200904113

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96128985

※ 申請日期：96.8.7　　※IPC 分類：H04L 9/14 (2006.01)

一、發明名稱：（中文/英文）

呈現供人類感知用刺激之材料的編解碼器無關加密技術

CODEC-INDEPENDENT ENCRYPTION OF MATERIAL THAT REPRESENTS STIMULI INTENDED FOR HUMAN PERCEPTION

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

杜比實驗室特許公司 / DOLBY LABORATORIES LICENSING CORPORATION

代表人：（中文/英文）

張莉妮 / CHEUNG, LILY S.

住居所或營業所地址：（中文/英文）

美國加州舊金山市・帕翠洛街 100 號

100 Potrero Avenue, San Francisco, CA 94103, U.S.A

國　籍：（中文/英文）

美國 / U.S.A.

三、發明人：（共 1 人）

姓　名：（中文/英文）

蔣文宇 / JIANG, WENYU

國　籍：（中文/英文）

中國 / CHINA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. PCT/美國、　2007/07/13、　PCT/US07/15988

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

發明領域

本發明係大致屬於加密技術，且更明確地屬於欲呈現如靜止與活動視覺影像與聲音之供人類感知用刺激的材料之加密技術。

【先前技術】

發明背景

欲呈現供人類感知用刺激之多媒體娛樂內容與其他材料正透過包括網際網路的各種分佈媒體以數位格式被傳遞給消費者。數位格式之使用一方面已促進此材料的發佈，但另一方面亦已促進該媒體之未獲授權的複製與提出。

一般被稱為數位權利管理(DRM)之各種方法已被發展且正在被發展來協助針對應該受到版權保護之材料的未獲授權的使用加以保護。普通之DRM將一些或全部材料加密且允許此材料自由地被發包佈，但控制對只有已獲得使用該材料之個體將被加密的資訊解密之構件的發佈。被加密的資訊解密之構件一般分為二種做法。

第一種DRM做法使用以與材料相關聯之材料導向式的密碼金鑰之加密與解密技術。用於解密所需之材料導向式的金鑰係對此材料為獨一的且以某種安全且受控制之方式被發佈給所有被授權之接收人。此做法之一例由Washington州之Redmond的微軟公司可取得之Windows Media播放器軟體被施作，且被稱為Windows Media DRM。

此特定之施作對每一個被授權的接收人給予對此接收人為獨一的內容證書或數位檔案。該內容證書包含一材料導向式之金鑰，其已使用以對此接收人為獨一的一些接收人導向式之主金鑰為基礎的加密技術被加密。

第二種DRM做法使用以與材料的所欲接收人相關聯之接收人導向式的密碼金鑰之加密與解密技術。用於解密所需之接收人導向式的金鑰係對此接收人為獨一的且對不同之材料為不同的。此做法之一例在Cali,nia州之Cupertino的Apple電腦公司所提供之iTunes服務中被施作，且被稱為FairPlay DRM。此特定之施作對每一個被授權的接收人給予使用以接收人導向式之主金鑰為基礎的加密技術被加密的一接收人導向式金鑰。

針對此二種做法之任一而言，接收人一般只有一主金鑰。每一種做法相對於彼此均具有優點。第一材料導向式之做法會是比較有效率但也比較不安全。作用於第一材料導向式之做法的發佈伺服器之電腦系統由於材料可對被授權的接收人一次地被加密而一般需要較少之計算資源。不幸的是，若一材料導向式之金鑰透過密碼分析或未被授權之揭露對公眾成為可得可用的時，材料之所有的發佈之安全性會被折衷。

然而，針對此二種做法之任一而言，由於要執行如非對稱金鑰或公共/私人金鑰方法之較安全的方法所需之計算資源通常是高不可攀地昂貴，當所有的材料被加密時，對稱之金鑰或秘密金鑰加密方法經常被使用。效率可藉由

施用較高安全之加密處理至該材料的被選擇之部分及對該材料之其餘部分施用較低安全的加密處理或不使用加密技術而不致犧牲安全性地被提高。該被選擇之部分係較佳地被選擇，使得該材料的其餘部分基本上沒有被選擇之部分的值。

用於選用被選擇之部分者所存在之二種基本的做法使用較高安全之加密處理被加密。第一種做法係以材料的邏輯結構為基礎，其依次係與被用以將材料編碼為用於傳輸或儲存之信號及將該信號隨後解碼用於播放或呈現的編碼/解碼(編解碼器)技術為相依的。此編解碼器相依做法允許被選擇之部分被選用的方式為安全性可就加密效率之被給予的水準被最佳化，但就不同型式之材料或就用不同編碼技術被編碼的被給予之型式的材料一般是無單一之選用為可接受的。編解碼器無關之方法對較廣的使用範圍為較佳的。

【發明內容】

發明概要

本發明之目標為要以編解碼器無關之方式而不致使保護水準降級地提供處理效率的改進、不致降低效率地提供處理效率的改進或在效率與安全二者提供平衡的改進，而保護欲呈現供人類感知用刺激之材料的未被授權之複製與呈現。

這些目標係藉由如在申請專利範圍之獨立項中被設立的本發明被達成。有利的施作係依在依附的申請專利範圍

被設立。

本發明與較佳施作之各種特點可藉由參照下列討論與附圖較佳地被了解，其中類似的元件編號在數圖中係指類似之元件。下列之討論與附圖的內容只被設立為例子且不應被了解要呈現對本發明之領域的限制。

圖式簡單說明

第1與2圖為其中處理器準備被加密之材料用於傳輸或儲存以便後續傳遞至接收器的系統之示意方塊圖。

第3圖為處理器與接收器之網路的示意方塊圖。

第4與5圖準備被加密之材料用於傳輸或儲存以便後續傳遞至接收器的處理器之示意方塊圖。

第6與7圖為接收將被解密及被提出至接收人之被加密的材料之接收器的示意方塊圖。

第8圖為被用以施作本發明之各種層面的裝置之示意方塊圖。

【實施方式】

較佳實施例之詳細說明

A.簡介

第1與2圖為系統之示意方塊圖，其產生如靜止或活動的影像與聲音之呈現欲供人類感知用刺激的特定材料的被加密之呈現。該等被加密之呈現被發佈至接收器用於解密與呈現給所欲的接收人。在整個此揭露中，更特別之提及係由以一個或多個訊框被安排之資料所呈現的材料加以做成。該「訊框」一詞係指所欲之資料的任何分割或段落。

在此內文中此處被稱用的訊框不須對應於對被用以將傳輸或儲存用之材料編碼的任何編碼技術為恆久的資料之分割。呈現單一影像之資料可被組織成為一訊框。例如，呈現動畫中之影像的資料係典型地被組織成為一系列之訊框。

參照第1圖，處理器3由路徑1接收一個或多個信號，該路徑1輸送該特定材料之一指標、獲得包括有呈現一部分之該特定材料的被選擇的資料之控制資料、對該控制資料施用一第一加密處理以產生第一被加密之資料、及組合該第一被加密之資料成為沿著路徑5被傳送之一第一被編碼的信號。該第一加密處理係對一第一加密金鑰響應，及該控制資料以某種方式呈現或對應一第二加密金鑰。

處理器4由路徑2接收一個或多個信號，該路徑2輸送該資料訊框、獲得未被納入該被選擇的資料中之該資料訊框中的非被選擇的資料、對該非被選擇的資料施用一第二加密處理以產生第二被加密之資料、及組合該第二被加密之資料成為沿著路徑6被傳送之一第二被編碼的信號。該第二加密處理係對一第二加密金鑰響應。

沿著路徑5與6被傳送之該等被編碼的信號分別被傳遞至發佈媒體7與8，其可為包括由超音波至紫外線頻率之整個頻譜的基帶或調變通訊信號用之電氣、光學或無線傳輸媒體，或為基本上使用包括磁帶、磁卡或磁碟、光學卡或光碟、與在包括紙之媒體上可偵測的標記之任何記錄技術的儲存媒體。發佈媒體7與8分別傳遞該等第一與第二被編

碼之信號至路徑11與12。

接收器15分別由路徑11與12接收該等第一與第二被編碼之信號。接收器15對該第一被加密之資料施用該一第一解密處理，以獲得包括有該特定材料的資料訊框中之被選擇的資料的控制資料。該第一解密處理係對一第一解密金鑰響應且該控制資料包括一第二解密金鑰由之可被獲得或被導出的資訊。接收器15對該第二被加密之資料施用該一第二解密處理，以獲得非被選擇的資料。接收器15對該第二被加密金鑰響應。該被選擇的資料與該非被選擇的資料被組合成為呈現欲呈現供人類感知用之刺激的特定材料的資料訊框。

該等被選擇的資料與非被選擇的資料的每一個包括至少一些呈現在資料訊框中之特定材料的資料；然而該等被選擇的資料與非被選擇的資料在集合上不須構成呈現在資料訊框中之特定材料的所有資料。訊框中之其他資料可用非被第一加密處理或第二加密處理加密的形式被發佈至接收器15。此其他資料因其可未被加密地被發佈至接收器15而在此處被稱為「明文資料」，然而此所謂之明文資料在所欲時可用一些其他處理被加密或被打散。

在一較佳實施例中，該第一加密金鑰與該第一解密金鑰係與該所欲之接收人相關聯，且該第一加密金鑰與該第一解密金鑰被設計使得任何非該所欲之接收人要將該第一被加密的資料解密為不可行的，而使得如圖中被標示為處理器3成為接收人導向式之處理器。較佳的是，該第二加密

金鑰與該第二解密金鑰係與該所欲之接收人相關聯，且該第二加密金鑰與該第二解密金鑰被設計使得任何沒有該第二解密金鑰者要將該第二被加密的資料解密為不可行的，而使得如圖中被標示為處理器4成為材料導向式之處理器。

第2圖中被顯示之系統係類似第1圖被顯示之系統，但不同之處在於處理器10執行被處理器3與4所執行的作業。

第3圖為如上述之第1與2圖所顯示的處理器與接收器之網路的示意方塊圖。發佈設施20呈現發佈媒體7與8之施作。例如，發佈設施20可為一廣域網路、一地方區域網路、實體儲存媒體之一輸送、或網路與輸送之組合。

針對處理器3與處理器4被描述之作業可同時或在不同時間被執行。該第一被加密的資料可與該第二被加密的資料的產生之前、之後或同時被產生。該第一被編碼之信號與該第二被編碼之信號的傳輸之前、之後或同時被發佈。該等處理可依據可得可用的資源被分配給不同之電腦系統。例如就動畫而言，該第二被加密的資料可針對所有之接收人一次被產生，且可在一個或多個媒體上被記錄用於對所欲的接收人之立即或隨後的發佈。第一被加密的資料之獨一的集合可在稍後之時間對所欲的接收人以需求隨選之方式被產生及被發佈。

