第一金鑰、待加密資料和第一簽名。利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證。對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，利用與第二金鑰成對的第七金鑰，對混淆運算後的解密得到的第一金鑰與待加密資料，和第一簽名進行驗證，完成解密和驗證的全過程。若加密文件中的內容被篡改，則可通過驗證檢測得到，提高了資料保護的安全性。

【0086】 圖 10 為本發明另一實施例提供的一種解密裝置的結構示意圖。圖 10 與圖 9 的不同之處在於，圖 10 所示的解密裝置 20 還可包括安全確定模組 205 和第二金鑰生成模組 206。

【0087】 安全確定模組 205，用於若對目標密文和第二簽名的驗證成功，且對得到混淆運算結果資料和第一簽名的驗證成功，確定加密文件未被篡改。

【0088】 第二金鑰生成模組 206，用於生成並向加密裝置發送第三金鑰。

【0089】 在一些示例中，第一金鑰為加密裝置生成的金鑰。第一金鑰為公開金鑰。

【0090】 在一些示例中，第三金鑰為公開金鑰或對稱金鑰。若第三金鑰為公開金鑰，第五金鑰為與第三金鑰對應的私密金鑰。若第三金鑰為對稱金鑰，第三金鑰與第五金鑰為相同的金鑰。

【0091】 在一些示例中，第二金鑰與第四金鑰為加密裝置生成的金鑰。第二金鑰與第四金鑰為私密金鑰。

【0092】 進一步地，在第一金鑰為公開金鑰且第四金鑰為與第一金鑰對應的私密金鑰的情況下，第六金鑰即為對目標密文解密得到的第一金鑰。在第一金鑰為公開金鑰且第二金鑰為與第一金鑰對應的私密金鑰的情況下，第七金鑰即為對目標密文解密得到的第一金鑰。

【0093】 在一些示例中，上述混淆運算中的混淆因子包括第一金鑰。

【0094】 圖 11 為本發明實施例提供的一種加密裝置的結構示意圖。如圖 11 所示，加密裝置 50 包括記憶體 501、處理器 502 及存儲在記憶體 501 上並可在處理器 502 上運行的電腦程式。

【0095】 在一個示例中，上述處理器 502 可以包括中央處理器(CPU，Central Processing Unit)，或者特定積體電路(ASIC，Application Specific IC)，或者可以被配置成實施本發明實施例的一個或多個積體電路。

【0096】 記憶體 501 可以包括用於資料或指令的大容量記憶體。

舉例來說而非限制，記憶體 501 可包括 HDD(硬碟機，Hard Disk Drive)、軟碟機、快閃記憶體、光碟、磁光碟、磁帶或通用序列匯流排(USB，Universal Serial Bus)驅動器或者兩個或更多個以上這些的組合。在合適的情況下，記憶體 501 可包括可移除或不可移除(或固定)的介質。在合適的情況下，記憶體 501 可在終端熱點開啟加密裝置 50 的內部或外部。在特定實施例中，記憶體 501 是非易失性固態記憶體。在特定實施例中，記憶體 501 包括唯讀記憶體(ROM，Read-Only Memory)。在合適的情況下，該 ROM 可以是掩模程式設計的 ROM、可程式設計 ROM(PROM，Programmable Read-Only Memory)、可擦除 PROM(EPROM，Erasable Programmable Read-Only Memory)、電可擦除 PROM(EEPROM，Electrically Erasable Programmable Read-Only Memory)、電可改寫 ROM(EAROM，Electrically Alterable Read-Only Memory)或快閃記憶體或者兩個或更多個以上這些的組合。

【0097】 處理器 502 通過讀取記憶體 501 中存儲的可執行程式碼來運行與可執行程式碼對應的電腦程式，以用於實現上述實施例中資料的加密方法。

【0098】 在一個示例中，加密裝置 50 還可包括通信介面 503 和匯流排 504。其中，如圖 11 所示，記憶體 501、處理器 502、通信介面 503 通過匯流排 504 連接並完成相互間的通信。

