

293222

申請日期	85.4.05
案 號	85103957
類 別	H04L 9/58

A4
C4

293222

(以上各欄由本局填註)

發 明 專 利 說 明 書

一、發明 名稱	中 文	具有雙前向雜湊函數之密碼裝置
	英 文	"CRYPTOGRAPHIC APPARATUS WITH DOUBLE FEEDFORWARD HASH FUNCTION"
二、發明 人	姓 名	1. 艾瑞克·史賓克 2. 保羅·莫瑞尼 3. 肯迪克·安德生
	國 籍	均美國
三、申請人	住、居所	1. 美國加州克爾貝德市坎尼巷6421號 2. 美國加州奧利文漢市西泉路3411號 3. 美國加州殷斯坦市戴門海德路1385號
	姓 名 (名稱)	美商德來懷通用儀器公司
	國 籍	美國
	住、居所 (事務所)	美國伊利諾州芝加哥市西拜諾爾大道8770號13樓
	代 表 人 姓 名	哈洛德·姆·柯斯伯吉

(由本局填寫)

承辦人代碼：
大 類：
I P C 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
美 1995.7.3 08/497,880

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

五、發明說明(1)

發明背景：

本發明係關於密碼裝置，且尤其係關於密碼處理器，其使用一雙前向配置以實施一具有互補性之加密演算法，使得密碼處理機之輸入的倒數能從此其輸出端檢出。

密碼裝置係用以將信息轉譯，以使其除了指定的接收器外，無法由其他人解讀。例如，有線及衛星電視系統內，加密係用於在防止服務被竊盜。在電腦通信中，資料加密則用於使信息無法解讀，並確保接收者所收之信息非偽造。加密亦能允許接收者向第三人證明該信息非偽造。這些種種的功能係分別稱為通訊安全、真實性、及數位簽名。

其用於信息加密之變換包含加密演算法及鍵之使用。該鍵資訊係維持保密。為了信息加密，該加密演算法運用至信息而該鍵係用作輔助輸入以控制該加密動作。其解加密之工作係反作業，其操作相類似。

密碼系統依賴鍵資訊量，該鍵資訊無關於信息長度。理論上，此等系統可破解的。然而，由於人類設法破解密碼必須使用難以計數的計算資源，因此實際上它們仍係有用的。換句換說，所需要破解密碼之「工作因素」係高到足以防止成功的攻擊。

目前廣泛使用的密碼系統之一例係資料加密標準(DES)，該資料加密標準由美國國家標準局於1976年所核准。該DES演算法在一64位元鍵之控制下加密一64位元信息方塊以產生一64位原密文。DES演算法的細節可參見FIPS刊物第46期，1977年1月15日所載「資料加密標準之說明書

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

編

五、發明說明(2)

」，及於FIPS刊物第74期，在1981年4月1日所載「實施與使用NBS資料加密標準指引」，兩者皆可向美國商務部國家技術諮詢服務索取。

加密演算法一般係用作雜湊函數之一部份，其中，該輸入信號之確認係藉由以一加密鍵處理(即"雜湊法")輸入信號所提供。傳統的單前向雜湊函數(SFFH)內，該函數之輸入的信號之逆轉不能於該函數之輸出偵測出來。此種傳統處理在諸多的應用中無法令人滿意，因為輸入至安全處理器之資料有所改變而又沒有裝置來偵測出此等改變時，資料之安全性會受到破壞。若設法破壞安全性的人能獲得該系統如何因應於輸入資料內之改變的資訊而不會被該系統偵測到，則此人有機會經由長時間之測試而可能成功地破壞安全性。

因此最好能提供實現雜湊函數之裝置，該雜湊函數能使改變於雜湊函數之輸出處偵測，該等改變係例如輸入端之資料逆轉。此種實施將供應互補之特性至該雜湊函數。

另外也須有於使用串接密碼雜湊函數之系統中提供互補性之裝置。此種裝置應提供一輸入鍵至每個連續級，此鍵之產生係可確保互補性，因而，可使輸入處之逆轉能使於輸出偵測出。

本發明提供具有前述優點之裝置。

發明概要：

根據本發明，提供一種密碼裝置，其中之密碼處理器具有一接收第一輸入資料之八個平行位元組 F_1-F_8 之第一輸

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

編

五、發明說明(3)

入，一接收第二輸入資料之八個平行位元組 S_1-S_8 之第二輸入，以及一輸出藉由以密碼方式處理第一及第二輸入資料而產生的密文之八個平行位元組 C_1-C_8 輸出。第一裝置係供作處理密文及第一輸入資料以產生含有八個平行位元組 FD_1-FD_8 之第一密文導出。第二裝置處理第一密文導出及第二輸入資料用以輸出一第二密文導出 SD_1-SD_8 。第一裝置將每個密文位元組 C_1-C_8 與第一輸入資料位元組 F_1-F_8 予以邏輯「互斥或」，以產生第一密文導出。第二裝置將每個第一密文導出位元組 FD_1-FD_8 與第二輸入資料位元組 S_1-S_8 予以邏輯「互斥或」以產生第二密文導出。可於第一裝置及第二裝置中提供非線性函數以替代使用互斥或之邏輯操作，以分別產生第一及第二密文導出。該非線性函數可為輸出一半所輸入位元之類型。

