

公告本

申請日期	88 年 12 月 13 日
案 號	88121816
類 別	G46F13/44

A4
C4

517189

(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
	英 文	
二、發明 創作人	姓 名	(1) 大木優 (2) 福澤寧子 (3) 奧原進
	國 籍	(1) 日本 (2) 日本 (3) 日本
	住、居所	(1) 日本國東京都千代田區丸の内一丁目五番一號 新丸ビル(株)日立製作所知的所有權本部内 (2) 日本國東京都千代田區丸の内一丁目五番一號 新丸ビル(株)日立製作所知的所有權本部内 (3) 日本國東京都千代田區丸の内一丁目五番一號 新丸ビル(株)日立製作所知的所有權本部内
三、申請人	姓 名 (名稱)	(1) 日立製作所股份有限公司 株式会社日立製作所
	國 籍	(1) 日本
	住、居所 (事務所)	(1) 日本國東京都千代田區神田駿河台四丁目六番地
	代 表 人 姓 名	(1) 庄山悦彦

裝 訂 線

經濟部智慧財產局員工消費合作社印製

申請日期	88 年 12 月 13 日
案 號	88121816
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 新型名稱	中 文	
	英 文	
二、發明 創作人	姓 名	(4) 神永正博
	國 籍	(4) 日本 (4) 日本國東京都千代田區丸の内一丁目五番一號 新丸ビル(株)日立製作所知的所有權本部内
三、申請人	住、居所	
	姓 名 (名稱)	
	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝
訂
線

經濟部智慧財產局員工消費合作社印製

(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

日本 1998 年 12 月 14 日 10-354156 ☒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

經濟部智慧財產局員工消費合作社印製

五、發明說明(1)

本發明係關於資訊處理裝置，特別是關於，很適合當作機密性很高之IC卡等之耐搗固裝置(tamper resistance equipment)使用之資訊處理裝置。

IC卡主要是被用在，保持不能被隨意改寫之資訊，或機密資訊之使用密碼鍵之資料之加密(encryption)，或密碼文件(cipher text)之解密(decryption)之裝置。

IC卡因為沒有電源，因此插入讀寫機後，則受到電源之供應，成為可動作狀態。成為可動作狀態後，從讀寫機接受指令，依照指令進行資料之傳送。

IC卡之架構係如第1圖所示，在卡片101上載置IC卡用晶片102而成。一般IC卡有接點，而經由接點由讀寫機接受電源之供應，或與讀寫機進行資料之通信。

IC卡用晶片之架構基本上是與電腦相同。其架構係如第2圖所示，由中央運算裝置201、記憶裝置204、輸出輸入埠207、協處理器(coprocessor)202所構成。中央運算裝置201係進行邏輯運算或算術運算之裝置，記憶裝置204係儲存程式或資料之裝置。輸出輸入埠207係與讀寫機進行通信之裝置。協處理器係用以進行剩餘運算(modular calculus)之特別運算裝置，係用以運算非對稱密碼(anti-symmetric cryptography)之RSA之裝置。IC卡用處理器中，有很多不具備協處理器。資料匯流排203係用以連接各裝置之匯流排。

記憶裝置204由ROM、RAM、EEPROM等構成。ROM係無法變更之記憶器，主要是用以儲存程式之記憶器。RAM係可以自由更改之記憶器，但電源中斷後，所記憶之內容

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(2)

便會消失。從讀寫機抽出IC卡後，電源之供應便中斷，因此，RAM之內容無法保存。EEPROM係電源之供應中斷後，仍可保持其內容之記憶器。有需要改寫，從讀寫機抽出IC卡後仍需儲存所保持之資料時使用。例如預付卡之預付之度數，必須每一次使用後改寫，且從讀寫機抽出後仍需保持資料，因此用EEPROM來保持。

IC卡因為在IC卡用晶片中密封有程式或重要之資訊，因此被用以儲存重要資訊或在卡片內處理密碼。在IC卡處理之密碼之解讀難度，被認為與密碼運算法之解讀之困難度相同。但有人指出，若觀測IC卡在進行密碼處理時所消耗之電流，加以分析，便可以較解讀密碼運算法容易推測密碼處理之內容或密碼鍵。消耗電流可以藉由測量從讀寫機供給之電流觀測到。這種危險性記載於John Wiley & sons公司出版，W. Rankl & W. Effing 著，「Smart Card Handbook」之8.5.1.1 Passive protective mechanisms (263頁)。

搭載IC卡用晶片之CMOS，在輸出狀態從1變成0或從0變成1時，會消耗電流。尤其是，資料匯流排203之匯流排具有很大的電氣容量，因此匯流排之值從1變成0或從0變成1時，會消耗很大之電流。因此可以瞭解，若觀測消耗電流，便有可能知道在IC卡用晶片內是什麼在動作。

第3圖表示，IC卡用晶片之一個周期之消耗電流之波形。因處理之資料電流波形會如301或302不相同。這樣之差別會因流過匯流排203之資料，或在中央運算裝置201處理

五、發明說明 (3)

之資料而不同。

假設將資料轉送至16位元之預充電匯流排。預充電匯流排係在轉送資料前將所有之匯流排之值變成0之匯流排。向此匯流排傳送值不同但“1”之位元數相同之資料，例如“1”之位元數為2之16進數“88”與“11”時，電流波形成為大致相同之波形。這個理由是從“0”變化到“1”之位元數相同，因此，消耗同樣之電流，成為相同之電流波形之故。若傳送“1”之位元數相差一個之資料，例如“1”之位元數為3之“89”或“19”時，其消耗電流與“1”之位元數為2之資料之消耗電流不一樣。這是因為有3位元分匯流排之值從“0”變化到“1”，而多消耗這部分之電流之故。因此，較之先前之2位元變化之資料，消耗電流會大出1位元分。一般有“1”之位元數愈多，電流波形愈高之規則性。從此規則性可以推測出轉送中之資料。

第3圖所示之電流波形，不只是匯流排，係構成IC卡片用晶片之構成要素所消耗之電流之總和。惟諸如IC卡片用晶片之微電腦，係分成主要是將資料轉送至匯流排之階段，主要是CPU在運算之階段，及將資料寫入暫存器之階段。因此，若注意到各階段，便知道電流消耗主要是起因於那一階段，而可以猜測在該部分之資料操作。

茲以下示之向左移位命令為例子，說明具體命令有什麼差別。

shift R1 (式1)

此命令係，將暫存器1之內容向左移動，使暫存器之位

(請先閱讀背面之注意事項)

裝

訂

線

五、發明說明(4)

元列向左移動，最上位位元之值成為載體而進入條件碼暫存器之命令。因為，暫存器R1之最上位位元經由資料匯流排轉送至條件碼暫存器，因此，比較電流波形之大小便有可能識別出最上位之位元是“0”或“1”。若R1內有重要之資料，便有可能知道該資料之第1位元是“0”或“1”。尤其是像DES之密碼處理，會經常有將密碼鍵移位之操作。在此項移位操作時產生可以猜測密碼鍵之資料之電流波形，而有密碼鍵被猜出來之危險性。

這在使用協處理器202運算時也相同。若運算內容有依存密碼鍵之偏移時，便有可能被從該偏移求出消耗電流，而被猜測出密碼鍵。

本發明之課題在於，減低以IC卡片用晶片進行之資料處理與消耗電流之關連性。消耗電流與晶片之處理之關連性一降低，要從觀測到之消耗電流之波形推測IC卡片用晶片內之處理或密碼鍵，便很困難。本發明之著眼點在於將以IC卡片用晶片處理之資料變形後再處理，藉此使由消耗電流之波形推測處理或密碼鍵很困難。

以IC卡片用晶片所代表之耐搗固裝置可以當作是，具備有：備有儲存程式之程式儲存部，及保存資料之資料儲存部之記憶裝置；依照程式執行一定之處理，進行資料處理之中央運算裝置；而程式係由指示中央運算裝置執行處理之處理命令構成之一個以上之資料處理手段所構成之資訊處理裝置。本發明之減低所處理之資料與IC卡片用晶片所消耗電流之關連性之方法是，以攪亂用資料將欲處理之

(請先閱讀背面之注意事項
填寫本頁)

裝
訂
線

五、發明說明(5)

資料變形，以變形之資料進行處理資料，處理後，使用攪亂用資料進行反變形，求出正確之處理結果。資料處理後使用之攪亂用資料，如有需要，可使用進行與資料處理相同處理之已完成處理之攪亂用資料。而攪亂用資料係按每一次處理隨機設定。如此即可在資料處理時，不使用本來之資料，每次使用不同之變形之資料。因此要從電流波形猜測資料十分困難。

具体上是，首先作成攪亂用資料 X_i ，將資料 D_1 加以變形，作成變形資料 H_1 。變形之方法有，互斥邏輯和或加法、減法等。處理資料時，使用變形資料 H_1 ，進行資料處理，生成已完成處理變形資料 H_2 。本來是要使用資料 D_1 ，但是因為使用變形資料 H_1 ，因此從處理變形資料 H_1 之電流波形很難能猜測出資料 D_1 之資料。變形資料 H_1 在每一次處理時，均由攪亂用資料 X_i 加以變形，因此每一次均成不同之資料。因此，處理變形資料 H_1 之電流波形也是每一次成不同之波形，從該波形猜測出變形資料 H_1 也不具意義。

攪亂用資料 X_i 也與資料 D_1 一樣需要處理資料時，以攪亂用資料 X_i 為輸入，進行資料處理，作成已完成處理攪亂用資料 X_o 。而使用已完成處理攪亂用資料 X_o 處理已完成處理變形資料 H_2 ，獲得以輸入資料處理構件處理輸入資料 D_1 之結果之已完成處理資料 D_2 。

有需要使用資料變形方法不相同之方法時，有時需要連結資料變形(connect several data transformation)而加以執行之必要。這個時候是組合資料變形、變形資料處理、

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明 (6)

攪亂用資料處理、資料反變形處理，使資料變形連續，避免對本來之資訊進行資料處理。

本發明可以使用在，密碼運算法之對調資料之轉置或換字，或者表格擷取等之資訊隱蔽。對調資料時，將互斥邏輯和使用在資料之變形，資料處理時同樣處理變形之資料與攪亂用資料，恆常對變形之資料與攪亂用資料執行互斥邏輯和，進行變形處理以獲得本來之資料，是最有效之方法之一。

本發明之一個較具代表性之架構如下。係一種，具備有：備有儲存程式之程式儲存部，及保存資料之資料儲存部之記憶裝置；依照程式執行一定之處理，進行資料處理之中央運算裝置；具有程式是指示中央運算裝置執行處理之處理命令之一個以上之資料處理手段；及由一個資料處理手段處理其輸入資料，處理輸出資料之輸入資料處理構件之資訊處理裝置，其特徵在於，具備有：

使用攪亂用資料 X_i 將輸入資料 D_1 加以變形，而作成變形資料 H_1 之資料變形處理構件；在上述輸入資料處理構件對上述變形資料 H_1 實施運算處理 OP_1 ，取代對上述輸入資料 D_1 實施上述運算處理 OP_1 ，以作成已完成處理變形資料 H_2 之變形資料處理構件；對上述攪亂用資料 X_i 實施上述運算處理 OP_1 ，以作成已完成處理攪亂用資料 X_o 之攪亂用資料處理構件；以及，使用上述已完成處理攪亂用資料 X_o 對已完成處理變形資料 H_2 實施運算處理 OP_2 ，而獲得，與對輸入資料 D_1 實施運算處理 OP_1 之結果相同之已完成處理資料 D_2 之

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明(7)

資料反變形處理構件。

上述 OP1 對應，例如後述之第 4 圖所示之實施例中之處理。而上述 OP1' 所對應的是，例如後述之第 5 圖所示之實施例中之攪亂用資料 2 之處理 (510 至 513 及 516 至 520)。其他申請專利範圍所述之 OP1、OP1' 也可以同樣解釋。

茲參照附圖，說明本發明之實施例如下。

第 1 圖表示 IC 卡之外觀。IC 卡 101 由 ISO 7816 規格規定其大小，IC 卡用晶片 102 之位置或接點數及分配。

第 2 圖係 IC 卡用晶片 102 之內部架構。該架構係在傳統技術之說明已予詳述。本發明係將程式 205 要處理之資料加以搗亂，使其很難能由處理中所產生之 IC 卡用晶片之硬體所消耗之電流波形，猜測原來之資料。

先藉下列簡單之命令列，說明其基本構想。

logica_shiftl R1 (式 2)

xor R1 R2 (式 3)

式 2 是要將暫存器 R1 之值，邏輯方式向左繞行 (loop) 之命令。最上位位元移動到最下位位元。將其結果，儲存在暫存器 R1。再取其結果與暫存器 R2 之內容之互斥邏輯和，將結果儲存在暫存器 R2 之命令列。這種命令在諸如 DES 之密碼運算法會頻繁出現。式 2 及式 3 係直接處理資料，因此資料之內容會使電流波形之大小改變。因此觀測電流波形，便有可能猜測到資料。

將上述命令列變更成下列命令列，以免直接處理由式 2 及式 3 之命令處理之資料。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (8)

xor X1 R1 (式 4)

xor X2 R2 (式 5)

logica_shift1 R1 (式 6)

xor R1 R2 (式 7)

logica_shift1 X1 (式 8)

xor X1 X2 (式 9)

xor X2 R2 (式 10)

其中 X1 與 X2 係隨便選之亂數，係搗亂用資料。式 4 與式 5 係在暫存器 R1 與 R2 進行亂數 X1 與 X2 之互斥邏輯和，將原來之資料加以變形之變形處理。式 6 及式 7 與式 2 及式 3 是相同之資料處理，但因有變形處理，因而成為 R1 與 R2 之值與本發明之資料不同值之資料。式 8 與式 9 係進行搗亂用資料本身之資料處理。藉式 10 取得搗亂用資料之資料結果與式 7 之處理結果之互斥邏輯和，而回到原本之資料之反變形處理。這是申請專利範圍第 7 項之實施例。

若以具體之數值表示值之變化，則如下。假設 R1 與 R2 之值為

R1 : 11001010 (式 11)

R2 : 01010111 (式 12)

式 2 之結果之 R1 之值為

R1 : 10010101 (式 13)

而式 3 之處理結果如下。

R2 : 11000010 (式 14)

接下表示進行本發明之變形時之情形。首先使搗亂用

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明 (9)

資料如下。假設 R1 與 R2 之值相同。

X1 : 10010111 (式 15)

X2 : 00111010 (式 16)

處理式 4 與式 5 之結果，暫存器 R1 與 R2 之值成為

R1 : 01011101 (式 17)

R2 : 01101101 (式 18)

處理式 6 與式 7 之結果，暫存器 R1 與 R2 之值成為

R1 : 10111010 (式 19)

R2 : 11010111 (式 20)

在式 8 與式 9 對搗亂用資料 X1、X2 也同樣進行資料處理之結果成為如下。

X1 : 00101111 (式 21)

X2 : 00010101 (式 22)

而進行式 10 之反變形處理之結果，獲得與直接處理原本之資料時之處理結果式 14 同樣之結果。

R2 : 11000010 (式 23)

如本例所示進行變形處理，變形之資料與搗亂用資料均進行同樣之處理，使用其結果進行反變形，便可以求出原來之值。而因資料處理時未使用原本之資料，因此看其波形，雖可猜測正在處理之變形資料，但很難猜測真正的資料。再以一般之形式，表示以上之藉具體數值表示之例子。假設實際之處理如下。

Output(j) = f(Input(i)) (式 24)

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明 (10)

這是輸入 i 個之輸入 Input，進行處理 f ，輸出 j 個輸出 Output 之處理。式 2 與式 3 之例子，係 R1 與 R2 之兩個輸入，輸出有一個，儲存在 R2 之例子。爲了要使其很難從處理式 24 中之電流波形猜測所處理資料，依下列方式進行。

$$\text{InputX}(i) = h(\text{Input}(i), X(i)) \quad (\text{式 } 25)$$

$$\text{OutputX}(j) = f(\text{inputX}(i)) \quad (\text{式 } 26)$$

$$X_{\text{output}}(j) = f(X(i)) \quad (\text{式 } 27)$$

$$\text{Output}(j) = g(\text{OutputX}(i), X_{\text{output}}(i)) \quad (\text{式 } 28)$$

式 25 係使用搗亂用資料 $X(i)$ ，將輸入資料 $\text{Input}(i)$ 加以變形，作成變形之輸入資料 $\text{InputX}(i)$ 之處理。 h 係變形操作。式 26 係使用變形之輸入資料進行資料處理之資料處理。式 27 係將搗亂用資料與輸入資料同樣處理之搗亂用資料處理。式 28 係對變形之輸入資料之資料處理結果 $\text{OutputX}(j)$ 與搗亂用資料之處理結果 $X_{\text{output}}(j)$ 進行變形之反變換之反變形處理。 g 係反變換操作。