例如在用於動畫之特定材料的加密與發佈的系統中，輸送第二被編碼之信號所需要的帶寬或儲存容量典型上比輸送第一被編碼之信號較大很多。就如這些之系統而言，為該等二被編碼之信號使用不同型式的發佈媒體會是較佳

的。例如，第一被編碼的信號可用一傳輸媒體被發佈，而第二被編碼的信號可用儲存媒體之實體傳遞被發佈。替選的是，第一被編碼的信號可用無線傳輸媒體被發佈，而第二被編碼的信號可用光學或電氣傳輸媒體被發佈。該第二被編碼之資料在所欲時亦可在層對層網路上被發佈，其可減少發佈之成本。任何明文資料基本上可用包括具有該第二被加密的資料之發佈的所欲之任何方式被發佈。

B.發射器

第4與5圖為處理器10之施作的示意方塊圖。這些施作之特點對處理器3與4為可應用的。

參照第4圖，金鑰伺服器31由輸送特定材料之指示的路徑1接收一個或多個信號。該特定材料之此指示或該特定材料之資料訊框沿著路徑2被傳送至選擇器42。沿著路徑2被傳送之資料訊框可被儲存且用金鑰伺服器31為直接可存取的，其可在施作該特定材料之指示下由圖中未被畫出的來源被獲得。選擇器42獲得該資料訊框、選擇其之一部分、及沿著路徑43傳送被選擇的資料至加密器33。在所欲時被選擇的資料可與其他資料被組合且構成控制資料。加密器33對控制資料施用一第一加密處理以沿著路徑36產生第一被加密的資料。第一加密處理係對透過路徑32被金鑰伺服器31提供之第一加密金鑰響應。若所欲時，第一加密處理亦可對由路徑35被接收之一第一初始化向量(IV)響應。若所欲時，第一IV可被金鑰伺服器提供。第一IV之使用係為備選的，但若有一被使用，其較佳地以該圖中未被顯示之一

些方法被加密。

至少一部分呈現一第二加密金鑰的被選擇的資料沿著路徑43被傳送至加密器45。加密器45對資料訊框中之非被選擇的資料施用一第二加密處理以沿著路徑6產生第二被加密的資料。該非被選擇的資料呈現未被納入該被選擇的資料之資料訊框中的至少一部分資料。該第二加密處理係對該第二加密金鑰響應且亦可對由路徑46被接收之一第二IV響應。若所欲時，第二IV可被金鑰伺服器31提供。第二IV之使用為備選的，但若其被使用，其被傳送至加密器33，且與該被選擇的資料被組合成為控制資料。

組合器34組合該第一被加密的資料與任何第一IV，其可已被使用成為沿著路徑5被傳送之被編碼的輸出信號。該第二被加密的資料亦可被組合成圖中被顯示之輸出信號。在將呈現動畫之材料加密與發佈的施作中，例如該等第一與第二施作可被組合成為不同之輸出信號，用於被如上述第1與2圖中被顯示地用不同的發佈媒體傳遞。

在第5圖中被顯示之處理器10的施作類似第4圖中被顯示之施作，但不同之處在於加密器45施用一第二加密處理，其對未被該被選擇的資料呈現但透過路徑44由金鑰伺服器31被接收之一第二加密金鑰響應。此第二加密金鑰被傳送至加密器33且與被選擇的資料被組合成為控制資料。

C.接收器

第6與7圖為接收器15之施作的示意方塊圖。在第6圖中被顯示之接收器15可有利地被使用以接收及解密由第4圖

中被顯示之處理器10產生的信號。在第7圖中被顯示之接收器15可有利地被使用以接收及解密由第5圖中被顯示之處理器10產生的信號。

參照第6圖，解密器51由路徑11接收第一被加密的資料、由路徑52接收一第一解密金鑰、及對第一被加密的資料施用一第一解密處理以沿著路徑53產生控制資料。該第一解密處理係對該第一解密金鑰響應。該控制資料包括在呈現欲於人類感知用之刺激的特定材料之資料訊框中被選擇的資料。該被選擇的資料呈現一第二解密金鑰由之可被獲得或被導出的資訊。該第二解密金鑰沿著路徑53被傳送至解密器61。第一解密金鑰亦可對由路徑55被接收之一第一IV響應。第一IV的使用原則上為備選的，但若該第一被加密的資料係被在使用一IV之處理器10中的一互補之第一加密處理加以產生時，其應被使用。

加密器61由路徑12接收第二被加密的資料、由路徑53接收該第二解密金鑰、及對該第二被加密的資料施用一第二解密處理以沿著路徑63產生非被選擇的資料。該非被選擇的資料呈現未被納入該被選擇的資料之資料訊框中的至少一部分資料。該第二解密處理係對該第二解密金鑰響應且亦可對一第二IV響應。若第二IV被使用，其由控制資料被獲得，且沿著路徑65被傳送。第二IV的使用原則上為備選的，但若該第二被加密的資料係被在使用第二IV之處理器10中的一互補之第二加密處理加以產生時，其應被使用。

組合器54組合該被選擇的資料與該非被選擇的資料成

為呈現該特定材料之資料訊框。如明文資料之其他資料亦可與該被選擇的資料及該非被選擇的資料被組合成為資料訊框。

第7圖中被顯示之接收器15的施作係類似第6圖中被顯示之施作，但不同之處在於解密器61施用一第二解密處理，其係對由未被該被選擇的資料呈現之控制資料中的資訊被獲得或被導出之一第二解密金鑰響應。該第二解密金鑰係由路徑62被接收。

D.加密處理

1.概要

該等第一與第二加密處理可用各種方法被執行。該等二處理可相同地或用不同的方法被執行。例如在動畫用之特定材料的加密之系統的施作中，較有效率之對稱的的秘密金鑰加密方法被使用以執行第二加密處理，及較沒有效率之非對稱的公共金鑰/私人金鑰加密方法被使用以執行第一加密處理。對稱金鑰加密方法之少數例子包括先進加密標準(AES)區塊加密法、資料加密標準(DES)之變形、Lai與Massey所提出之國際資料加密運算法、及下面被描述之加密法。非對稱金鑰加密方法之少數例子包括Rivest, Shamir與Adleman所提出之RSA加密法、及ElGamal所提出之ElGamal加密法。廣泛種類之加密-金鑰發佈與交換協定可被使用。正常的考慮可被採用以選用適合之金鑰發佈與交換協定。

在一較佳施作中，第一加密金鑰為公共金鑰及第一解

密金鑰為特定材料之所欲的接收人相關聯之一對公共金鑰/私人金鑰的私人金鑰，且該第二加密金鑰與該第二解密金鑰為與特定材料相關聯之對稱金鑰。可就特定材料之所有訊框被使用的一對稱金鑰或對稱金鑰之一實例可如上面被討論與下面被描述地由每一個訊框中的資料被獲得。在一較佳施作中，該等第一加密/解密處理與相關之金鑰為接收人導向式者，及該等第二加密/解密處理與相關之金鑰為材料導向式者。此在第1圖中被反映，其顯示處理器3為一接收人導向式處理器及顯示處理器4為一材料導向式處理器。

被用以執行第二加密處理之數種方法在下面被描述。

該第二加密處理基本上可被任何可逆之轉換被施作。一種適合的轉換型式可被表達為：

$$Y = A \cdot X \qquad (1)$$

此處A = k列與m行之矩陣；

X =將被加密之資料的訊框中之非被選擇的資料；以及

Y =被加密處理產生之第二被加密的資料。

互補之解密處理可被表示為：

$$X = A^{-1} \cdot Y \qquad (2)$$

此處A^{-1}為矩陣A之反矩陣。

將被加密的資料訊框以列與行被組織而包含在有限欄位之具有m符號或元素的固定長度之k個封包。k個封包之每一個為在資料訊框中的一列，及在一封包中之m個符號的每一個為在資料訊框中的各行。結果所得之被加密的資料Y為如下面被討論的具有k-1列與m行之資料訊框。

下列之例子假設每一個符號為一位元組的資料，此處每一個位元組包含8個位元。封包之特定長度並非關鍵的，但較佳地被選用為至少與加密金鑰之長度相同，使得因其位元值隨機猜測而對第一被加密的封包暴力加密分析不會比被用以將封包加密之金鑰的暴力隨機猜測較輕易。

在公式1中被顯示之轉換的施作可被表示為：

$$y_0 = x_0 \qquad (3)$$

$$y_i = a \cdot x_i + b \cdot y_{i-1} + c \cdot x_{i-1} \qquad 1 \le i < k$$

此處x_0=在X資料訊框中之列或封包0；

x_i=在X資料訊框中之列或封包i；

y_i=在Y被加密的資料訊框中之列或封包i；以及

a, b, c =非零矩陣係數。

下列被討論之這些矩陣係數以及其他矩陣係數的值之被建立的方式為其是所欲的，但較佳的是其係利用產生至少響應每一個要被加密的資料訊框之部分被選擇的資料之虛擬隨機值的處理被建立。該等值應為非零的，以確保加密矩陣為可逆的。

公式3呈現下面被討論的被稱為基本轉換之轉換。該基本轉換不將資料之第一列或封包x_0加以加密。此封包對應於上面被討論之控制資料內被選擇的資料，其被第一加密處理加密。

在一施作中，公式3中之每一項為一個8位元的數值，其在一個8位元之有限欄位中被定義。若所欲時，較長之有限欄位可被使用，其可允許該矩陣被施用至比8位元更長的

資料符號。有限欄位之使用允許轉換對具有固定個數之位元(在此例中為8個位元)的資料元素用算術運算被施作，而不須憂心進位位元或算術之上或下溢位。在公式3中被顯示的算術運算可就i=1,2可被表示為：

$$y_0 = x_0$$

$$y_1 = a \cdot x_1 + b \cdot y_0 + c \cdot x_0 = a \cdot x_1 + (b+c) \cdot x_0 \qquad (4)$$

$$y_2 = a \cdot x_2 + b \cdot y_1 + c \cdot x_1 = a \cdot x_2 + c \cdot x_1 + b \cdot (a \cdot x_1 + (b+c) \cdot x_0)$$

$$= a \cdot x_2 + (b \cdot a + c) \cdot x_1 + b \cdot (b+c) \cdot x_0$$

此公式與在公式5中被顯示之矩陣A的主對角線下面之三角形矩陣的乘法為等值的。

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ \cdots \\ y_{k-1} \end{bmatrix} = Y = A \cdot X = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ b+c & a & 0 & 0 & \cdots & 0 \\ b \cdot (b+c) & b \cdot a + c & a & 0 & \cdots & 0 \\ b^2 \cdot (b+c) & b \cdot (b \cdot a + c) & b \cdot a + c & a & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_{k-1} \end{bmatrix} \qquad (5)$$

