



385411

申請日期	87 年 4 月 21 日
案 號	87106081
類 別	G06F 9/44

A4

C4

385411

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	資訊處理裝置及方法和記錄介質
	英 文	Information processing apparatus and method and recording medium
二、發明 創作人	姓 名	(1) 竹內彰一 (2) 難波慎二
	國 籍	(1) 日本 (2) 日本 (1) 日本國東京都品川區北品川六丁目七番三五號 蘇妮股份有限公司
三、申請人	住、居所	(2) 日本國東京都品川區北品川六丁目七番三五號 蘇妮股份有限公司
	姓 名 (名稱)	(1) 蘇妮股份有限公司 ソニー株式会社
	國 籍	(1) 日本 (1) 日本國東京都品川區北品川六丁目七番三五號
	住、居所 (事務所)	
	代 表 人 姓 名	(1) 出井伸之

裝

訂

線

(由本局填寫)

承辦人代碼：
大類：
IPC分類：

A6
B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ☐有 ☐無主張優先權

日本 1997 年 4 月 30 日 9-112179 ☒有主張優先權

有關微生物已寄存於： 寄存日期： 寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部中央標準局員工消費合作社印製

五、發明說明(1)

發明背景

本發明是有關資訊處理裝置及方法和記錄介質。尤其是由一合法程式開發者開發的程式，在某一程式執行環境下執行之資訊處理裝置及方法和記錄介質，其程式。

爪哇（美國太陽微系統公司的商標）由於適合網際網路，近年來流傳很廣引起很大的注意。“爪哇”一詞用以指稱每一個目標導向語言的爪哇語言、一虛擬機器（以下專指“爪哇虛擬機”）使得處理器構造配合一以爪哇語言寫成之程式予以執行（以下專指“爪哇程式”），及其他有關爪哇之元素，或是其總稱項目。“虛擬機”並非意味表示以單一電腦讓使用者以多機使用，而是一虛擬機執行一語言處理系統。

一爪哇虛擬機被用以操作各種不同的軟體、操作系統及硬體。另一方面，一爪哇程式編譯成二元碼組成爪哇虛擬機的指令組。該二元碼可以爪哇虛擬機能操作之任何硬體予以執行。因此，只要爪哇虛擬機的操作，一編譯過的爪哇程式即可在任何各種平台上執行。

基於爪哇虛擬機一旦被執行爪哇程式即可在任何機器上執行的事實，及其他事實根據，爪哇虛擬機將廣為使用者所流傳。同時，許多應用程式也將被開發出來分配至許多這類使用者（無論他們是否付費或免費）。

上述的情況下，可能發生有人已開發並分配一如爪哇虛擬機的程式執行環境，想要限定由第三者開發而成之應用程式的分配及由前者開發而成在程式執行環境下予以執

（請先閱讀背面之注意事項再填寫本頁）

張

訂

五、發明說明(2)

行，如：前者希望容許應用程式只分配予特許者。

另一方面，爪哇虛擬機內稱作位元碼（爪哇碼）的中間碼被釋譯並執行，其是藉由一爪哇編譯器編譯一爪哇程式而得。爪哇位元碼不予編譯則相當容易了解，使得抄襲該程式的回復工程變得容易。因此，防止他人的抄襲偽造應用程式是有其必要。

發明簡述

本發明如上所述，其目的在可能限定某一程式在某一程式執行環境內執行以防止程式的抄襲偽造。

本發明提供一資訊處理裝置以執行處理執行程式的程序，包含用以解密加密版程式的解密元件及從該解密元件輸出用以執行該程式的執行元件。

本發明還提供一執行程式的資訊處理裝置，包含加密元件用以將一程式加密至加密文句以解密成可執行碼。

本發明另外還提供一資訊處理裝置以執行一供執行程式用之程序，包含執行程式用之執行元件，檢查該程式是否合法獲准執行的檢查元件，及供應元件用以供應由該檢查元件證實為合法程式之執行元件。

本發明更提供一資訊處理裝置執行一程式，包含處理元件用以處理如專利範圍第5項之資訊處理裝置內被該實為合法的程式。

本發明的另一個觀點在提供一資訊處理方法，用以執行一執行程式的處理程序，包含將一加密版的程式予以解

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(3)

密的步驟，及執行由該解密步驟而得之程式。

本發明另提供一資訊處理方法用以執行程式，包含將程式加密成加密文句以解密成可為一資訊處理裝置執行之符碼的步驟。

本發明也提供一資訊處理方法用以執行一供執行程式用之程序，包含檢查該程式是否合法獲准執行的步驟，及當該程式證實為合法才執行該程式的步驟。

本發明還提供一資訊處理方法用以執行程式，包含處理程式的步驟，以證實專利範圍第5項資訊處理裝置內程式的合法性。

本發明更進一步提供另一觀點，在於一記錄媒介，程式記錄在上面，該程式使電腦執行將一加密版之程式予以解密的步驟，及執行由該解密步驟而得之程式。

本發明另外提供一有程式記錄在上面的記錄介質，該程式被加密成加密文句以解密為可由如專利範圍第1項之資訊處理裝置執行的符碼。

本發明也提供一上面記錄有程式的記錄介質，該程式用以促使電腦執行檢查的步驟，檢查程式是否合法，只有當證實其為合法時才會執行該程式。

本發明更提供一上面記錄有程式的記錄介質，該程式被加以處理以證實其合法性如專利範圍第5項所述之資訊處理裝置。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

結

五、發明說明(4)

附圖簡述

圖 1 是顯示一程式執行系統其功能配置之第一個例子的簡圖；

圖 2 是顯示一程式確認授權伺服器 3 2 之處理程序流程圖；

圖 3 是顯示一程式執行系統其功能配置之第三例的簡圖；

圖 4 是顯示程式確認授權伺服器 3 2 之處理程序的流程圖；

圖 5 是顯示電腦 1 的來源與其所完成之爪哇虛擬機 1 1 之間的相互關係；

圖 6 是表示爪哇虛擬機 1 1 的處理程序；

圖 7 是表示爪哇虛擬機 1 1 的處理程序；

圖 8 是表示爪哇虛擬機 1 1 的處理程序；

圖 9 是本發明之程式供應系統，其具體實施例之配置例子之一的簡圖；

圖 1 0 是圖 9 軟體開發伺服器 3 1 之配置例子之一的簡圖；

圖 1 1 是圖 9 程式認證授權伺服器 3 2 之配置例子之一的簡圖；

圖 1 2 是顯示圖 9 中使用者終端 3 3 之配置例子之一的簡圖；

圖 1 3 是軟體開發伺服器 3 1 之處理程序的流程圖；

圖 1 4 是一加密／解密系統之配置例子之一的簡圖；

五、發明說明 (5)

圖 1 5 是顯示一程式執行系統其功能配置第二個例子的簡圖；及

圖 1 6 是顯示一使用數位簽名之加密／解密系統的配置例子簡圖。

主要元件對照表

1	真實電腦
2	中央處理單元
3	暫存器
4	記憶體
1 1	虛擬機
1 3	暫存器
1 4	記憶體
2 1	爪哇編譯器
3 1	軟體開發者伺服器
3 2	程式認證授權伺服器
3 3	使用者終端機
3 4	網路
4 1	中央處理單元
4 2	唯讀記憶體
4 3	隨機存取記憶體
4 4	輸入區
4 5	輸出區

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (6)

- | | |
|-----|---------------|
| 4 6 | 輔助儲存裝置 |
| 4 7 | 通訊控制區 |
| 5 1 | 中央處理單元 |
| 5 2 | 唯讀記憶體 |
| 5 3 | 隨機存取記憶體 |
| 5 4 | 輸入區 |
| 5 5 | 輸出區 |
| 5 6 | 輔助儲存裝置 |
| 5 7 | 通訊控制區 |
| 6 1 | 中央處理單元 |
| 6 2 | 唯讀記憶體 |
| 6 3 | 隨機存取記憶體 |
| 6 4 | 輸入區 |
| 6 5 | 輸出區 |
| 6 6 | 輔助儲存裝置 |
| 6 7 | 通訊控制區 |
| 7 1 | 加密器 |
| 7 2 | 解碼器 |
| 8 1 | 輸入區 |
| 8 2 | 解碼區 |
| 8 3 | 執行區 (爪哇虛擬機) |
| 9 1 | 摘要生成器 |
| 9 2 | 加密器 |
| 9 3 | 解碼器 |

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (7)

- 9 4 摘要生成器
- 9 5 簽名檢查機
- 1 0 1 輸入區
- 1 0 2 信息摘要系統
- 1 0 3 簽名檢查區
- 1 0 4 虛擬機輸入控制區

較佳具體實施例的詳細說明

本發明的具體實施例詳如下述。在此之前，爲了說明本發明申請專利範圍的個別元件與其後之具體實施例的要素間的相互關係，本發明的特點將以個別元件括弧內爲與其對應之具體實施例的要素之方法詳如後述。

申請專利範圍第一項所引用之資訊處理裝置是一種資訊處理裝置的執行一供執行程式之用的程序，包含解碼元件（如：圖 1 顯示之解碼區 8 2）用以將一加密版的程式予以解密；及執行元件（如：圖 1 顯示之爪哇虛擬機 8 3）以執行從該解密元件輸出之程式。

申請專利範圍第 2 項所引用之資訊處理裝置是一種資訊處理裝置用以執行程式，包含加密元件（如：圖 2 顯示之程式處理步驟 S 1 4）用以將程式加密成加密文句以便解密爲可執行之符碼。

申請專利範圍第 5 項引用之資訊處理裝置是一種資訊處理裝置（如：圖 3 顯示之爪哇虛擬機 8 3）以執行程式

（請先閱讀背面之注意事項再填寫本頁）

表

訂

五、發明說明(8)

，檢查元件（如：圖 3 顯示之簽名檢查區 1 0 3）以檢查該程式是否為合法准予執行；及供應元件（如圖 3 所示之虛擬機輸入控制區 1 0 4）用以供應由檢查元件證實為合法程式之執行元件。

申請專利範圍第 8 項所引用之資訊處理裝置是一執行程式的資訊處理裝置，包含處理元件（如圖 4 所示之程式處理步驟 2 4 和 2 5）以處理依照申請專利第 5 項資訊處理裝置內證實為合法之程式。

當然，上述說明並不意味個別元件僅限於下述的要素。

其次，須詳加說明本發明應用於一爪哇虛擬機，雖然本發明除了應用於一虛擬機如一爪哇虛擬機外，本身也可應用於一真實機上。

因為爪哇已由 Nikkei 商業出版公司在 1 9 9 6 . 3 . 2 5（第 6 5 8 號）及 1 9 9 , 6 6 , 1 7（第 6 6 4 號）出版的 Nikkei 電子學中詳細說明過，以下僅做簡要的說明。

一爪哇虛擬機是一抽象的執行機器，而且是一由一真實的電腦實際予以執行的真實程式。如同一真實的電腦，爪哇虛擬機有一程式計算器、一堆積暫存器，一般目的暫存器、一堆積記憶體、及其他與一真實電腦相同的資源配備。

真實的電腦 1 有一中央處理單元 2、一暫存器 3 與中央處理單元 2 結合、一記憶體 4 及其他配備如圖 5 所示。

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明(9)

當一爪哇虛擬機 1 1 在電腦 1 上執行時，真實電腦上的資源配備即圖示於一爪哇虛擬機 1 1 之上。圖 5 之爪哇虛擬機 1 1 的具體實施例有一暫存器 1 3、一記憶體 1 4 及其他資源配備。該暫存器 1 3 圖示於暫存器 3，而記憶體 1 4 的位址 2 0 0 則圖示於記憶體 4 的位址 1 0 0 之上。

真實的電腦 1，其中中央處理單元 2 執行一指令以巧妙處理其資源配備。同樣地，爪哇虛擬機 1 1 的指令，被巧妙處理其資源配備的指令，其執行均予以定義。爪哇語言是一種描述爪哇虛擬機 1 1 之指令的語言。爪哇虛擬機 1 1 的爪哇位元碼予以翻譯並執行，其是由爪哇編譯器編譯一以爪哇語言寫成的來源程式而得到的。