在先前之例子，式 4 與 5 對應式 25 之處理，變形操作 h 係互斥邏輯和。式 6 與 7 對應式 26 之變形之輸入資料之資料處理。式 8 與 9 對應式 27 之搗亂用資料之資料處理。式 10 對應式 28 之反變形處理。變形操作 g 係互斥邏輯和。

變形操作 h 與變形操作 g 選擇什麼，由資料處理 f 之特性

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (11)

而定。在式 2 與式 3 之處理，互斥邏輯和是變形操作 h，也是與變形操作 g。這是因為，在移位操作或 XOR 操作時，將互斥邏輯和選擇為變形操作 h，因此變形操作 g 也可以選擇互斥邏輯和。若取相同資料之互斥邏輯和，邏輯上互斥邏輯和等於零，取互斥邏輯和之操作會消失之故。

若資料處理 f 是加減法，則可以在變形操作 h 選擇加法或減法，在反變形操作選擇減法或加法。例如，

$$\text{Output} = \text{Input}(1) + \text{Input}(2) - \text{Input}(3) \quad (\text{式 } 29)$$

之操作可以進行下述變形處理

$$\text{InputX}(1) = \text{Input}(1) + X(1) \quad (\text{式 } 30)$$

$$\text{InputX}(2) = \text{Input}(2) + X(2) \quad (\text{式 } 31)$$

$$\text{InputX}(3) = \text{Input}(3) + X(3) \quad (\text{式 } 32)$$

而藉處理變形之輸入資料，獲得變形之輸入資料之處理結果。

$$\text{OutputX} = \text{InputX}(1) + \text{InputX}(2) - \text{InputX}(3) \quad (\text{式 } 33)$$

搗亂用資料同樣進行資料處理。

$$X_{\text{output}} = X(1) + X(2) - X(3) \quad (\text{式 } 34)$$

而進行反變形處理。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (12)

$$\begin{aligned}\text{Output} &= g(\text{Xoutput}) = \text{OutputX} - \text{Xoutput} \\ &= \text{InputX}(1) + \text{InputX}(2) - \text{InputX}(3) - (\text{X}(1) + \text{X}(2) - \text{X}(3)) \\ &= \text{Input}(1) + \text{Input}(2) - \text{Input}(3) \quad (\text{式 } 35)\end{aligned}$$

可以獲得正確之輸出資料。這是因為在加減法之運算中，加上某值運算，從最後之結果減去加上之值，即可決定正確之結果之故。這是申請專利範圍第8、9項之實施例。

若資料處理f是乘除法，則可以在變形操作h選擇乘法或除法，在反變形操作選擇除法或乘法，而實現變形處理及反變形處理。其理由是，與加減法相同，在乘除法之運算中，乘上(除以)某值進行運算，在最後之結果除以(乘上)所乘(所除)之值即可獲得正確之結果。這是申請專利範圍第10、11項之實施例。

若資料處理f是剩餘運算之加減法(addition and subtraction in modular calculation)，則可以在變形操作h選擇法N之整數倍之加減法。例如考量下述加減剩餘運算。

$$\text{Output} = \text{Input}(1) + \text{Input}(2) - \text{Input}(3) \bmod N \quad (\text{式 } 36)$$

將輸入Input(i)加以變形如下。

$$\text{InputX}(i) = \text{Input}(i) + k(i) * N \quad (\text{式 } 37)$$

而使用變形之輸入資料進行加減剩餘運算。

$$\text{OutputX} = \text{InputX}(1) + \text{InputX}(2) - \text{InputX}(3) \bmod N \quad (\text{式 } 38)$$

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (13)

使用式 37 即可將此式變形成

$$\begin{aligned} \text{OutputX} &= (\text{Input}(1) + k(1)*N) + (\text{Input}(2) + k(2)*N) - \\ &(\text{Input}(3) + k(3)*N) \bmod N = (\text{Input}(1) + \text{Input}(2) - \text{Input}(3)) + \\ &(k(1)*N + k(2)*N - k(3)*N) \bmod N \quad (\text{式 } 39) \end{aligned}$$

而因使用剩餘運算特徵之

$$0 = k * N \bmod N \quad (\text{式 } 40)$$

式 39 之第 2 個括弧內之值成為 0，式 39 變成

$$\text{OutputX} = (\text{Input}(1) + \text{Input}(2) - \text{Input}(3)) \bmod N \quad (\text{式 } 41)$$

亦即，變形之輸入資料之運算結果與本來之運算結果一樣。這是，因為使用剩餘運算之特徵，而不需要搗亂用資料之資料處理及反變形處理之例子。這是因為搗亂用資料之資料處理結果

$$X_{\text{output}(i)} = k(1) * N + k(2) * N - k(3) * N \bmod N \quad (\text{式 } 42)$$

會成為 0，因此不需要搗亂用資料之資料處理及反變形處理。此為申請專利範圍第 12 項之實施例。

若資料處理 f 是剩餘運算之乘法，可以在變形操作 h 使用在法 N 之整數倍加 1 者。例如考量下述乘法剩餘運算。

$$\text{Output} = \text{Input}(1) * \text{Input}(2) * \text{Input}(3) \bmod N \quad (\text{式 } 43)$$

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (14)

將輸入 Input(i) 加以變形如下。

$$\text{InputX}(i) = \text{Input}(i) + k(i) * N + 1 \quad (\text{式 } 44)$$

而使用變形之輸入資料，進行乘法剩餘運算。

$$\text{OutputX} = \text{InputX}(1) * \text{InputX}(2) * \text{InputX}(3) \bmod N \quad (\text{式 } 45)$$

使用式 44 即可將此式變形成

$$\begin{aligned} \text{OutputX} = & (\text{Input}(1) * (k(1)*N + 1)) + (\text{Input}(2) + (k(2)*N + 1) - \\ & (\text{Input}(3) + (k(4)*N + 1)) \bmod N = (\text{Input}(1) * \text{Input}(2) * \text{Input}(3)) * \\ & ((k(1)*N + 1) * (k(2)*N + 1) * (k(3)*N + 1)) \bmod N \quad \dots \quad (\text{式 } 46) \end{aligned}$$

而因使用剩餘運算特徵之

$$0 = k * N \bmod N \quad (\text{式 } 47)$$

式 46 變成

$$\begin{aligned} \text{OutputX} = & (\text{Input}(1) * \text{Input}(2) * \text{Input}(3)) * (1 * 1 * 1) \bmod N \\ = & \text{Input}(1) * \text{Input}(2) * \text{Input}(3) \bmod N \quad (\text{式 } 48) \end{aligned}$$

亦即，變形之輸入資料之運算結果與本來之運算結果一樣。這是因為使用剩餘運算之特徵(式 48)而不需要搗亂用

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明 (15)

資料之資料處理及反變形處理之例子。

若資料處理 f 是剩餘運算之乘法，也可以在變形操作 h 使用對某數 X 與法 N 為倒數之 Y。

$$1 = X * Y \bmod N \quad (\text{式 4 9})$$

此數之簡單者有 X 為 2，而 Y 為 $(N+1) / 2$ 者。這是乘上 X 作為變形操作，而在反變形時乘上等於乘上 X 之次數之 Y，藉此求出本來之處理結果者。例如可以考量下述加減剩餘運算。

$$\text{Output} = \text{Input}(1) * \text{Input}(2) * \text{Input}(3) \bmod N \quad (\text{式 5 0})$$

將輸入 Input(i) 加以變形如下。

$$\text{InputX}(i) = \text{Input}(i) * X \quad (\text{式 5 1})$$

而使用變形之輸入資料，進行乘法剩餘運算。

$$\text{OutputX} = \text{InputX}(1) * \text{InputX}(2) * \text{InputX}(3) \bmod N \quad (\text{式 5 2})$$

而若選擇乘上等於乘上 X 之次數之 Y，做為反變形處理 g，則可以在 OutputX 操作反變形處理 g (式 48) 而獲得正確之結果。

五、發明說明 (16)

$$\begin{aligned}
 \text{Output} &= \text{OutputX} * Y * Y * Y \bmod N \\
 &= \text{InputX}(1) * \text{InputX}(2) * \text{InputX}(3) * Y * Y * Y \bmod N \\
 &= \text{Input}(1) * X * \text{Input}(2) * X * \text{Input}(3) * X * Y * Y * Y \bmod N \\
 &= \text{Input}(1) * \text{Input}(2) * \text{Input}(3) * X * X * X * Y * Y * Y \bmod N \\
 &= \text{Input}(1) * \text{Input}(2) * \text{Input}(3) * X * Y * X * Y * X * Y \bmod N \\
 &= \text{Input}(1) * \text{Input}(2) * \text{Input}(3) \bmod N \quad (\text{式 } 53)
 \end{aligned}$$

式 53 係使用式 49 之性質。本例不需要搗亂用資料之資料處理，但在法 N 將其倒數乘上反變形處理，相等於乘上搗亂用資料之次數，即可獲得正確之結果。這是申請專利範圍第 13 及 14 項之實施例。

以上是資料處理 f 為資料操作之例子，但搗亂從表格之取出資料，搗亂

操作，對防止從電流波形猜測資料上是必要的動作。茲使用從第 33 圖之表格取出資料之例子，來說明有關表格之資料之搗亂，及表格之位址之搗亂。

以搗亂用資料 X1，取第 33 圖之表格之資料之互斥邏輯和。搗亂用資料之值取“9”，而執行表格之值與 9 之互斥邏輯和。其結果便是第 34 圖之表格。然後，為了搗亂表格之位址，執行行號碼與選擇之搗亂用資料 X2 之“3”之互斥邏輯和，執行列號碼與選擇之搗亂用資料 X3 之“2”之互斥邏輯和，重排表格。其結果便是第 35 圖。在原來之表格之第 33 圖之表格第 1 行第 2 列之資料 3301 之“0”，在執行搗亂用資料 X1 與互斥邏輯和之結果，在第 34 圖之表格成為“9” (3401)。而對行號碼與列號碼分別執行與搗亂用資料 X2 及搗亂用資

五、發明說明 (17)

料 X3 之互斥邏輯和之結果，3401 便移到 3501 之位置。爲了搗亂從表格取出資料之操作，製成這些表格。

假設在位址計算之前，已經以搗亂用資料 Y1 與 Y2 分別以互斥邏輯和將行號碼變數 Gyou 及列號碼變數 Retsu 加以變形。亦即，假設正確之行號碼 Gyou 與列號碼 Retsu 必須要對 Y1 及 Y2 與 Gyou 及 Retsu 執行互斥邏輯和方可獲得。其關係如下。

$$Gyou = GyouY1 \text{ xor } Y1 \quad (\text{式 } 54)$$

$$Retsu = RetsuY2 \text{ xor } Y2 \quad (\text{式 } 55)$$

惟進行此反變形處理而使用第 33 圖之表格時，會使用真的位址資料，因此有可能會被從電流波形猜測出來位址資料。於是，首先在製作第 35 圖之表格時，使用在搗亂行號碼及列號碼時使用之搗亂用資料 X2 及搗亂用資料 X3。

$$GyouY1X2 = GyouY1 \text{ xor } X2 \quad (\text{式 } 56)$$

$$RetsuY1X3 = RetsuY2 \text{ xor } X3 \quad (\text{式 } 57)$$

而進行一直在使用之搗亂用資料之反變形處理。

$$GyouX2 = GyouY1X2 \text{ xor } Y1 \quad (\text{式 } 58)$$

$$RetsuX3 = RetsuY2X3 \text{ xor } Y2 \quad (\text{式 } 59)$$

如此做時，因爲沒有使用真的行號碼或列號碼，因此要從電流波形猜測其值很困難。使用 GyouX2 與 RetsuX3，

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (18)

參照第 35 圖之表格 TableX1X2X3，取出 DataX1。

$$\text{DataX1} = \text{TableX1X2X3}(\text{GyouX2、RetsuX3}) \quad (\text{式 6 0})$$

因第 35 圖之表格已經由搗亂用資料 X1 加以變形，此後即以 X1 當作搗亂用資料進行處理，從式 56 至式 60 之處理並沒有使用真的資料。這是申請專利範圍第 16 及第 17 項之實施例。

按一定之處理，隨機生成表格之資料之搗亂用資料 X1，行號碼之搗亂用資料 X2，及列號碼之搗亂用資料 X3，將表格加以變形。如此便可以在每一次處理將表格變形，要從電流波形猜測資料很困難。

以上係說明搗亂用資料之種類及資料變形之方法。接著說明其處理程序。第 4 圖表示，使用基本之搗亂用資料之資訊隱蔽(concealment)程序之實施例。

第 4 圖係基本之程序。藉搗亂用資料生成構件生成搗亂用資料 Xi(401)。此一般性方法有使用亂數產生器或虛擬亂數(Pseudo random number)生成索需要長度之亂數之方法。接著在資料變形處理構件(406)，以搗亂用資料 Xi 將輸入資料 D1(405)變形，生成變形資料 H1(407)。變形方法如上述，有互斥邏輯和、加減法、乘除法等。而以變形資料處理構件(408)，使用變形資料 H1 進行資料處理，生成已完成處理變形資料 H2。另一方面，藉搗亂用資料處理構件(403)，對搗亂用資料 Xi 進行與輸入資料一樣之資料處理，作成已完成處理之搗亂用資料 Xo(404)。而使用搗亂用資料 Xo 與已完

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (19)

成處理變形資料 H2，在資料反變形處理構件(410)，求出真的已完成處理資料 D2(411)。資料變形處理構件(406)或資料反變形處理構件(410)之方法有上述之互斥邏輯和、加減法、乘法、剩餘運算等。這是申請專利範圍第1項之實施例。

第5圖之實施例，係使用兩個搗亂用資料之例子。係在使用第1搗亂用資料之資訊隱蔽處理中，含使用第2搗亂用資料之資訊隱蔽處理之情形。主要流程與第4實施例相同。以第1搗亂用資料對變形之變形資料 H1(507)進行資料處理，再使用第2搗亂用資料 X2i，在第2資料變形處理構件(510)，對其處理結果之已完成處理變形資料 H2(509)進行資料處理，作成已完成處理變形資料 H3(511)。再於第2變形資料處理構件(512)，對該資料進行資料處理，生成已完成處理變形資料 H4，以第2資料反變形處理構件(520)，進行第2搗亂用資料之反變換，生成已完成處理變形資料 H5(521)。而以第1資料反變形處理構件(514)進行第1搗亂用資料之反變換，求出真的已完成處理資料 D2(515)。在變形使用互斥邏輯和之例子如下。

$$H1 = D1 \text{ xor } X1i$$

$$H2 = f1(H1)$$

$$X1o = f1(X1i)$$

$$H31 = H2 \text{ xor } X2i$$

$$H32 = D2 \text{ xor } X2i$$

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (20)

$$H4 = f2(H31、H32)$$

(式 6 1)

$$X2o = f2(X2i、X2i)$$

$$H5 = H4 \text{ xor } X2o$$

$$D2 = H5 \text{ xor } X1o$$

其中 f1 與 f2 係資料處理操作。如本例所示，在第 2 資料處理 f2 使用別的資料 D2 時，以第 2 搗亂用資料將該資料 D2 加以變形而使用時，使用本實施例之處理程序將非常有效。此為申請專利範圍第 2 項之實施例。

第 6 圖之實施例也是使用兩個搗亂用資料之例子。與第 5 圖最大之差別在於，使用第 1 搗亂用資料之資訊隱蔽處理與使用第 2 搗亂用資料之資訊隱蔽處理連接在一起。係在恢復使用第 1 搗亂用資料之變換之反變形處理以前，以第 2 搗亂用資料加以變形，以隱蔽使用真的資料之處理用之處理程序。以第 1 搗亂用資料變形之變形資料 H1(609)，在第 1 變形資料處理構件(610)進行資料處理，使用第 2 搗亂用資料，在第 2 變形資料製作構件(612)，將已完成處理變形資料 H2(611)加以變形，生成已完成處理變形資料 H3(613)。而在第 2 資料反變形構件(614)，使用該處理結果之已完成處理變形資料 H4(606)，生成已完成處理變形資料 H5(615)。而在第 2 資料反變形處理構件(616)進行反變換，生成真的已完成處理資料 D2(617)。在變形使用互斥邏輯和之例子如下。

$$H1 = D1 \text{ xor } X1o$$

$$H2 = f1(H1)$$

$$X1o = f1(X1i)$$

五、發明說明 (21)

$$H3 = H2 \text{ xor } X2i$$

(式 6 2)

$$H4 = H3 \text{ xor } X1o$$

$$H5 = f2(H4)$$

$$X2o = f2(X2i)$$

$$D2 = H5 \text{ xor } X2i$$

此在有多數之處理操作，需要使用多數搗亂用資料時有效。此為申請專利範圍第3項之實施例。

第7圖之實施例係從搗亂用資料之面，預先計算資料處理，以提高處理效率者。係預先以搗亂用資料處理構件生成已完成處理搗亂用資料 $Xo(706)$ ，用已完成處理搗亂用資料記錄構件(704)記錄下來。在處理中，資料反變形處理構件(713)讀出所記錄之已完成處理搗亂用資料(714)加以使用。這在執行同樣資料好多次時，在效率面有效。惟因搗亂用資料會被使用好多次，就資訊之隱密性而言，如第4圖之實施例每次更換搗亂用資料比較有效。這可由處理速度與資訊隱密性來權衡(trade-off)而定。此為申請專利範圍第5項之實施例。