公式5顯示公式3僅為公式1中被顯示之轉換的特例。若係數a，b，c均為非0，公式3中之等式係與全階可逆的矩陣轉換為等值的。公式3中之轉換只為很多滿足可逆的性質其中之一，但其因可用一個3接頭之線性濾波器被施作而為吸引人的。此轉換之計算複雜性針對每一行為O(k)，其比整個矩陣具有非0係數之轉換之計算複雜性$O(k^2)$為較低很多。

在公式3中被施作之加密處理可用漸進或增量的方式被施用至資料之列或封包。輸入資料的整個封包可不須在加密處理開始前為可得可用的。此允許為加密要儲存資料所需之記憶體數量的減少或緩衝延遲之降低。相同之利益亦適用於互補的解密處理，其可被表示為：

$x_0 = y_0$

$$a \cdot x_i = y_i - b \cdot y_{i-1} - c \cdot x_{i-1} \Rightarrow x_i = \frac{(y_i - b \cdot y_{i-1} - c \cdot x_{i-1})}{a}, \qquad 1 \le i < k \qquad (6)$$

公式6中之等式顯示若係數a具有非0值，公式3之轉換為可逆的；然而確保係數b與c亦具有非0值為重要的，使得每一個被解密之封包係依前一個封包的內容而定的。此確保未被授權之接收人在沒有將所有先前的封包解密下無法將封包解密。

3.替選之施作

可被用以施作第二加密處理之替選的基本轉換與替選的逆基本轉換及其互補之解密處理可分別藉由逆轉矩陣乘法運算之項目順序由等式1與2中被顯示之轉換被導出。這些替選的轉換在此處未詳細地被討論。其施作細節利用可逆轉矩陣乘法運算之項目順序、重置矩陣、對調列與行向量、及交換對列與行之參用，而由基本轉換的討論直接被獲得。

上面被討論之基本轉換與具有下面被討論之額外特點

的施作對應於將矩陣A之係數乘以要被加密的資料訊框X的算術處理。公式3中被顯示之等式的檢查揭露資料訊框X或資料訊框Y之每一行的算術運算針對其他行的算術運算獨立地被執行。基本轉換所提供之安全水準藉由使用下面被討論的一個或多個特點被改進。

若上面被提及之替選的轉換或具有額外特點之變形被用以施作第二加密處理，此施作對應於將要被加密的資料訊框X乘以矩陣A之係數的算術處理。X或資料訊框Y之每一列的算術運算針對其他列的算術運算獨立地被執行。替選的基本轉換所提供之安全水準藉由使用下面被討論的一個或多個特點之適當的變形被改進，其可藉由交換對列與行之參用及進行如上面被解釋之其他改變而由下列的討論被導出。

轉換之施用在下面的討論一般被指為以矩陣運算或以列與行被安排之矩陣係數的各種運算為準。這些參用為要描述替選的施作之方便的方法，且不欲意指其中此轉換必須被施作之任何特定的方法。如利用上面被描述之多接頭濾波器施用的其他方法為可能的。

(a)額外之特點

其中替選之施作可被實現的一方法為藉由執行除了基本轉換的施用外的各種運算而將額外之特點納入加密處理。

(1)行排列

基本轉換所提供之安全水準可藉由變更或排列在加密

轉換之行的順序而被提高。此可如下面被討論之各種方法被完成。被用以導出該方法之方法或函數可具有的實務重要性在於影響加密處理之整體安全性，但原則上無特定之方法為絕對必要的。可能的方法在下面被描述。

(i)矩陣係數

一特點為在施用至將被加密的資料訊框X前重組轉換矩陣A之行。矩陣之m行可用 m! 之可能的順序任何之一被安排，此或者被稱為排列。該順序係至少以部分之上述的控制資料被定出。在一施作中，其排列順序如下列等式所呈現地由在從資料訊框之被選擇的資料的第一封包或列X_0被導出：

$$A'[i,j]=A[i,F(x_0,j)], \qquad 0\le i<k, \quad 0\le j<m \qquad (7a)$$

此處 $A[i,j]$=矩陣A在第i列與第j行之係數；

$F(x_0,j)$=第i行之被排列的行編號；以及

$A'[i,j]$=具有被排列之行的矩陣A的係數。

依據此記法，$F(x_0,j)$代表被移位至第j行之原始行的下標編號。

行排列可為列相依的，意為其被允許隨著矩陣逐列地改變。此基本上以對列編號相依之任何方法被完成。一種方法藉由其中每一列激發不同次數之排列函數而達成此結果。排列函數之每一個後續的激發對前一個激發所獲得之被排列的結果執行其排列處理。在一例中，排列函數被激

發之次數等於列編號，其可被呈現為：

(ii)資料封包

$$A'[i,j]=A[i,F^i(x_0,j)], \qquad 0\le i<k, \quad 0\le j<k \qquad (7b)$$

另一特點是在對要被加密的資料施用轉換矩陣之前或之後重組資料的行。當以上述之公式3的基本轉換被使用，相同之結果可藉由在施用基本轉換之前重組非被選擇的資料X之行或在施用基本轉換之後重組非被選擇的資料Y之行被達成。

矩陣之m行可用 m! 之可能的順序任何之一被安排，此或者被稱為排列。該順序至少以部分之上述的控制資料被定出。在資料訊框X之行排列的一施作中，其排列順序如下列等式所呈現地由在從資料訊框之被選擇的資料的第一封包或列X_0被導出：

$$X'[i,j]=X[i,F(x_0,j)], \qquad 1\le i<k, \quad 0\le j<m \qquad (8a)$$

此處 $X[i,j]$=資料訊框X在第i列與第j位元組之資料；

$F(x_0,j)$=第j行之被排列的行編號；以及

$X'[i,j]$=在排列後資料訊框X在第i列與第j位元組之資料。

行排列可為列相依的，意為其被允許隨著矩陣逐列地改變。此基本上以對列編號相依之任何方法被完成。一種方法藉由其中每一列激發不同次數之排列函數而達成此結

果。排列函數之每一個後續的激發對前一個激發所獲得之被排列的結果執行其排列處理。在一例中，就資料X要被加密而言，排列函數被激發之次數等於列編號，其可被呈現為：

$$X'[i,j]=X[i,F^{i}(x_0,j)], \quad 1\le i<k, \quad 0\le j<m \qquad (8b)$$

(2)列排列

基本轉換所提供之安全水準可藉由變更或排列在加密轉換之列的順序而被提高。此可如下面被討論之各種方法被完成。被用以導出該方法之方法或函數可具有的實務重要性在於影響加密處理之整體安全性，但原則上無特定之方法為絕對必要的。可能的方法在下面被描述。

(i)要被加密之資料封包

一特點為在施用轉換矩陣前重組資料訊框X中之資料的列。較佳的是第一列未被移未。要施作之列排列可被表示為：

$$X'[i,j]=X[G(x_0,i),j], \quad 1\le i<k, \quad 0\le j<m \qquad (9)$$

此處 $X'[i,j]$=在排列後資料訊框X在第i列與第j位元組之資料。

$G(x_0,i)$=第i列被排列後之列編號。

依據此記法，$G(x_0,i)$代表被移位至第I列之原始列的下標

編號。

列排列可為列相依的，意為其被允許隨著矩陣逐列地改變。此基本上以對列編號相依之任何方法被完成。一種方法藉由其中每一列激發不同次數之排列函數G而達成此結果。排列函數之每一個後續的激發對前一個激發所獲得之被排列的結果執行其排列處理。在一例中，排列函數被激發之次數等於列編號，其可被呈現為：

$$X'[i,j]=X[G^{j+1}(x_0,i),j], \quad 1\le i<k, \quad 0\le j<m \qquad (10)$$

(ii)已被加密的資料封包

另一特點重組被加密的資料之列的順序。此可藉由排列轉換矩陣A之列或藉由在施用轉換矩陣後排列被加密的資料訊框Y中之被加密的資料的列被達成。轉換矩陣中之列的排列可被表示為：

$$A'[i,j]=A[G(x_0,i),j], \quad 1\le i<k, \quad 0\le j<m \qquad (11a)$$

此處 $A'[i,j]$=在排列後矩陣A在第i列與第j行之係數；以及

$G(x_0,i)$=第i列被排列後之列編號。

被加密的資料Y之列的排列可被表示為：

$$Y'[i,j]=Y[G(x_0,i),j], \quad 1\le i<k, \quad 0\le j<m \qquad (11b)$$

此處 $Y'[i,j]$=在排列後在第i列與第j行之被加密的資料。

列排列可被允許隨著行至行而改變，其基本上可用與行編號相依之任何方法被完成。一種方法配合上面公式10被描述。用於轉換矩陣A與被加密的資料Y之列排列的方法可被表示為：

$$A'[i,j]=A\left[G^{j+1}(x_0,i),j\right],\quad 1\le i<k,\quad 0\le j<m \qquad (12a)$$

$$Y'[i,j]=Y\left[G^{j+1}(x_0,i),j\right],\quad 1\le i<k,\quad 0\le j<m \qquad (12b)$$

(3)行與列排列

另一特點為使用一個或多個列與行排列。若所欲時，列及/或行可在施用轉換矩陣之前與之後被排列。進一步言之，任何列相依與列無關行排列的組合可與行相依與行無關列排列被使用，但其中排列被完成之順序為重要的。在解密之際，互補的逆排列以相反順序被執行。

(4)一維之動態係數

另一特點為修改基本轉換矩陣A之係數a，b與c，使得不同組之係數可針對每一列被使用。以此特點下，在公式3被顯示之公式可被重寫為：

$$y_{0,j} = x_{0,j}\ ,\qquad 0\le j<m$$

$$y_{i,j} = a_i\cdot x_{i,j} + b_{i\text{-}a,j} + c_i\cdot x_{i\text{-}1,j}\quad ,\ 1\le i<k,\ 0\le j<m \qquad (13)$$

此處 $x_{0,j}$ =資料訊框X中第0列之第j位元組的資料；

$x_{i,j}$ =資料訊框X中第i列之第j位元組的資料；

$y_{i,j}$ =資料訊框Y中第i列之第j位元組的資料；以及

a_i, b_i, c_i =第i列之用於轉換的矩陣係數。

類似公式3中之等式地，公式13中之等式亦可如在公式14中被顯示地被表示為矩陣乘法。

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ \cdots \\ y_{k-1} \end{bmatrix} = Y = A \cdot X = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ b_1 + c_1 & a_1 & 0 & 0 & \cdots & 0 \\ b_2 \cdot (b_1 + c_1) & b_2 \cdot a_1 + c_2 & a & 0 & \cdots & 0 \\ b_3 \cdot b_2 \cdot (b_1 + c_1) & b_3 \cdot (b_2 \cdot a_1 + c_2) & b_3 \cdot a_2 + c_3 & a_3 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_{k-1} \end{bmatrix} \quad (14)$$