【0099】 通信介面 503，主要用於實現本發明實施例中各模組、裝置、單元和/或設備之間的通信。也可通過通信介面 503 接入輸入裝置和/或輸出設備。

【0100】 匯流排 504 包括硬體、軟體或兩者，將加密裝置 50 的部件彼此耦接在一起。舉例來說而非限制，匯流排 504 可包括高速圖形連接埠(AGP，Accelerated Graphics Port)或其他圖形匯流排、增強工業標準架構(EISA，Enhanced Industry Standard Architecture)匯流排、前端匯流排(FSB，Front Side Bus)、超傳輸(HT，Hyper Transport)互連、工業標準架構(ISA，Industry Standard Architecture)匯流排、無限頻寬互連、低引腳數(LPC，

Low Pin Count)匯流排、記憶體匯流排、微通道架構(MCA，Micro Channel Architecture)匯流排、周邊元件連接(PCI，Peripheral Component Interconnect)匯流排、PCI-Express(PCI-X，Peripheral Component Interconnect Express)匯流排、串列進階技術附件(SATA，Serial Advanced Technology Attachment)匯流排、視頻電子標準協會局部(VLB，Video Electronics Standards Association Local Bus)匯流排或其他合適的匯流排或者兩個或更多個以上這些的組合。在合適的情況下，匯流排 504 可包括一個或多個匯流排。儘管本發明實施例描述和示出了特定的匯流排，但本發明考慮任何合適的匯流排或互連。

【0101】 本發明實施例還可提供一種解密裝置，解密裝置的具體結構可參見圖 11 所示的加密裝置 50。需要說明的是，解密裝置中的處理器通過讀取記憶體中存儲的可執行程式碼來運行與可執行程式碼對應的電腦程式，以用於實現上述實施例中資料的解密方法，其餘內容可參見上述實施例中的相關說明，在此不再贅述。

【0102】 本發明一實施例還提供一種電腦可讀存儲介質，該電腦可讀存儲介質上存儲有電腦程式，該電腦程式被處理器執行時可實現上述實施例中的資料的加密方法或資料的解密方法。

【0103】 需要明確的是，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或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。對於加密文件實施例、裝置實施例和電腦可讀存儲介質實施例而言，相關之處可以參見方法實施例的說明部分。本發明並不局限於上文所描述並在圖中示出的特定步驟和結構。本領域的技術人員可以在領會本發明的精神之後，作出各種改變、修改和添加，或者改變步驟之間的順序。並且，為了簡明起見，這裡省略對已知方法技術的詳細描述。

【0104】 本領域技術人員應能理解，上述實施例均是示例性而非限制性的。在不同實施例中出現的不同技術特徵可以進行組合，以取得有益效果。本領域技術人員在研究圖式、說明書及申請專利範圍的基礎上，

應能理解並實現所揭示的實施例的其他變化的實施例。在申請專利範圍中，術語“包括”並不排除其他裝置或步驟；不定冠詞“一個”不排除多個；術語“第一”、“第二”用於標示名稱而非用於表示任何特定的順序。請求項中的任何圖式標記均不應被理解為對保護範圍的限制。請求項中出現的多個部分的功能可以由一個單獨的硬體或軟體模組來實現。某些技術特徵出現在不同的從屬請求項中並不意味著不能將這些技術特徵進行組合以取得有益效果。

【符號說明】

【0105】

10,50:加密裝置

20:解密裝置

101:混淆運算模組

102:簽名模組

103:加密模組

104:加密文件生成模組

105,201:接收模組

106:第一金鑰生成模組

202:解密模組

203:第一驗證模組

204:第二驗證模組

205:安全確定模組

206:第二金鑰生成模組

501:記憶體

502:處理器

503:通信介面

504:匯流排

S301,S302,S303,S304,S305,S401,S402,S403,S404:步驟

申請專利範圍

1、一種資料的加密方法，其特徵在於，包括：

加密裝置獲取第一金鑰，對所述第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料，其中，所述第一金鑰是作為混淆因子參與所述混淆運算的；