第8圖之實施例係統合使用第1及第2搗亂用資料之反變形，然後使用其結果進行資料之反變形。第1及第2搗亂用資料，係分別由第1搗亂用資料處理構件(803)及第2搗亂用資料處理構件(807)作成已完成處理搗亂用資料 $X1o$ 及 $X2o$ 。而以資料反變形統合構件統合這些資料，生成統合已完成處理搗亂用資料 Xo 。使用此資料，進行第1變形資料處理(

(請先閱讀背面之注意事項
填寫本頁)

裝

訂

線

五、發明說明 (22)

814)及第2變形資料處理(818)之結果之已完成處理變形資料H4(819)之反變形處理(820)，生成真的已完成處理資料D2。這是統合已完成處理搗亂用資料，然後整合進行變形處理之方法，而不是個別反變形之情形。對反變形處理之處理時間較長者有效。此為申請專利範圍第4項之實施例。

其次說明，以對稱密碼DES(data encryption standard)為例子之實施例。本發明也可以使用在其他密碼。DES以56位元之密碼鍵，對64位元之資料(明碼文或密碼文)進行加密及解密。因為加密及解密使用同一密碼鍵，因此被稱作對稱密碼。DES跟洗牌一樣，將明碼文(plaintext)(擬加密之資料)之位元交錯移位，而加密。資料之移位係按照密碼鍵為之。解密時，則按照密碼鍵以移位之相反動作，使資料回到原先之位置。DES之交錯移位有單一位元及多數位元為一個單位之方法。前者稱作轉置(permutation process)，後者稱作換字(substitution process)。

再使用第9圖，說明DES之加密方法。變形處理a (901)、變形處理b (904)、反變形處理(916)與本發明有關，與DES之本來之密碼處理無關。密碼文先在初期轉置(IP: Initial Permutation)902予以轉置。這是依照初期轉置表格，以位元單位對調密碼文之64位元之資料。此後，到初期轉置之反轉置(IP-1)916，進行16段之一組操作。

各段處理，係以前段之結果之前半或後半之32位元資料與密碼鍵作為輸入，進行叫做f函數903之處理，再使用前段剩下之一半之32位元，進行取其互斥邏輯和之操作。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (23)

密碼鍵也要置換。對密碼鍵，首先進行使用PC-1表格之選擇性轉置(selectable permutation)PC-1(905)。然後進行，使用PC-2表格之選擇性轉置PC-2 (908)，對調密碼鍵。下一段則依照LS表格，令每次28位元巡迴(round)而加以使用。

本實施例係在IP處理前，追加將明碼文變形之變形處理a (901)，及使密碼鍵變形之變形處理b (904)，最後追加反變形處理(916)。變形處理a (901)將明碼文變形，而IP處理(902)或f函數(903)之處理並不是處理明碼文本身，而是處理變形之明碼文，藉此使其無法從該處理之電流波形猜測出明碼文之資料。變形處理b (904)並不是在PC-1處理(905)、LS處理(907)、PC-2處理(908)、f函數(903)處理密碼鍵本身，而是處理變形之密碼鍵，藉此使其從該處理之電流波形很困難猜測密碼鍵。

第10圖表示f函數303之處理。首先，依據選擇性轉置行列E對f函數之輸入文進行選擇性轉置(1002)。然後，取選擇性轉置之輸入資料與密碼鍵之互斥邏輯和(1003)，進行S盒之處理(1004)，再進行P轉置處理(1005)。S盒之處理係從1003之互斥邏輯和之處理結果之48位元，每次各取出6位元，求出8個S盒表格之行號碼與列號碼，而生成4位元之資料之處理。各S盒表格因每6位元所示之資料之位置而異。P轉置處理係依照P轉置表進行32位元之位元位置之對調操作。

變形處理a (901)與變形處理b (902)基本上是相同之處理。茲使用第11圖說明變形處理a之明碼文之變形資料之製作處理如下。隨機生成搗亂用資料X1。這是每一次DES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(24)

加密(或解密)處理時，使用亂數產生器或虛擬亂數生成(1102)。每次使用不同之搗亂用資料。然後執行搗亂用資料X1與明碼文P之XOR(互斥邏輯和)，生成(變形之明碼文)PX1(1103)。DES時，明碼文為64位元，但生成之亂數可以是64位元也可以是8位元。若是64位元以下，則有必要加以擴充等，以生成64位元之搗亂用資料X1。若生成之亂數是8位元，則可以返覆8次以生成64位元之搗亂用資料X1。在此，因為是使用互斥邏輯和(XOR)變形，因此取搗亂用資料X1與變形明碼文PX1之XOR，則可生成明碼文P。此為申請專利範圍第6項之實施例。

變形處理b (904)之密碼鍵之變形資料之製作程序係如第36圖所示。僅使用密碼鍵K與搗亂用資料X2取代明碼文與搗亂用資料X1，這一點與第11圖之實施例不同。在DES密碼鍵與明碼文同樣是64位元。藉處理生成變形之密碼鍵KX2。

接下說明 IP處理(902)。IP處理(902)係依照第37圖所示之表格對調明碼文64位元之排列。依照表格，將輸出之第1位元換至輸入之第58位元、將輸出之第2位元換至輸入之第50位元、將輸出之第64位元換至輸入之第7位元。使用第12圖說明本實施例之IP處理如下。首先，對變形明碼文PX1進行IP處理，生成已完成IP處理變形明碼文PX1IP(1202)。位元之對調係依照第37圖之表格。接著，搗亂用資料X1也同樣進行IP處理，生成已完成IP處理搗亂用資料X1IP(1203)。若取已IP處理明碼文PX1IP與已完成IP處理搗亂用資料X1IP之互斥邏輯和，則可以生成將明碼文IP處理之結果。這是

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (25)

因爲IP處理是位元之移動，搗亂用資料也與明碼文PX1同樣移動，因此維持有，對每一個位元執行互斥邏輯和，則可求出真資料之關係之故。IP處理之下位32位元被用以取第1段之f函數(903)與第2段之互斥邏輯和，上位32位元成爲互斥邏輯和(909)之輸入。此爲申請專利範圍第1、7、18、20項之實施例。

在IP處理，變形明碼文PX1之位元之值，與原來之明碼文之位元之值不同，因此，看IP處理之電流波形，要猜測明碼文之資料非常困難。“1”之位元數會使電流變大，但變形明碼文之“1”之位元數與明碼文之“1”之位元數並無任何關係。因此，要從電流之大小猜測明碼文之資料非常困難。如此，以搗亂用資料將明碼文加以變形，則可以使，藉由觀測處理中之電流波形猜測原來之資料非常困難。

PC-1處理與IP處理幾乎相同。使用第38圖之PC-1用之變換表格，去除64位元之密碼鍵之8位元之同位位元，使成56位元，且更換位元之順序。第38圖之表格之看法與第37圖之看法一樣。對已完成PC-1處理之變形密碼鍵KX2PC1與已完成PC-1處理之搗亂用資料X2PC1執行互斥邏輯和時，則可求得正確之已完成PC-1處理之密碼鍵。

LS處理係將PC-1處理所生成之58位元，分成左右各28位元，分別依照LS表格向左移位1位元或2位元。使用第15圖說明實施例如下。首先，在1502，對已完成PC-1處理結果之變形密碼鍵KX2PC1進行LS處理，生成已完成PC-1及LS處理之變形密碼鍵KX2PC1LS，在1503，對已完成PC-1處

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (26)

理結果之搗亂用資料 X2PC1 進行 LS 處理，生成已完成 PC-1 及 LS 處理搗亂用資料 X2PC1LS。LS 處理也是位元位置之調換，因此，若執行已完成 PC-1 及 LS 處理變形密碼鍵 KX2PC1LS 與已完成 PC-1 及 LS 處理搗亂用資料 K2PC1LS 之互斥邏輯和，便可以獲得真的已完成 LS 處理之密碼鍵之結果。因 LS 處理也是使用搗亂用資料，因此實際操作之資料與真的密碼鍵不同，觀測電流波形也很難能猜測密碼鍵。

PC-2 處理係依照 PC-2 表格，將 LS 處理結果之 56 位元縮小轉置成 48 位元。在 1402，將已完成 PC-1、LS 處理之變形密碼鍵 KX2PC1LS 加以 PC-2 處理，生成已完成 PC-1、LS、PC-2 處理之變形密碼鍵 KX2PC1LSPC2。在 1403，將已完成 PC-1、LS 處理之搗亂用資料 X2PC1LS 加以 PC-2 處理，生成已完成 PC-1、LS、PC-2 處理之搗亂用資料 X2PC1LSPC2。因基本上是使用表格之轉置，因此基本上是跟 PC-1 處理相同。

其次說明 f 函數 903 之處理。f 函數係如第 10 圖所示，由選擇性轉置 E 處理 (1002)、密碼鍵與選擇性轉置之執行結果之互斥邏輯和 (1003)、S 盒處理 (1004)、P 轉置處理 (1005) 所構成。

再參照第 16 圖說明選擇性轉置 E 處理如下。選擇行轉置 E 係與 IP 處理一樣使用第 28 圖之轉置表，變更位元之排列。在 1602，對已完成 IP 處理之變形明碼文 PXIP 進行選擇性轉置 E 處理，生成已完成 IP 處理及 E 轉置處理之變形明碼文 PXIPE。而在 1603，對已完成 IP 處理搗亂用資料 XIP 進行選擇性轉置 E 處理，生成已完成 IP 處理及 E 轉置處理之搗亂用

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (27)

資料 XIPE。與 IP 處理或 PC-1 處理一樣，取已完成 IP 處理及 E 轉置處理變形明碼文 PXIPE 及已完成 IP 處理及 E 轉置處理之搗亂用資料 XIPE 之互斥邏輯和，即可決定正確之已完成 IP 處理及 E 轉置處理之明碼文。而使用轉置 E 表格進行位元之對調時，位元之值也是變形之位元之值，因此看該處理之電流波形，也很難猜測真正之資料。

接著，進行 f 函數之第 2 項處理，密碼鍵與選擇性轉置之執行結果之互斥邏輯和之處理。茲使用第 17 圖說明本處理如下。在 1702，將從明碼文生成之已完成 IP 處理及 E 轉置處理之變形明碼文 PXIPE，與從密碼鍵生成之已完成 PC-1 及 LS、PC-2 處理之變形密碼鍵 KX2PC1LSPC2 加以 XOR，製作成為 S 盒處理之輸入之 48 位元之 S 盒輸入資料 SinputX。然後在 1703，將從明碼文用之搗亂用資料生成之已完成 IP 處理及 E 轉置處理之搗亂用資料 XIPE，與從密碼鍵用之搗亂用資料生成之已完成 PC-1 及 LS、PC-2 處理之搗亂用資料 X2PC1LSPC2，加以 XOR，生成 S 盒輸入資料 SinputX 用之搗亂用資料之 S 盒輸入資料搗亂用資料 XSinput。因互斥邏輯和之性質，S 盒輸入資料搗亂用資料 XSinput 可以藉由將兩個搗亂用資料(已完成 PC-1 及 LS、PC-2 處理之搗亂用資料 X2PC1LSPC2，已完成 PC-1 及 LS、PC-2 處理之搗亂用資料 X2PC1LSPC2，)XOR 而生成。以簡單之例子表示如下。假設明碼文為 P，鍵為 K，其變形明碼文為 PX1，變形鍵為 KX2。該等之關係便是式 63 及式 64。X1 及 X2 係明碼文與鍵之搗亂用資料。

五、發明說明 (28)

$$PX1 = P \text{ xor } X1 \quad (\text{式 } 6 \ 3)$$

$$KX2 = K \text{ xor } X2 \quad (\text{式 } 6 \ 4)$$

於是，若執行P與K之互斥邏輯和之結果為Z時，執行PX1與PX2之互斥邏輯和之結果Z1與Z之關係如下。

$$Z = P \text{ xor } K \quad (\text{式 } 6 \ 5)$$

$$\begin{aligned} Z1 &= PX1 \text{ xor } KX2 \\ &= (P \text{ xor } X1) \text{ xor } (K \text{ xor } X2) \\ &= P \text{ xor } X1 \text{ xor } K \text{ xor } X2 \\ &= (P \text{ xor } K) \text{ xor } (X1 \text{ xor } X2) \\ &= Z \text{ xor } (X1 \text{ xor } X2) \end{aligned} \quad (\text{式 } 6 \ 6)$$

亦即，從以上可以瞭解，要使Z1恢復到真的之資料時，使用P與K之搗亂用資料之互斥邏輯和做為搗亂用資料即可。在取密碼鍵與選擇性轉置之執行結果之互斥邏輯和之處理時，S盒輸入資料SinputX用之搗亂用資料，使用，將從明碼文用之搗亂用資料生成之已完成IP處理及E轉置處理之搗亂用資料XIPE，與從密碼鍵用之搗亂用資料生成之已完成PC-1及LS、PC-2處理之搗亂用資料X2PC1LSPC2，加以XOR，生成S盒輸入資料之搗亂用資料XSinput即可。這是申請專利範圍第18項之實施例。

接著，再參照第18圖說明S盒之處理。從S盒輸入資料

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (29)

SinputX取出各6位元，對8個S盒進行處理。第25圖表示在DES所使用之第1個S盒。8個S盒之形式相同，但其場資料不相同。各S盒之處理，係首先取出S盒輸入資料SinputX之上位第i號之6位元之副資料SubSinputX(i)(1805)。將預先作成之將S盒變形之變形S盒表格之位址搗亂用資料Xsa(i)，與SubSinputX(i)加以XOR，生成SubSinputXXsa(i) (1806)。將該SubSinputXXsa(i)與S盒輸入資料搗亂用資料XSinput之上位第i個之6位元XOR，生成SubSinputXsa(i) (1807)。

SubSinputXXsa(i)係取出第i個S盒之真正之位址資料，與位址搗亂用資料Xsa(i)互斥邏輯和之值。取SubSinputX(i)與XSinput(i)之互斥邏輯和(XOR)時，便會回到真的資料，因此與XSinput(i)互斥邏輯和以前，先取SubSinputX(i)與Xsa(i)之互斥邏輯和，然後執行XSinput(i)之互斥邏輯和(XOR)。如此便不必進行真正的資料處理，要從其電流波形猜測資料很困難。接著，使用SubSinputXsa(i)計算變形S盒表格之位址(1808)。因為，參照本來之S盒表格用之位址已被變形，因此必須預先將表格變形。依據所計算之位址，從變形S盒表格S(i)取出S盒輸出資料SoutputX3(i) (1809)。而同時取出S盒之輸出資料SoutputX3(i)用之搗亂用資料X3(i) (1810)。處理8個S盒，分別將SoutputX3(i)及X3(i)之i從1到8之資料加以連結，藉此生成SoutputX3與X3。此後之處理資料成為SoutputX3，搗亂用資料成為X3。

接著，參照第23圖及第24圖說明變形S盒表格之生成方法。在此之S盒，作成S(i)盒用之位址搗亂用資料Xsa(i)與資

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (30)

料搗亂用資料 $X3(i)$ (2306)。 $Xsa(i)$ 爲 6 位元，而 $X3(i)$ 爲 4 位元。搗亂用資料 $X3$ 係集中 8 個各 4 位元之 $X3(i)$ 之 32 位元之資料。接著叫出變形 $S(i)$ 盒表格製作常式 (2307)。再參照第 24 圖說明第 i 號之變形 S 盒表格製作常式之處理。 k 指定行號碼， l 指定列號碼。 k 行 l 列之處理係 2408 至 2413。第 1 號之 S 盒之表格係如第 25 圖所示。首先，取出第 i 號之原來之 S 盒之行號碼 k 列號碼 l 之資料 d (2408)。而取該資料 d 與搗亂用資料 $X3(i)$ 之互斥邏輯和，假設爲 $d2$ (2409)。這是，若搗亂用資料爲“7”，對原來之 S 盒之資料 2504，其結果是 2604。若在各區進行，則如第 26 圖所示。第 26 圖之表格，係對第 25 圖之第 1 號 S 盒之資料，以搗亂用資料爲“7”取其互斥邏輯和者。