較佳地，係數由至少部分之控制資料被導出的方式為使得係數之值在沒有存取控制資料下為難以預測的。在一施作中，係數係由資料訊框之被選擇的資料中由第一列x_0被導出。雖然被用以導出係數之方法或函數的選用會具有實務的重要性而影響加密處理之整體安全性，原則上無特定的方法為絕對必要的。可能之方法在下面被描述。由於係數只在一維變化，此特點被稱為一維動態係數。

一維動態係數亦可在與上述任何行與列排列技術組合被使用。

(5)二維動態係數

另一特點為以列相依與行無關之方式變更轉換矩陣係數。此可被完成之一種方法為如上述就一維動態係數地產生列相依的係數、產生第二組之行相依的係數d，e與f、及

將行相依之係數乘以列相依之係數。以此特點下，公式3或公式13中被顯示之等式可被重寫為：

$$y_{0,j} = x_{0,j}, \quad 0 \le j < m$$

$$y_{i,j} = a_i \cdot d_j \cdot x_{i,j} + b_i \cdot e_j \cdot y_{i-1,j} + c_i \cdot x_{i-1,j}, \ 1 \le i < k, \ 0 \le j < m \qquad (15)$$

此處d_j, e_j, f_j＝第j行用於轉換之行相依的矩陣係數。

若該等行與列相依係數無一為0，該轉換為可逆的。此轉換為可逆的係為充分卻非必要之條件。

公式15中之等式可使用此處被稱為動態矩陣之資料結構被表示成為矩陣乘法。動態矩陣中之係數具有被執行以產生資料訊框Y中不同的列及/或行之算術運算變化的值。例如，公式15的動態矩陣中之係數在下列二表式中被顯示：

$$A\{0,1\} = \begin{bmatrix} 1 & 0 \\ b_1 \cdot e_j + c_1 \cdot f_j & a_1 \cdot d_j \\ b_2 \cdot e_j \cdot (b_1 \cdot e_j + c_1 \cdot f_j) & b_2 \cdot e_j \cdot a_1 \cdot d_j + c_2 \cdot f_j \\ b_3 \cdot e_j \cdot b_2 \cdot e_j \cdot (b_1 \cdot e_j + c_1 \cdot f_j) & b_3 \cdot e_j \cdot (b_2 \cdot e_j \cdot a_1 \cdot d_j + c_2 \cdot f_j) \\ \cdots & \cdots \\ \cdots & \cdots \end{bmatrix} \qquad (16)$$

$$A\{2,3,\cdots(k-1)\} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ a_2 \cdot d_j & 0 & \cdots & 0 \\ b_3 \cdot e_j \cdot a_2 \cdot d_j + c_3 \cdot f_j & a_3 \cdot d_j & \cdots & 0 \\ \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & 0 \end{bmatrix} \qquad (17)$$

此處A{θ}=被用以產生資料訊框Y之該組的行{θ}中之被加密的資料的矩陣A之係數。

動態矩陣所呈現之轉換可用各種方法被施作。該轉換可用資料訊框X使用由一組矩陣{A}被選擇之一矩陣而被施作成為矩陣乘法。該轉換亦可藉由使用由一組濾波器被選用之多接頭濾波器對資料訊框X施用濾波器而被施作。該矩陣或濾波器係以在資料訊框Y中被產生之第二被加密的資料的列及/或行為基礎動態地被選用。更特定之提述在此揭露中針對矩陣乘法之施作被做成。

例如，公式15所呈現之轉換可用由公式16與17的一組二個矩陣被選用之一矩陣的矩陣乘法被施作。此二矩陣之適當者被選用作為針對資料訊框Y被產生的資料行之函數。在此特定例中，公式16中被顯示之矩陣在對第0或1行產生被加密的資料時被選用，及公式17中被顯示之矩陣在對資料訊框Y的所有其他行產生被加密的資料時被選用。

較佳地，列相依係數與行相依係數係由至少部分之控制資料被導出的方式為使得係數之值在沒有存取控制資料下為難以預測的。在一施作中，係數係由資料訊框之被選擇的資料中由第一列x_0被導出。雖然被用以導出係數之方法或函數的選用會具有實務的重要性而影響加密處理之整體安全性，原則上無特定的方法為絕對必要的。可能之方法在下面被描述。由於係數只在二維變化，此特點被稱為二維動態係數。

二維動態係數亦可在與上述任何行與列排列技術組合

被使用。

(6)0位元組之防止

若資料訊框X中一列或多列資料之所有位元組具有0值或具有相同值，則第二加密處理所提供之安全性水準會被受損。此情形將發生之機率可藉由添加非0項至轉換公式可基本上被減為0。由於重複值較可能就0比任何其他值而發生，此特點在此處被稱為0位元組防止技術。二種不同之方法在公式18與19中被顯示，其可被使用為公式15之轉換施作0位元組防止技術：

$$y_{i,j} = a_i \cdot d_j \cdot x_{i,j} + b_i \cdot e_j \cdot y_{i-1,j} + c_i \cdot f_j \cdot x_{i-1,j} + g_i \cdot h_j,\ 1 \le i < k,\ 0 \le j < m \quad (18)$$

$$y_{i,j} = a_i \cdot d_j \cdot (x_{i,j} + g_i \cdot h_j) + b_i \cdot e_j \cdot y_{i-1,j} + c_i \cdot f_j \cdot x_{i-1,j},\ 1 \le i < k,\ 0 \le j < m \quad (19)$$

此處 g_i=列相依之非0係數；以及

h_j=行相依之非0係數。

較多之非0項可在所欲時被添加。只有一個非0項之添加呈現該轉換被施用至具有相同值的一列位元組之機率減少數量與施作該技術所需要之計算資源間的平衡。

上面被顯示之二種0位元組防止技術係在數學上等值於如下列的添加0位元組防止動態矩陣B至下列之轉換：

$$Y = A \cdot X + B \quad (20)$$

此處之動態矩陣B為：

$$B\{j\}=\begin{bmatrix} 1 \\ g_1 h_j \\ b_2 e_j \cdot g_1 h_j + g_2 h_j \\ b_3 e_j \cdot (b_2 e_j \cdot g_1 h_j + g_2 h_j) + g_3 h_j \end{bmatrix}, \text{(針對公式18)；以及} \quad (21)$$

$$B\{j\}=\begin{bmatrix} 1 \\ a_1 d_j g_1 h_j \\ b_2 e_j \cdot a_1 d_j g_1 h_j + a_2 d_j g_2 h_j \\ b_3 e_j \cdot (b_2 e_j \cdot a_1 d_j g_1 h_j + a_2 d_j g_2 h_j) + a_3 d_j g_3 h_j \end{bmatrix}, \text{(針對公式18)} \quad (22)$$

此處 $B\{j\}$=矩陣B在第j行中之係數。

雖然在矩陣A之係數值與非0防止動態矩陣B的表式就所有之列與行維持是相同的，該等係數之實際值由於是由上面被討論的二維動態係數技術被導出，故會隨列至列及隨行至行而變化。

若為所欲時，0位元組防止技術可使用如上述就一維動態係數技術藉由設定行相依係數d，e與f等於1之靜態矩陣。0位元組防止技術可藉由設定係數a，b與c為不會隨列至列變化而以基本轉換被使用。

(7)初始化向量

上面所討論之排列與動態係數技術的較佳施作係響應由控制資料中之資訊被獲得或被導出的資料來控制係數之排列與修改。在一施作中，訊框之第一列x_0中的資料被使用。若被使用之資料為常數或針對不同資料訊框為可預測的，則結果所得之排列順序與係數修改亦為可預測的，其會降低第二加密處理所提供之安全性水準。

此情況基本上可藉由使用在被用以獲得排列順序或動

態係數內導入不可預測之數值或初始化向量(IV)的特點被消除。IV與如資料x_0之第一列的資料被使用。在較佳實施例中IV係較佳施作中之特定材料相關聯，但其可與如所欲的接收人之一些其他元素相關聯。被使用之任何IV被納入控制資料且被第一加密處理加密。

IV在將一系列之訊框加密時可偶而被改變。若IV之新值的存在無由已在信號中之其他資料被預測且被決定時，IV中之改變用被納入第一被加密的資料或第二被加密的資料或與之相關聯的一些額外之資料指出。若為所欲時，不同之IV可就每一個資料訊框被使用。該新值為可預測或不可預測的。可預測之值可被產生的一方法為以可預測的或特定之方式由一訊框至下一個地修改IV。例如，IV可針對每一個連續之訊框被增加固定數量，或其可被增加由控制資料被獲得的數量。

雖然被用以獲得IV之方法或函數的選用可具有的實務重要性在於影響加密處理之整體安全性，但原則上無特定之方法為絕對必要的。可能的方法在下面被描述。

b)初始化

使用行與列排列及動態係數之較佳施作在響應如由第一列資料x_0之由資料訊框中被選擇的資料被導出的初始化資料下，控制被排列之列與行的順序與動態係數之值。若初始化資料之每一個位元係依被選擇的資料中之每一個位元而定的，第二加密處理之安全性可被加強。此可藉由使用具有如為密碼區塊連結(CBC)之一些連結機制的區塊密

碼被完成。此加密模式執行目前資料與在目前區塊加密前之前一個資料區塊的被加密結果間之互斥OR(XOR)。

在一施作中，第一列之資料x_0被分割為P_0，P_1，P_2，...P_S資料區塊。一區塊密碼依序被施用至每一個區塊。由區塊密碼被獲得之被加密的資料C_0，C_1，C_2，...C_S呈現可被用以計算IV之位元組資料的虛擬隨機串流或將上面被討論之排列與動態係數初始化。若初始化需要比列x_0之長度更長的位元串流，密碼可捲繞至列之開始，且藉由使用來自該列的結尾被加密之區塊C_S以將第一資料區塊P_0作XOR，以在將其再次加密前而繼續其處理。第一資料區塊P_0之初使加密可使用IV、加密金鑰、或二者均是，其係由第一列資料x_0之全部或任何部分被導出。很多變形為可能的。無特定之技術為關鍵的。

若為所欲時，密碼可在產生初始化資料前進行對在第一列x_0中所有之資料區塊P_0，P_1，P_2，...P_S的初始傳送。在一施作中，由該初始傳送被獲得之被加密的資料區塊C_0，C_1，C_2，...C_S的初始集合取代第一列資料x_0被使用。