也就是說，如圖 2 所示，一爪哇語言程式是一種以爪哇語言寫成的來源程式而由一爪哇編譯器 2 1 編譯成爪哇位元碼。爪哇位元碼輸入主爪哇虛擬機 1 1 以轉換成機器語言碼，由真實的電腦 1（中央處理單元 2）加以翻譯。尤其是如圖 7 所示，當一指令以爪哇位元碼寫成（爪哇位元碼指令）“移動 # 1 2 5、暫存器 1 3”意味著“設定數字 # 1 2 5 在暫存器 1 3 在”而輸入至爪哇虛擬機 1 1 時，爪哇虛擬機 1 1 將其轉換成一以機器語言碼寫成“移動 # 1 2 5、暫存器 3”之指令〈機器語言指令〉。

電腦 1 內的數字“1 2 5”設定在其暫存器 3 內如圖 8 A 所示之以機器語言碼寫成而執行該指令的結果。

如上所述，爪哇虛擬機 1 1 的暫存器 1 3 圖示於電腦 1 的暫存器 3 之上。因此，設定電腦 1 的暫存器 3 內的數

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (10)

字“125”如圖8A所示，即意味當從爪哇虛擬機11觀察如圖8B所示設定數字“125”在暫存器13內。

上述方法是一輸入主爪哇虛擬機11的爪哇位元碼轉換成機器語言碼以供電腦1之用，然後被巧妙地執行於電腦1的資源配備，該資源配備圖示於爪哇虛擬機11之資源配備。當觀察爪哇虛擬機11，上述的巧妙處理對應於爪哇虛擬機11之資源配備上的巧妙處理，前者之巧妙處理的執行意味爪哇位元碼指令的執行。

因此，如上所述，藉由定成一在真實電腦上的爪哇虛擬機，一經編譯過的爪哇程式能執行而不須考慮該電腦內的中央處理單元及操作系統。

一種供轉換爪哇位元碼成為機器語言碼並執行該機器語言碼的技術，其中的一例是一翻譯機計畫，將指令翻譯成機器語言碼並逐一執行該機器語言碼，如同執行一基本語言程式。另外的一例是一即時編譯器計畫，將指令翻譯成機器語言碼並總括全體執行該機器語言碼。

使用翻譯機計畫執行一基本語言程式不同於翻譯爪哇位元碼，其來源碼以前者的計畫翻譯而中間碼（爪哇位元碼）以後者的計畫翻譯，然而這兩種計畫在本具體實施例並不加以區別（毋需這麼做）。

圖9顯示依照本發明之程式供應系統，其具體實施例之配置的例子之一（“系統”意味著多數彼此邏輯相關之裝置的集合，該裝置是否適合一單一架構無關）。

在程式供應系統內，當軟體開發者分配給使用者的應

（請先閱讀背面之注意事項再填寫本頁）

訂

續

五、發明說明 (11)

用程式未經一程式認證授權的認證時，該使用者其使用者終端 3 3 上的應用程式的執行即受到限制。

例如，一軟體開發者已經發展出一套在爪哇虛擬機上操作的應用程式，該軟體開發者藉由編譯該應用程式得以傳送爪哇位元碼，透過網路 3 4 如網際網路、公共管線、有線電視網路、地面波網路、衛星網路，或從一軟體開發伺服器 3 1 到一程式認證授權伺服器 3 2。

當接收從軟體開發伺服器 3 1 而來的爪哇位元碼時，程式認證授權伺服器認證後，透過網路 3 4 將其傳遞到軟體開發伺服器 3 1。軟體開發伺服器 3 1 接收並儲存從程式認證授權伺服器 3 2 傳遞來經認證過的爪哇位元碼。

當接收到從一使用者終端 3 1 對應用程式的要求時，軟體開發伺服器 3 1 即透過網路 3 4 傳遞該應用程式到使用者終端 3 3。如：一爪哇虛擬機藉由程式認證授權已經發展或分配成為一程式執行環境，或是在使用者終端 3 3 內完成程式認證授權對認證程式的要求。使用者終端 3 3 作為爪哇虛擬機時，從軟體開發伺服器傳遞來的應用程式，只有當由程式認證授權認證過後才會正確地執行。

也就是說，如果從軟體開發伺服器 3 1 傳遞而來的應用程式未經由程式認證授權加以認證者，該應用程式即無法在使用者終端 3 3 上作為爪哇虛擬機而加以執行。

結果，開發一爪哇虛擬機作為一程式執行環境並加以分配者，可藉由第三者開發的應用程式限制其分配，並在爪哇虛擬機上執行。如：前者能允許應用程式的分配予經

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (12)

授權之軟體開發者。

軟體開發者藉由一記錄介質 3 5 如：唯讀記憶體光碟或磁碟片加以記錄而分配給使用者的應用程式，以郵寄方式寄送或在計數器上出售。即使在如上所述的例子中，如果該應用未藉由程式認證授權加以認證者，該應用程式即無法在使用者終端機 3 3 內當做一爪哇虛擬機予以執行。

雖然上述的例子中，軟體開發者與程式認證授權間的資料經由網路 3 4 交換，該交換資料也可經由如一記錄介質 3 5 上已記錄之資料法郵寄方式傳送。

此外，雖然圖 9 所具體實施例中的軟體開發伺服器 3 1、程式認證授權伺服器 3 2、及使用者終端 3 3 彼此間以單一供應，也可以每一個均提供多數。

圖 1 0 顯示圖 9 中軟體開發伺服器 3 1 的結構例。

一中央處理單元 4 1 在儲存（記錄）於輔助儲存設備 4 6 內之操作系統的控制下，由儲存於輔助儲存設備 4 6 內的執行程式執行各種不同的處理程序。一唯讀記憶體 4 2 儲存一原始程式載入的程式及其他程式。一隨機存取記憶體 4 3 儲存一由中央處理單元 4 1 執行的程式及操作於中央處理單元之所需之資料。輸入區 4 4，如：鍵盤或嘴巴，被以妙地輸入一所需的指令或資料等等。輸出區 4 5，如顯示螢幕設備或印表機，顯示或列印需要的資訊。輔助儲存設備 4 6，如硬碟機，儲存由中央處理單元 4 1 執行之操作系統或其他程式，如同中央處理單元 4 1 及其他必需資訊的執行結果。通訊控制區 4 7 控制經由網

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (13)

路 3 4 完成的通訊。

圖 1 1 顯示圖 9 內程式認證授權伺服器 3 2 的結構例，而圖 1 2 顯示圖 9 中使用者終端 3 3 的結構例。

程式認證授權伺服器 3 2 由一中央處理單元 5 1 組成連接一通訊控制區 5 7，而使用者終端 3 3 由一中央處理單元 6 1 組成連接一通訊控制區 6 7。固為上述元素的結構與圖 1 0 之中央處理單元之連接通訊控制區 4 7 相同，茲不贅述。

其次，軟體開發者伺服器 3 1 的處理程式參考圖 1 3 的流程圖加以說明。

由該軟體開發者開發之應用程式在一爪哇虛擬機上執行，儲存（記錄）於輔助儲存設備 4 6 內。首先在軟體開發者伺服器 3 1 的步驟 S 1，中央處理單元 4 1 根據一爪哇編譯程式將儲存於輔助儲存設備 4 6 內的應用程式編譯成爪哇位元碼。該爪哇位元碼也供應予輔助儲存設備 4 6 並儲存在內。

處理程序進入步驟 S 2，通訊控制區 4 7 讀出作為應用程式儲存於輔助儲存設備 4 6 內的爪哇位元碼，並透過網路 3 4 傳送至程式認證授權伺服器 3 2。然後進入步驟 S 3 的程序，中央處理單元 4 1 判斷該加密文句作為一加密版的應用程式，也就是說，一經認證過之應用程式（爪哇位元碼）是否已經從程式認證授權伺服器傳送出去。如果沒有，則程序重回到 S 3。

如果步驟 S 3 判斷該加密文句已經傳送出去，則程序

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (14)

進行到步驟 S 4，該加密文句由通訊控制區 4 7 加以接收。程序進行到步驟 S 5，該加密文句由通訊控制區 4 7 接收後轉移至輔助儲存設備 4 6。本程序即告完成。

接著，一程式認證授權伺服器 3 2 的處理程序將參考圖 2 的流程圖加以說明。

如程式認證授權是應某人需求發展或分配一爪哇虛擬機作為一程式執行環境或一個組織。例如：程式認證授權伺服器 3 2 執行一程式認證程式以確認從一許可者送出之應用程式。

尤其是以下列方式為之。首先，在步驟 S 1 1，程式認證授權伺服器 3 2 的中央處理單元 5 1 判斷爪哇位元碼，即認證主題的應用程式是否已經從軟體開發者伺服器 3 1 透過網路 3 4 傳送出來。如果判斷該爪哇位元碼尚未傳送出來，則程序回到步驟 1 1。如果判斷該爪哇位元碼在步驟 1 1 已經傳送出去，則程序進行到步驟 S 1 2，中央處理單元 5 1 判斷爪哇位元碼是否從一許可的軟體開發者而來的符碼（以下專指「定期的軟體開發者」）。

程式認證授與一軟體開發者訂立契約允許軟體開發者開發並分配在爪哇虛擬機上執行的應用程式。然後，程式認證授權即發給軟體開發者一個身份證明及密碼。該身份證明及密碼在經許可的契約與爪哇位元碼經認證一起從該許可（即定期）的軟體開發者傳送至程式認證授權時發布。在步驟 S 1 2。程式認證授權根據這些身份證明及密碼判斷該爪哇位元碼是否從一定期軟體開發者而來。

五、發明說明 (15)

如果在步驟 S 1 2 的判斷是該爪哇位元碼並非從一定期的軟體開發者而來，即它們是從沒有經過契約的許可的軟體開發者傳送而來時，程序即進入步驟 S 1 3，通訊控制區 5 7 即傳送一信息予該軟體開發者，除非經契約許可，否則該爪哇位元碼無法加以認證。程序即告結束。

另一方面，如果在步驟 1 2 的判斷，該爪哇位元碼是從一定期軟體開發者傳送而來時，程序即進入步驟 S 1 4，中央處理單元 5 1 將爪哇位元碼加密成為加密文句。該爪哇位元碼即因此而被認證。

程序即進入步驟 S 1 5，通訊控制區 5 7 將作為爪哇位元碼之認證結果的加密文句經由網路 3 4 傳送至傳送該爪哇位元碼的軟體開發者（本例即為軟體開發者伺服器 3 1）。程序即告結束。

接著，在步驟 S 1 4，程式認證授權伺服器 3 2 完成加密方法的詳細說明。

程式認證授權伺服器 3 2 內的爪哇位元碼根據由如 R S A 方法（由麻省理工學院三位研究員開發；R S A 為其字首）而作為典型的公開鍵加密方法予以加密。

圖 1 4 顯示根據該公開鍵加密方法作為加密方法之例的加密／解密系統，其結構例子之一。

一作為加密主題的正常文句輸入至一加密器 7 1。該加密器 7 1 藉由使用一稱為秘密鍵且對每個人是唯一的加密鍵將正常文句加密成為一加密文句。

另一方面，一由加密器 7 1 產生之加密文句輸入至一

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明 (16)