其次進行位址之搗亂。首先，假定 $Xsa1$ 係由 $Xsa(i)$ 之上位 1 位元及下位 1 位元作成之 2 位元， $Xsa2$ 係由 $Xsa(i)$ 之上位 2 位元至 5 位元作成之 4 位元之資料。這是來自 S 盒之位址之計算方法。而第 26 圖之行號碼與列號碼分別爲 k 與 l 時，分別對其進行 $Xsa1$ 與 $Xsa2$ 之互斥邏輯和 (2412)。若新形成之行號碼及列號碼分別爲 $k2$ 與 $l2$ 時，將資料 $d2$ 儲存在第 i 號之變形 S 盒表格 $S(i)$ 之 $k2$ 行 $l2$ 列 (2413)。本處理之例子示於第 27 圖。第 27 圖係對第 26 圖之行與列選擇“2”“9”作爲搗亂用資料而作成者。爲了使其容易明瞭，行與列之位置保持不動，僅變更行與列之號碼。在第 25 圖之 3 行 1 列之資料 12(2504)到第 27 圖時移到 1 行 8 列，值則變形成 11。本例之資料之搗亂用資料爲“7”，位址之搗亂用資料則行爲“2”列爲“9”。如此將 8

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (31)

個S盒予以變形。在本實施例，此項處理係在DES之最初時實施。變形之S盒表格在DES之第16段使用。這是申請專利範圍第5項之實施例。

結束S盒之處理後，處理資料成為32位元之SoutputX3，搗亂用資料成為32位元之X3。這便成為f函數最後之處理之轉置P處理(1005)之輸入。使用第19圖說明轉置P處理之詳情如下。將S盒之輸出SinputX3加以轉置P處理生成SinputX3P(1902)。將SinputX3之搗亂用資料X3加以轉置P處理，生成X3P(1903)。轉置P所使用之表格係如第29圖所示。此表格之用法也與IP處理之表格一樣。

結束f函數之處理後，進行轉置P處理與前段之結果之XOR (909或914)。首先，將S盒之結果轉置P之SinputX3P與前段之結果加以XOR (2002)。而將X3P與前段之搗亂用資料X加以XOR (2003)。此項XOR處理與選擇性轉置E處理結果與密碼鍵之XOR處理(1701)相同。

在DES，最後進行IP-1處理(915)。本處理示於第21圖。IP-1處理係類似IP處理之位元排列之調整處理，使用IP-1表格取代IP表格 (2102)。將前面之一連串處理結果加以IP-1處理，同樣將搗亂用資料X加以IP-1處理 (2103)。

最後，為了回到正確的處理結果，而進行反變形處理(916)。反變形處理示於第22圖。以IP-1處理之搗亂用資料X，將IP-1處理結果加以XOR，而求出正確之結果。在此始獲得沒有變形之正確之處理結果。

以上係在說明被處理之資料之隱蔽，但搗亂用資料有

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (32)

時也須要隱蔽。基本的想法是，取搗亂用資料與搗亂用之搗亂用資料XR之互斥邏輯和，而加以變形。但XR是固定不變，而預先計算位元位置之調換等求出反變形用之XR_o。而在需要搗亂用資料時，使用XR_o，求出原來之搗亂用資料，藉此提高搗亂用資料之變形與反變形之實施效果。首先以密碼鍵用之搗亂用資料為例子說明如下。第30圖之處理，係以搗亂用之搗亂用資料XR取與搗亂用資料之互斥邏輯和之變形操作。以變形處理b (3601)生成搗亂用資料X₂後，進行第30圖之搗亂用資料之變形處理。密碼鍵用之搗亂用資料X₂要接受PC-1處理或LS處理、PC-2處理。這些是一定位元之位置調換，因此對預先決定之值XR，求出執行到PC-2處理時之搗亂用資料XR_o而加以記錄(3102至3105)。PC-2處理後，取在1403所生成之已完成PC-1及LS、PC-2處理之搗亂用資料X₂PC₁LSPC₂，與所記錄之搗亂用資料XR_o之XOR(3202)，而求出本來之已完成PC-1及LS、PC-2處理之搗亂用資料X₂PC₁LSPC₂。如此便可以隱蔽搗亂用資料。搗亂用之搗亂用資料XR及其已完成處理之搗亂變形資料XR_o，可以使用相同之資料。

在DES之實施例係加密，但DES之運算法在解密時也幾乎相同，因此在本實施例幾乎可以不變更則可適用。而DES以外之密碼運算法，也使用很多之轉置處理，換字處理或剩餘運算，因此可以應用本發明，將資料加以變形，使其很難能從電流波形猜測本來之資料。

採用本發明時，因為將IC卡晶片之處理資料變形，因

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (33)

此要從消耗電流之波形猜測處理或密碼鍵非常困難。

圖式之簡單說明

第1圖係表示習知之IC卡之硬體架構之構成例子。

第2圖係表示習知之IC卡用晶片內之硬體架構之構成例子。

第3圖係表示IC卡之消耗電流之波形之例子。

第4圖係說明本發明一實施例用之圖，表示使用一個攪亂用資料將資料變形之程序圖。

第5圖係說明本發明一實施例用之圖，表示交替使用兩個攪亂用資料將資料變形之程序圖。

第6圖係說明本發明一實施例用之圖，表示連續使用兩個攪亂用資料將資料變形之程序圖。

第7圖係說明本發明一實施例用之圖，表示預先計算攪亂用資料之資料處理之資料變形之程序圖。

第8圖係說明本發明一實施例用之圖，表示統合兩個攪亂用資料之反變形之資料變形之程序圖。

第9圖係說明本發明一實施例用之圖，表示DES之整體處理之流程圖。

第10圖係說明本發明一實施例用之圖，表示DES之f函數之處理之流程圖。

第11圖係說明本發明一實施例用之圖，說明變形處理a之圖。

第12圖係說明本發明一實施例用之圖，說明IP處理之

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (34)

圖。

第13圖係說明本發明一實施例用之圖，說明PC-1處理之圖。

第14圖係說明本發明一實施例用之圖，說明PC-2處理之圖。

第15圖係說明本發明一實施例用之圖，說明LS處理之圖。

第16圖係說明本發明一實施例用之圖，說明選擇性轉置E處理之圖。

第17圖係說明本發明一實施例用之圖，說明選擇性轉置E處理結果及密碼鍵之XOR處理之圖。

第18圖係說明本發明一實施例用之圖，說明S盒處理之圖。

第19圖係說明本發明一實施例用之圖，說明轉置P處理之圖。

第20圖係說明本發明一實施例用之圖，說明轉置P處理與前段之結果XOR處理之圖。

第21圖係說明本發明一實施例用之圖，說明IP-1處理之圖。

第22圖係說明本發明一實施例用之圖，說明反變形處理之圖。

第23圖係說明本發明一實施例用之圖，說明變形S盒表格之製作程序之圖。

第24圖係說明本發明一實施例用之圖，說明第i號之變

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (35)

形 S 盒表格製作常式之圖。

第 25 圖係說明本發明一實施例用之圖，表示第 1 號之 S 盒表格。

第 26 圖係說明本發明一實施例用之圖，表示將第 1 號之 S 盒表格之資料變形之表格。

第 27 圖係說明本發明一實施例用之圖，表示將第 1 號之 S 盒表格之配置變形之表格。

第 28 圖係說明本發明一實施例用之圖，表示選擇轉置 E 表格。

第 29 圖係說明本發明一實施例用之圖，表示轉置 P 表格。

第 30 圖係說明本發明一實施例用之圖，表示搗亂用資料之加密處理之圖。

第 31 圖係說明本發明一實施例用之圖，表示搗亂用資料之加密用資訊之變形計算處理之圖。

第 32 圖係說明本發明一實施例用之圖，表示搗亂用資料之解密處理之圖。

第 33 圖係說明本發明一實施例用之圖，表示原表格之例子。

第 34 圖係說明本發明一實施例用之圖，表示改變第 33 圖內容之表格。

第 35 圖係說明本發明一實施例用之圖，表示改變第 34 圖表格之配置之表格。

第 36 圖係說明本發明一實施例用之圖，表示變形處理 b

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (36)

。

第37圖係說明本發明一實施例用之圖，表示IP轉置表格。

第38圖係說明本發明一實施例用之圖，表示PC-1選擇性轉置表格。

主要元件對照表

101-----	卡片
102-----	IC卡片用晶片
201-----	中央運算裝置
202-----	協處理器
203-----	資料匯流排
204-----	記憶裝置
205-----	程式區
206-----	資料區
207-----	輸出輸入埠

(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： 資訊處理裝置)

本發明之目的在於，減少 I C 卡用晶片與消耗電流之關連性。

該課題之解決手段如下。在進行 I C 卡用晶片之輸入處理前，對其資料施加變形處理，以減低 I C 卡用晶片與消耗電流之關連性。而在結束其變形處理後，對該變形資料施加反變形處理，藉此獲得正確之處理結果。

英文發明摘要(發明之名稱：)

六、申請專利範圍

1.一種資訊處理裝置，具備有，配設儲存程式用之程式儲存部，及保存資料之資料儲存部之記憶裝置，依照程式進行資料處理之中央運算裝置，配設有，程式係指示中央運算裝置執行處理之處理命令之一個以上之資料處理構件，由一個資料處理構件處理輸入資料，並具有，輸出已處理資料之輸入資料處理構件之資訊處理裝置，其特徵在於，具備有；

使用攪亂用資料(Data for disturbance)Xi將輸入資料D1加以變形(transform)而作成變形資料(transformed data)H1之資料變形處理構件；

在上述輸入資料處理構件對上述變形資料H1實施運算處理OP1，取代對上述輸入資料D1實施上述運算處理OP1，以作成已完成處理之變形資料(processed and transformed data)H2之變形資料處理構件；

對上述攪亂用資料Xi實施上述運算處理OP1，以作成已完成處理攪亂用資料Xo之攪亂用資料處理構件；以及，

使用上述已完成處理攪亂用資料Xo，對已完成處理變形資料H2實施運算處理OP2，而獲得對輸入資料D1實施加運算處理OP1之結果之已完成處理資料D2之資料反變形處理(untransformed process)構件。

2.一種資訊處理裝置，具備有，配設儲存程式用之程式儲存部，及保存資料之資料儲存部之記憶裝置，依照程式執行一定之處理，進行資料處理之中央運算裝置，及一個以上之資料處理構件之資訊處理裝置，其特徵在於，具

六、申請專利範圍

備有，

使用第1搗亂用資料X1i，對上述第1輸入資料D1施加一定之運算處理OP1，以作成將上述第1輸入資料D1變形之變形資料H1，以取代對上述第1輸入資料D1進行運算處理OP1，獲得第1已完成處理資料D2，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述第1搗亂用資料X1i，施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成第1已完成處理搗亂用資料X1o，

使用第2搗亂用資料X2i，將上述已完成處理變形資料H2加以變形，以作成已完成處理變形資料H3，

對上述已完成處理變形資料H3施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H4，

對上述第2搗亂用資料X2i施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成第2已完成處理搗亂用資料X2o，

使用上述第2已完成處理搗亂用資料X2o，處理上述已完成處理變形資料H4，以作成已完成處理變形資料H5，

使用上述第1已完成處理搗亂用資料X1o，處理上述已完成處理變形資料H5，以取得上述第1已完成處理資料D2之構件。

(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

3.一種資訊處理裝置，具備有，配設儲存程式用之程式儲存部，及保存資料之資料儲存部之記憶裝置，依照程式進行資料處理之中央運算裝置，並設有一個以上之資料處理構件之資訊處理裝置，其特徵在於，具備有，

使用第1搗亂用資料X1i對上述第1輸入資料D1施加一定之運算處理OP1，以作成將上述第1輸入資料D1變形之變形資料H1，以取代對上述第1輸入資料D1進行運算處理OP1，獲得第1已完成處理資料D3，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述第1搗亂用資料X1i，施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'之任一運算處理，以作成第1已完成處理搗亂用資料X1o，

使用第2搗亂用資料X2i，將上述已完成處理變形資料H2加以變形，以作成已完成處理變形資料H3，

使用上述第1已完成處理搗亂用資料X1o，對上述已完成處理變形資料H3施加反變形運算處理，以作成已完成處理變形資料H4，

對上述已完成處理變形資料H4施加上述運算處理 OP2，或施加與上述運算處理 OP2不同之運算處理 OP2'，以作成已完成處理變形資料H5，取代以第1已完成處理資料D3作為輸入，進行一定之運算處理OP2，以獲得第1處理及第2處理之已完成處理資料D2，

(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

對上述第1搗亂用資料X2i，施加上述運算處理 OP2，或施加與上述運算處理 OP2不同之運算處理 OP2'，以作成第2已完成處理搗亂用資料X2o，

使用上述第2已完成處理搗亂用資料X2o處理上述已完成處理變形資料H5，以作成上述已完成處理資料D2之構件。

4.一種資訊處理裝置，其特徵在於，具備有，

使用第1搗亂用資料X1i對上述第1輸入資料D1施加一定之運算處理OP1，以作成將上述第1輸入資料D1變形之變形資料H1，以取代對上述第1輸入資料D1進行運算處理OP1，獲得第1已完成處理資料D3，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述第1搗亂用資料X1i，施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'之任一運算處理，以作成第1已完成處理搗亂用資料X1o，

使用第2搗亂用資料X2i，將上述已完成處理變形資料H2加以變形，以作成已完成處理變形資料H3，

使用上述第1已完成處理搗亂用資料X1o，對上述已完成處理變形資料H3施加反變形運算處理，以作成已完成處理變形資料H4，

施加上述運算處理 OP2，或施加與上述運算處理 OP2不同之運算處理 OP2'，以作成已完成處理變形資料H5，取

六、申請專利範圍

代以第1已完成處理資料D3作為輸入，進行一定之運算處理OP2，以獲得第1處理及第2處理之已完成處理資料D2，

對上述第1搗亂用資料X2i，施加上述運算處理OP2，或施加與上述運算處理OP2不同之運算處理OP2'，以作成第2已完成處理搗亂用資料X2o，

統合上述第1已完成處理搗亂用資料X1o，與第2已完成處理搗亂用資料X2o，以生成統合已完成處理搗亂用資料Xo，

使用上述統合已完成處理搗亂用資料Xo，反變形處理已完成處理變形資料H4，以獲得上述已完成處理資料D2。

5.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，具備有：

用以記錄上述已完成處理搗亂用資料Xo之已完成處理搗亂用資料記錄構件，以及，

可使用所記錄之上述已完成處理搗亂用資料Xo處理上述已完成處理變形資料，藉此重新獲得別的已完成處理變形資料之資料反變形處理構件。

6.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，使用亂數以生成上述搗亂用資料。

7.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述變形處理係取上述搗亂用資料Xi與輸入資料D1之互斥邏輯和之處理，上述反變形處理係取上述已完成處理搗亂用資料Xo與上述已完成處理變形資料H2之互斥邏輯和之處理。

(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

8.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述變形處理係在上述搗亂用資料 X_i 與輸入資料 D_1 間進行之加法處理，上述反變形處理係在上述已完成處理搗亂用資料 X_o 與上述已完成處理變形資料 H_2 間進行之減法處理。

9.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述變形處理係在上述搗亂用資料 X_i 與輸入資料 D_1 間進行之減法處理，上述反變形處理係在上述已完成處理搗亂用資料 X_o 與上述已完成處理變形資料 H_2 間進行之加法處理。

10.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述變形處理係在上述搗亂用資料 X_i 與輸入資料 D_1 間進行之乘法處理，上述反變形處理係在上述已完成處理搗亂用資料 X_o 與上述已完成處理變形資料 H_2 間進行之除法處理。

11.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述變形處理係在上述搗亂用資料 X_i 與輸入資料 D_1 間進行之除法處理，上述反變形處理係在上述已完成處理搗亂用資料 X_o 與上述已完成處理變形資料 H_2 間進行之乘法處理。

12.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述輸入資料之資料處理，有剩餘運算之加減法運算處理時，在上述資料變形處理使用法 N 之整數倍之加減法
(Addition and subtraction of the number multiplying