第一裝置可包括一藉由第一輸入資料及密文，所定位址之查表以輸出相同數目位元組之互斥或。同樣地，第二裝置可包括一藉由第二輸入資料及第一密文導出所定址之查表，以輸出相同數目位元組之互斥或。另外，第一及第二裝置可包括傳統的邏輯互斥或閘。

本發明亦包含第二密碼處理器級。此級類似於第一級，並具有一接收第三輸入資料之八個平行位元組之第一輸入，及接收來自前級之第二密文導出之第二輸入。第二密碼處理器亦具有一輸出，可輸出藉由密碼處理第三輸入資料及第二密文導出而產生的第二密文之八個平行位元組。在具體實施例中，該密碼處理器係DES處理器。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

紉

五、發明說明(4)

本發明亦提供密碼裝置，其中，密碼處理器具有一接收輸入資料之八個平行位元組 F_1-F_8 之第一輸入，一接收第一輸入資料之平行位元組 F_2-F_8 以作為一鍵之第二輸入，以及一輸出，用以輸出藉由密碼處理輸入資料及鍵所產生的密文之七組平行位元組 C_1-C_7 。第一裝置分別互斥或(或應用一非線性函數)每個第一組的七個輸入資料位元組 F_1-F_7 與接續的輸入資料位元組 F_2-F_8 以產生前向資料 FF_1-FF_7 之七個位元組。第二裝置係提供作為互斥或(或應用一非線性函數)每個前向資料位元組 FF_1-FF_7 與相同數目的密文位元組 C_1-C_7 之以產生一包括七個平行位元組 D_1-D_7 之密文導出。

第一裝置可包括一藉由第一組之七個及接續的輸入資料位元組所定址之查表，以輸出其中之互斥或操作。同樣地，第二裝置包括一藉由前向資料位元組及相同數目之密文導出所定位址之查表，以輸出其中之互斥或操作。互斥或函數亦可藉由傳統的互斥或閘來提供。該密文處理器能包括一DES處理器。

圖式簡述：

圖1係一方塊圖，說明一習知技藝之前向雜湊函數。

圖2係一本發明之雙前向雜湊函數之方塊圖。

圖3A係根據本發明，在一與單前向雜湊函數之串接實施中使用雙前向雜湊函數之方塊圖。

圖3B係根據本發明，在一與另一雙前向雜湊函數之串接實施中使用雙前向雜湊函數之方塊圖。

五、發明說明(5)

圖4係實施根據本發明之雙前向雜湊函數之特定連接之示意圖。

圖5係根據本發明之另一雙前向雜湊函數的實施例之特定連接之示意圖。

密碼處理係於許多應用中用以確證資訊。用途之一係衛星收費電視服務之通訊。此一系統揭露於美國專利第4,613,901號，由Gilhousen等人所發明，發明名稱爲「控制電視信號之攪頻與選擇性遙控解攪頻之信號加密與分配系統」。在Gilhousen之系統內，有各類密碼鍵之使用以供應一加密電視信號中。在所敘述中的鍵中有類別鍵，每個含連接至用戶解攪頻器之一不同副組，且含有節目鍵，針對每個不同電視節目而使授權用戶解密一特別節目信號。

該節目鍵之處理一般係以一種確證之方式來實施以防止誤認頻道。尤其，含有包括如節目費用等項目之頻道辨識資訊，係以一種確認之方式送出以防止其改變。此種確認可藉由將「節目預設鍵」與頻道辨識資訊相雜湊(hashing)以產生真實的節目鍵，此真實的節目鍵係用以產生一解密。所要節目所需之工作鍵。

習知技藝在加密或解密的過程中所使用的雜湊函數爲已知的「前向DES」，且示於圖1中。所欲確證之資訊(明文)係經端子10輸入至DES處理器14。該明文係以八位元組(64位元)爲一部份輸入至DES處理器14及經由線路16輸入至一互斥或閘(XOR)18。一組七位元組(56位元)之密碼節目預設鍵係經由端子12輸入至該DES處理器14。該明文

五、發明說明(6)

係藉由輸入鍵依照DES演算法而處理以提供八位元組(64位元)之密文，該密文已透過XOR閘18與明文作互斥或邏輯運算。雖XOR閘18輸出64位元，但僅56位元係經線22輸出，並作為一輸入鍵輸入至連續的串接前向DES級。在線路20上剩餘之八個密文位元係未使用。因此，在每個雜湊級中皆留下一整個密文位元組，又，圖1之雜湊函數不提供互補。因而，輸入轉換(及因而輸入資料之改變而)不能由後級偵測出。

本發明提供一具有互補性之雙前向雜湊函數，如圖2所示。明文由端子30引入至一DES處理器34，且經線36至XOR閘38。該明文以八位元組(64位元)為一部份來處理。一八位元組(64位元)輸入鍵係經端子32供應。此八位元組之七位元組藉由DES處理器34來處理，而剩下之一位元組則輸入至互斥或閘35。該輸入鍵亦經線42連接至XOR閘44。閘44互斥或運算由XO閘38所輸出的64位元中之56位元以及64位元輸入鍵之56位元以提供56位元之運算結果至線45之上。由XOR閘38所輸出於線40上之剩餘8位元密文則於XOR閘35中與線路43上64位元輸入鍵之剩餘8位元作互斥或運算。該XOR閘35之輸出係與線45的56位元結合而形成線46上的64位元。

本發明利用饋入額外之前向資訊，經線42及43至額外之XOR閘44及35，而確保互補性的提供，並克服習知技藝的缺點。

XOR閘35，38及44能以查表替換，該等查表提供一

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(7)