解密器 7 2。該解密器 7 2 藉由使用一稱為公開鍵且對大眾公開的解密鍵將該加密文句解密成為原來的正常文句。

程式認證授權伺服器 3 2 藉由使用一特定於爪哇位元碼的秘密鍵，將從軟體開發者伺服器傳送而來的爪哇位元碼加密成為加密文句。

該加密方法不限於公開鍵加密方法，其他如由 D E S 方法（資料加密標準，由 I B M 公司開發實務上作為美國政府標準）之典型的秘密鍵加密法也可使用。

圖 1 顯示使用者終端 3 3 內用以執行一應用程式，作為一程式執行環境的程式執行系統，其功能結構的例子之一。

輸入區 8 1 接收加密文句（經加密之爪哇位元碼）並將其供應予解密區 8 2。解密區 8 2 的操作如同圖 1 4 的解碼器 7 2。解密區 8 2 藉由使用一公開鍵將輸入區 8 1 輸出的符碼予以解密成原來的爪哇位元碼。由解密區 8 2 而得之爪哇位元碼供應予爪哇虛擬機 8 3。該爪哇虛擬機執行一從解密區 8 2 供應而來之爪哇位元碼所限定的程序。

上述結構程式執行系統內，首先，輸入區 8 1 得到加密文句作為一應用程式。如：作為一應用程式的加密文句經由網路 3 4 預先從軟體開發者伺服器 3 1 傳送而來並儲存於輔助儲存設備 6 6 內的檔案，或者在使用者終端 3 3 內設定一記錄有檔案的記錄介質 3 5，輸入區 8 1 打開這些檔案並讀出該加密文句。

（請先閱讀背面之注意事項再填寫本頁）

訂

終

五、發明說明 (17)

假設該軟體開發者伺服器 3 1 連接至網際網路的網路 3 4。作為一應用程式的加密文句與一軟體開發者伺服器 3 1 內的同源定位器為共生關係，輸入區 8 1 接收經由網路 3 4 從軟體開發伺服器 3 1 傳送而來作為應用程式的加密文句，當使用者藉由巧妙操作輸入區 6 4 指定該同源定位器時。

假設另一種情況，軟體開發者伺服器 3 1 藉由地面波或透過衛星網路 3 4 數位化廣播作為一應用程式的加密文句。輸入區 8 1 即接收這些廣播的加密文句。

輸入區 8 1 將以這種方式得到作為應用程式的加密文句供應予解密區 8 2。

解密區 8 2 不只從輸入區供應加密文句，還有一相對應使用於產生加密文句之秘密鍵的公開鍵。

該公開鍵由程式認證授權加以管理，並透過網路 3 4 位送至使用者終端 3 3 以回應使用者的需求。或是透過郵件傳遞至使用者。該加密文句作為程式記錄在一記錄介質 3 5 的一個檔案內傳遞至使用者，該公開鍵可與該加密文句一起記錄於記錄介質 3 5 上。也可能在經由程式認證授權伺服器 3 2 認證爪哇位元碼之後，該公開鍵與作為認證結果的加密文句一起傳送至軟體開發者伺服器 3 1，然後該公開鍵從軟體開發者傳遞至使用者。

解密區 8 2 藉由使用公開鍵將從輸入區 8 1 供應而來之加密文句予以解密，並將作為解密結果的爪哇位元碼供應予爪哇虛擬機 8 3。爪哇虛擬機 8 3 翻譯並執行從解密

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (18)

區 8 2 供應而來之爪哇位元碼。

如上所述，解密區 8 2 藉由使用一相對於用以在程式認證授權伺服器 3 2 內加密之秘密鍵的公開鍵，將加密文句予以解密，而該解密結果輸入至爪哇虛擬機 8 3。因此，如果輸入至解密區 8 2 的爪哇位元碼未經程式認證授權，則被爪哇虛擬機 8 3 正常執行的爪哇位元碼即不會從解密區 8 2 輸出，例如：相對於一種情況，發生未加密之爪哇位元碼輸入時，在程式認證授權伺服器 3 2 內根據一不同的加密算法加密的爪哇碼，或者根據與程式認證授權伺服器 3 2 內使用相同的算法而不使用秘密鍵，應該使用於一定期的情況下。結果可能限制在爪哇虛擬機 8 3 上操作而未經由程式認證授權的爪哇位元碼分配給有使用者終端 3 3 內實行爪哇虛擬機 8 3 的使用者。

上述的方法可能僅允許與程式開發者訂定契約的軟體開發者，將在爪哇虛擬機 8 3 上操作之爪哇位元碼分配給有使用者終端 3 3 內實行爪哇虛擬機 8 3 的使用者。爪哇虛擬機 8 3 的開發者或分配者接收許可費以供分配從想分配在爪哇虛擬機 8 3 上操作之軟體開發者使用爪哇虛擬機 8 3 的應用程式。

有必要採取一有限度只准許解密區 8 2 輸入爪哇位元碼至爪哇虛擬機 8 3。

一旦接收某一輸入，圖 1 的輸入區 8 2 即執行一關於輸入及輸出一處理結果的解密程序。因此，通常當爪哇位元碼未經程式認證授權輸入解碼區 8 2 時，爪哇虛擬機

(請先閱讀背面之注意事項再填寫本頁)

訂

終

五、發明說明 (19)

8 3 即離開，而與這些爪哇位元碼一起得到之處理結果供應至爪哇虛擬機 8 3。因此看來，檢查解密區 8 2 的輸出是否為合法（正常）爪哇位元碼的程序也許可行，而爪哇虛擬機 8 3 只有當該解密區 8 2 輸出之爪哇位元碼為合法爪哇碼時，才允許翻譯並執行爪哇位元碼。例如：當 3 2 位元資料稱為「魔術」者位於爪哇位元碼前而有一定值（「C A F E B A B E」以 6 0 進位法），判斷區 8 2 的輸出為合法爪哇位元碼，爪哇虛擬機 8 3 也許被准予翻譯並執行爪哇虛擬機。爪哇虛擬機 8 3 因此不用離開。

程式認證授權伺服器 3 2 可藉由加密部分爪哇位元碼如上述資料「魔術」加以認證爪哇位元碼而不需要全部的爪哇位元碼。然而，既然資料「魔術」由如 3 2 等 2 位元組成，可能偽造資料「魔術」更容易，因此，解密區輸出正確的值而非所有爪哇位元碼。所以將所有爪哇位元碼予以加密是迫切需要的。

順帶一提的是，從限制爪哇虛擬機 8 3 上之應用程式的執行觀點來看，即使圖 1 2 之解密區 8 2 的解密算法或使用之公開鍵被第三者得知，只要加密算法或使用於加密的秘密鍵不知道，也不會有問題。也就是說，爪哇虛擬機上一應用程式之執行能加以限制，即使得知加密文句的解密方法，只要將產生加密文句的方法給予解密區 8 2 以供應爪哇位元碼予爪哇虛擬機，即可正確地執行。

然而，如果有人知道加密文句的解密方法，即可從加密文句獲得爪哇位元碼（加密文句的產生是由程式認證授

五、發明說明 (20)

權認證爪哇位元碼的結果)。既然爪哇位元碼的內容能藉由解譯而相對地容易了解，則可容易地進行回復工程。

為防止這樣的回復工程，加密文句的解密方法即需保密。例如：用以將加密文句解密的公開鍵，雖然它通常是公開的。

圖 1 5 顯示內有保密之公開鍵的程式執行系統，其結構例子之一。圖 1 5 的要素與圖 1 相對應的要素其參數相同，茲不贅述。

本具體實施例中，一公開鍵位於單一位置或分散在一程式的多數位置，組成一包括一爪哇虛擬機 8 3 的程式執行系統。解密區 8 2 藉由使用此一公開鍵將加密文句予以解密。因此本例的公開鍵未曾從程式執行系統漏出而防止加密文句非法解密致實行回復工程（或降低回復工程發生的可能性）。

上述說明直接針對使用者終端 3 3 基本上解密區 8 2 之解密結果輸入至爪哇虛擬機 8 3 的情況。在使用者終端 3 3 內可能執行一檢查爪哇位元碼是否合法的程序，也就是說，藉由程式認證授權加以認證並非偽造，且只有證實為合法的爪哇位元碼才會輸入至爪哇虛擬機 8 3。

本例中的程式認證授權伺服器 3 2 根據圖 4 流程圖在作為一應用程式的爪哇位元碼執行一程式認證程序，該爪哇位元碼從軟體開發伺服器 3 1 傳送而來。

步驟 S 2 1 - S 2 3 分別與圖 2 的步驟 S 1 1 - S 1 3 相同。

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (21)

如果在步驟 S 2 2 判斷送來的爪哇位元碼來自一定期的軟體開發者，則程序接著進行步驟 S 2 4 - S 2 6，簽名（數位簽名）附加於爪哇位元碼用以確認爪哇位元碼的合法性。

步驟 S 2 4，中央處理單元 5 1 對爪哇位元碼作一摘要。程序進入步驟 S 2 5，中央處理單元 5 1 從步驟 S 2 4 產生之摘要中製造一數位簽名。程序進入步驟 S 2 6，通訊控制區 4 7 將該數位簽名附加於爪哇位元碼上（爪哇位元碼附加數位簽名以下專稱為“簽名附加位元碼”）並將簽名附加位元碼傳送至軟體開發者伺服器 3 1。程序即告結束。

其次，在步驟 S 2 4 - S 2 6 將詳細說明程式認證授權伺服器 3 2 內製造簽名附加位元碼的方法。

在程式認證授權伺服器 3 2 內，簽名附加位元碼是根據 R S A 方法之典型公開鍵加密法而產生的。

圖 1 6 顯示根據使拐一數位簽名之公開鍵加密法的加密／解密系統，其結構的例子之一。

一正常文句作為一認證主體而輸入至摘要生成器 9 1，根據如 M D S 或 S H A - 1 的演算法製造該接收文句的摘要。

一摘要相對應一正常文句的自動濃縮句，而不同的摘要產生以供不同的正常文句輸入之用。藉由使用一堆功能轉換一正常文句以製造摘要。

順帶一提的，碎址法是一種映射一組由一關鍵字搜尋

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明 (22)

一資料庫的範圍至某一限定數字範圍的方法（相對應一記錄數字或一系列後置）此一映射的轉換功能稱為碎址功能。

由摘要生成器 3 2 生成之摘要供應予一加密器 9 2。加密器 9 2 使用一如圖 1 4 所示之加密器 7 1 的秘密鍵將該摘要予以加密，並以一數位簽名方式輸出一加密摘要。數位簽名附加於原來正常文句上輸出一結果為簽名附加的正常文句。

另一方面，數位簽名作為簽名附加正常文句的一部分輸入至一解密器 9 3，而作為保留部分的文句輸入至一摘要生成器 9 4。解密器 9 3 藉由使用如圖 1 4 所示之解密器 7 2 的公開鍵將該數位簽名解密為一摘要。如此得到的摘要供應至簽名檢查機 9 5。

如同摘要生成器 9 1，摘要生成器 9 4 生成一接收正常文句的摘要並將其提供予簽名檢查機 9 5。

簽名檢查機 9 5 判斷該簽名（數位簽名）的合法性，即檢查該簽名。尤其該簽名檢查機 9 5 檢查從解密器 9 3 輸出的摘要與從摘要生成器 9 4 輸出之摘要是否相符。如果 2 種摘要彼此不相符，判斷該簽名不具合法性，該正常文句是偽造或者解密器 9 3 內使用的公開鍵不正確。

另一方面，從解密器 9 3 輸出之摘要與從摘要生成器 9 4 輸出之摘要如果相符，則證實該簽名為合法，判斷該正常文句並非偽造或者解密器 9 3 內使用之公開鍵是正確的。

簽名檢查機 9 5 也供應組成簽名附加正常文句的正常

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明 (23)

文句。簽名檢查機 9 5 當證實簽名之合法性時即輸出正常文句。

在程式認證授權伺服器內的爪哇位元碼，從軟體開發者伺服器 3 1 傳送而來加以轉換成簽名附加位元碼對應上述簽名附加文句，認證該爪哇位元碼。

簽名產生方法不限於上述利用該公開鍵加密方法。

圖 3 顯示一程式執行系統作為一程式執行環境以檢查一應用程式的合法性及當使用者終端 3 3 為合法而予以執行，其功能結構的例子之一。

圖 3 中的要素與圖 1 中對應的要素有相同的參數，茲不贅述。

一輸入區 1 0 1 接收輸入基本上與圖 1 輸入區 8 1 的方式相同。輸入區 1 0 1 與後者不同之處在於其接收簽名附加位元碼（簽名（數位簽名）附加於爪哇位元碼）。輸入區 1 0 1 將該簽名附加位元碼分離為簽名和爪哇位元碼而將其輸出。簽名部分提供予簽名檢查區 1 0 3，而爪哇位元碼則供應予一信息摘要系統 1 0 2 及一虛擬機輸入控制區 1 0 4。