(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

modulus N by a voluntary integer)。

13.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述輸入資料之資料處理f是剩餘運算之乘法運算，

數X、Y滿足式 $1 = X * Y \bmod N$ 時，

在資料變形處理之剩餘運算時，乘上X整數倍，

並在資料反變形處理時，乘上Y相同於在資料變形處理時以變形處理構件乘上X之次數之整數倍。

14.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述輸入資料之資料處理f是剩餘運算之乘法運算，

數X、Y滿足式 $1 = X * Y \bmod N$ 時，

在資料變形處理之剩餘運算時，以N作為剩餘運算之法，而乘上 $(N+1) / 2$ 整數倍，

並在資料反變形處理時，乘上2相同於在資料變形處理時以變形處理構件乘上 $(N+1) / 2$ 之次數之整數倍。

15.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述輸入資料之資料處理f是剩餘運算之乘法運算，

數X、Y滿足式 $1 = X * Y \bmod N$ 時，

在資料變形處理之剩餘運算時，乘上2整數倍，

並在資料反變形處理時，以N作為剩餘運算之法，乘上 $(N+1) / 2$ 相同於在資料變形處理時以變形處理構件乘上2之次數之整數倍。

16.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述資料之上述變形，係依據規則之方法將排列之

資料之配置加以變更，上述資料之上述反變形，係依據摺

(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

取由上述變形變更之上述排列之資料之處理。

17.如申請專利範圍第16項所述之資訊處理裝置，其特徵在於，上述以規則之方法將排列之資料之配置加以變更之變更方法，係以排列之索引數取互斥邏輯和，藉此對調資料之配置，

以上述資料變形處理使用之數字取上述排列之索引，作為變形後之索引，而在上述資料反變形處理時，依據上述變形後之索引擷取上述排列之資料。

18.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述運算處理OP1係以位元單位調換資料之轉置處理，上述資料變形處理及上述資料反變形處理係取資料之互斥邏輯和之處理。

19.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述運算處理OP1係以位元組單位調換資料之換字處理(substitution process)，上述資料變形處理及上述資料反變形處理係取資料之互斥邏輯和之處理。

20.如申請專利範圍第1項所述之資訊處理裝置，其特徵在於，上述運算處理OP1係使用表格調換資料之處理(process to replace data)，上述資料變形處理及上述資料反變形處理係取資料之互斥邏輯和之處理。

21.一種資訊處理裝置，具有可以依照電腦程式對輸入資料進行運算處理，而輸出已完成處理資料之運算裝置之資訊處理裝置，其特徵在於，具備有，

使用搗亂用資料Xi對輸入資料D1實施運算，作成將上

六、申請專利範圍

述輸入資料D1變形之變形資料H1，取代對上述輸入資料D1實施一定之運算處理OP1獲得已完成處理之資料D2之處理，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述搗亂用資料Xi施加對上述變形資料H1施加之上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'之任一運算處理，以作成已完成處理搗亂用資料Xo，

使用上述已完成處理之搗亂用資料Xo，對上述已完成處理變形資料H2施加資料反變形處理OP2，作成對上述輸入資料D1進行上述運算處理OP1之結果之上述已完成處理之資料D2之構件。

22.一種資訊處理裝置，具有可以依照電腦程式對輸入資料進行運算處理，而輸出已完成處理資料之運算裝置之資訊處理裝置，其特徵在於，具備有，

使用搗亂用資料Xi對輸入資料D1實施運算，作成將上述輸入資料D1變形之變形資料H1，取代對上述輸入資料D1實施一定之運算處理OP1獲得已完成處理之資料D2之處理，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述已完成處理變形資料H2施加資料反變形處理OP2處理，藉此作成對上述輸入資料D1進行上述運算處理OP1之

六、申請專利範圍

結果之上述已完成處理資料D2之構件。

23.一種資訊處理裝置，其特徵在於，

具有可以依照電腦程式對輸入資料進行運算處理而輸出已完成處理之資料之運算裝置，

作成將上述輸入資料D1變形之變形資料H1，取代對上述輸入資料D1實施一定之運算處理OP1獲得已完成處理之資料D2之處理，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處理變形資料H2，

對上述已完成處理變形資料H2施加資料反變形處理OP2之構件，

而上述運算處理 OP1，或與上述運算處理 OP1不同之運算處理 OP1'，及上述資料反變形處理OP2，可用以對上述已完成處理變形資料H2施加資料反變形處理OP2，以獲得上述已完成處理之資料D2。

24.一種資訊處理裝置，具有可以依照電腦程式對輸入資料進行運算處理，而輸出已完成處理資料之運算裝置之資訊處理裝置，其特徵在於，具備有，

對輸入資料D1實施一定之運算，作成將上述輸入資料D1變形之變形資料H1，取代對上述輸入資料D1實施一定之運算處理OP1，獲得已完成處理之資料D2，

對上述變形資料H1施加上述運算處理 OP1，或施加與上述運算處理 OP1不同之運算處理 OP1'，以作成已完成處

(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

理變形資料 H2 之構件，

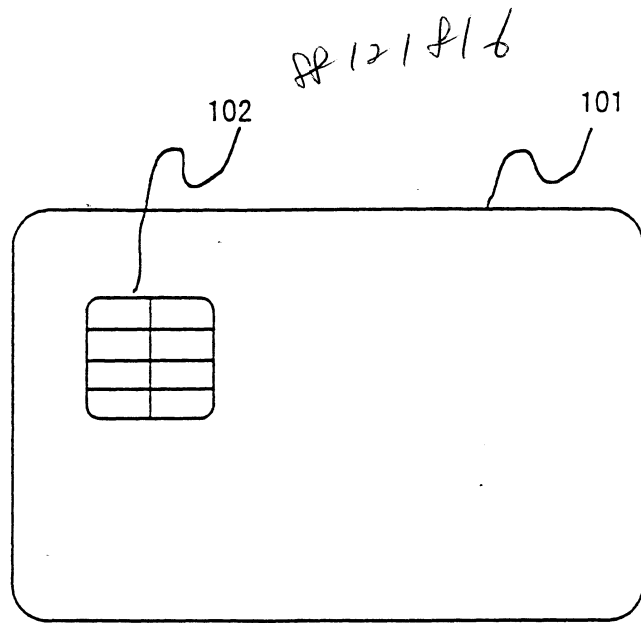
而選擇，可使已完成處理變形資料 H2 與已完成處理資料 D2 為相同資料之上述一定之運算。

(請先閱讀背面之注意事項再填寫本頁)