所述加密裝置獲取第二金鑰，根據所述第二金鑰，得到所述混淆運算結果資料的第一簽名；

所述加密裝置獲取第三金鑰，利用所述第三金鑰對所述第一金鑰、所述待加密資料和所述第一簽名加密，得到目標密文；

所述加密裝置獲取第四金鑰，根據所述第四金鑰，得到所述目標密文的第二簽名；

所述加密裝置生成包括所述目標密文和所述第二簽名的加密文件。

2、如請求項 1 所述的方法，其中，還包括：

接收解密裝置生成並發送的所述第三金鑰。

3、如請求項 1 所述的方法，其中，所述第一金鑰為所述加密裝置生成的金鑰，所述第一金鑰為公開金鑰。

4、如請求項 1 所述的方法，其中，所述第三金鑰為公開金鑰或對稱金鑰。

5、如請求項 1 所述的方法，其中，

所述第二金鑰與所述第四金鑰為所述加密裝置生成的金鑰；

所述第二金鑰與所述第四金鑰為私密金鑰；

所述第一金鑰為公開金鑰，所述第二金鑰和/或第四金鑰為與所述第一金鑰對應的私密金鑰。

6、如請求項 1 或 5 所述的方法，其中，所述第二金鑰與所述第四金鑰相同。

7、如請求項 1 所述的方法，其中，所述混淆運算中的混淆因子包括所述第一金鑰。

8、一種資料的解密方法，其特徵在於，包括：

解密裝置接收包括目標密文和第二簽名的加密文件，所述第二簽名為加密裝置根據第四金鑰得到的所述目標密文的簽名；

所述解密裝置利用預存的與第三金鑰成對的第五金鑰，對所述目標密文解密，得到第一金鑰、待加密資料和第一簽名；

所述解密裝置利用與所述第四金鑰成對的第六金鑰，對所述目標密文和所述第二簽名進行驗證；

所述解密裝置對解密得到的所述第一金鑰與所述待加密資料進行與所述加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對得到的所述混淆運算結果資料和所述第一簽名進行驗證，所述第一簽名為所述加密裝置根據所述第二金鑰得到的所述混淆運算結果資料的簽名，其中，所述第一金鑰是作為混淆因子參與所述混淆運算的。