信息摘要系統 1 0 2 執行的程序與圖 1 6 摘要生成器 9 4 執行的程序相同。也就是說，信息摘要系統 1 0 2 從爪哇位元碼生成一摘要並將其提供予簽名檢查區 1 0 3。簽名檢查區 1 0 3 對應於圖 1 6 的解密器 9 3 和簽名檢查器 9 5 檢查從輸入區 1 0 1 提供而來之簽名的合法性。

簽名檢查區 1 0 3 接收從輸入區 1 0 1 而來的簽名和

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明 (24)

從信息摘要系統而來的摘要。此外，簽名檢查區 1 0 3 提供一公開鍵以對應使用於生成該簽名的秘密鍵，與圖 1 之解密區所供應之公開鍵用同樣的方法。簽名檢查區 1 0 3 使用該接收之公開鍵將簽名解密成爲一摘要，透過與從信息摘要系統 1 0 2 供應而來的摘要與用上述方法得到的摘要作比較的簽名檢查的合法性。此外，簽名檢查區 1 0 3 還控制該虛擬機輸入控制區 1 0 4 遵守檢查的結果。

虛擬機輸入控制區 1 0 4 在簽名檢查區 1 0 3 的控制之下，供應爪哇虛擬機 8 3 從輸入區 1 0 1 而來的爪哇位元碼。

上述結構化程式執行系統內，首先，輸入區 1 0 1 獲得作爲一應用程式的簽名附加位元碼，如同圖 1 之輸入區 8 1 的方法。然後輸入區 1 0 1 將該簽名附加位元碼分離成簽名和爪哇位元碼，並將該簽名供應予簽名檢查區 1 0 3，而將爪哇位元碼提供信息摘要系統 1 0 2 和虛擬機輸入控制區 1 0 4。

信息摘要系統 1 0 2 生成一由輸入區供應從爪哇位元碼來的摘要，並將該摘要提供予簽名檢查區 1 0 3。簽名檢查區 1 0 3 藉由使用一公開鍵將從輸入區 1 0 1 提供之簽名解密成一摘要。此外，簽名檢查區 1 0 3 將從解密而得之摘要與從信息摘要系統 1 0 2 供應之摘要加以比較，並判斷從輸入區 1 0 1 供應而來之簽名的合法性，是否二者彼此符合。

如果證實其簽名的合法性，也就是說，將簽名解密後

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (25)

所得之摘要與從信息摘要系統 1 0 2 供應之摘要相符，簽名檢查區 1 0 3 控制虛擬機輸入控制區 1 0 4。因此，從輸入區 1 0 1 提供之爪哇位元碼輸出至爪哇虛擬機 8 3。虛擬機輸入控制區 1 0 4 在簽名檢查機 1 0 3 的控制下，將輸入區提供之爪哇位元碼，提供予爪哇虛擬機 8 3。

所以，爪哇虛擬機 8 3 經由虛擬機輸入控制區 1 0 4 將輸入區 1 0 1 提供之爪哇位元碼加以翻譯並執行。

另一方面，如果簽名的合法性未被證實，也就是說，從解密該簽名而得之摘要與信息摘要系統 1 0 2 供應之摘要不符時，簽名檢查機 1 0 3 控制虛擬機輸入控制區 1 0 4，從輸入區 1 0 1 供應之爪哇位元碼將不會輸出至爪哇虛擬機 8 3。

在這種情況下，虛擬機輸入控制區 1 0 4 不會輸出至爪哇虛擬機 8 3，爪哇位元碼從輸入區 1 0 1 供應。因此，爪哇虛擬機不執行任何程序。

如上所述，當簽名附加法認證一應用程式，可能限制在爪哇虛擬機上操作之爪哇位元碼的分配，而非藉由程式認證授權加以認證，分配予使用者，該使用者具有使用者終端 3 3 在內實行爪哇虛擬機 8 3。也就是說，可能只准許與程式認證授權簽約之軟體開發者，分配在爪哇虛擬機 8 3 上操作的爪哇位元碼予使用者，該使用者有一其內可實行爪哇虛擬機 8 3 的使用者終端 3 3。爪哇虛擬機 8 3 的開發者可從想分配在爪哇虛擬機 8 3 操作之爪哇位元碼的軟體開發者收受許可費用。

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (26)

附加簽名也變得有可能，限定在一偽造版簽名附加爪哇位元碼之爪哇虛擬機 8 3 上執行。

圖 3 的具體實施例，有必要採取一個標準，只許可虛擬機輸入控制區 1 0 4 輸入爪哇位元碼至爪哇虛擬機 8 3。

值得一提的是，爪哇位元碼本身存在於簽名附加於爪哇位元碼的情況，不像爪哇位元碼被加密的情況。因此，在一個沒有檢查簽名之合法性的程式執行系統（例如：從輸入區 1 0 1 輸出的爪哇位元碼直接輸入至爪哇虛擬機 8 3 的程式執行系統內），爪哇位元碼可以毫無限制地翻譯並執行。

相反地，在簽名附加爪哇位元碼的情況，爪哇虛擬機的開發者和銷售者，銷售者銷售一爪哇虛擬機作為在使用者終端 3 3 內實行，而類似使用可組織一如圖 3 所示之程式執行系統。不想限定爪哇位元碼之執行的使用者可組織一程式執行系統，其中簽名的合法性不予檢查。

本發明不但可應用於上述兩種翻譯型和及時編譯型的爪哇虛擬機，還可應用於其他不是爪哇虛擬機的虛擬機上。本發明還可應用於一程式執行系統，透過 C 語言或 C++ 語言之處理系統的機器碼，及輸入一程式執行系統，透過基本語言之處理系統的來源碼。

雖然圖 1，1 5 和 3 的基體實施例只有單一程式執行系統，然而，使用者終端 3 3 內的程式執行系統可提供多數，例示如下：當提供多數輸入區 8 1 或 1 0 1 時，一加

(請先閱讀背面之注意事項再填寫本頁)

訂 1

五、發明說明 (27)

密文句或簽名附加位元碼可從多種路徑輸入。當提供多數解密區 8 2 時，可根據多數解密演算法將一加密文句解密。當提供多數爪哇虛擬機 8 3 時，即有可能支持多數爪哇位元碼格式化。甚至，當提供多數信息摘要系統 1 0 2 和多數簽名檢查區 1 0 3 時，即有可能根據多數的技術，個別檢查多數附加的簽名。

上述具體實施例中，爪哇位元碼可以是任何型式如：Java Application Java Applet Java Benas 和 Java Class Library。

根據本發明的資訊處理裝置和方法，一加密版的程式被解密而由解密所得之程式予以執行。根據本發明之記錄介質，一程式用以使電腦完成解密一加密版程式的步驟和用以執行由該解密步驟所得之程式被記錄下來。因此，有可能僅准許執行一加密程式。

根據本發明之資訊處理裝置和方法，一程式被加密成加密文句以便被解密為可執行碼。根據本發明之記錄介質，一程式被加密成加密文句以便解密為可由如申請專利範圍第 1 項之資訊處理裝置執行之符碼而被記錄下來。因此有可能提供一種由如申請專利範圍第 1 項之資訊處理裝置執行之加密程式。

根據本發明之資訊處理裝置和方法，檢查一程式是否合法許可執行及該程式只有當證實其為合法時才予以執行。根據本發明之記錄介質，一程式用以使電腦完成檢查步驟，一程式是否合法，並只有當證實其為合法時才執行該

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (28)

程式而記錄下來。因此，有可能僅准許執行一合法程式。

根據本發明之資訊處理裝置和方法，如申請專利範圍第 5 項之資訊處理裝置，一程式處理程序被證實為合法。根據本發明之記錄介質，一程式處理程序在如申請專利範圍第 5 項之資訊處理裝置中證實其合法性而記錄下來。因此，有可能提供一經處理之程式，由申請專利範圍第 5 項之資訊處理裝置予以執行。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

續

四、中文發明摘要(發明之名稱：資訊處理裝置及方法和記錄介質)

一種應用程式，其使用一先設定好秘密鍵予以加密，輸入一程式執行系統的輸入區，而該加密之應用程式的加密文句提供予一解密區。該解密區不但提供該加密文句，還提供一與使用於製造該加密文句之秘密鍵相對應的公開鍵。解密區以公開鍵將加密文句予以解密並提供爪哇位元碼的解密結果至爪哇虛擬機。爪哇虛擬機翻譯從解密區而來的爪哇位元碼並執行之。

英文發明摘要(發明之名稱：INFORMATION PROCESSING APPARATUS AND METHOD AND RECORDING MEDIUM)

An application program that was encrypted by using a predetermined secret key is input to an input section that is a part of a program execution system, and encrypted sentences as the encrypted application program are supplied to a decoding section as they are. The decoding section is supplied not only with the encrypted sentences from the input section but also with a publicized key corresponding to a secret key that was used in generating the encrypted sentences. The decoding section decodes the encrypted sentences by using the publicized key and supplies Java byte codes as a decoding result to a Java virtual machine. The Java virtual machine interprets and executes the Java byte codes that are supplied from the decoding section.

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

六、申請專利範圍

1. 一種資訊處理裝置，執行一個用以執行程式的序，包含：

解碼元件用以將加密版的程式予以解碼；及

執行元件用以執行從該解碼元件輸出之程式。

2. 一種資訊處理裝置，執行一程式，包含加密元件供將一程式加密成為加密文句以解密為可執行碼。

3. 如申請專利範圍第1項所述之資訊處理裝置，其中該解密元件藉由使用一預先設定好的鍵將該加密版的程式予以解密，該預先設定好的鍵對應使用於加密程式的鍵。

4. 如申請專利範圍第1項所述之資訊處理裝置，其中該裝置本身有一預先設定好的鍵與用以加密程式之鍵相對應，而且該解密元件藉由使用該預先設定好的鍵將該加密版的程式予以解密。

5. 一種資訊處理裝置，執行一處理程序以執行一程式，包含：

用以執行程式的執行元件；檢查元件用以檢查該程式是否合法許可執行；及

供應元件用以提供該執行元件予被該檢查元件證實為合法的程式。

6. 如申請專利範圍第5項所述之資訊處理裝置，該檢查元件藉由檢測可執行程式碼的預設位元以檢查該程式是否合法許可執行。

7. 如申請專利範圍第5項所述之資訊處理裝置，其

(請先閱讀背面之注意事項再填寫本頁)