XOR功能或合適的非線性函數。舉例而言，可使用輸出為輸入之大小的一半之非線性函數。例如包括輸入(x,y)兩位元及輸出(f)一位元，其中 $f=x+xy+y$ ；或是四位元輸入(w,x,y,z)而兩位元輸出(f1,f2)，其中：

$$f1 = w + x + y + z + wx + wy + wz + xy + xz + yz + wxy + wxz + wyz + xyz + wxyz$$

$$\text{及 } f2 = wx + wy + wz + xy + xz + yz + wxy + wxz + wyz + xyz ;$$

以及六位元輸入(a,b,c,d,e,f)與三位元輸出(x,y,z)，其中：

$$x = a + b + c + d + e + f + abc + bcd + cde + def + efa + fab + abcdef ,$$

$$y = abc + def + abd + cef + abcd + bcde + ace + abcef , \text{ 及}$$

$$z = abcde + abcdf + abcef + abdef + acdef + bcdef .$$

該等查表可為唯讀記憶體(ROM)之形式。取代XOR閘35查表將由元件38所輸出之八位元的「第一個密文導出」及線43上64位元輸入鍵之8位元來定址。取代XOR閘38之查表將由來自DES處理器34的密文及於線36上的明文所定址。取代XOR閘44之查表將由元件38所輸出的56位元之「第一個密文導出」及線42上64位元之輸入鍵的56位元所定址。對此，元件44將輸出64位元「第二個密文導出」之56位元供經由線46輸入至次一雜湊級。該第二密文導出之剩餘8位元係於函數(例如，XOR)35之輸出處獲得。

圖3A係根據本發明之兩個DES雜湊函數之串接。第一級80係類似於圖2中之雙前向DES雜湊函數級，於端子30具

五、發明說明(8)

有第一64位元輸入(明文)但於端子32'僅有56位元第二輸入。在線47上之56位元之「第二個密文導出」係視做輸入鍵輸入至一第二雜湊函數級82。此級包括一DES處理器70，該處理器70經端子31接收一第二64位元之明文輸入(第二明文)。該第二明文輸入經線72前饋至一XOR或非線性函數74，在此第二明文與來自DES處理器70輸出之密文一起處理。來自線76所輸出之合成64位元包括已確證資料對應至原始明文輸入之已確證資料。雖然圖3A中僅有二個雜湊函數級(即一個雙前向結構後接一單前向結構)，但應可瞭解在發明中可提供任何之級數，而最後一級前之每級皆包括一個雙前向結構。

圖3B係本發明中兩DES雜湊函數之串接，其中第一級80'係有圖2中已說明的雙前向DES雜湊函數級相同，於端子30具有一第一64位元輸入(第一明文)，以及於端子32具有一64位元之第二輸入。輸出在線45上之64位元之「第二密文導出」係與來自XOR或非線性函數35輸出之8位元相結合以於線路46上形成一64位元鍵，作為第二雜湊函數級82之輸入。此級包括一DES處理器70，DES處理器70接收一經由端子31之一第二64位元明文輸入(第二明文)。該第二明文輸入係經由線72前饋至一XOR或非線性函數74，在此第二明文與由DES處理器70所輸出之密文一起處理。來自線76之合成64位元輸出包括對應於原始的明文輸入之確證資訊，其中56位元係輸入至一XOR或非線性函數75以產生該64位元輸入中之56位元至次一級。如圖3A之

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(9)

具體實施例所示，任何級數皆能提供，而最後一級以前之每一級皆包括一如圖2所示之雙前向結構。

圖4係本發明之第一應用之示意圖。DES處理器90接收輸入資料92之8位元組(每位元組包括8位元)及一密碼鍵94，以輸出8位元組之加密資料96。該輸入資料係經由輸入端子100而以8個平行位元組 F_1-F_8 之方式供應。第二輸入端子101接收第二輸入資料之8個平行位元組 S_1-S_8 ，其第一組7個位元組(S_1-S_7)係視為密碼鍵使用。DES處理器90處理輸入資料92及鍵94以供應輸出資料96，該輸出資料96包括8個平行位元組之密文。

該密文經由互斥或運算以產生一含有8個平行位元組 FD_1-FD_8 之第一密文導出。詳言之，每一密文位元組 C_1-C_8 ，係與相同數目之第一輸入資料位元組 F_1-F_8 作互斥或運算以產生第一密文導出。因此，密文位元組 C_1 係藉於互斥OR閘103內與輸入資料 F_1 作互斥或運算以產生第一密文導出位元組 FD_1 。密文位元組 C_2 係藉與輸入位元組 F_2 經由互斥OR閘105作互斥或運算以產生第一密文導出 FD_2 。依此類推，直到密文位元組 C_8 與輸入資料位元組 F_8 經由互斥OR閘117作互斥或運算為止。

第一密文導出及第二輸入資料經由處理以輸出一第二密文導出，其包括8個平行位元組 SD_1-SD_8 。詳言之，每個第一密文導出位元組 FD_1-FD_8 係與相同數目之第二輸入資料位元組 S_1-S_8 作互斥或運算以產生第二密文導出。因此，第一密文導出 FD_1 係與第二輸入資料位元組 S_1 經互斥或

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(10)