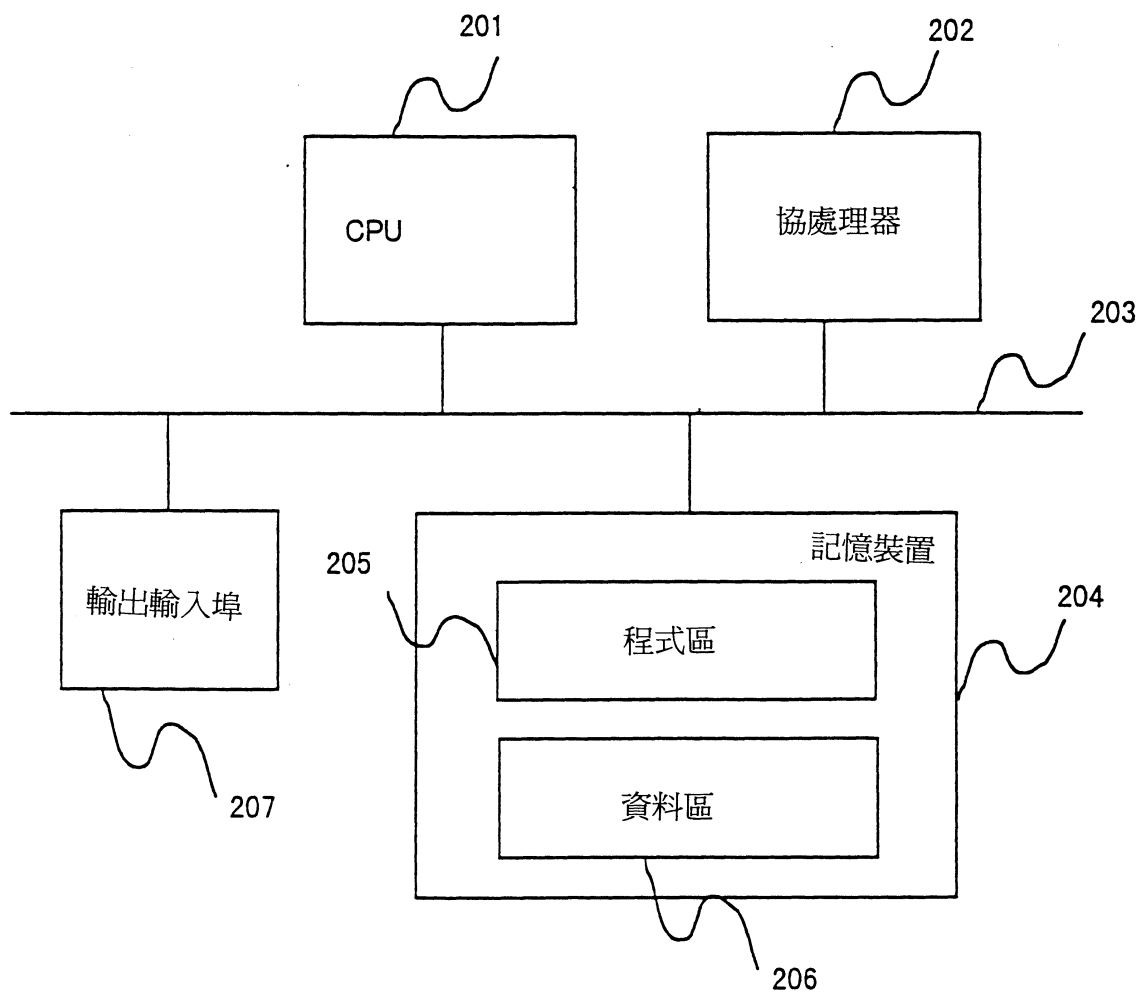
裝

訂

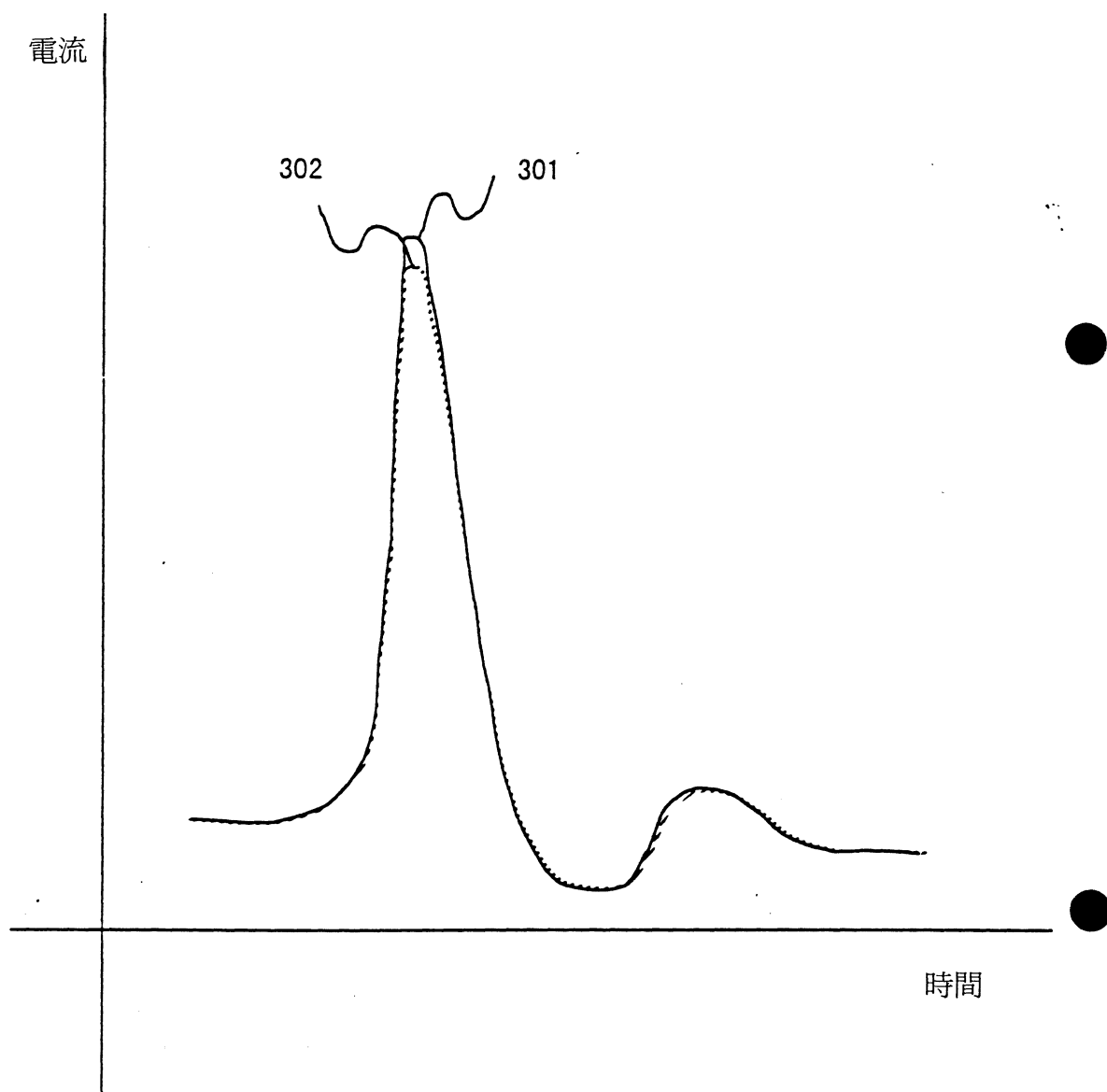
線



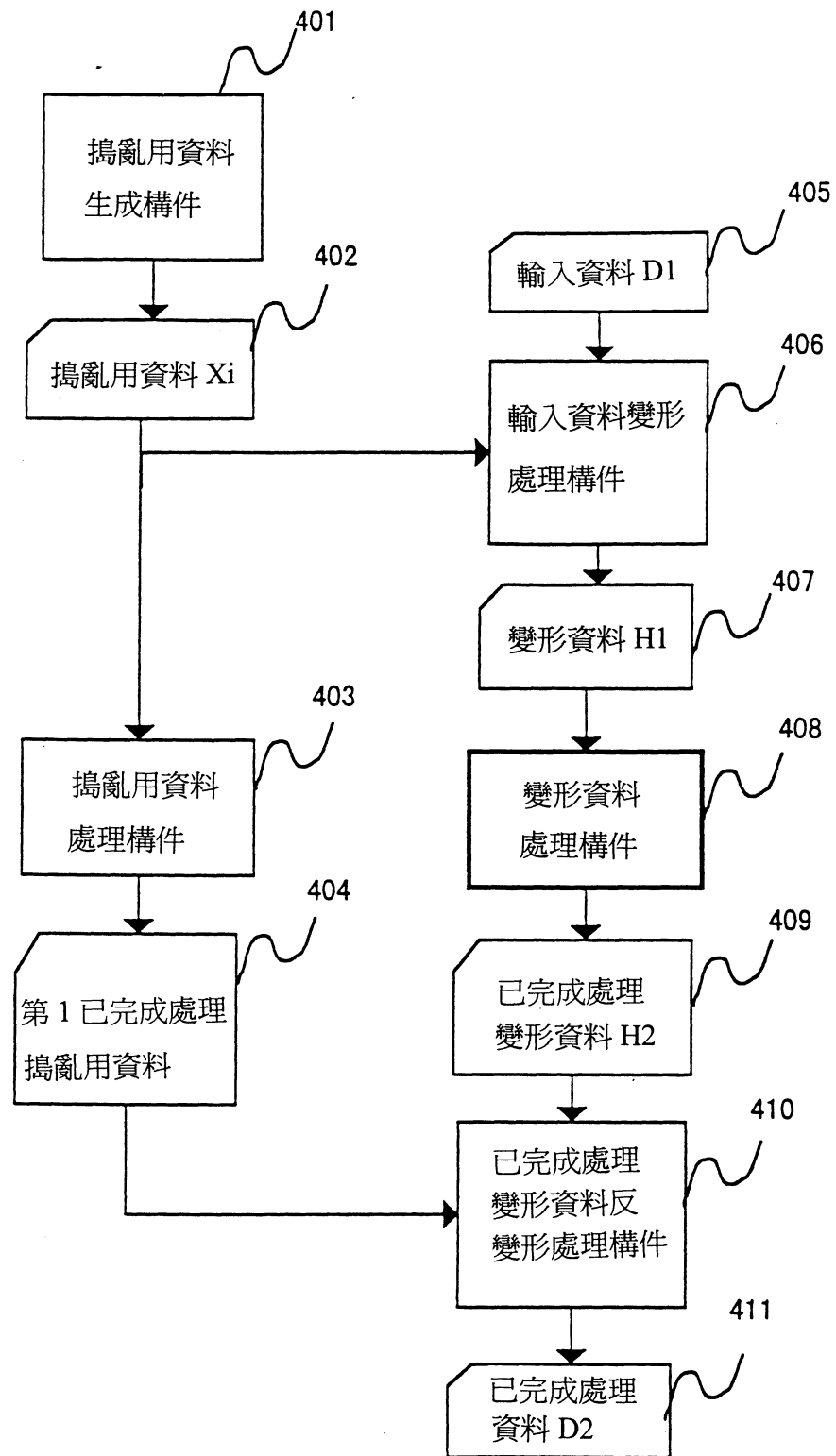
第 1 圖



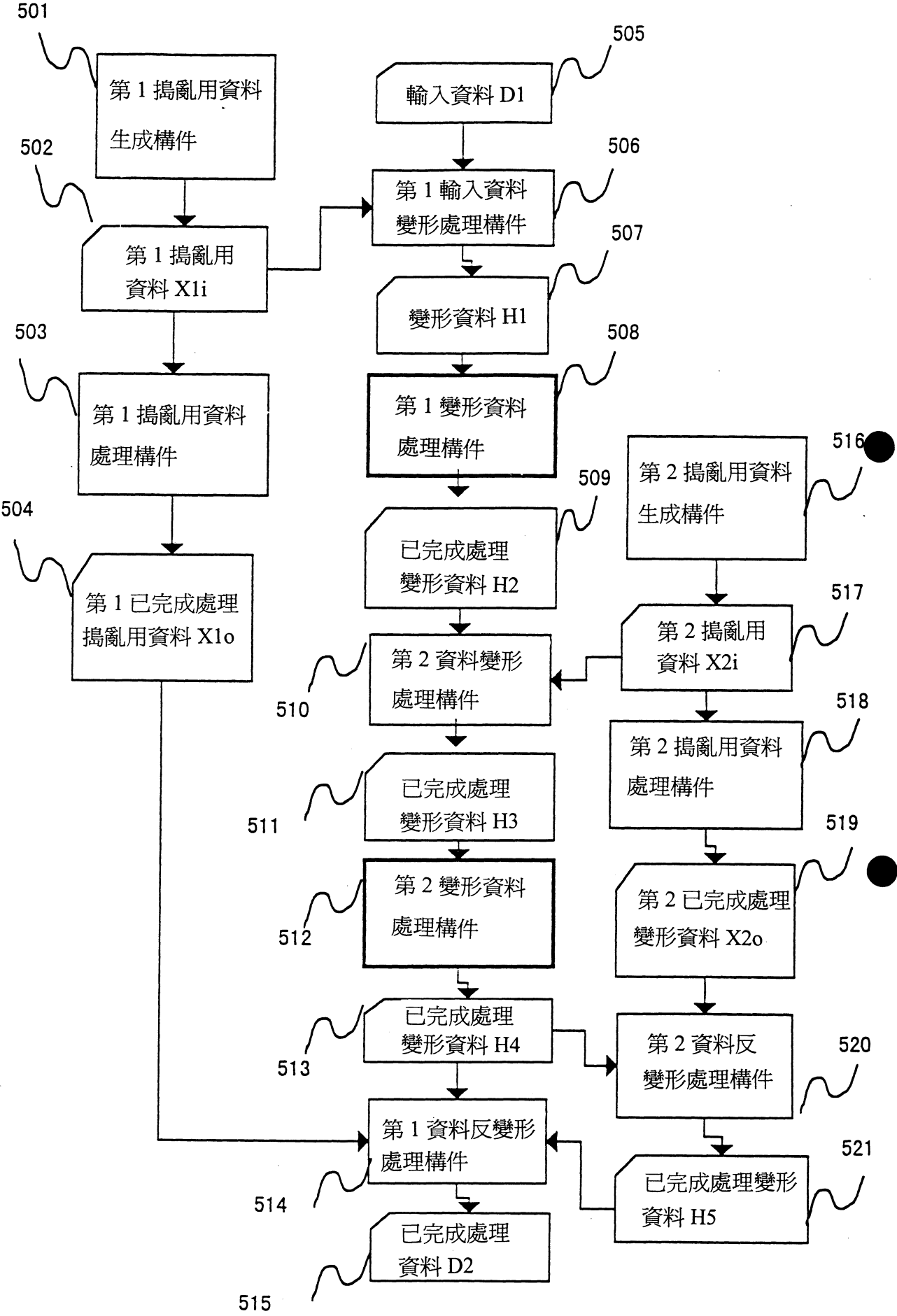
第 2 圖



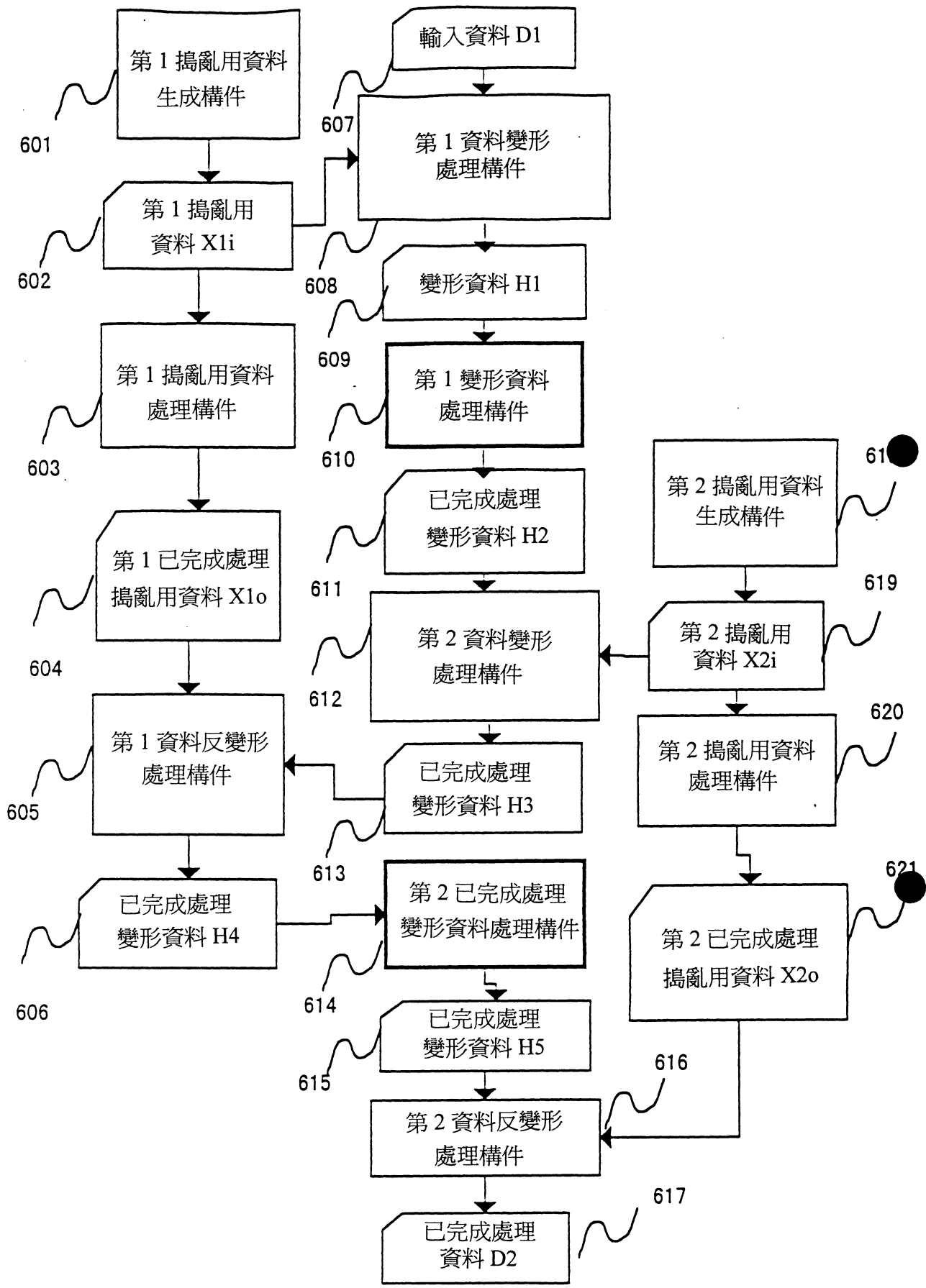
第 3 圖



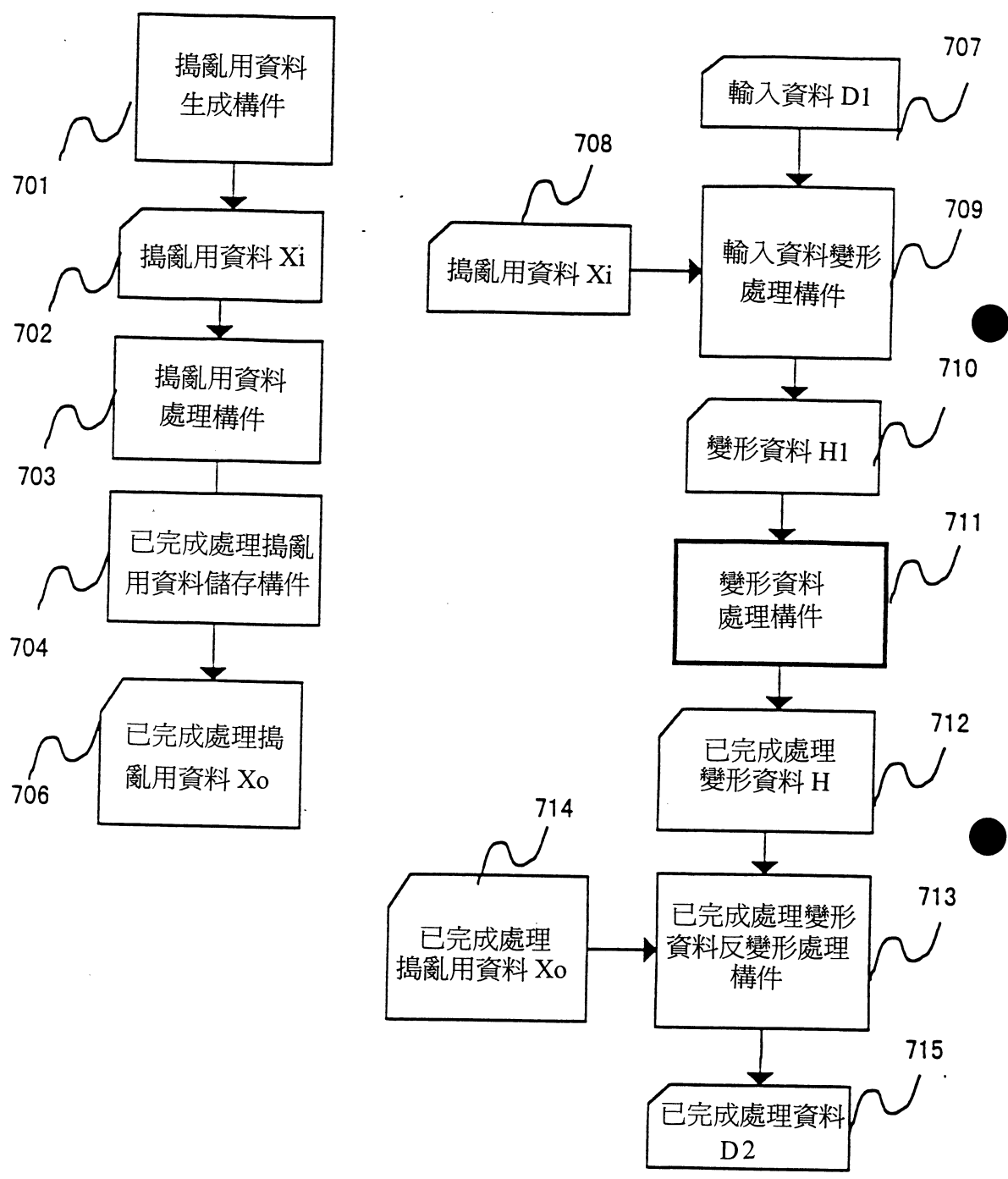
第 4 圖



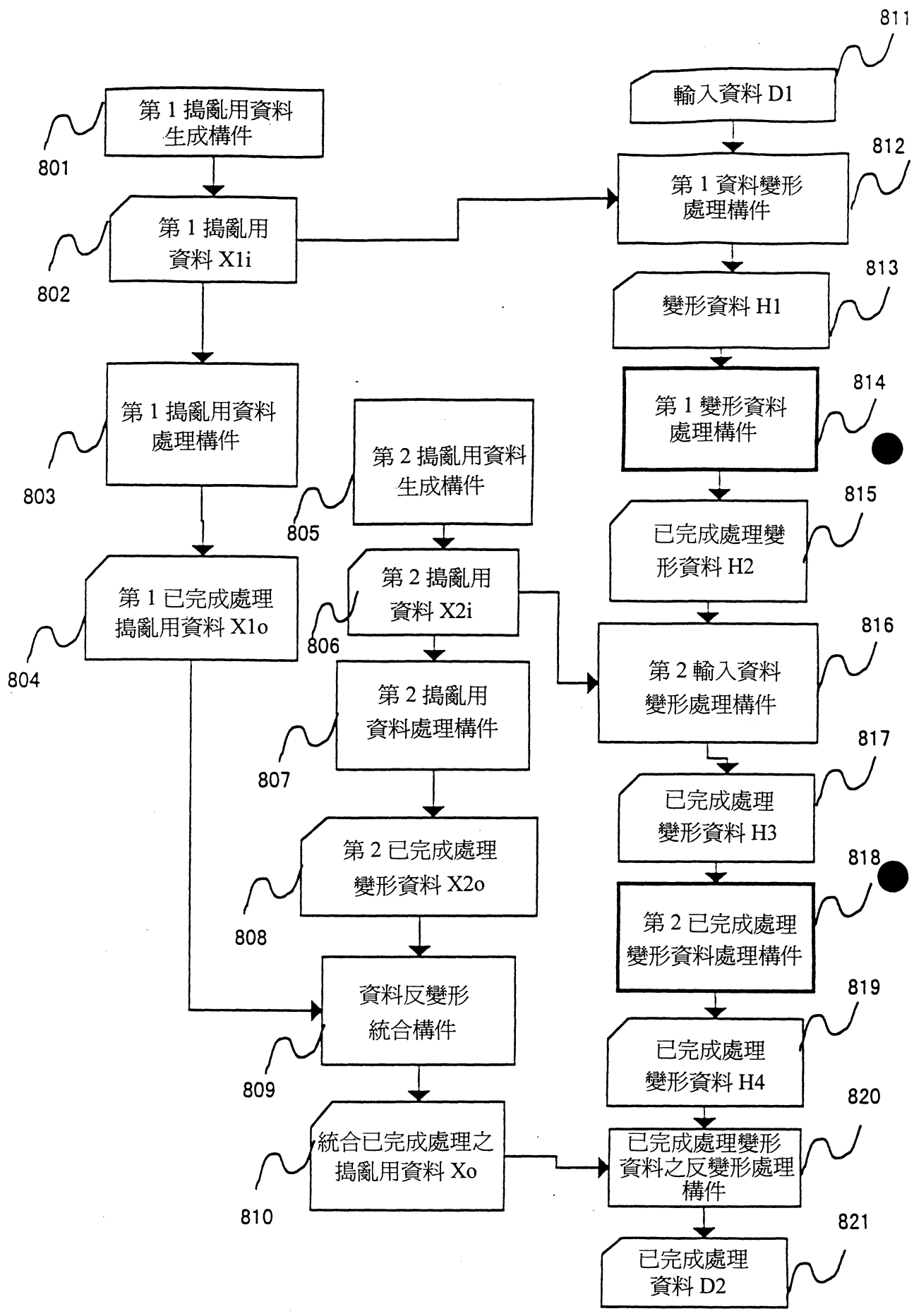
第 5 圖



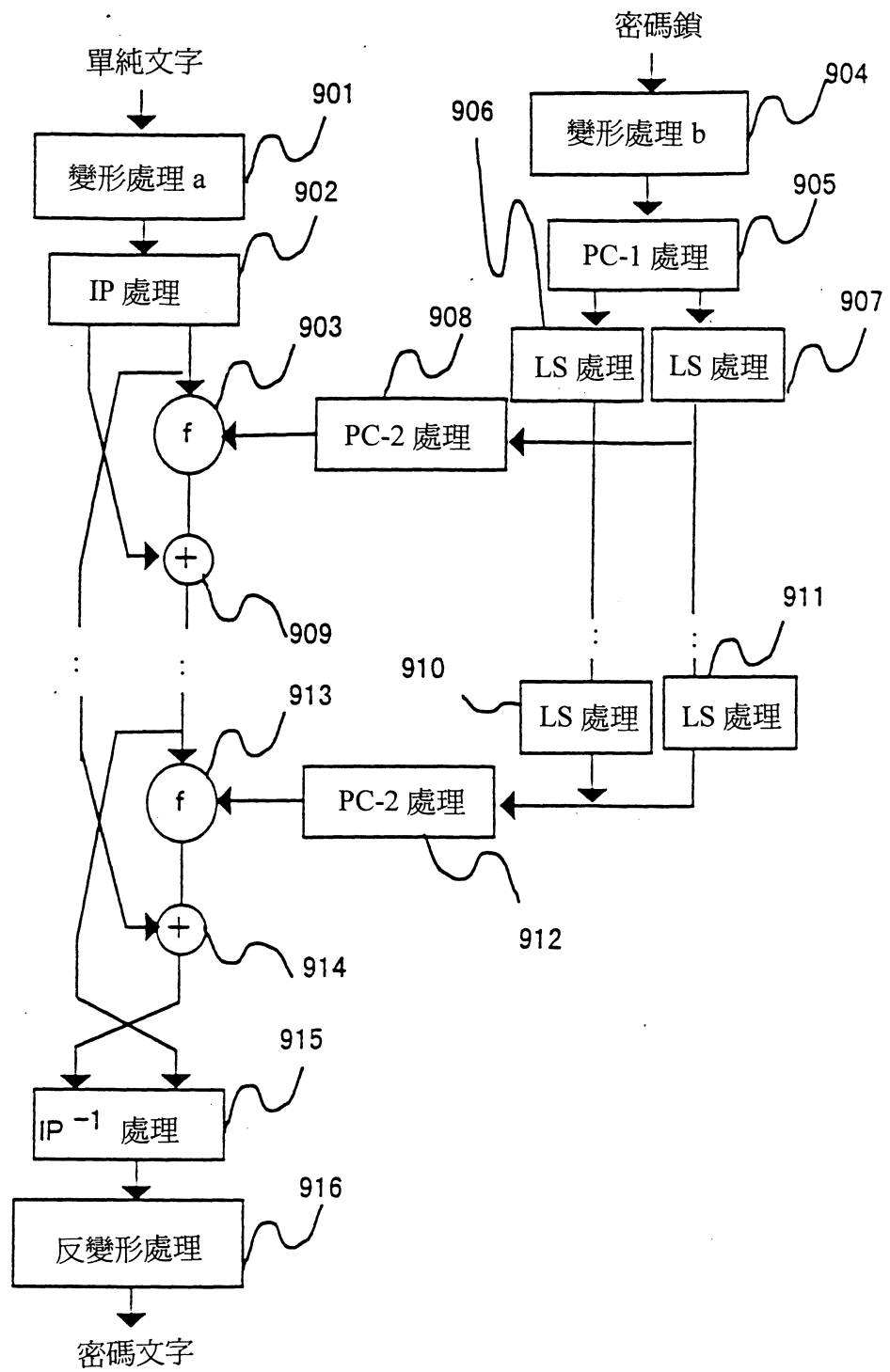
第 6 圖



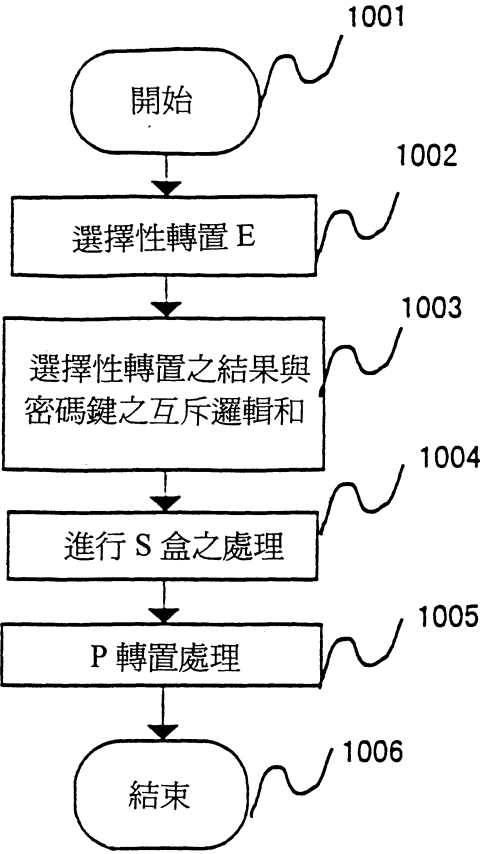
第 7 圖



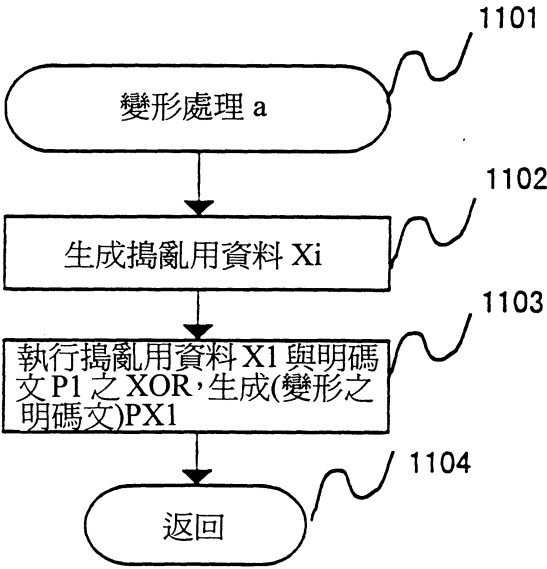
第 8 圖



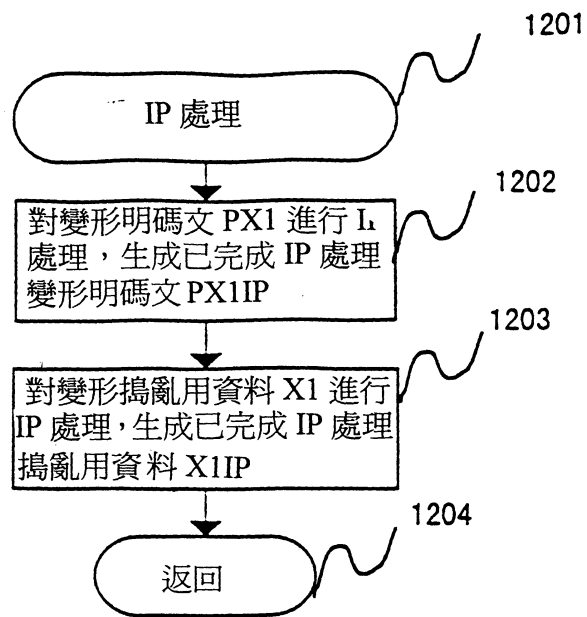
第 9 圖



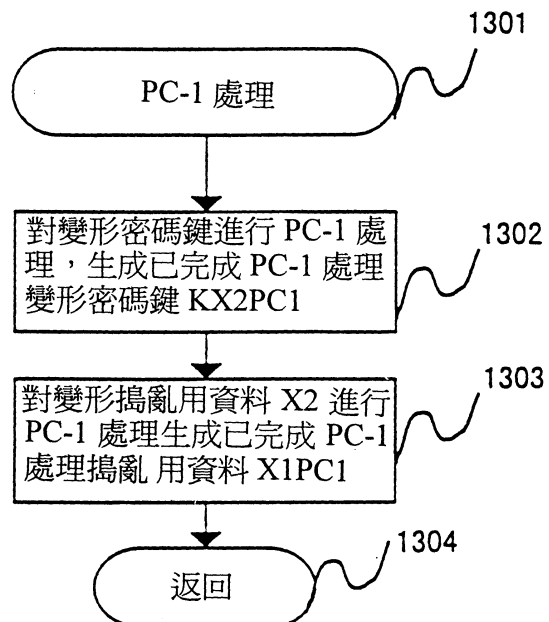
第 10 圖



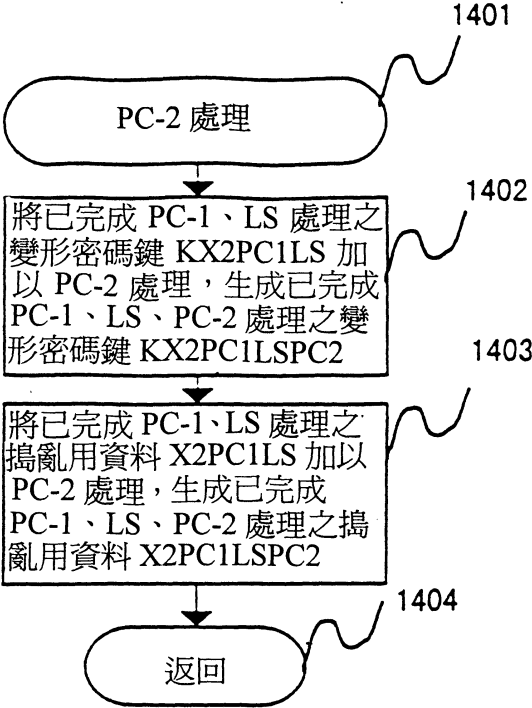
第 11 圖



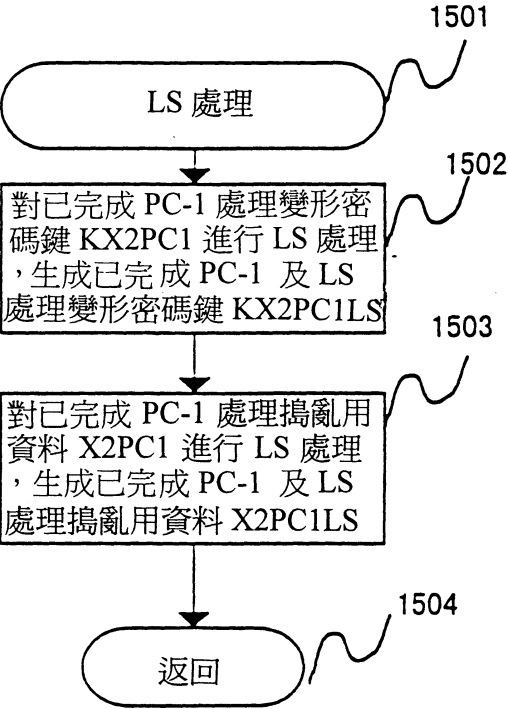
第 12 圖



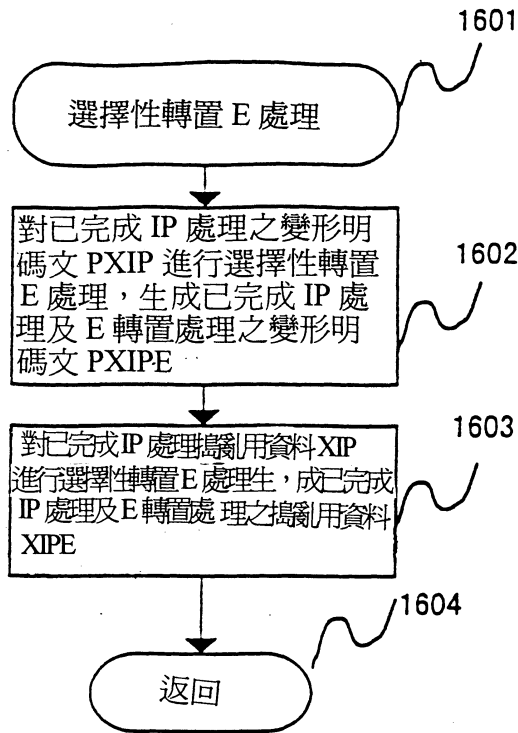
第 13 圖



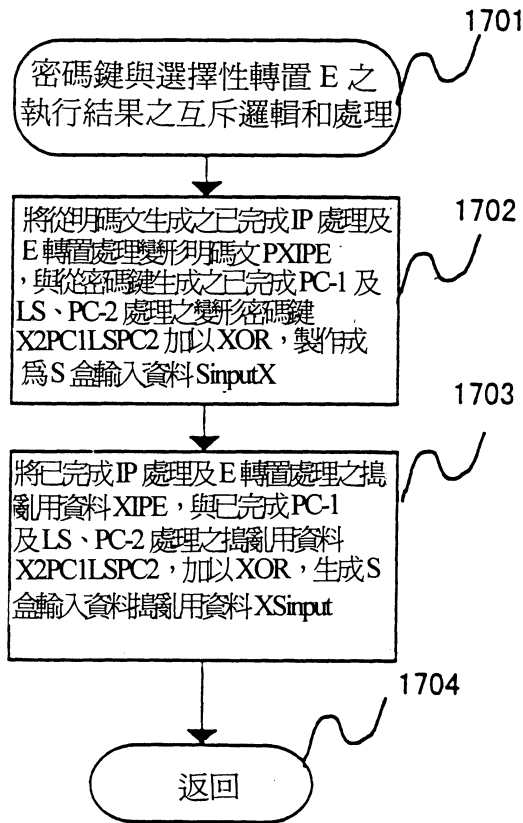