訂

六、申請專利範圍

中該程式附加簽名，該檢查元件根據該簽名而檢查該程式是否合法許可執行。

8．一種資訊處理裝置，以執行一程式，包含：程序處理元件以處理根據專利範圍第5項之資訊處理裝置內該程式被證實為合法的程式。

9．一種資訊處理方法，用以執行一執行程式的處理程序，包含下列步驟：

將一加密版的程式予以解密；及

執行藉由該解密步驟而得的程式。

10．一種資訊處理方法，用以執行一程式，包含將一程式加密為加密文句以解密為可由一資訊處理裝置執行之符碼的步驟。

11．一種資訊處理方法，用以執行一執行程式的處理程序，包含下列步驟：

檢查該程式是否合法許可執行之程式；及

只有當該程式被證實為合法程式才予以執行。

12．一種資訊處理方法，用以執行一程式，包含處理一程式的步驟，以證實如專利範圍第5項之資訊處理裝置內之程式為合法程式。

13．一種記錄介質，以記錄一程式，該程式是用以使得一電腦執行下列步驟：

將一加密版的程式予以解密；及

執行由該解密步驟而得之程式。

14．如申請專利範圍第13項所述之記錄介質，其

六、申請專利範圍

中一預先設定好的鍵也記錄在該記錄介質上，藉由使用該預先設定的鍵將該加密版的程式予以解密。

1 5 . 一種記錄介質，其上記錄一程式，該程式被加密為加密文句以解密成可被申請專利範圍第 1 項所述之資訊處理裝置執行之符碼。

1 6 . 一種記錄介質，其上記錄一程式，該程式用以使一電腦執行下列步驟：

檢查一程式是否合法；及

只有當該程式被證實為合法時才予以執行。

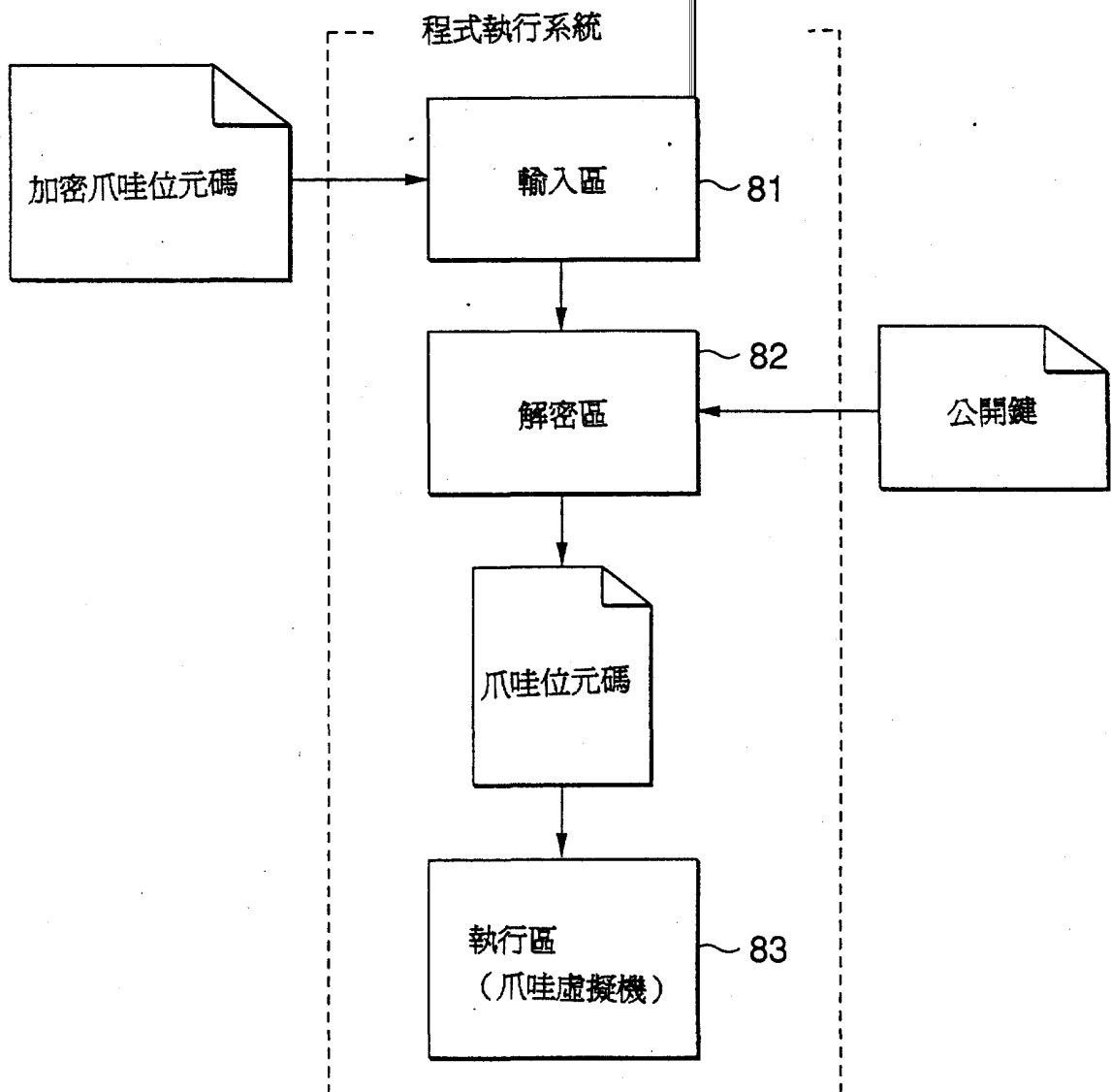
1 7 . 一種記錄介質，其上記錄一程式，該程式處理如申請專利範圍第 5 項所述之資訊處理裝置內被證實為合法的程式。

(請先閱讀背面之注意事項再填寫本頁)