開119作用以產生第二密文導出 SD_1 。第一密文導出 FD_2 係與第二輸入資料位元組 SD_2 經由互斥或開121作互斥或運算以產生第二密文導出 SD_2 。依此類推直到一密文導出 FD_8 與第二輸入資料位元組 S_8 (經互斥或開133)作互斥或運算以產生第二密文導出 SD_8 為止。

圖5所示之具體實施例中，輸入至DES處理器90之7個位元組鍵94係由輸入資料92之位元組 F_2-F_8 所提供。另外，僅輸出資料96之第一組7個位元組有使用。

根據圖5之具體實施例，每個第一組7個輸入資料位元組 F_1-F_7 係與後續的輸入資料位元組 F_2-F_8 分別作互斥或運算，以產生7個位元組之前向資料 FF_1-FF_7 。因此，輸入資料位元組 F_1 係於互斥或開102內與輸入資料位元組 F_2 作互斥或運算以產生前向資料 FF_1 。同理，輸入資料位元組 F_2 於互斥或開104內與輸入資料位元組 F_3 作互斥或運算以產生前向資料 FF_2 。依此類推，直至經由剩餘之互斥或開106，108，110，112及114之作用以產生剩餘之前向資料為止。

每個前向資料位元組 FF_1-FF_7 與相同數目之密文位元組 C_1-C_7 作互斥或運算產生一包括7個平行組 D_1-D_7 之密文導出。因此，舉例而言，前向位元組 FF_1 係於互斥OR開120內與密文位元組 C_1 作互斥或運算以產生密文導出位元組 D_1 。剩餘的資料輸出位元組分別於互斥或開122，124，126，128，130及132中與剩餘之前向資料位元組作互斥或運算以產生剩餘的密文導出位元組 D_2-D_7 。

五、發明說明(11)

請注意於圖4、圖5中之互斥或閘可由查表予以代替，該等查表由個別的輸入予以定址以提供其中之互斥或運算。

現應可瞭解本發明提供之密碼裝置可克服習知技藝之不具有互補特性之安全結構中潛在的保全問題。

雖然本發明已透過不同之具體實施例予以詳述，但熟手本行之人士在不脫離本發明之精神和範圍內，仍可作種種之修改與變型，本發明之範圍以申請專利範圍所界定者為準。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

四、中文發明摘要(發明之名稱:

具有雙前向雜湊函數之密碼裝置

本裝置係使用一雙前向雜湊函數來確證資訊以於實施密碼演算法時提供互補性。密碼處理器具有一接收明文之第一輸入、具有一接收一鍵之第二輸入及一用以輸出藉由加密性地處理該明文及鍵所產生之密文之輸出。第一迴路元件係因應於該密文及明文而輸出一第一密文導出。第二迴路元件係因應於至少一部份第一密文導出及輸出及該鍵而輸出一第二密文導出。第一及第二迴路元件可為XOR閘。另外，此等元件能以查表之方式來提供。後續的密碼處理器級具有接收一第二明文之第一輸入、接收第二密文導出以作為一鍵之第二輸入，及一用以輸出藉由加密性地處理第二明文與第二密文導出所產生之第二密文之輸出。於具體實施例中，該密碼處理器係一DES處理器。

英文發明摘要(發明之名稱:

"CRYPTOGRAPHIC APPARATUS WITH
DOUBLE FEEDFORWARD HASH FUNCTION"

Apparatus is provided for authenticating information using a double feedforward hash function to provide complementarity in the implementation of an encryption algorithm. A cryptographic processor has a first input for receiving plaintext, a second input for receiving a key and an output for outputting ciphertext generated by cryptographically processing the plaintext and key. A first circuit element is responsive to the ciphertext and plaintext for outputting a first ciphertext derivative. A second circuit element is responsive to at least a portion of the first ciphertext derivative and the key for outputting a second ciphertext derivative. The first and second circuit elements can be XOR gates. Alternatively, these elements can be provided using lookup tables. Subsequent cryptographic processor stages can be provided having a first input for receiving second plaintext, a second input for receiving the second

四、中文發明摘要（發明之名稱：

)

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

英文發明摘要（發明之名稱：

)

ciphertext derivative as a key, and an output for outputting second ciphertext generated by cryptographically processing the second plaintext and the second ciphertext derivative. In an illustrated embodiment, the cryptographic processor is a DES processor.

六、申請專利範圍

1. 一種密碼裝置，包括：

一密碼處理器，具有一第一輸入端供接收第一輸入資料之八個平行位元組 F_1-F_8 ，一第二輸入端供接收第二輸入資料之八個平行位元組 S_1-S_8 ，以及一輸出端供輸出藉由將該第一及第二輸入資料予以加密處理所產生之八個平行位元組 C_1-C_8 之密文；

第一裝置，供處理該密文及第一輸入資料以產生一含有八個平行位元組 FD_1-FD_8 之第一密文導出；以及

第二裝置，供處理該第一密文導出及第二輸入資料，用以輸出一含有八個平行位元組 SD_1-SD_8 之第二密文導出；其中：

該第一裝置將每一密文位元組 C_1-C_8 與相同數目之第一輸入資料位元組 F_1-F_8 予以邏輯處理，以產生該第一密文導出；以及

該第二裝置將每一個第一密文導出位元組 FD_1-FD_8 與相同數目之第二輸入資料位元組 S_1-S_8 予以邏輯處理，以產生該第二密文導出。

2. 根據申請專利範圍第1項之密碼裝置，其中：

該第一裝置含有一非線性函數，用以邏輯處理每一密文位元組 C_1-C_8 與相同數目之第一輸入資料位元組 F_1-F_8 ，以產生該第一密文導出；以及

該第二裝置含有一非線性函數，用以邏輯處理每一個第一密文導出位元組 FD_1-FD_8 與相同數目之第二輸入資料位元組 S_1-S_8 ，以產生該第二密文導出。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