由於若某些係數為0，結果所得之轉換不會是可逆的，故對動態係數技術須特別注意。此問題可藉由刪除來自初始化資料之所有的非0位元組而可被避免。施作此技術之一方法為檢查該虛擬隨機串流中的位元組，且在只在其若具有非0值時將此位元組插入初始化資料中。

被行與列排列技術使用之被排列的順序可用很多方法被產生。較佳地，該被排列的順序係根據第一列之資料x_0

被導出。一種有效率且統計上不偏之方法藉由在單調漸減範圍的值內產生虛擬隨機數字產生被排列的順序以定出一序列數字之順序的重組。

例如，行之被排列的順序可用構建行編號之陣列CX並以某種隨機方式重組該等編號的順序之一種處理被產生。該陣列具有由0至m-1被編碼之m個元素且被初使化，使得每一個陣列元素CX[i]紀錄該編號i。該處理使用如上面被提及之CBC技術的一些技術由第一列資料x_0反覆地導出一系列之虛擬隨機數字N_1，N_2，...N_m。在第一次反覆之際被產生之數字N_1具有被限制為由0至包括m-1的範圍內。每一個連續反覆之數字被限制在逐漸減少的範圍內。若符號R代表該反覆數字，來自第R個反覆之虛擬隨機數字被限制於可被表達為$0 \le N_R \le m-R$的範圍內。例如被第一次反覆產生的數字N_1之範圍為$0 \le N_1 \le m-1$，及被最後一次或第m次反覆產生的數字N_m之範圍為$0 \le N_m \le 0$。若所欲時，最後一次反覆的數字N_m可被設定為等於0，而不須導出虛擬隨機數字。該被排列之順序藉由重組陣列CX中的元素被產生。就每一次反覆而言，被記錄於陣列元素CX[m-R]中之值與被記錄於陣列元素CX[N_R]中之值交換。在最後一次反覆完成之際，陣列元素CX[i]，i=0至m-1之數列以由第一列資料x_0被導出之被排列的順序來記錄行編號。

相同之技術可被用以產生在陣列元素RX[i]中之列的被排列之順序。虛擬隨機數字對由R=k-1至1延續的反覆被產生，而具有之值被限制於可被表達為$1 \le N_R \le k-R$的範圍

內。在最後一次反覆完成之際，陣列元素RX[i]，i=0至k-1之數列以由第一列資料x_0被導出之被排列的順序來記錄行編號。

初始化向量基本可由如被虛擬隨機數字產生器被產生之虛擬隨機數字串流的任何所欲之來源被獲得。一種簡單之程序使用虛擬隨機串流的開頭作為IV。若IV例如為128位元長，其可由該虛擬隨機串流的前128個位元被獲得。

此處被提及之特定施作與程序僅為初始化可被執行之方法的例子。基本上，可產生虛擬隨機資料之任何技術可被使用。

(c)簡化之強化轉換

在此處被稱為簡化之強化轉換(SET)的以動態矩陣之特殊轉換現在將被描述。SET為如上面被解釋之使用由第一列資料x_0被導出之位元組資料的虛擬隨機串流所初始化之處理來排列矩陣係數及使要被加密之非被選擇的資料隨機化的特點加以強化之基本轉換的變形。SET為有效率的且對很多應用提供良好水準之安全性。

SET可如公式23顯示被表示為：

$$y_{0,j} = x'_{0,j}, \qquad 0 \le j \le m$$

$$y_{i,j} = a'_{i,j} \cdot d'_{i,j} \cdot x'_{i,j}, \qquad 1 \le i < k,\ 0 \le j < m \qquad (23)$$

此處 $x'_{0,i}$ = 由資料列x_0被導出之位元組資料的虛擬隨機串流

(24a)

$a'_{a,j}$=列相依而行被移位之矩陣係數； (24b)

$d'_{i,j}=d_{S(i,j,m),j}$=行相依而列被移位之矩陣係數；以及

(24c)

$x'_{i,j}=x_{i,j}+x'_{P(i,j,m),j}$=要被加密之隨機化後的非被選擇的資料

(24d)

較佳地，被表示為$x'_{0,j}$之位元組資料的虛擬隨機串流係由被施用至第一列資料x_0之CBC處理的第一回被導出。矩陣係數a'與d'應具有非0值。

記號R(i,j,k)代表排列a係數之順序的函數。記號S(i,j,m)代表排列d係數之順序的。記號P(i,j,m)代表排列第一列資料x_0之區塊的函數。

上面被提及之排列函數可被施作為下列被顯示之公式：

$$R(i,j,k)=(i-ra(j)) \bmod k \quad (25)$$

$$S(i,j,m)=(j-rd(i)) \bmod m \quad (26)$$

$$P(i,j,m)=(j-rx(i)) \bmod m \quad (27)$$

此處ra(j)=介於0與k-1間之整數的虛擬隨機映射函數；

rd(i)=介於0與m-1間之整數的虛擬隨機映射函數；

rx(i)=介於0與m-1間之整數的虛擬隨機映射函數；以及

mod n=送回介於0與n-1間之非負數字的模數運算元。

在一較佳施作中，每一個映射函數ra(j)，rd(i)與rx(i)之值為每一個資料訊框被計算一次。該等映射函數可由上面被提及之虛擬隨機數字產生器或CBC初始化處理所產生

之數字被施作。

較佳地，映射函數ra(j)，rd(i)與rx(i)被施作成為針對非被選擇的資料之每一個訊框在輸出範圍0至k-1與0至m-1產生每一個整數一次且僅有一次的排列函數。若這些映射函數被施作成為排列函數，則係數a'為列相依之行被排列的矩陣係數及係數d'為行相依之列被排列的矩陣係數。

上面被提及之虛擬隨機映射函數的輸出範圍一般為較佳的。不同的輸出範圍可被使用，但結果所得之SET所提供的安全水準可能被損害。

在公式24d中之加(＋)運算元代表由第一資料列x_0被導出之位元組資料的虛擬隨機串流之排列與在其餘的資料列中非被選擇的資料之區塊間的XOR運算。該排列可被為每一列非被選擇的資料改變之數個位元組或位元旋轉該虛擬隨機串流的循環移位加以施作。若為所欲時，旋轉之一些或全部被要求之量可預先被計算及被儲存以便在加密處理之際使用。

若為所欲時，一替選的SET可被用以施作第二加密處理。該替選的SET可由SET藉由轉置上面之公式中被顯示的係數a'與d'交換列與行向量、及交換對列與行之參用而被導出。

上述之一些技術可使用一第二加密處理，其對加密處理金鑰與IV二者均響應。IV本身可被視為一種型式之加密處理金鑰。若為所欲時，上述用於產生IV或其他初始化資料之技術可被用以產生一加密處理金鑰。以此方式被獲得

之加密處理金鑰為一種材料導向式之金鑰。其可被用以將資料訊框之全部或至少部分的其餘資料加密。IV係被第一加密處理加密且被納入第一被加密的資料內。此做法之一利益在於其提供簡單之方法來發佈接收器15為第二解密處理導出解密金鑰所需的資料。

若為所欲時，相同之加密演算法就該等第一與第二加密處理被使用，及相同之解密演算法就該等第一與第二解密處理被使用。基本上任何演算法可被使用，但類似AES或DES之對稱金鑰運算法由於金鑰發佈被簡化而為便利之選擇。若為非對稱金鑰運算法就第一加密處理被使用，一方法被需要以發佈適當之解密金鑰。在一發佈方法中，處理器10導出解密金鑰並將之納入被第一加密處理加密的控制資料中。

E.解密處理

1.概要

被用以將第一與第二被加密的資料解密之第一與第二解密處理可用各種方法被執行，但應其為被用以產生被加密的資料之個別的第一及第二加密處理之逆處理。適於將上述之基本轉換所產生的資料解密處理之處理在下列的段落中被討論。

2.基本施作

第二解密處理可用被用以產生第二被加密的資料之轉換為逆轉的任何適合之轉換被施作。例子在上面的公式2中被顯示。在上面公式6中被顯示之基本轉換適於接收器2中

被顯示。在上面公式6中被顯示之基本轉換適於接收器15在連用公式3之基本轉換的系統中使用。

3.替選之施作

若第二加密處理使用公式3之基本轉換且納入上面被討論的任何額外之特點，下面被討論的對應之逆特點將以公式6的基本逆轉換被使用。

具有與不具有上面被討論之額外特點的基本逆轉換對應於將矩陣A^{-1}之係數乘以要被解密的資料訊框Y之算術處理。在公式6中被顯示之公式的檢查揭露針對資料訊框Y或資料訊框X之每一行的算術運算係與其他算術運算無關地被執行。安全性水準可藉由使用下面被討論之一個或多個特點被改進。

若第二加密處理使用具有上面被提及之額外特點的替選之基本轉換或一些變形，其解密處理應使用替選之逆基本轉換或其適當的變形。適當的逆轉換的施作對應於將要被解密之資料訊框Y乘以矩陣A^{-1}的係數。針對資料訊框Y或資料訊框X之每一列的算術運算係與其他算術運算無關地被執行。若第二加密處理亦納入上面被討論之額外特點的適當的變形，對應之逆特點應被納入解密處理。該等對應之逆特點可由下列討論藉由如上面被解釋地交換對列與行的參用及進行其他改變而被導出。

逆轉換之應用一般在下列討論中以列與行被配置的矩陣運算或各種算術運算為準地被參用。恰如就加密處理之討論地，這些參用為要描述該等替選的施作之方便的方

法，且不欲意為其中此逆轉換必須被施作之任何特定方法。施作之其他方法如對要被解密的資料訊框Y施用一個或多個多接頭濾波器地為可能的。

(a)額外之逆特點

對上面被討論之額外特點互補而在此處被稱為逆特點的特點可藉由如下面被解釋地執行除了基本逆轉換之施用外的各種運算被實現。

(1)行與列排列

一些逆特點以與在第二加密處理中被完成者逆向之方式重組逆矩陣A^{-1}、被加密的資料Y或被解密之資料X的行、列、行與列二者。此被稱為逆排列。若排列在轉換矩陣之施用前被執行，則對應的逆排列在逆轉換矩陣之施用後被執行。若排列在轉換矩陣之施用後被執行，則對應的逆排列在逆轉換矩陣之施用前被執行。

(2)動態係數

其他之逆特點修改逆矩陣的係數，使得其維持為被用以要加密資料之逆矩陣。該等係數可依據上面被討論的一維或二維動態係數技術之一被採用。

具有二維動態係數之逆轉換可被施作成為以動態矩陣的矩陣乘法，其中適當之矩陣係由一組逆矩陣$\{A^{-1}\}$被選用。在該組逆矩陣中之每一個矩陣為代表該第二加密轉換的一組矩陣$\{A\}$中各矩陣之一逆矩陣。若為所欲時，逆轉換亦可藉由施用其中代表該第二加密轉換的一組濾波器中各濾波器之一逆向濾波器的一組多接頭濾波器被施作。