9、如請求項 8 所述的方法，其中，還包括：

若對所述目標密文和所述第二簽名的驗證成功，且對得到所述混淆運算結果資料和所述第一簽名的驗證成功，確定所述加密文件未被篡改。

10、如請求項 8 所述的方法，其中，在所述接收包括目標密文和第二簽名的加密文件之前，還包括：

生成並向所述加密裝置發送所述第三金鑰。

11、如請求項 8 所述的方法，其中，所述第一金鑰為所述加密裝置生成的金鑰，所述第一金鑰為公開金鑰。

12、如請求項 8 所述的方法，其中，所述第三金鑰為公開金鑰或對稱金鑰。

13、如請求項 8 所述的方法，其中，

所述第二金鑰與所述第四金鑰為所述加密裝置生成的金鑰；

所述第二金鑰與所述第四金鑰為私密金鑰。

14、如請求項 8 所述的方法，其中，

在所述第一金鑰為公開金鑰且所述第四金鑰為與所述第一金鑰對應的私密金鑰的情況下，所述第六金鑰為對所述目標密文解密得到的所述第一金鑰；

在所述第一金鑰為公開金鑰且所述第二金鑰為與所述第一金鑰對應的私密金鑰的情況下，所述第七金鑰為對所述目標密文解密得到的所述第一金鑰。

15、如請求項 8 所述的方法，其中，所述混淆運算中的混淆因子包括上述第一金鑰。

16、一種加密裝置，其特徵在於，包括：

混淆運算模組，用於獲取第一金鑰，對所述第一金鑰與待加密資料進行混淆運算，得到混淆運算結果，其中，所述第一金鑰是作為混淆因子參與所述混淆運算的；

簽名模組，用於獲取第二金鑰，根據所述第二金鑰，得到所述混淆運算結果的第一簽名；

加密模組，用於獲取第三金鑰，利用所述第三金鑰對所述第一金鑰、所述待加密資料和所述第一簽名加密，得到目標密文；

所述簽名模組，還用於獲取第四金鑰，根據所述第四金鑰，得到所述目標密文的第二簽名；

加密文件生成模組，用於生成包括所述目標密文和所述第二簽名的加密文件。

17、一種解密裝置，其特徵在於，包括：

接收模組，用於接收包括目標密文和第二簽名的加密文件，所述第二簽名為加密裝置根據第四金鑰得到的所述目標密文的簽名；

解密模組，用於利用預存的與第三金鑰成對的第五金鑰，對所述目標密文解密，得到第一金鑰、待加密資料和第一簽名；

第一驗證模組，用於利用與所述第四金鑰成對的第六金鑰，對所述目標密文和所述第二簽名進行驗證；

第二驗證模組，用於對解密得到的所述第一金鑰與所述待加密資料進行與所述加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對所述混淆運算結果資料和所述第一簽名進行驗證，所述第一簽名為所述加密裝置根據所述第二金鑰得到的所述混淆運算結果資料的簽名，其中，所述第一金鑰是作為混淆因子參與所述混淆運算的。

18、一種加密裝置，其特徵在於，包括處理器、記憶體及存儲在所述記憶體上並可在所述處理器上運行的電腦程式，所述電腦程式被所述處理器執行時實現如請求項 1 至 7 中任意一項所述的資料的加密方法。

19、一種解密裝置，其特徵在於，包括處理器、記憶體及存儲在所述記憶體上並可在所述處理器上運行的電腦程式，所述電腦程式被所述處理器執行時實現如請求項 8 至 15 中任意一項所述的資料的解密方法。

20、一種電腦可讀存儲介質，其特徵在於，所述電腦可讀存儲介質上存儲電腦程式，所述電腦程式被處理器執行時實現如請求項 1 至 7 中任意一項所述的資料的加密方法或如請求項 8 至 15 中任意一項所述的資料的解密方法。

21、一種加密文件，其特徵在於，包括

目標密文，為利用第三金鑰對第一金鑰、待加密資料和第一簽名加密得到的密文，所述第一簽名為根據第二金鑰得到的混淆運算結果資料的簽名，所述混淆運算結果資料為對所述第一金鑰與所述待加密資料進行混淆運算得到的資料，其中，所述第一金鑰是作為混淆因子參與所述混淆運算的；