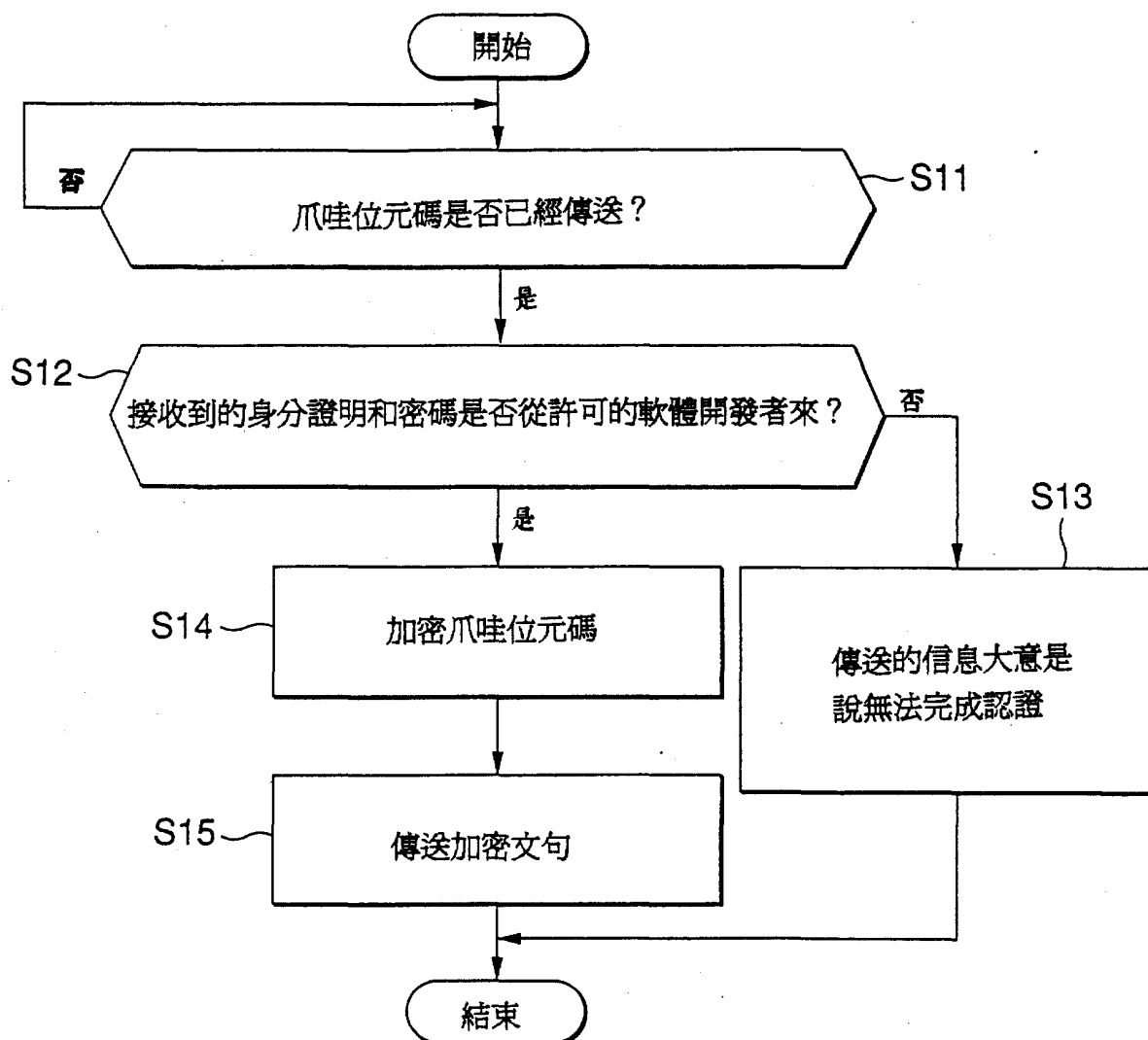
裝

訂

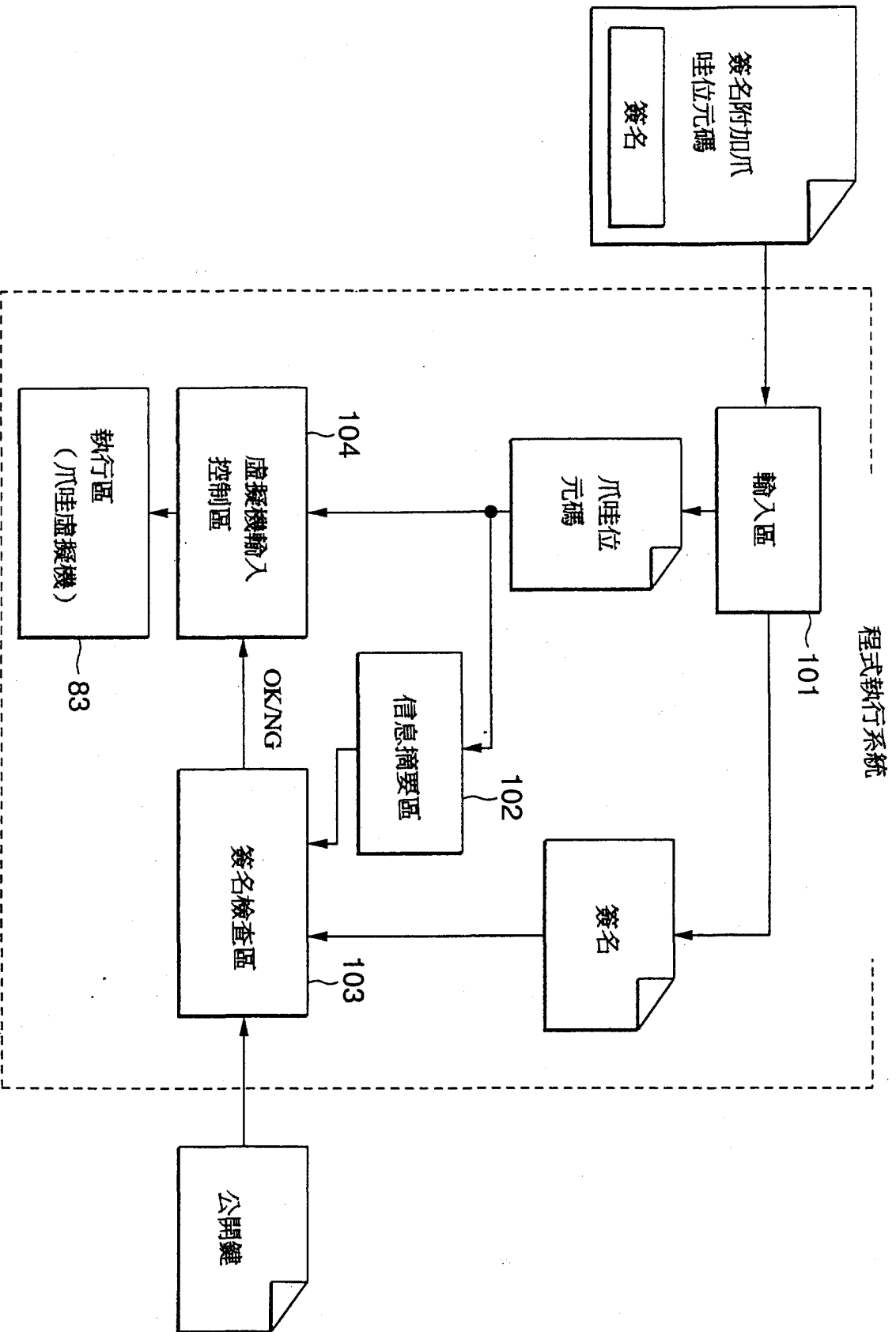
第 1 圖



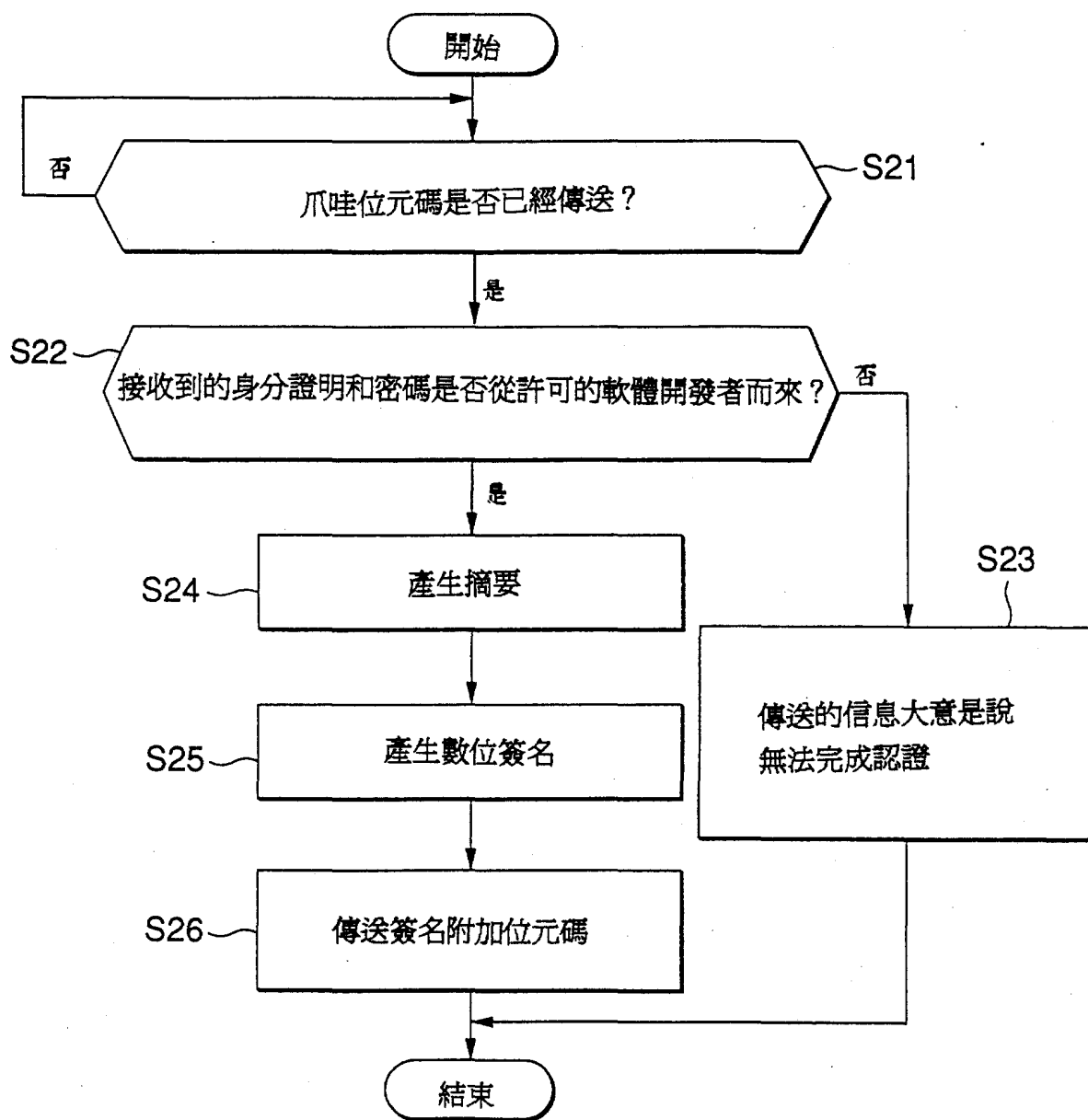
第 2 圖



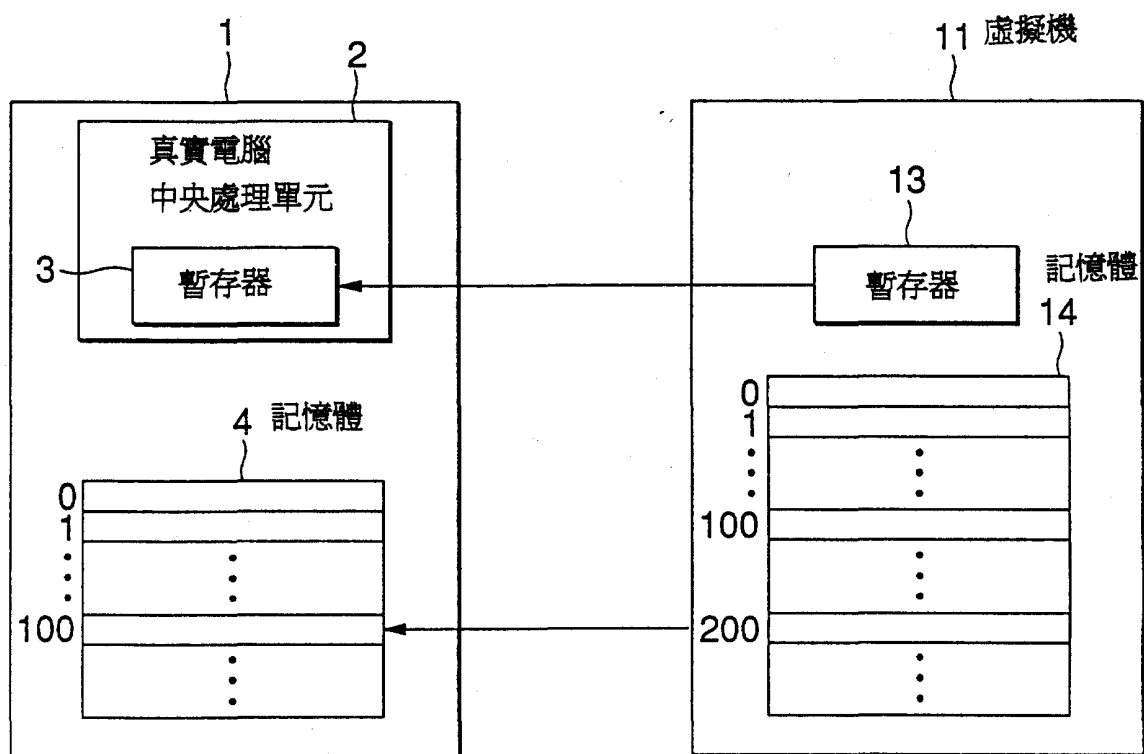
第 3 圖



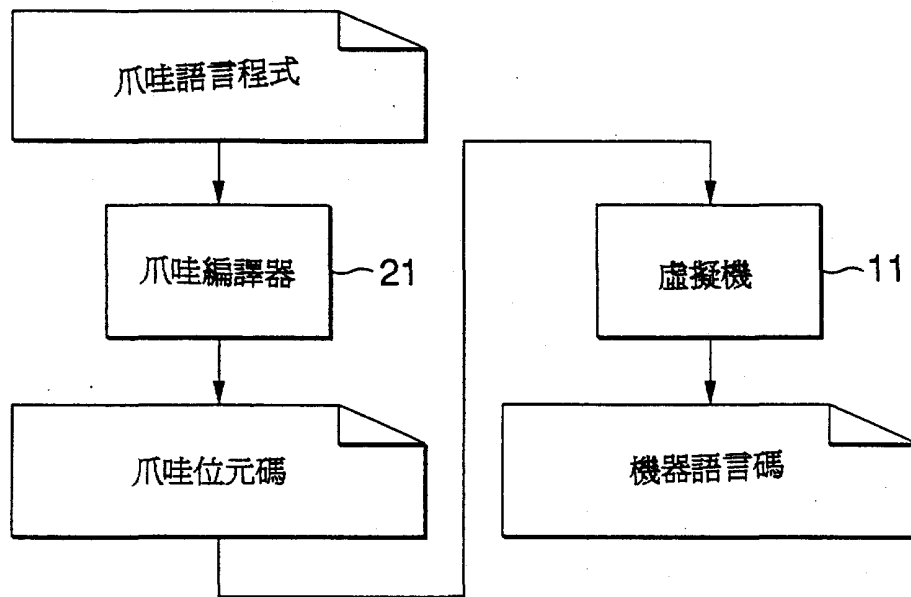
第 4 圖



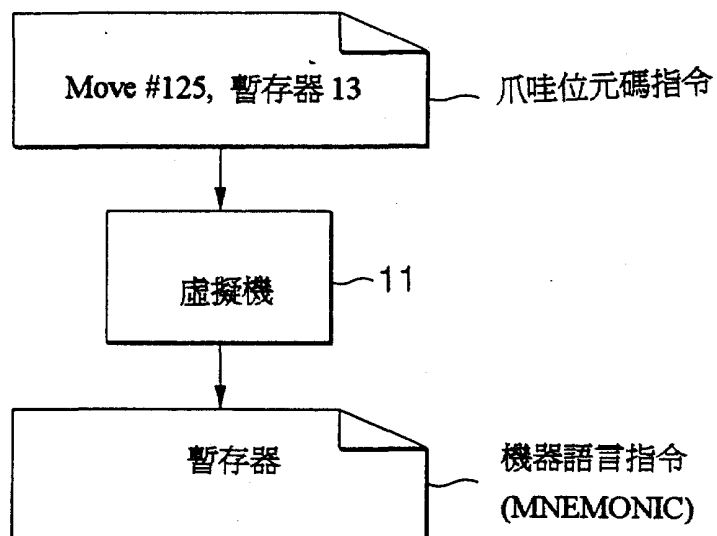