(3)防止0位元組

另一逆特點為上面被討論之0位元組防止技術的逆向。該逆技術在算術上等值於如下列由該逆轉換減掉0防止動態矩陣B之運算：

$$X=A^{-1}\cdot(Y-B)=A^{-1}\cdot Y-A^{-1}\cdot B=A^{-1}\cdot Y-B^{-1} \quad (28)$$

此處B^{-1}代表逆0防止動態矩陣。

動態矩陣B與其逆B^{-1}係一上面被描述地被使用且在公式21與22之0位元組防止技術的特定施作而定的。若為所欲時，逆動態矩陣B^{-1}可如下列地被計算：

$$B^{-1}=A^{-1}\cdot B \quad (29)$$

(4)初始化向量

上面所討論之排列與動態係數技術的較佳施作係響應由控制資料中之資訊被獲得或被導出的資料來控制係數之排列與修改。此控制資料被該第一加密處理加密並被納入該第一被加密的資料中。該排列與動態係數技術係響應於相同的資料，其係藉由將該第一被加密的資料解密而被獲得。被需要之任何IV被納入該第一被加密的資料中。

(b)初始化

在第二解密處理中之逆特點的施作可由在第二加密處理中之互補特點所使用的相同之初始化資料將其運算初始化。此初始化可用與就加密被導出的相同方法被導出。此導出所需之所有資料可被納入該第一被加密的資料內。

(c)逆簡化之強化轉換

若SET被用以執行第二加密處理，其第二解密處理用此

處被稱為逆簡化之強化轉換(ISET)的逆轉換被施作。ISET係用將矩陣係數排列並將非被選擇的資料解除隨機化之特點加以強化的基本逆轉換的變形。

ISET可如公式30所顯示地可被表示為：

$$x'_{0,j} = y_{0,j} \quad , \qquad 0 \le j < m$$

$$x'_{i,j} = \frac{y_{i,j}}{a'_{i,j} \cdot d'_{i,j}}, \quad 1 \le i < k, 0 \le j < m \qquad (30)$$

此處 $x_{i,j} = x'_{i,j} + x'_{P(i,j,m)}$ = 解密後之非被選擇的資料 (31)

在公式31d中之加(＋)運算元代表由第一資料列x_0被導出的之位元組資料的虛擬隨機串流之排列與在其餘的資料列中非被選擇的資料之被加密區塊間的XOR運算。該排列可被為每一列非被選擇的資料改變之數個位元組或位元旋轉該虛擬隨機串流的循環移位加以施作。若為所欲時，旋轉之一些或全部被要求之量可預先被計算及被儲存以便在解密處理之際使用。

若第二解密處理使用上面被討論的SET，對應之替選的ISET應被用以施作第二解密處理。該替選的ISET可由ISET藉由轉置30公式中被顯示的矩陣係數、交換列與行向量、及交換對列與行之參用而被導出。

(d)密碼金鑰

接收器15基本上可用所欲之任何方式獲得全部所需之解密金鑰。在較佳實施例中，第二解密金鑰係由藉由將第

一被加密的資料解密所恢復之控制資料被獲得或被導出。將第一被加密的資料解密所需之第一解密金鑰可用任何所欲的方式被發佈。例如，若該第一解密金鑰在與所欲的接收人相關聯之公共金鑰/一對私人-公共金鑰中的接收人之私人金鑰，該公共金鑰會被使用以產生第一被加密的資料，且該私人金鑰可能已用與該第一被加密的資料之發佈不同的某一安全之方法而將資料加密並發佈給接收人的個體加以創立。相反地，該對金鑰可能已被接收人創立且公共金鑰被提供給將資料加密之個體。此後者之方法的好處在於要發佈公共金鑰時不須用到安全之頻道。

F.施作

納入本發明之各種層面的裝置可用各種方法被施作，包括軟體用於電腦或包括類似被耦合至在通用電腦中被找到之元件的數位信號處理器電路之更專業的元件之執行。第8圖為可被用以施作本發明之層面的裝置70之示意方塊圖。處理器72提供計算資源。RAM 73為處理器72用於處理所使用之系統隨機存取記憶體(RAM)。ROM 74代表如用於儲存操作裝置70所需之程式及可能用於實施本發明之層面的唯讀記憶(ROM)之某種形式的永久儲存器。I/O控制75代表經由通訊頻道76、77接收及發射信號之介面電路。在所顯示之實施例中，所有的主要之系統元件連接至匯流排71，其代表多於一個之實體或邏輯匯流排。然而，要施作本發明並不需有匯流排架構。

在用通用電腦系統被施作之實施例中，額外的元件可

被納入用於與如鍵盤或滑鼠及顯示器之裝置成介面，與用於控制具有如磁帶或磁碟或光學媒體之儲存媒體的儲存裝置。該儲存媒體可被用以記錄作業系統用之指令的程式、公用程式與應用程式，且可包括施作本發明之各種層面的程式。

要實作本發明之各種層面的函數可用以廣泛各種方法被施作之元件加以執行，包括離散的邏輯元件、積體電路、一個或多個ASIC及/或程式控制式之處理器。這些元件被施作的方式對本發明並非重要的。

本發明之軟體施作可用如包括超音波至紫外線頻率的整個頻譜之基帶或調變後通訊路徑的各種可讀之媒體、或基本上使用包括磁帶、磁卡或磁碟、光學卡或光碟、與在包括紙之媒體上可偵測的標記之任何記錄技術輸送資訊的媒體加以輸送。

【圖式簡單說明】

第1與2圖為其中處理器準備被加密之材料用於傳輸或儲存以便後續傳遞至接收器的系統之示意方塊圖。

第3圖為處理器與接收器之網路的示意方塊圖。

第4與5圖準備被加密之材料用於傳輸或儲存以便後續傳遞至接收器的處理器之示意方塊圖。

第6與7圖為接收將被解密及被提出至接收人之被加密的材料之接收器的示意方塊圖。

第8圖為被用以施作本發明之各種層面的裝置之示意方塊圖。

【主要元件符號說明】

1...路徑

2...路徑

3...處理器

4...處理器

5...路徑

6...路徑

7...發佈媒體

8...發佈媒體

11...路徑

12...路徑

15...接收器

18...路徑

20...發佈設施

31...金鑰伺服器

32...路徑

33...加密器

34...組合器

35...路徑

36...路徑

42...選擇器

43...路徑

44...路徑

45...加密器

46...路徑

51...解密器

52...路徑

53...路徑

54...組合器

55...路徑

61...解密器

62...路徑

63...路徑

65...路徑

70...裝置

71...匯流排

73...RAM

74...ROM

75...I/O控制

76...通訊頻道

77...通訊頻道

78...儲存裝置

五、中文發明摘要：

在本案中將呈現影像與聲音之資料加密的處理器，例如使用一第一加密處理以將包括來自資料訊框之被選擇的資料的控制資料加密及使用一第二加密處理以將來自資料訊框之非被選擇的資料加密。該第一加密處理係對一加密響應，其可與資料訊框的接收人相關聯。該第二加密係對一金鑰響應，其為由該控制資料被獲得或被導出。該被加密的控制資料與該被加密的非被選擇之資料可使用分別的媒體被傳遞至一接收器。該接收器使用與該等第一及第二加密處理逆轉之解密處理恢復該等資料訊框。該第二加密處理之有效率的施作被揭露。

六、英文發明摘要：

Processors that encrypt frames of data representing images and sounds, for example, use a first encryption process to encrypt control data that includes selected data from the data frames and use a second encryption process to encrypt non-selected data from the data frames. The first encryption process is responsive to a key, which may be associated with an intended recipient of the data frames. The second encryption process is responsive to a key that is obtained or derived from the control data. The encrypted control data and the encrypted non-selected data may be delivered to a receiver using separate media. The receiver recovers the data frames using decryption processes that are inverse to the first and second encryption processes. Efficient implementations of the second encryption process are disclosed.

十、申請專利範圍：

1. 一種編碼方法，其包含：

接收一個或多個信號，其輸送之資料係定出或輸送呈現供人類感知用刺激的特定材料；

獲得一第一加密金鑰；

獲得控制資料，其包含在一資料訊框中之被選擇的資料及呈現與該特定材料相關聯且與該第一加密金鑰不同之一第二加密金鑰的資訊，其中該被選擇的資料呈現至少部分之該特定材料且少於在該資料訊框中所有的資料；

對該控制資料施用一第一加密處理以產生第一被加密的資料，其中該第一加密處理係對該第一加密金鑰響應；

組合該第一被加密的資料成為一第一被編碼的信號用於傳遞至一接收人以便在獲得一解密金鑰中使用，以將在該資料訊框中未被納入該被選擇的資料之非被選擇的資料的被加密之形式所呈現的第二被加密的資料加以解密。

2. 如申請專利範圍第1項之編碼方法，包含對該非被選擇的資料施用一第二加密處理以產生該第二被加密的資料，其中第二加密處理係對該第二加密金鑰響應。

3. 如申請專利範圍第2項之編碼方法，其中該非被選擇的資料包含符號，該第二加密處理包含將該非被選擇的資料的符號乘以其中該等符號以列與行被配置之係數的

算術運算，且每一行之算術運算係與其他行無關地被執行，或每一列之算術運算係與其他列無關地被執行。

4. 如申請專利範圍第3項之編碼方法，其中該被選擇的資料包含呈現該第二加密金鑰之資訊。

5. 如申請專利範圍第2、3或4項中任一項之編碼方法，包含組合該第二被加密的資料成為該第一被編碼的信號。

6. 如申請專利範圍第2、3或4項中任一項之編碼方法，包含組合該第二被加密的資料成為該第二被編碼的信號。

7. 如申請專利範圍第6項之編碼方法，包含：

沿著一第一發佈路徑發佈該第一被編碼的信號至該接收人；以及

沿著一第二發佈路徑發佈該第二被編碼的信號至該接收人。

8. 如申請專利範圍第7項之編碼方法，其中：

該第一加密金鑰係與該特定材料之所欲的接收人相關聯；

該第一發佈路徑係為促進對該所欲的接收人之發佈的一接收人導向式之發佈網路的一部分；以及

該第二發佈路徑係為促進對多個接收人之發佈的一材料導向式之發佈網路的一部分。

9. 如申請專利範圍第8項之編碼方法，其中該材料導向式的發佈網路係為一個層對層網路。

10. 如申請專利範圍第2-9項中任一項之編碼方法，其中該第一加密處理係對一第一電腦系統被執行以產生該第

一被加密的資料，及該第二加密處理係對一第二電腦系統被執行以產生該第二被加密的資料。

11. 如申請專利範圍第2-10項中任一項之編碼方法，其中該第二加密處理係對該非被選擇的資料漸增地被施用而以漸進之方式產生該第二被加密的資料。

12. 如申請專利範圍第3-10項中任一項之編碼方法，

其中該等算術運算將該等符號的列與行乘以動態矩陣中之係數；以及

該動態矩陣係利用一處理在響應被相乘的該等符號之列或行下由一組矩陣選出的係數之矩陣被施作。

13. 如申請專利範圍第3-11項中任一項之編碼方法，其中該第二加密處理進一步包含響應於該控制資料的行之排列。

14. 如申請專利範圍第13項之編碼方法，其中該等行之排列在遍及各列為變化的。

15. 如申請專利範圍第3-11項中任一項之編碼方法，其中該第二加密處理進一步包含在乘以該等係數前的響應於該控制資料之列的排列。

16. 如申請專利範圍第15項之編碼方法，其中該等列之排列在遍及各行為變化的。

17. 如申請專利範圍第3-11項中任一項之編碼方法，其中該第二加密處理進一步包含在乘以該等係數後的響應於該控制資料之列的排列。

18. 如申請專利範圍第17項之編碼方法，其中該等列之排列

在遍及各行為變化的。

19. 如申請專利範圍第3-11項中任一項之編碼方法，其中該等係數被配置成具有0值的係數之三角形陣列，使得該乘法等值於對該等符號的列或行之一個或多個濾波器的反覆施用。