第二簽名，為根據第四金鑰得到的所述目標密文的簽名。

22、如請求項 21 所述的加密文件，其中，所述第一金鑰為公開金鑰。

23、如請求項 21 所述的加密文件，其中，所述第三金鑰為公開金鑰或對稱金鑰。

24、如請求項 21 所述的加密文件，其中，所述第一金鑰為公開金鑰，

所述第二金鑰和/或第四金鑰為與所述第一金鑰對應的私密金鑰。

25、如請求項 21 所述的加密文件，其中，所述第二金鑰與所述第四金鑰相同。

26、如請求項 21 所述的加密文件，其中，所述混淆運算中的混淆因子包括上述第一金鑰。

圖 式

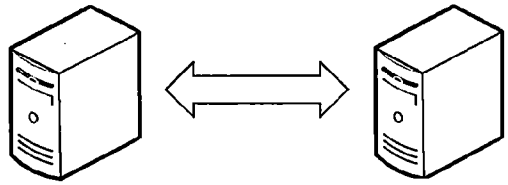
加密裝置 10
解密裝置 20

圖 1

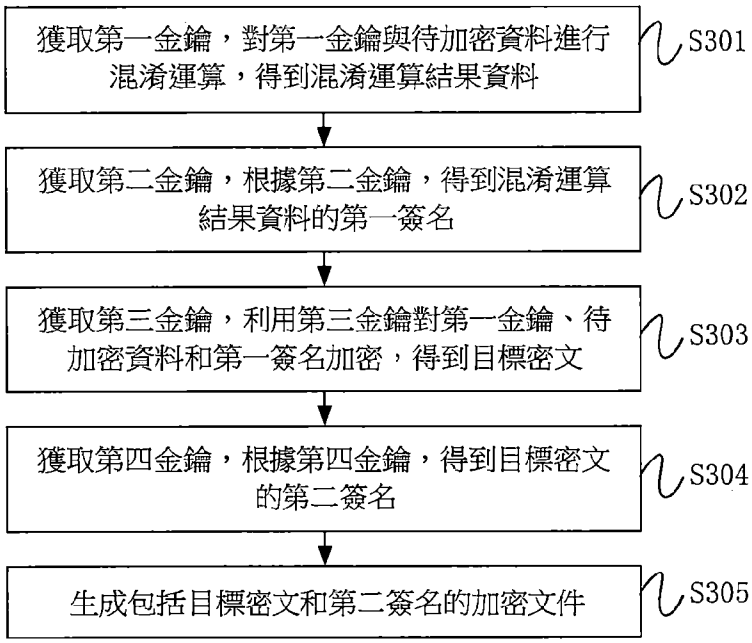
獲取第一金鑰，對第一金鑰與待加密資料進行混淆運算，得到混淆運算結果資料
S301
獲取第二金鑰，根據第二金鑰，得到混淆運算結果資料的第一簽名
S302
獲取第三金鑰，利用第三金鑰對第一金鑰、待加密資料和第一簽名加密，得到目標密文
S303
獲取第四金鑰，根據第四金鑰，得到目標密文的第二簽名
S304
生成包括目標密文和第二簽名的加密文件
S305