第 5 圖



第 6 圖

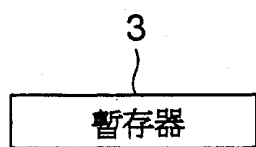


第 7 圖



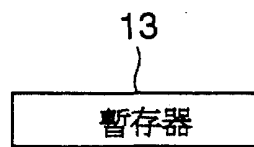
第8A圖

真實電腦的執行結果

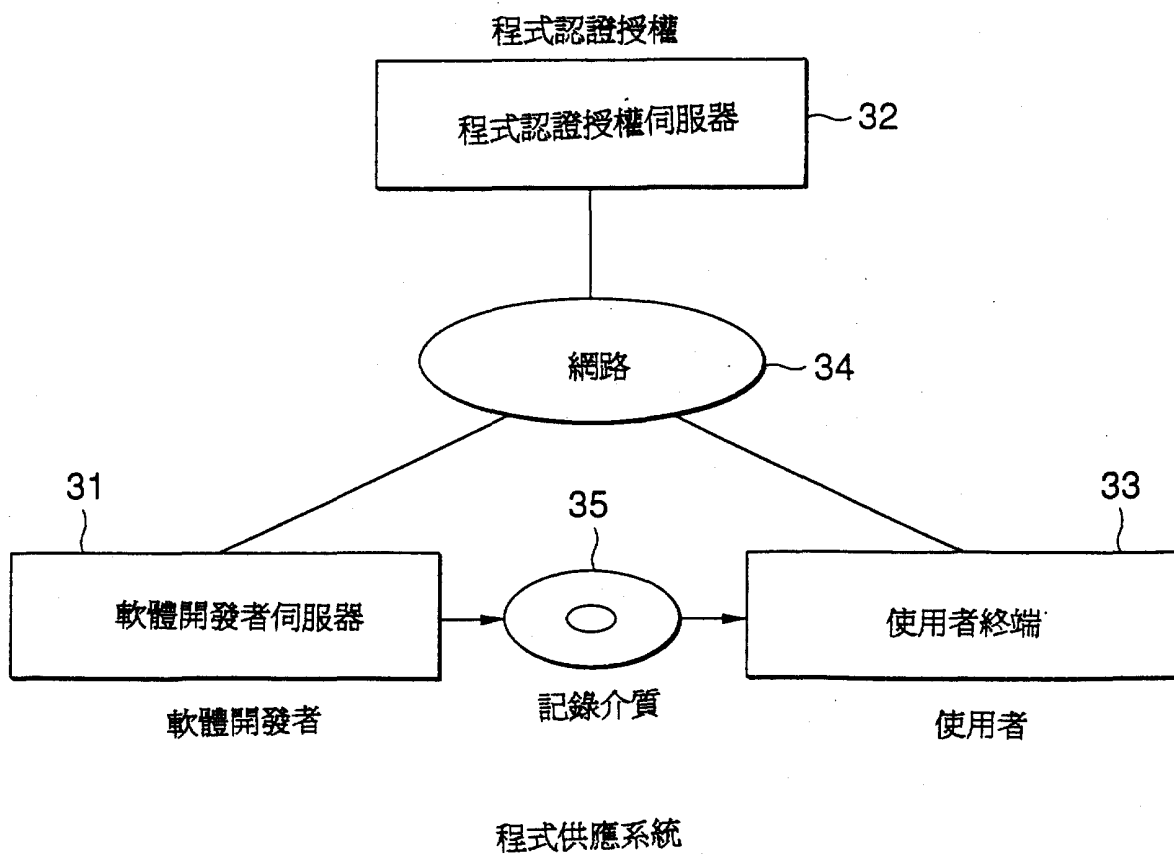


第8B圖

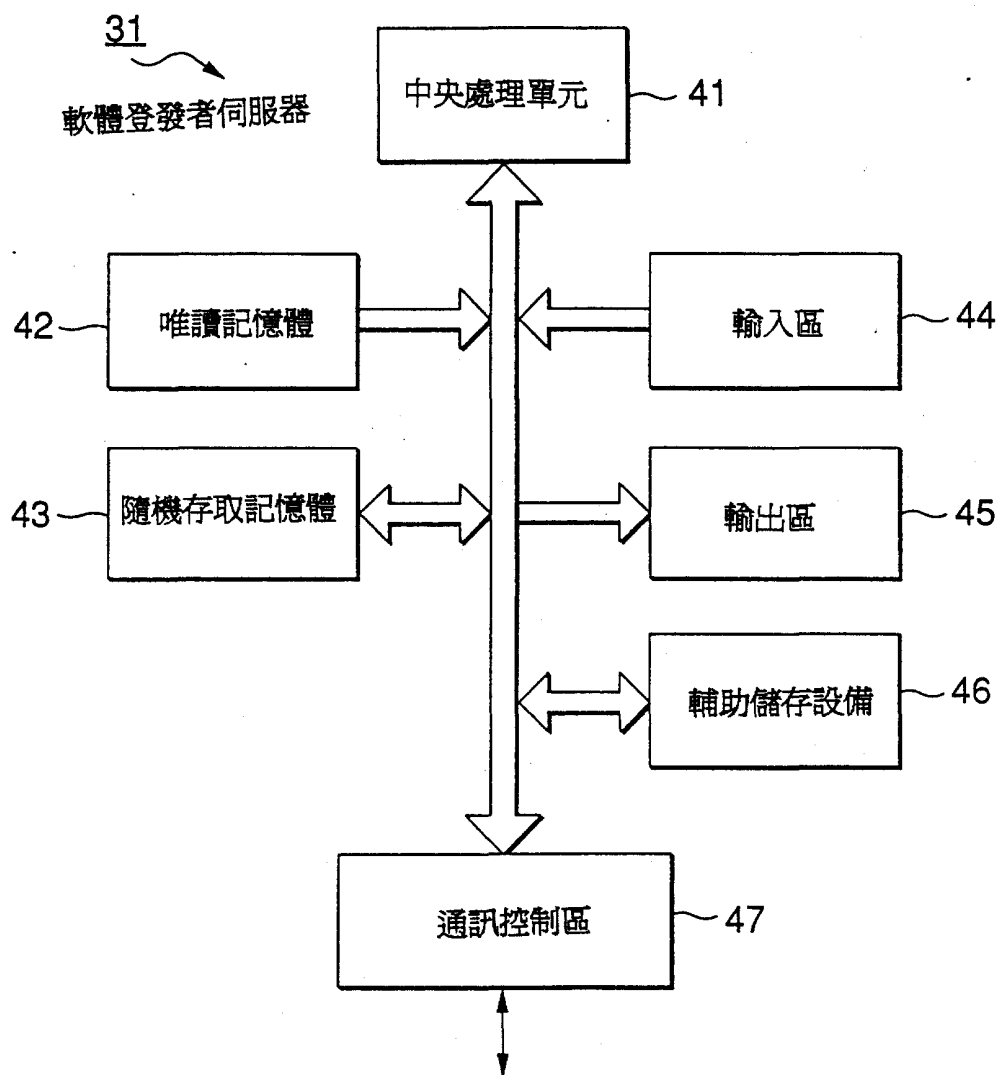
從爪哇虛擬機觀點的執行結果



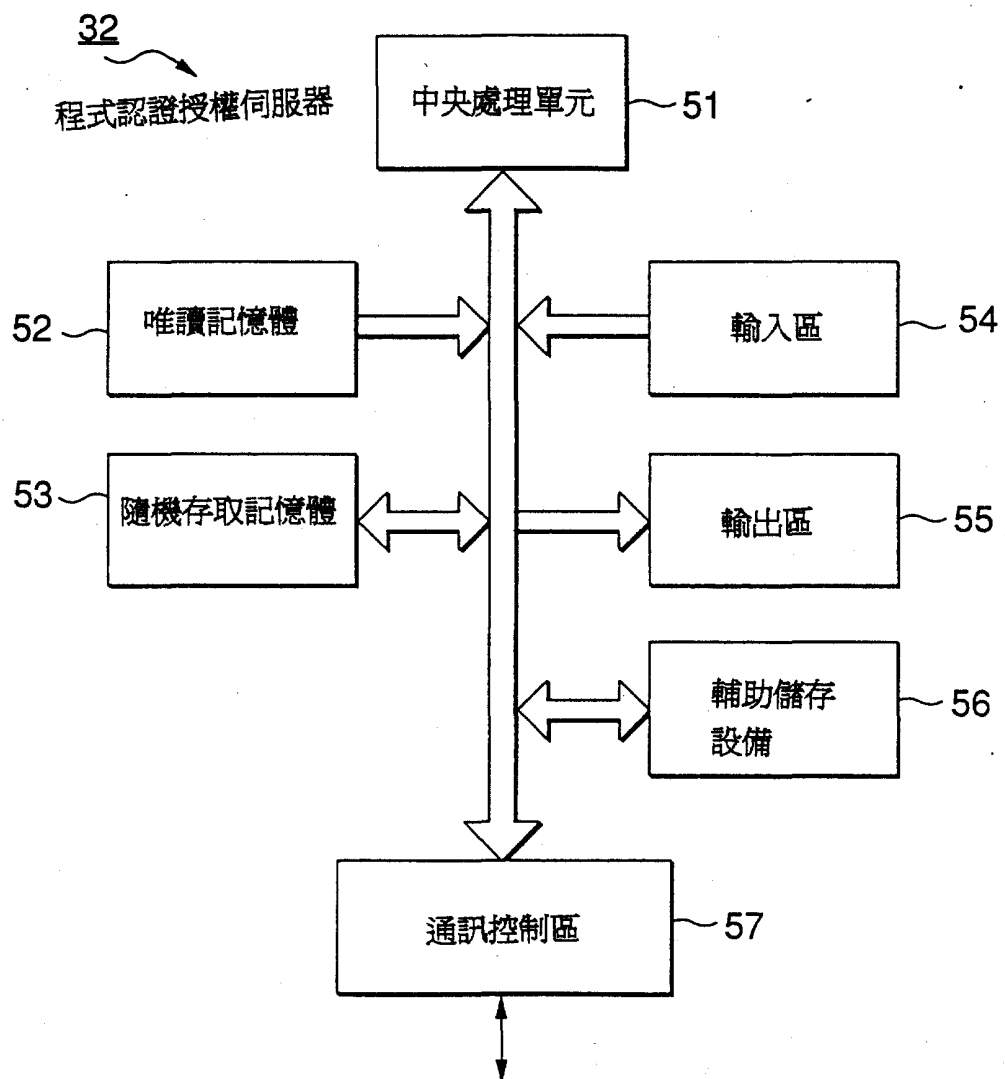
第 9 圖