20. 如申請專利範圍第19項之編碼方法，其中用於該等一個或多個濾波器的該等接頭之係數係就每一列響應於該控制資料而改變。

21. 如申請專利範圍第19項之編碼方法，其中用於該等一個或多個濾波器的該等接頭之係數係就每一列與行響應於該控制資料而改變。

22. 如申請專利範圍第1-21項中任一項之編碼方法，其中該第一加密金鑰係與該特定材料之所欲的接收人相關聯。

23. 一種解碼方法，包含：

接收一第一被編碼的信號，其輸送第一被加密的資料，呈現包含在一資料訊框中之被選擇的資料的控制資料，其中該被選擇的資料呈現至少一部分之供人類感知用刺激的特定材料，且其中被選擇的資料少於在該資料訊框中所有的資料；

對該第一被加密的資料施用一第一解密處理以恢復該控制資料，其中第一解密處理係對一第一解密金鑰響應，及其中該控制資料包含之資訊呈現與該特定材料相關聯且與該第一解密金鑰不同的一第二解密金鑰；

對第二被加密的資料施用一第二解密處理以恢復

在該資料訊框中未被納入該被選擇的資料之非被選擇的資料，其中該第二解密處理係對該第二解密處理金鑰響應；以及

藉由組合該被選擇的資料與該非被選擇的資料成為一資料訊框而呈現至少一部分之該特定材料。

24. 如申請專利範圍第23項之解碼方法，其對該第二被加密的資料施用該第二解密處理，其中該第二加密處理包含將該第二被加密的資料乘以其中該第二被加密的資料以列與行被配置之係數的算術運算，且每一行之算術運算係與其他行無關地被執行，或每一列之算術運算係與其他列無關地被執行。

25. 如申請專利範圍第24項之解碼方法，其中該被選擇的資料包含呈現該第二加密金鑰之資訊。

26. 如申請專利範圍第23、24或25項中任一項之解碼方法，包含由該第一被編碼的信號獲得該第二被加密的資料。

27. 如申請專利範圍第23、24或25項中任一項之解碼方法，包含由該第二被編碼的信號獲得該第二被加密的資料。

28. 如申請專利範圍第27項之解碼方法，包含：

由一第一發佈路徑接收該第一被編碼的信號；以及

由一第二發佈路徑接收該第二被編碼的信號。

29. 如申請專利範圍第28項之解碼方法，其中：

該第一解密金鑰係與該特定材料之所欲的接收人相關聯；

該第一發佈路徑係為促進對該所欲的接收人之發

佈的一接收人導向式之發佈網路的一部分；以及

該第二發佈路徑係為促進對多個接收人之發佈的一材料導向式之發佈網路的一部分

30. 如申請專利範圍第29項之解碼方法，其中該材料導向式的發佈網路係為一個層對層網路。

31. 如申請專利範圍第23-30項中任一項之解碼方法，其中該第二解密處理係對部分的第二被加密之資料漸增地被施用而以漸進之方式產生該該非被選擇的資料。

32. 如申請專利範圍第24-31項中任一項之解碼方法，

其中該等算術運算將該第二被加密之資料的列與行乘以動態矩陣中之係數；以及

該動態矩陣係利用一處理在響應被相乘的該等符號之列或行下由一組矩陣選出的係數之矩陣被施作。

33. 如申請專利範圍第24-31項中任一項之解碼方法，其中該第二解密處理進一步包含響應於該控制資料的行之排列。

34. 如申請專利範圍第33項之解碼方法，其中該等行之排列在遍及各列為變化的。

35. 如申請專利範圍第24-31項中任一項之解碼方法，其中該第二解密處理進一步包含在乘以該等係數前的響應於該控制資料之列的排列。

36. 如申請專利範圍第34項之解碼方法，其中該等列之排列在遍及各行為變化的。

37. 如申請專利範圍第24-31項中任一項之解碼方法，其中

該第二解密處理進一步包含在乘以該等係數後的響應於該控制資料之列的排列。

38. 如申請專利範圍第37項之解碼方法，其中該等列之排列在遍及各行為變化的。

39. 如申請專利範圍第24-31項中任一項之解碼方法，其中該等係數被配置成具有0值的係數之三角形陣列，使得該乘法等值於對該被加密之資料的列或行之一個或多個濾波器的反覆施用。

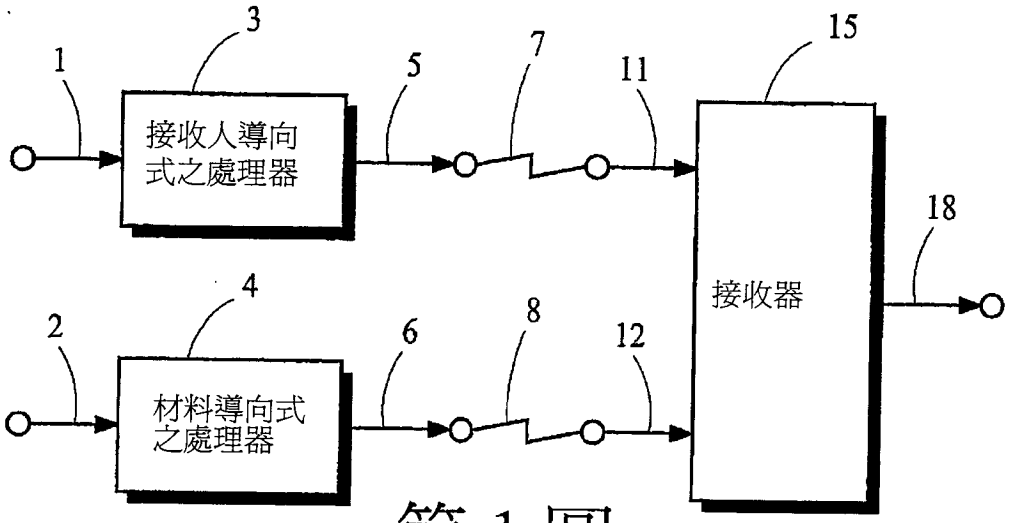
40. 如申請專利範圍第39項之解碼方法，其中用於該等一個或多個濾波器的該等接頭之係數係就每一列響應於該控制資料而改變。

41. 如申請專利範圍第39項之解碼方法，其中用於該等一個或多個濾波器的該等接頭之係數係就每一列與行響應於該控制資料而改變。

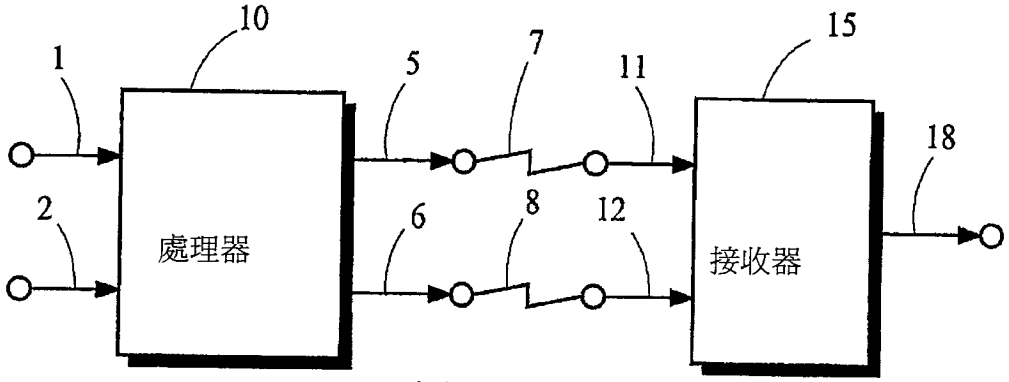
42. 如申請專利範圍第25-41項中任一項之解碼方法，其中該第一解密金鑰係與該特定材料之所欲的接收人相關聯。

43. 一種裝置，其包含用於執行如申請專利範圍第1-42項中任一項之方法的步驟之元件。

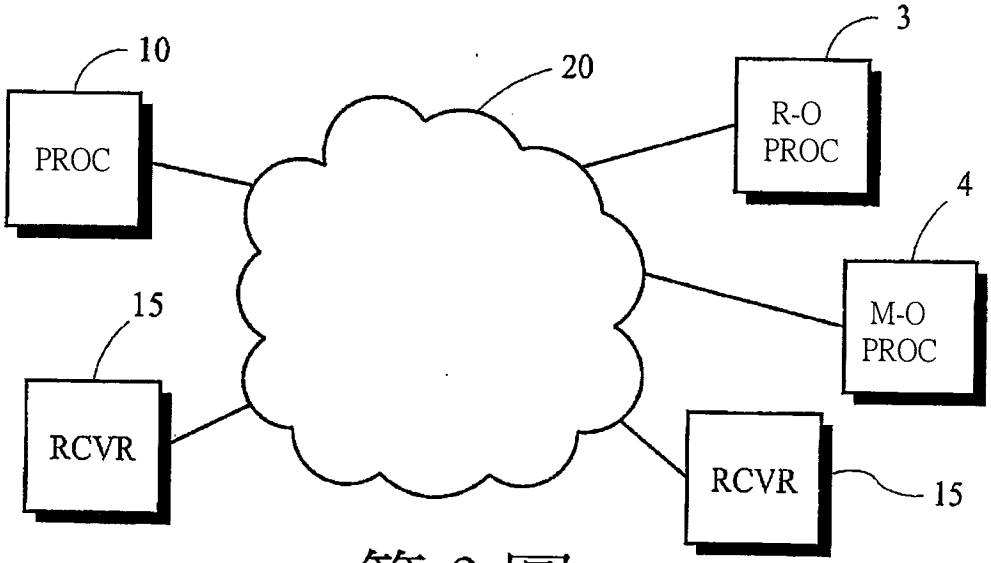
44. 一種輸送可用一裝置執行以執行如申請專利範圍第1-42項中任一項之方法的指令之程式的媒體。