3. 根據申請專利範圍第2項之密碼裝置，其中該等非線性函數輸出之位元數為輸入者之一半。
4. 根據申請專利範圍第1項之密碼裝置，其中第一裝置將每一密文位元組 C_1-C_8 與相同數目之第一輸入資料位元組 F_1-F_8 作互斥或運算，以產生該第一密文導出；以及
該第二裝置將每一密文導出位元組 FD_1-FD_8 與相同數目之第二輸入資料位元組 S_1-S_8 作互斥或運算，以產生該第二密文導出。
5. 根據申請專利範圍第4項之密碼裝置，其中第一裝置含有一查表，可由第一輸入資料與該密文予以定址，以輸出其中相同數目位元組之互斥或運算。
6. 根據申請專利範圍第5項之密碼裝置，其中第二裝置含有一查表，可由第二輸入資料與第一密文導出所定址，以輸出其中相同數目位元組之互斥或運算。
7. 根據申請專利範圍第4項之密碼裝置，其中第二裝置含有一查表，可由第二輸入資料及第一密文導出予以定址，以輸出其中相同數目位元組之互斥或運算。
8. 根據申請專利範圍第1項之密碼裝置，另包括：
一第二密碼處理器級，具有一第一輸入端供接收第二輸入資料之八個平行位元組，一第二輸入端供接收第二密文導出，以及一輸出端供輸出藉由將第三輸入資料與第二密文導出予以加密處理所產生之八個平行位元組之第二密文。
9. 根據申請專利範圍第8項之密碼裝置，其中該等密碼處

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

編

六、申請專利範圍

理器為DES處理器。

10. 根據申請專利範圍第1項之密碼裝置，其中該密碼處理器為一DES處理器。
11. 根據申請專利範圍第2項之密碼裝置，另含有查表供實施該第一及第二裝置之非線性函數。
12. 一種密碼裝置，包括：

一密碼處理器，具有一第一輸入端供接收第一輸入資料之八個平行位元組 F_1-F_8 ，一第二輸入端供接收第一輸入資料之平行位元組 S_1-S_8 以作為一鍵，以及一輸出端供輸出藉由將該輸入資料與該鍵予以加密處理所產生之七個平行位元組 C_1-C_7 之密文；

第一裝置供邏輯處理每一第一組七個輸入資料位元組 F_1-F_7 與後續之輸入資料位元組 F_2-F_8 ，以產生七個位元組的前向資料 FF_1-FF_7 ；以及

第二裝置供邏輯處理每一前向資料位元組 FF_1-FF_7 與相同數目之密文位元組 C_1-C_7 ，以產生一含有七個平行位元組 D_1-D_7 之密文導出。

13. 根據申請專利範圍第12項之密碼裝置，其中：

第一裝置含有一非線性函數，用以將每一第一組七個輸入資料位元組 F_1-F_7 分別與後續之輸入資料位元組 F_2-F_8 予以邏輯處理，以產生該七個位元組之前向資料 FF_1-FF_7 ；以及

第二裝置含有一非線性函數，用以將每一前向資料位元組 FF_1-FF_7 與相同數目之密文位元組 C_1-C_7 予以邏輯

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

處理，以產生該含有該七個平行位元組 D_1-D_7 之密文導出。

14. 根據申請專利範圍第13項之密碼裝置，其中該等非線性函數輸出之位元數為輸入者之一半。

15. 根據申請專利範圍第12項之密碼裝置，其中：

第一裝置將每一第一組七個輸入資料位元組 F_1-F_7 分別與後續之輸入資料位元組 F_2-F_8 作互斥或運算，以產生該七個位元組之前向資料 FF_1-FF_7 ；以及