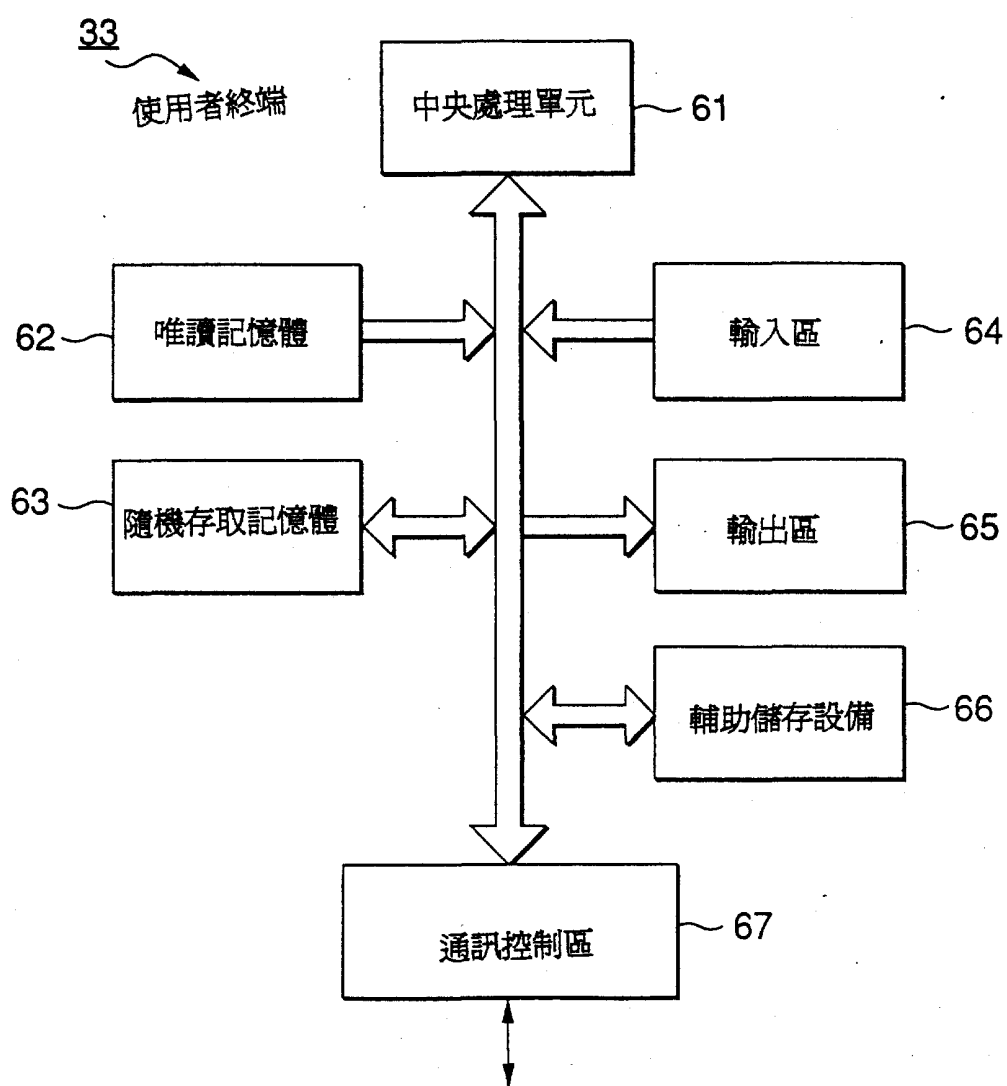
第10圖



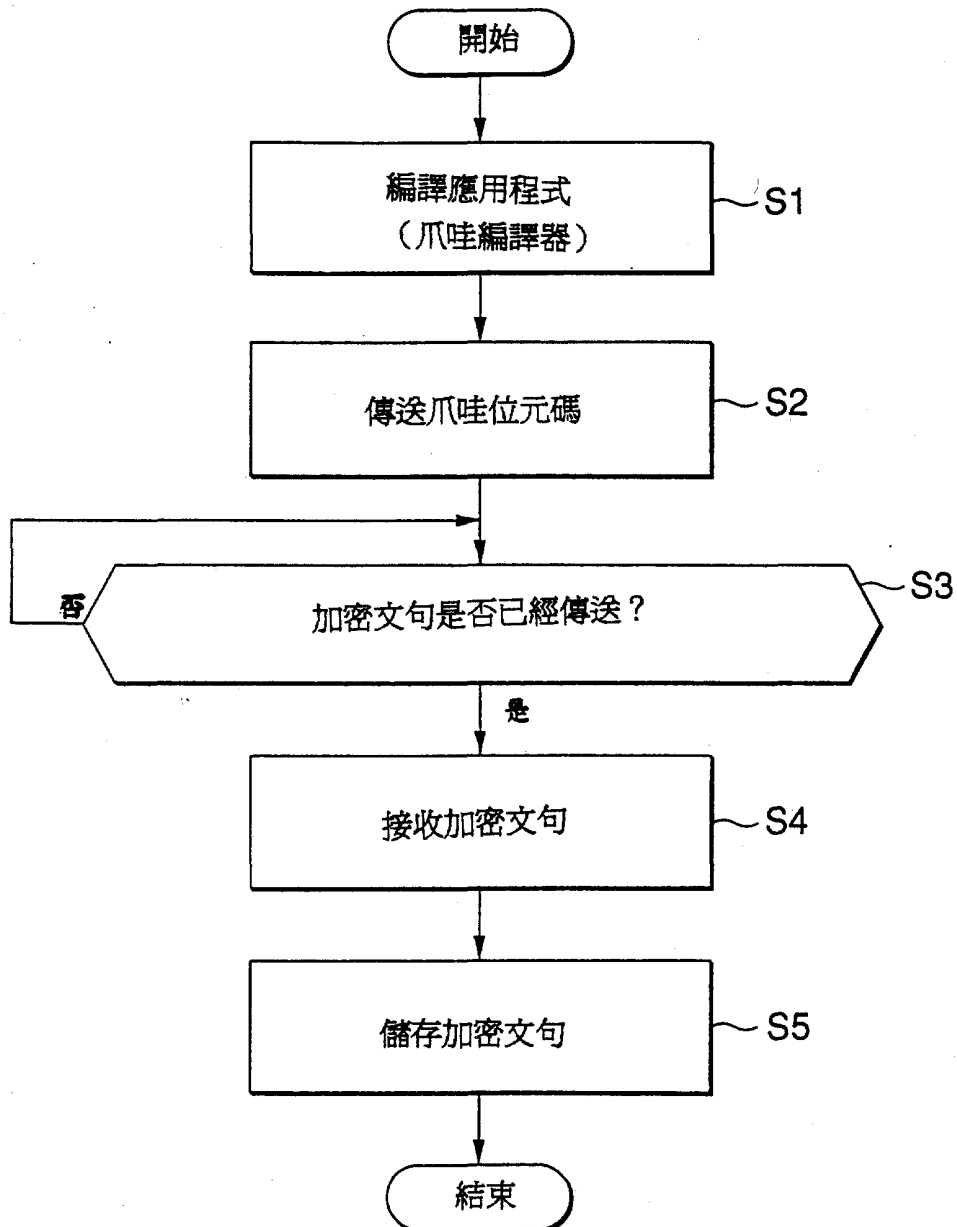
第 11 圖



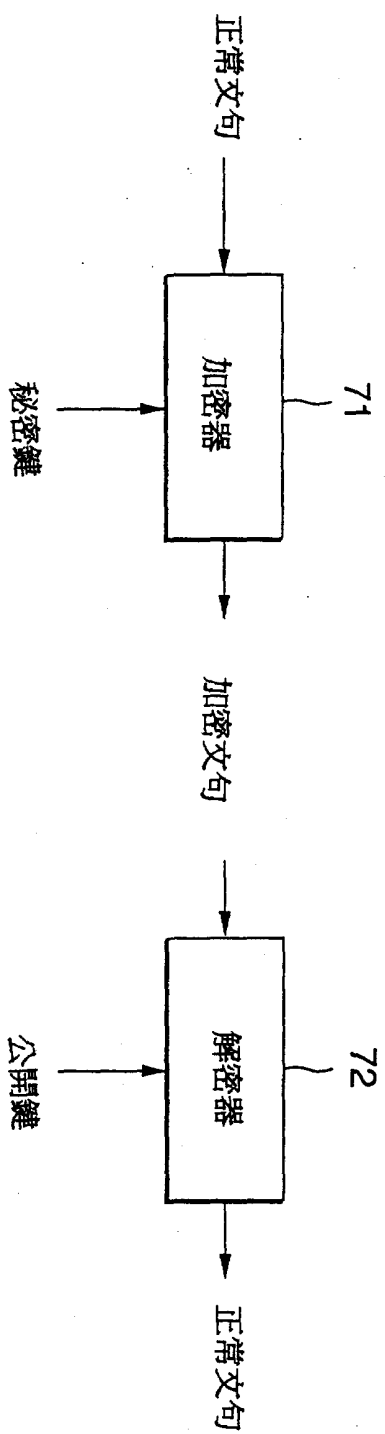
第12圖



第13圖

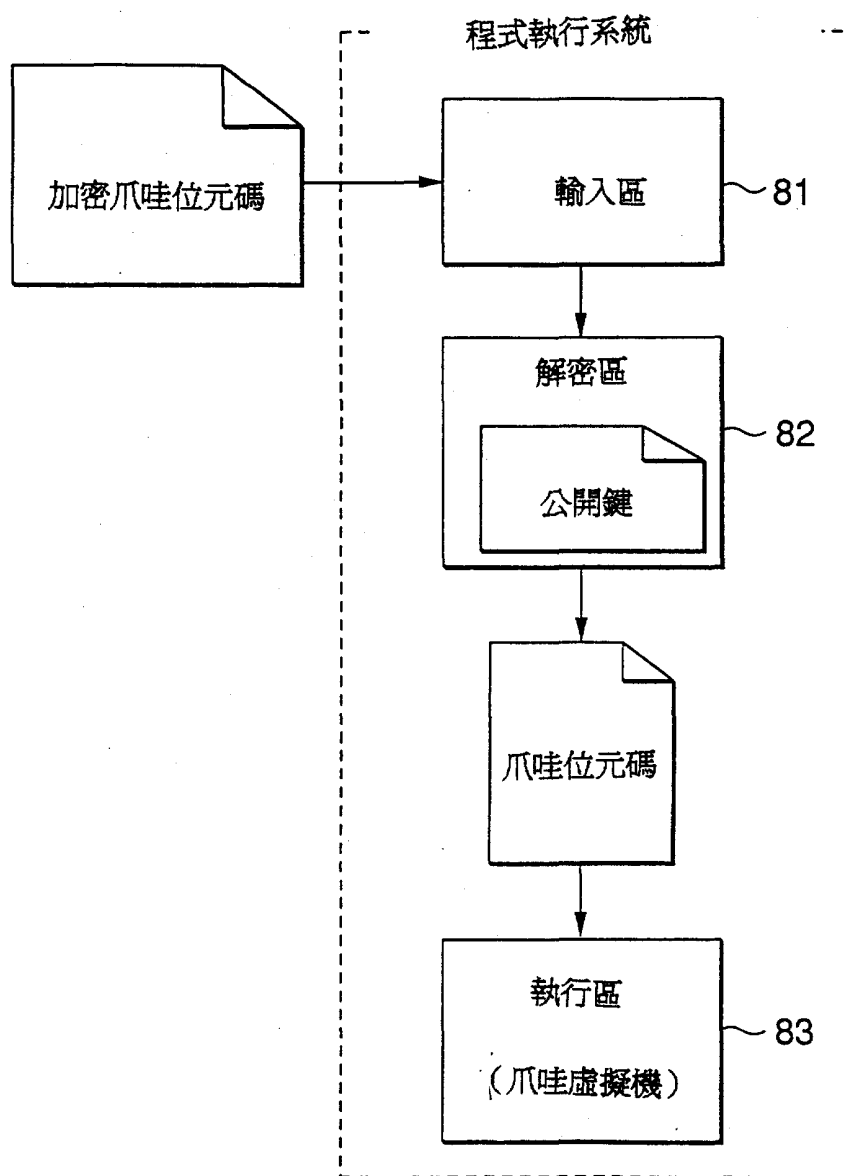


第14圖

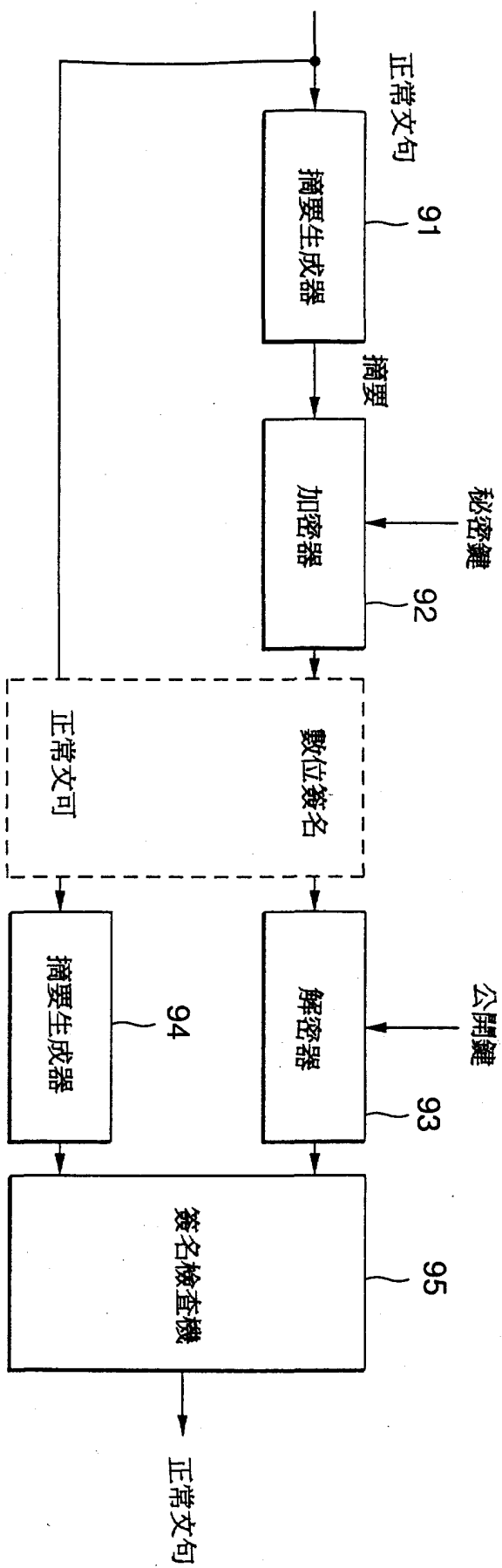


公開鍵加密／解密系統

第15圖



第16圖



使用數位簽名加密／解密系統

385471