第 14 圖



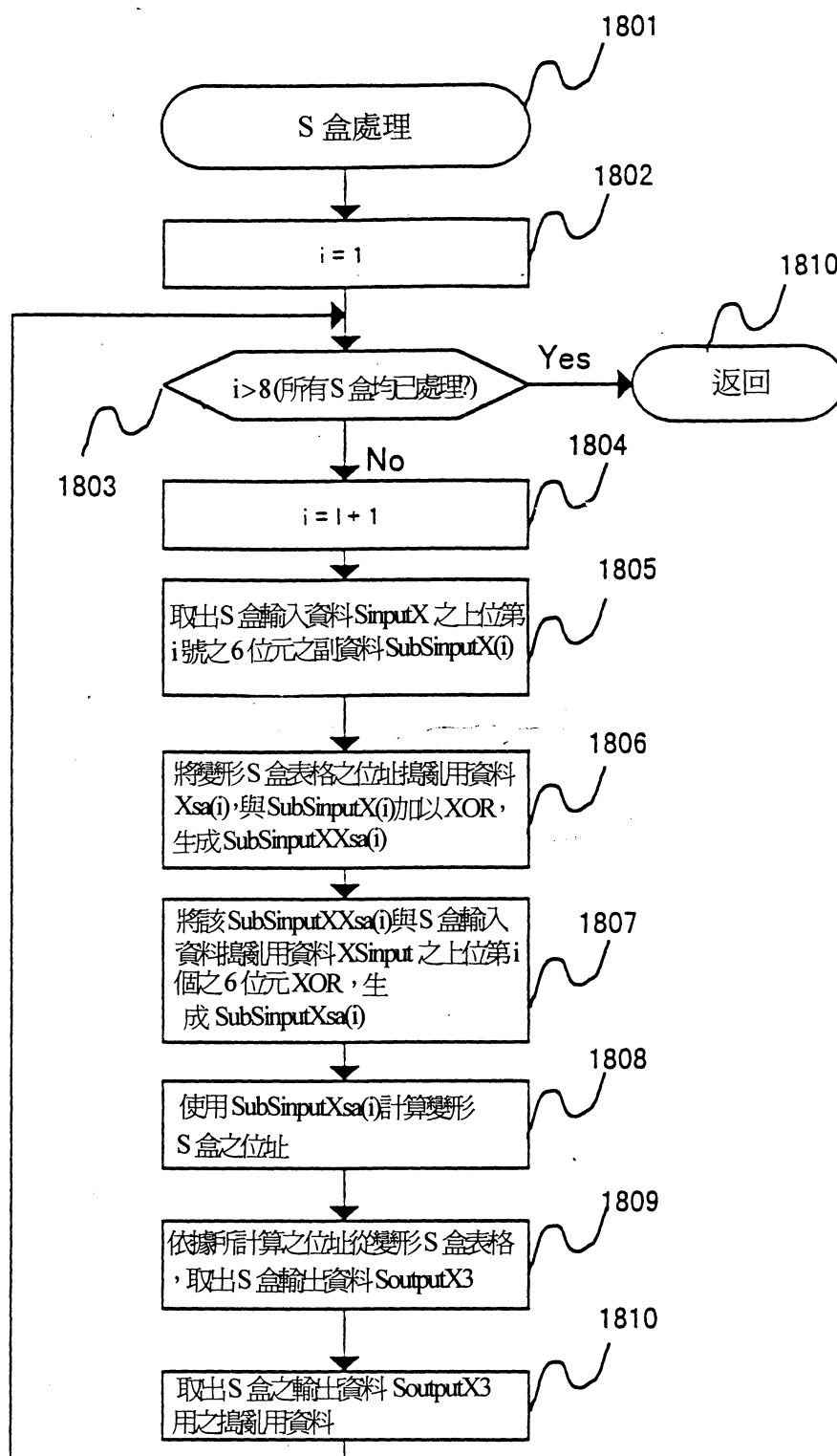
第 15 圖



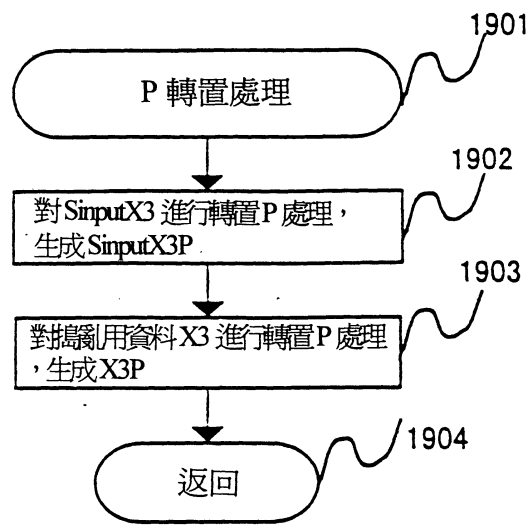
第 16 圖



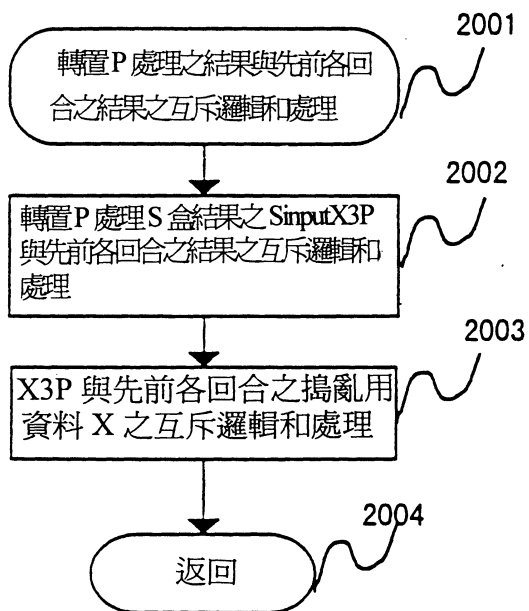
第 17 圖



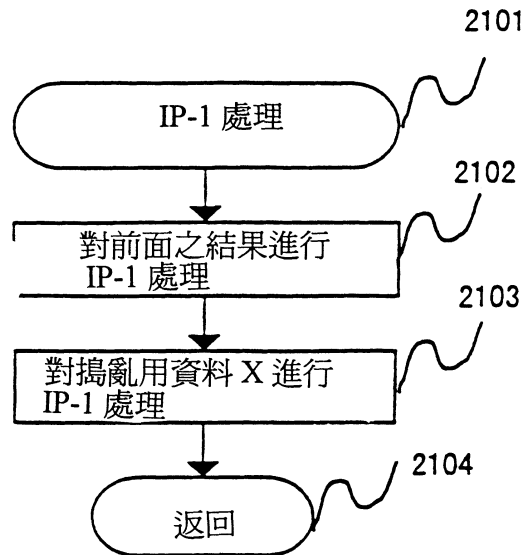
第 18 圖



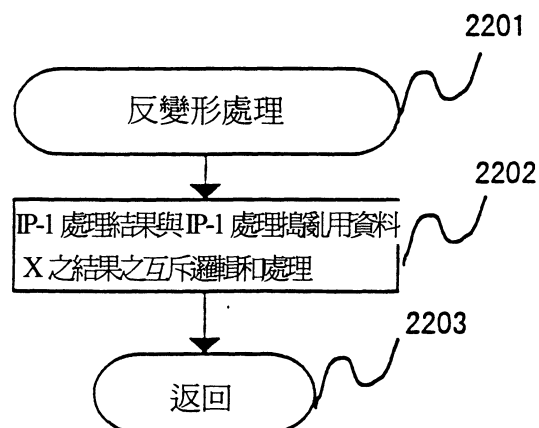
第 19 圖



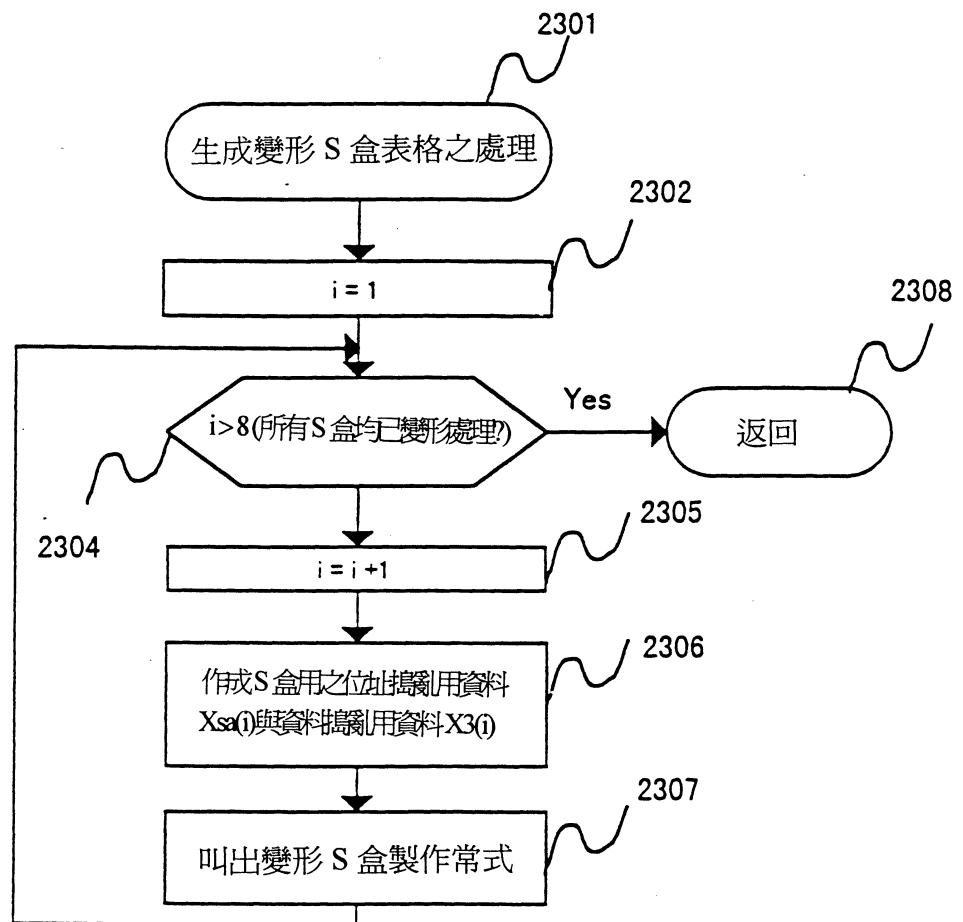
第 20 圖



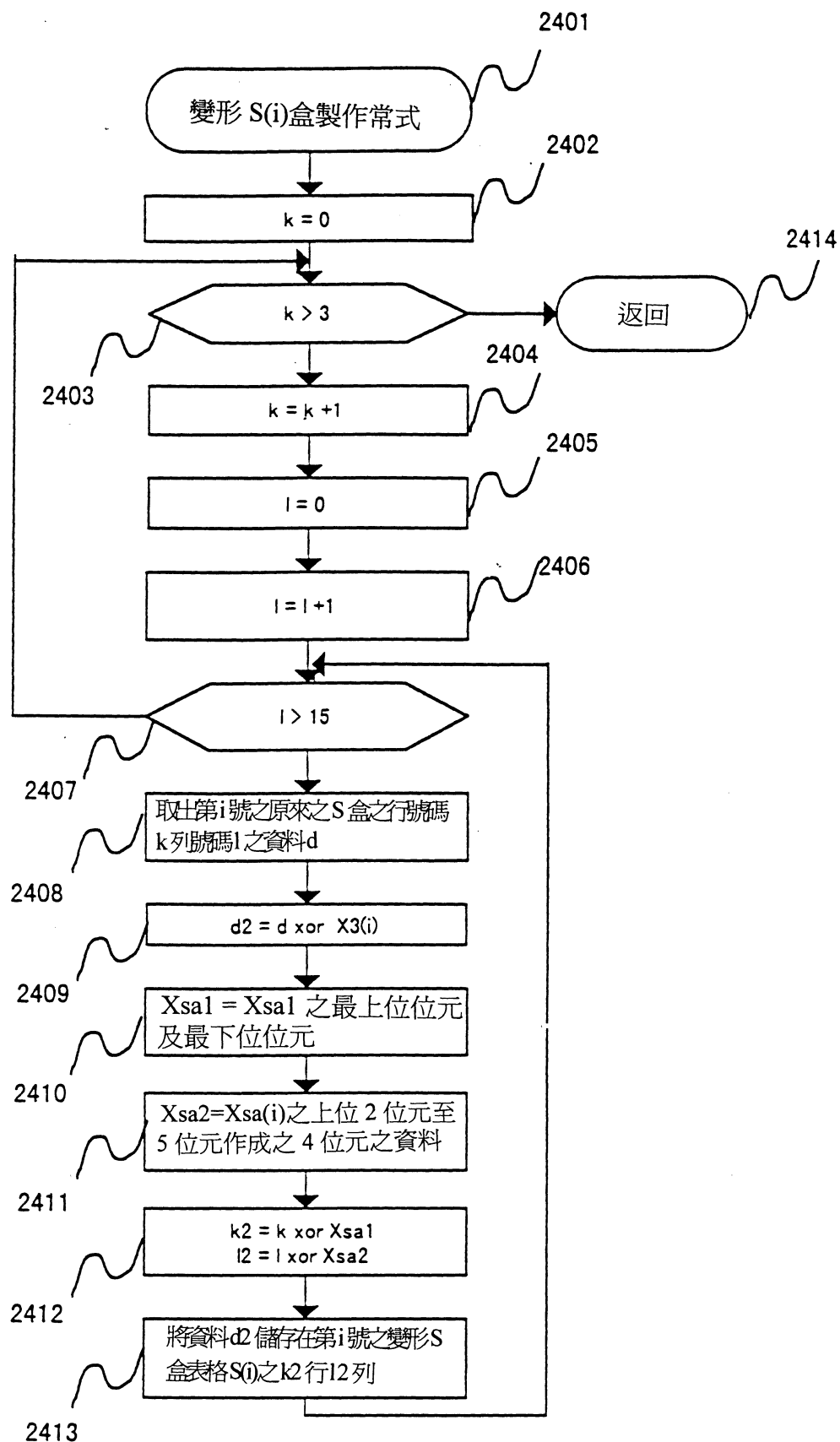
第 21 圖



第 22 圖



第 23 圖



第 24 圖

2501

2503

	0	1	2	3		15
0	14	4	13	1		7
1	0	15	7	4		8
2	4	1	14	8		0
3	15	12	8	2		13

2502

2504

第 25 圖

2601

2606

2603

	0	1	2	3		15
0	9	3	10	6		0
1	7	8	0	3		15
2	3	6	9	15		7
3	8	11	15	5		10

2605

對第 25 圖之表格 XOR 7 互斥邏輯和

2602

2604

第 26 圖

2701

2705

2703

	9	8	11	20		6
2	9	3	10	6		0
3	7	8	0	3		15
0	3	6	9	15		7
1	8	11	15	5		10

2704

對第 26 圖之行及列 XOR 2 與 9

2702

2704

第 27 圖