第二裝置將每一前向資料位元組 FF_1-FF_7 與相同數目之密文位元組 C_1-C_7 作互斥或運算，以產生該含有七個平行位元組 D_1-D_7 之密文導出。

16. 根據申請專利範圍第15項之密碼裝置，其中第一裝置含有一查表，可由第一組七個與後續之輸入資料位元組予以定址，以輸出其中之互斥或運算。

17. 根據申請專利範圍第16項之密碼裝置，其中第二裝置含有一查表，可由該等前向資料位元組與相同數目之密文位元組予以定址，以輸出其中之互斥或運算。

18. 根據申請專利範圍第15項之密碼裝置，其中第二裝置含有一查表，可由該等前向資料位元組與相同數目之密文位元組予以定址，以輸出其中之互斥或運算。

19. 根據申請專利範圍第12項之密碼裝置，其中該密碼處理器為一DES處理器。

20. 根據申請專利範圍第13項之密碼裝置，另包括有查表供實現第一及第二裝置之非線性函數。

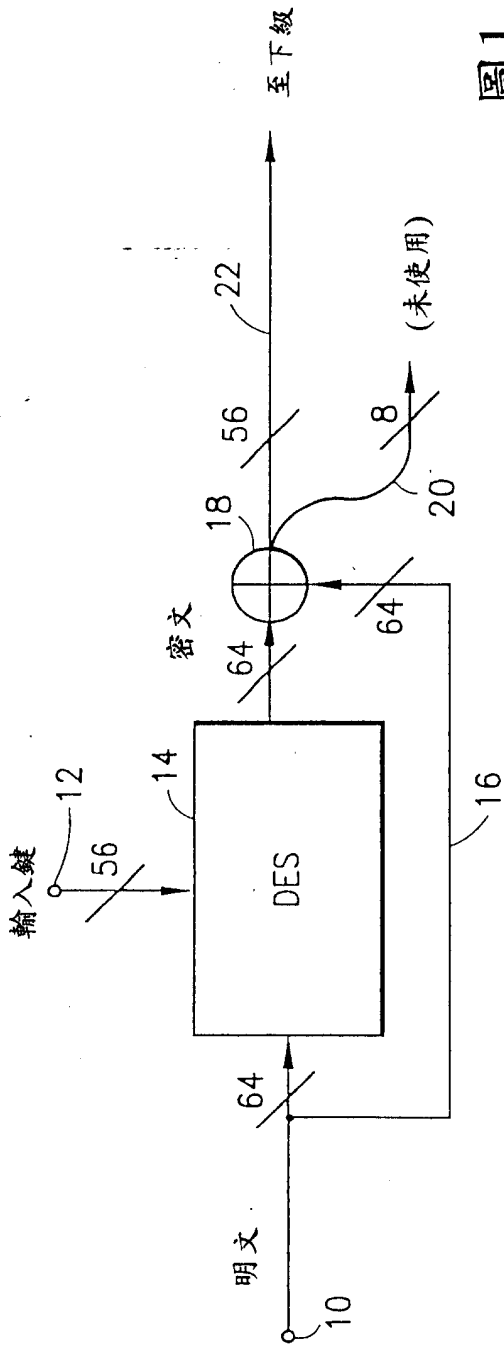