圖 2

1	#可公開的資料
2	
3	目標密文
4	
5	第二簽名
6	

圖 3

1	#可公開的資料
2	
3	第一金鑰
4	
5	敏感性資料 1
6	敏感性資料 2
7	敏感性資料 3
8	
9	第一簽名
10	
11	第二簽名
12	

圖 4

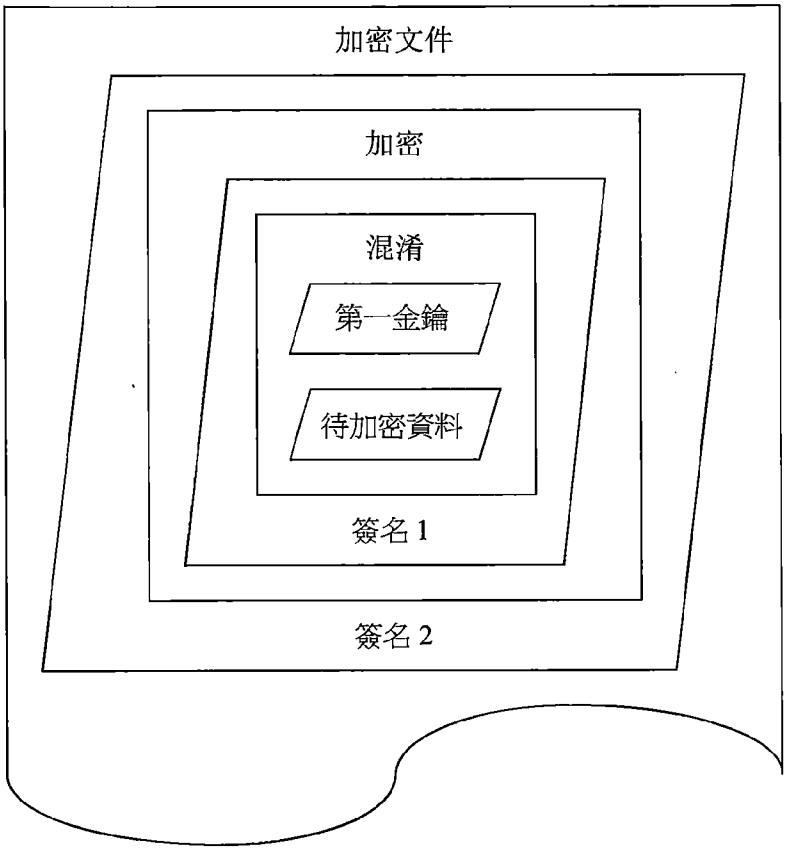
加密文件
加密
混淆
第一金鑰
待加密資料
簽名 1
簽名 2

圖 5

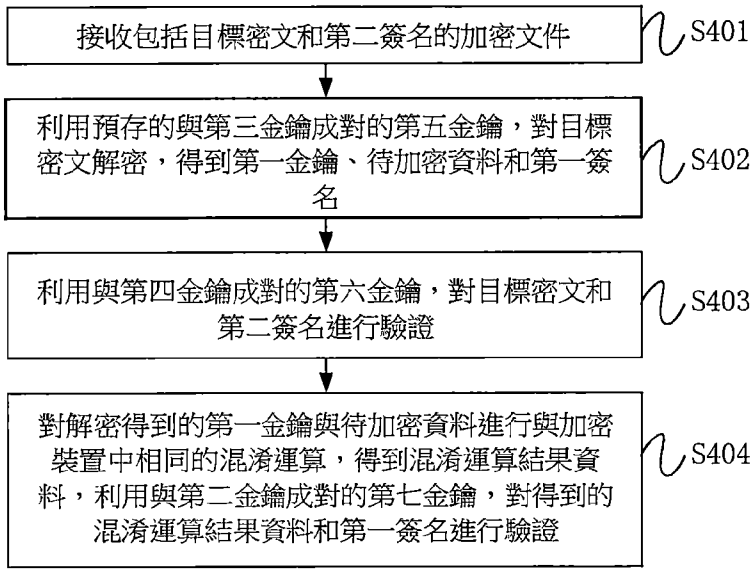
接收包括目標密文和第二簽名的加密文件
S401
利用預存的與第三金鑰成對的第五金鑰，對目標密文解密，得到第一金鑰、待加密資料和第一簽名
S402
利用與第四金鑰成對的第六金鑰，對目標密文和第二簽名進行驗證
S403
對解密得到的第一金鑰與待加密資料進行與加密裝置中相同的混淆運算，得到混淆運算結果資料，利用與第二金鑰成對的第七金鑰，對得到的混淆運算結果資料和第一簽名進行驗證
S404

圖 6

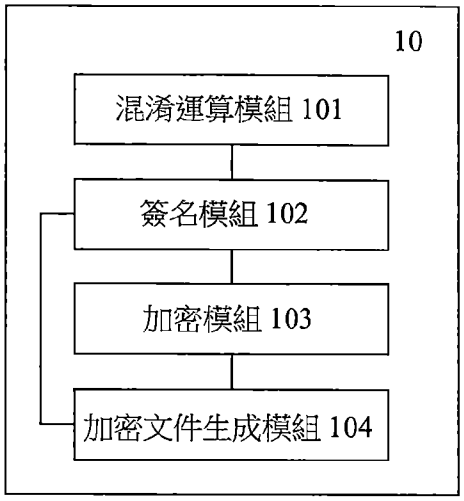
10
混淆運算模組 101
簽名模組 102
加密模組 103
加密文件生成模組 104

圖 7

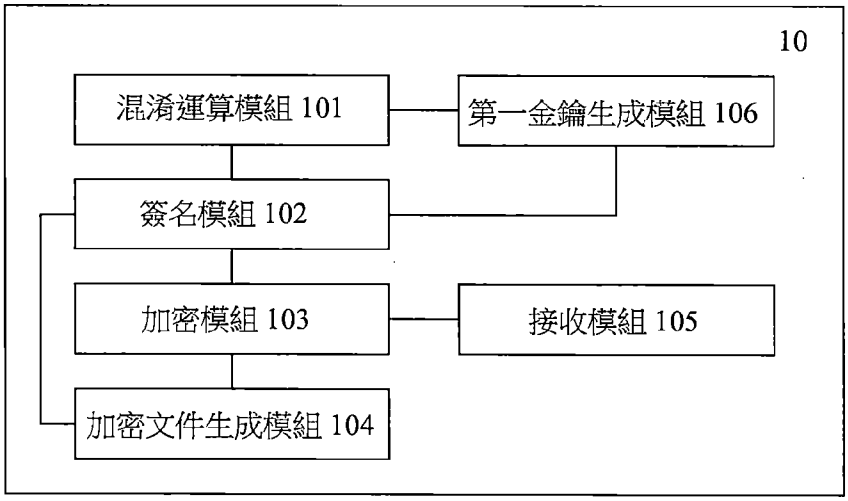
10
混淆運算模組 101
第一金鑰生成模組 106
簽名模組 102
加密模組 103
接收模組 105
加密文件生成模組 104