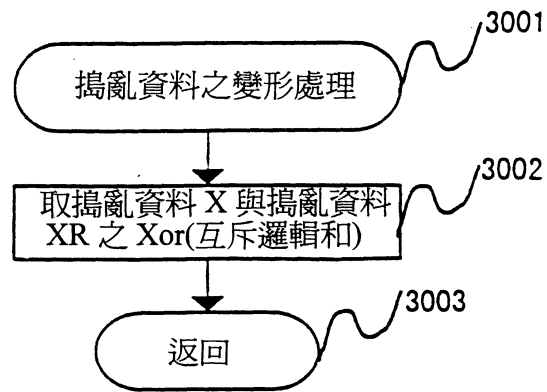
	1	2	3	4	5	6
1	32	1	2	3	4	5
2	4	5	6	7	8	9
3	8	9	10	11	12	13
4	12	13	14	15	16	17
5	16	17	18	19	20	21
6	20	21	22	23	24	25
7	24	25	26	27	28	29
8	28	29	30	31	32	1

第 28 圖

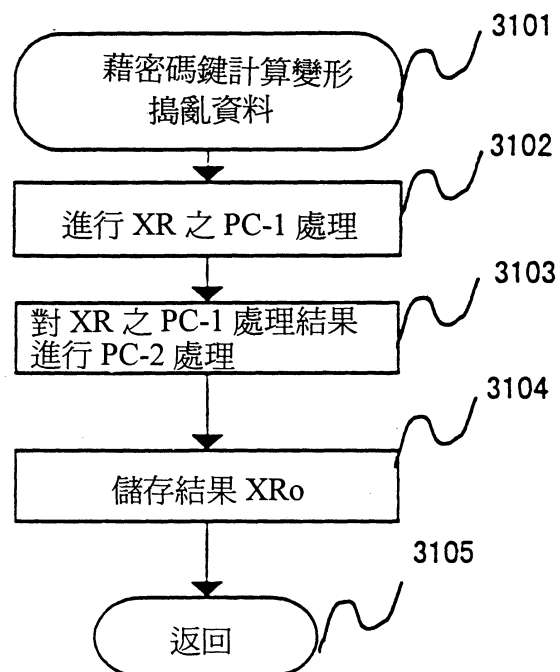
2901

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	21	14
32	27	3	9
19	13	30	6
22	11	4	25

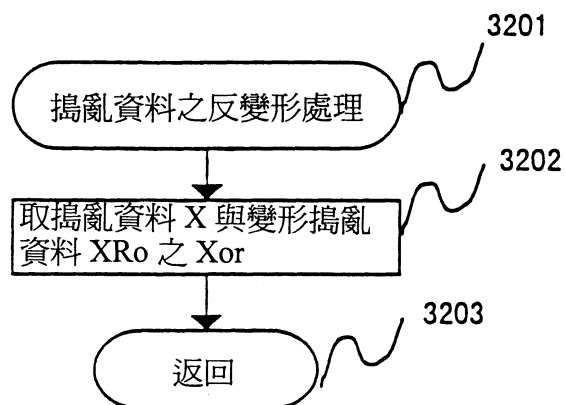
第 29 圖



第 30 圖



第 31 圖



第 32 圖

3301

	0	1	2	3
0	B	3	8	7
1	1	4	0	D
2	2	F	A	9
3	6	C	5	E

第 33 圖

3401

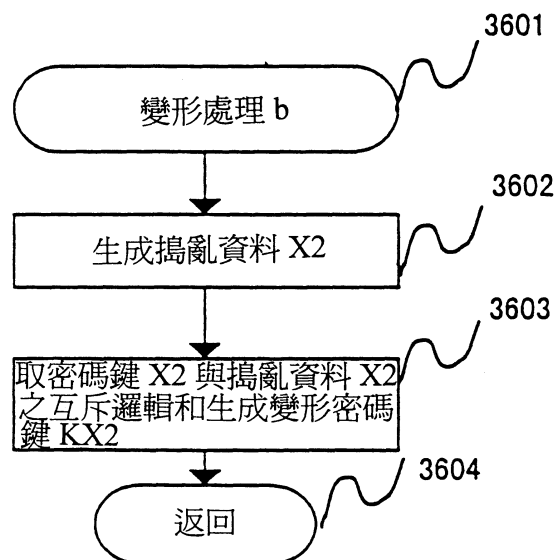
	0	1	2	3
0	2	A	1	E
1	8	D	9	4
2	B	6	3	0
3	F	5	C	7

第 34 圖

	0	1	2	3
0	5	F	7	C
1	6	B	0	3
2	D	8	4	9
3	A	2	E	1

3501

第 35 圖



第 36 圖

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

第 37 圖

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

第 38 圖