圖1

先前技藝

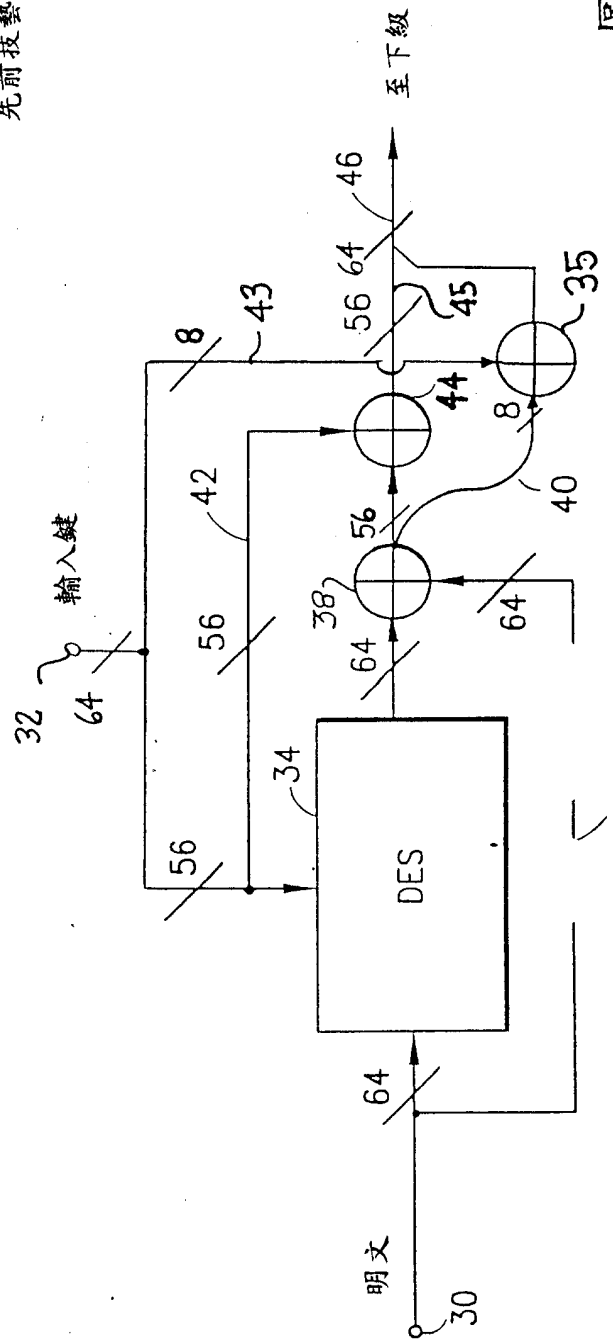


圖2

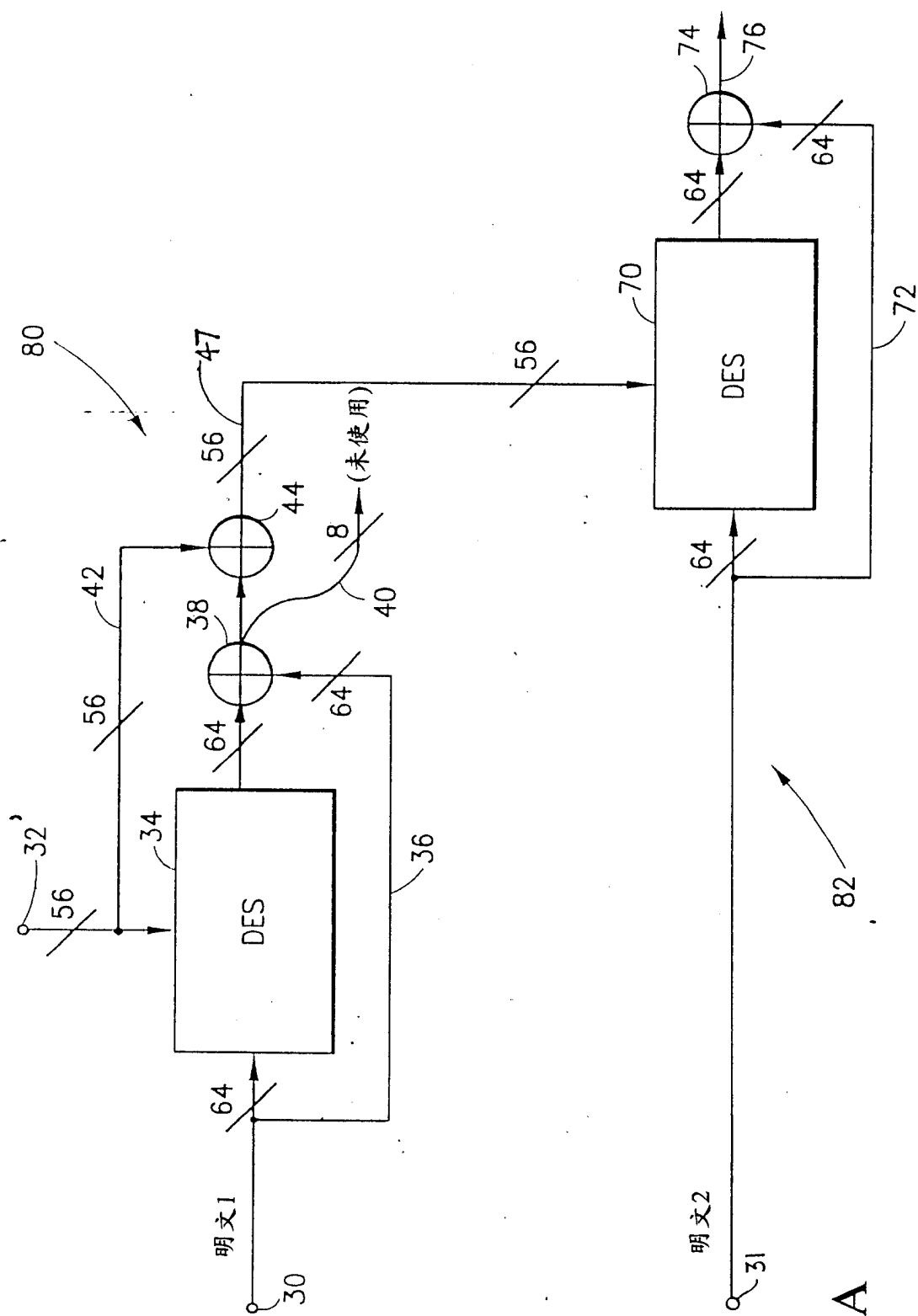


圖3A

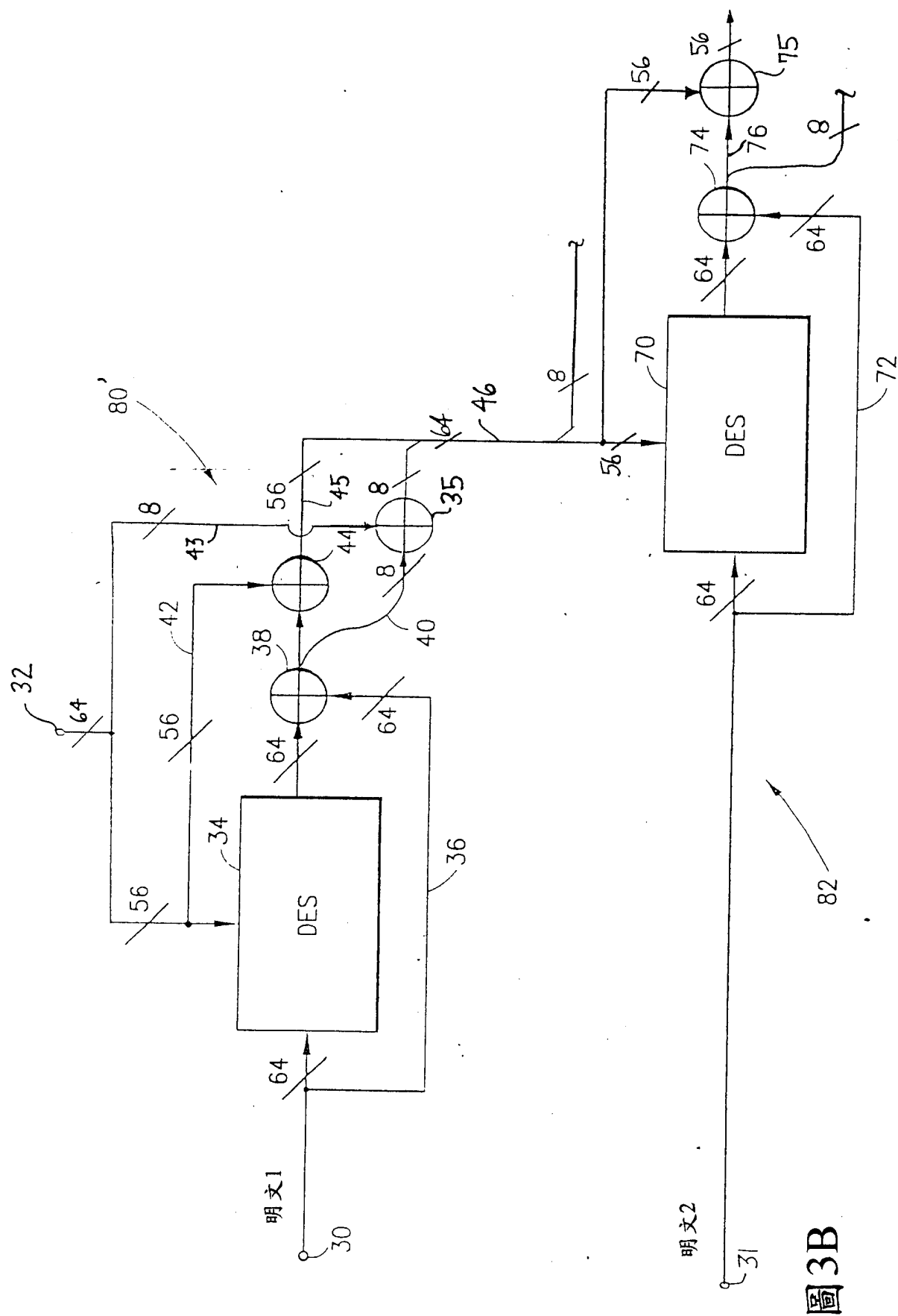


圖3B

圖4

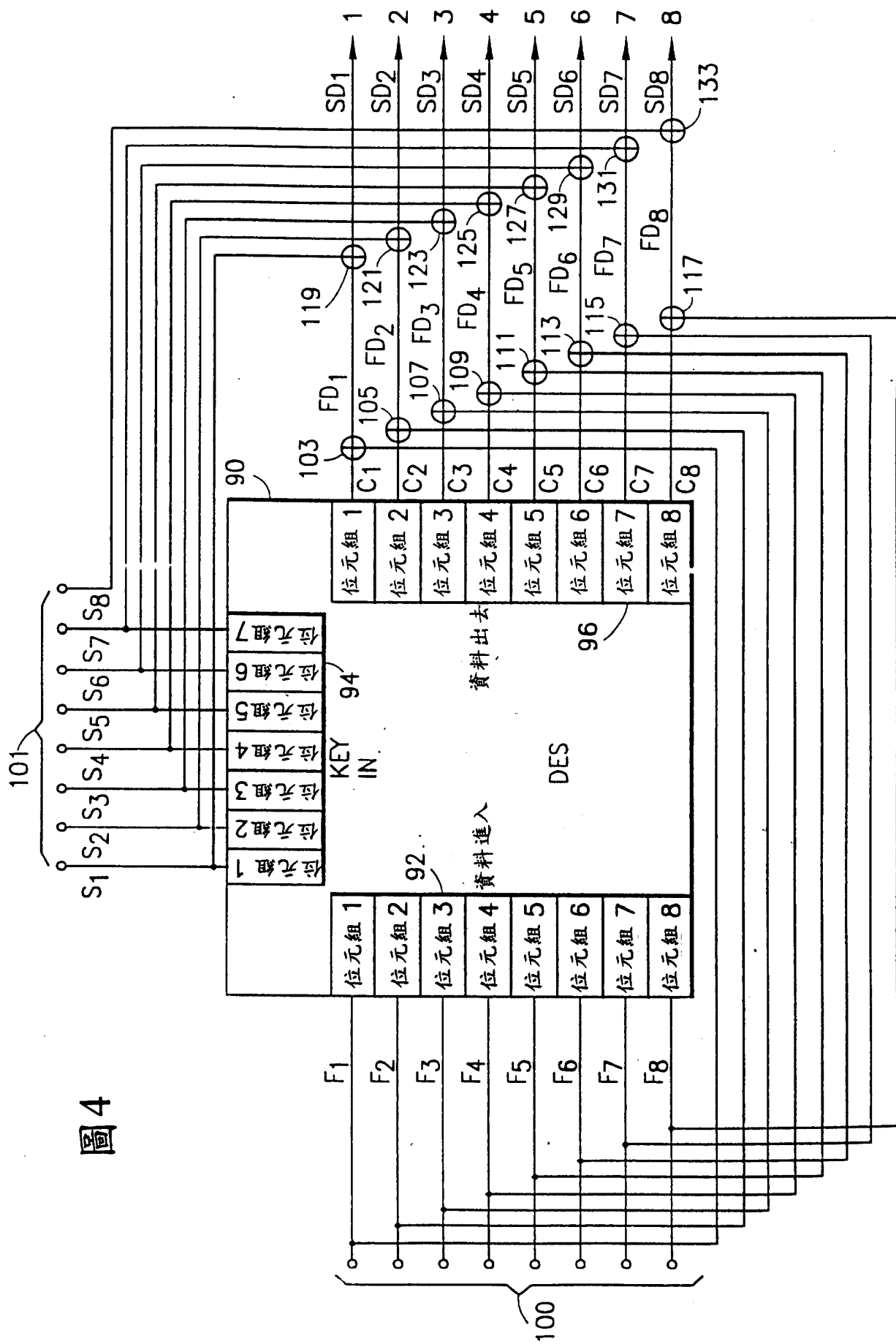


圖5