圖 8

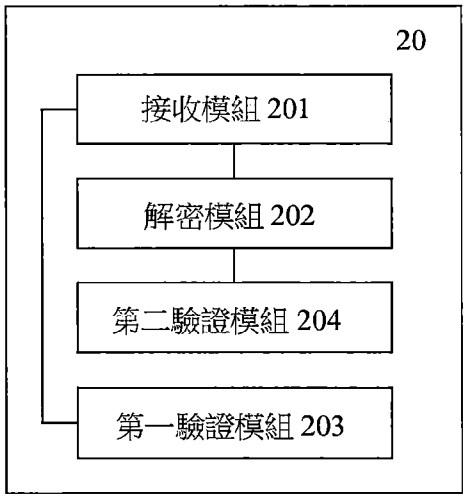
20
接收模組 201
解密模組 202
第二驗證模組 204
第一驗證模組 203

圖 9

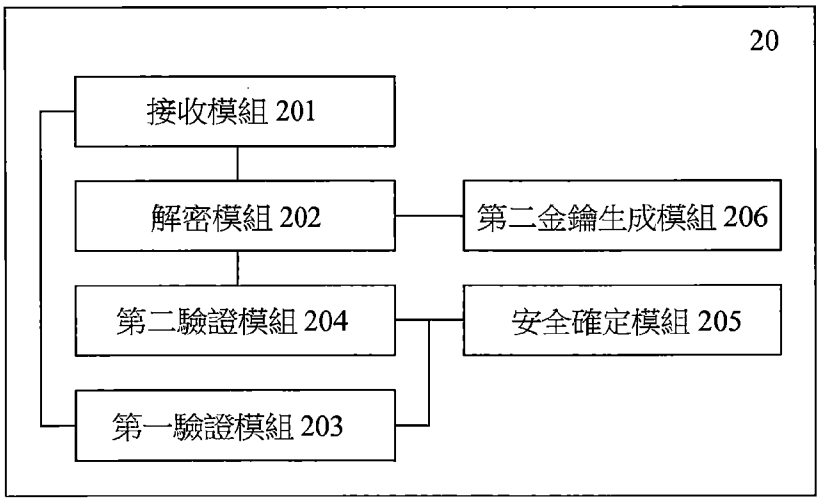
20
接收模組 201
解密模組 202
第二金鑰生成模組 206
第二驗證模組 204
安全確定模組 205
第一驗證模組 203

圖 10

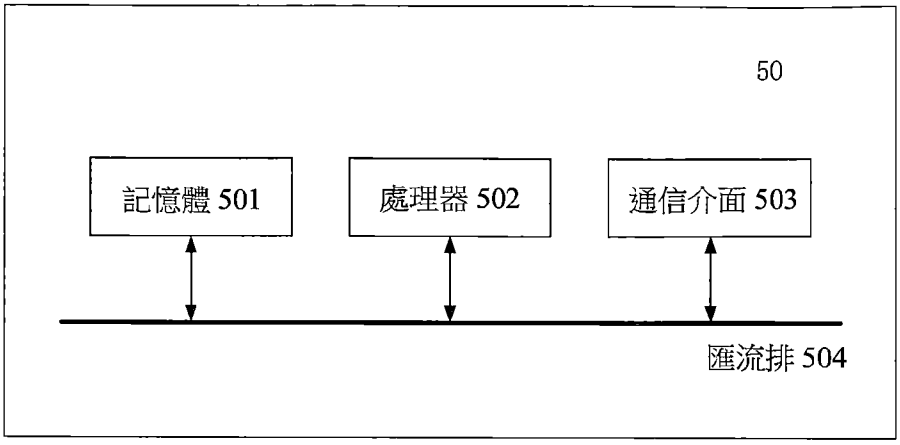

圖 11