1
3
接收人導向式之處理器
5
7
11
15
18
接收器
2
4
材料導向式之處理器
6
8
12

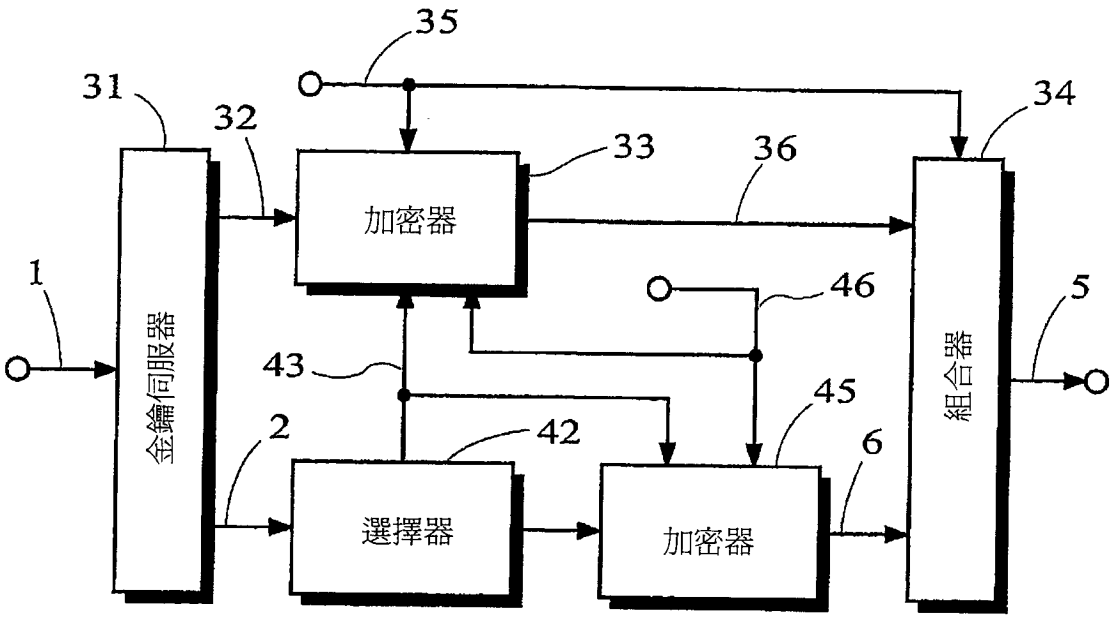
第 1 圖


10
1
5
7
11
15
18
處理器
接收器
2
6
8
12

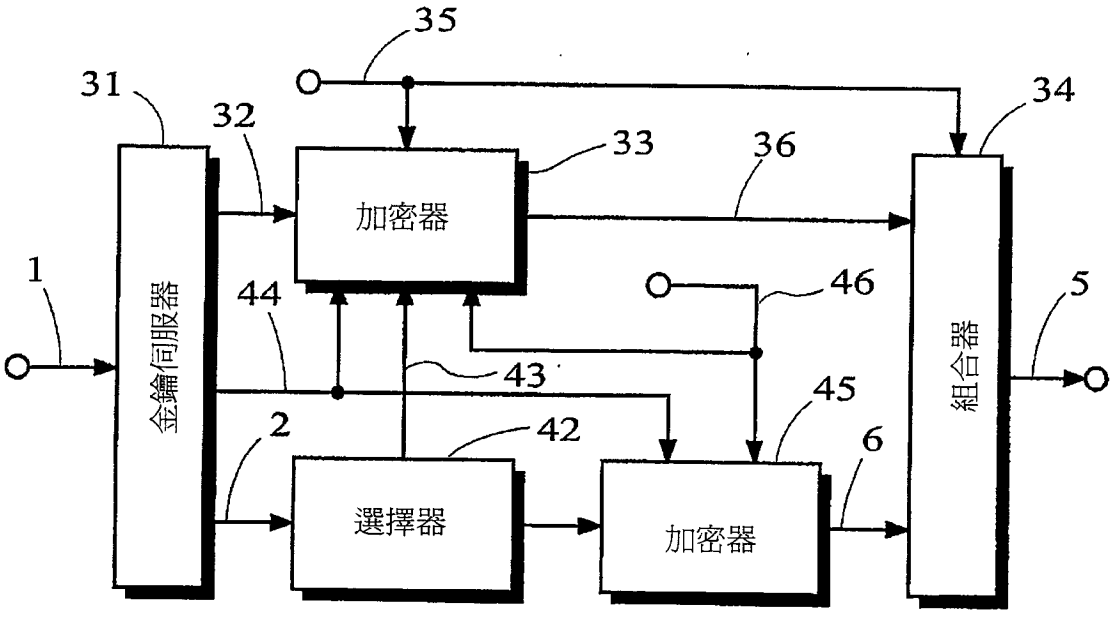
第 2 圖


10
PROC
20
3
R-O PROC
4
M-O PROC
15
RCVR
RCVR
15

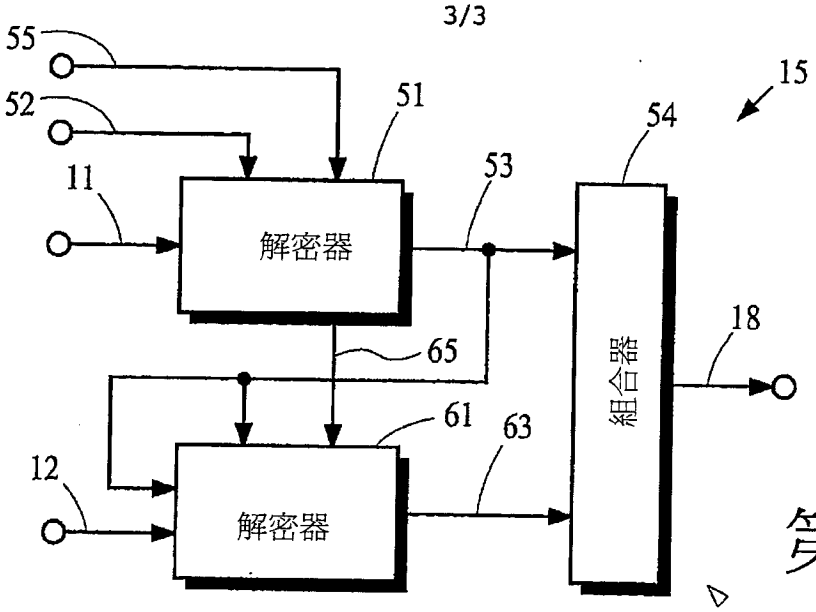
第 3 圖


35
31
32
33
36
34
加密器
1
金鑰伺服器
46
5
43
45
2
42
6
組合器
選擇器
加密器
10

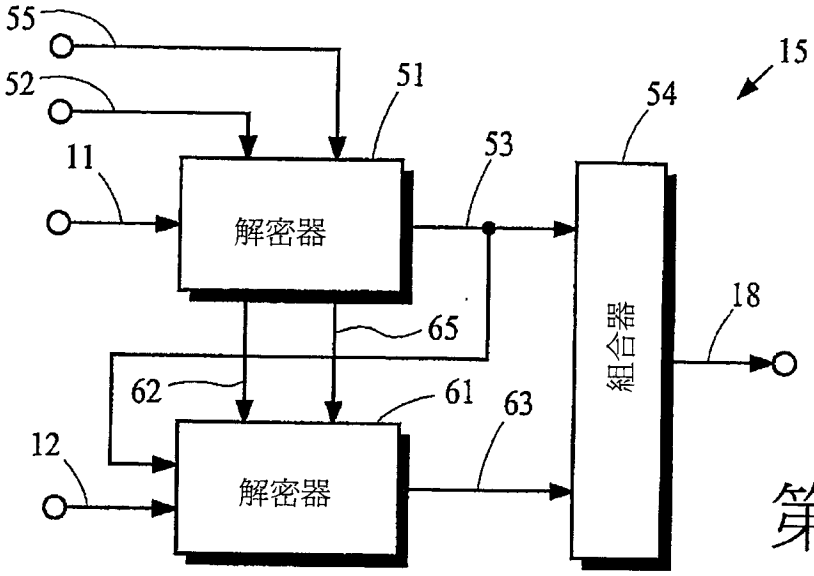
第 4 圖


35
31
32
33
36
34
加密器
1
金鑰伺服器
44
46
5
43
45
2
42
6
組合器
選擇器
加密器
10

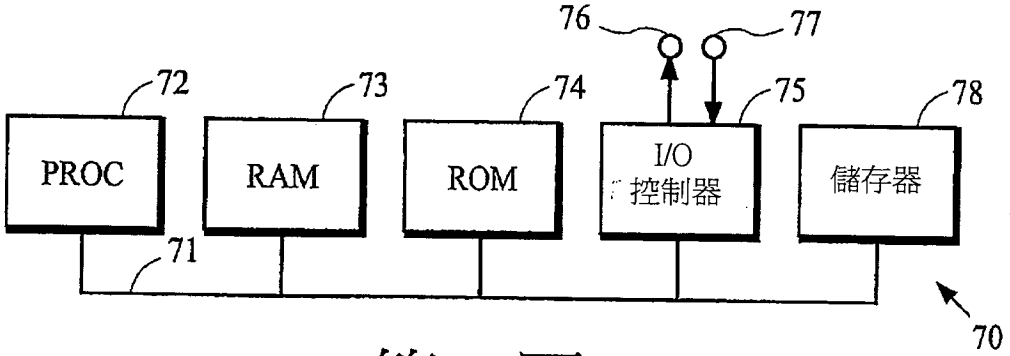
第 5 圖


55
52
11
51
53
54
15
解密器
65
61
63
18
12
解密器
組合器

第 6 圖


55
52
11
51
53
54
15
解密器
65
62
61
63
18
12
解密器
組合器

第 7 圖


76
77
72
73
74
75
78
PROC
RAM
ROM
I/O
控制器
儲存器
71
70

第 8 圖

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

1...路徑

2...路徑

3...處理器

4...處理器

5...路徑

6...路徑

7...發佈媒體

8...發佈媒體

11...路徑

12...路徑

15...接收器

18...路徑

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：