



(19) 中華民國智慧財產局

(12) 發明說明書公告本

(11) 證書號數：TW I474256 B

(45) 公告日：中華民國 104 (2015) 年 02 月 21 日

(21) 申請案號：101129234

(22) 申請日：中華民國 101 (2012) 年 08 月 13 日

(51) Int. Cl. : G06F7/58 (2006.01)

(30) 優先權：2012/06/21 美國 61/662,362

(71) 申請人：鈺創科技股份有限公司 (中華民國) ETRON TECHNOLOGY, INC. (TW)
新竹市科學工業園區科技五路 6 號

(72) 發明人：呂文閔 LU, WEN MIN (TW)

(74) 代理人：吳豐任；戴俊彥

(56) 參考文獻：

TW	453064	TW	I267829
TW	201102806A	CN	1490811A
US	4965881	US	2009/0204824A1
US	2009/0323942A1		

審查人員：劉季涵

申請專利範圍項數：20 項 圖式數：11 共 38 頁

(54) 名稱

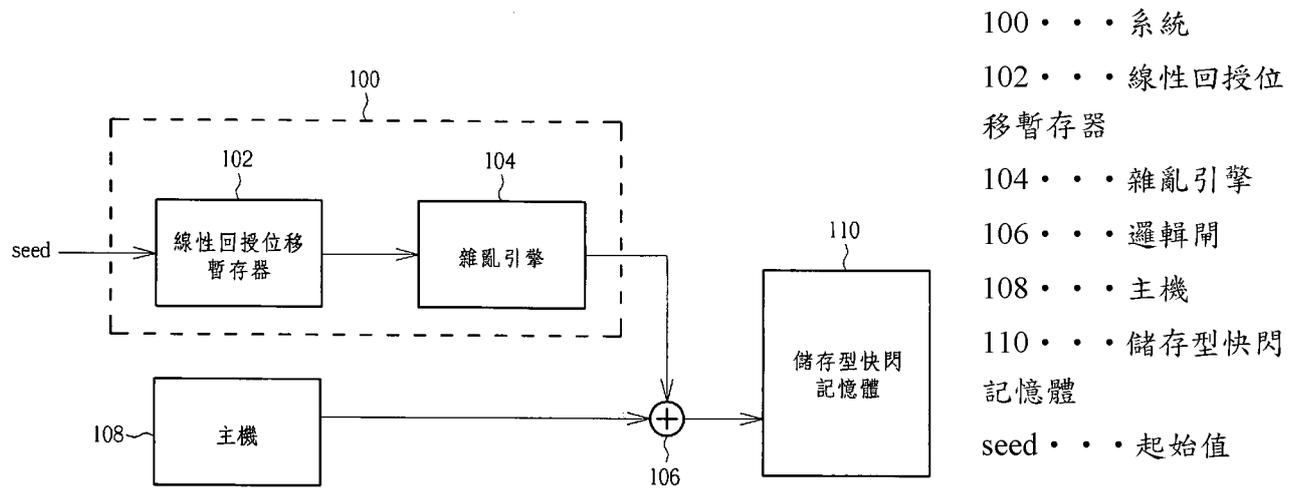
產生雜亂值的系統和產生雜亂值的方法

SYSTEM OF GENERATING SCRAMBLE DATA AND METHOD OF GENERATING SCRAMBLE DATA

(57) 摘要

產生雜亂值的系統包含一線性回授位移暫存器和一雜亂引擎。該線性回授位移暫存器是用以根據一起始值，產生複數個第一雜亂值；該雜亂引擎是耦接於該線性回授位移暫存器，用以利用該複數個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。

A system of generating scramble data includes a linear feedback shift register and a scramble engine. The linear feedback shift register is used for generating a plurality of first scramble values according to an initial value. The scramble engine is coupled to the linear feedback shift register for utilizing at least one bit of each first scramble value of the plurality of first scramble values to execute a first logic operation on other bits of the first scramble value to generate a second scramble value corresponding to the first scramble value. A bit number of the second scramble value is the same as a bit number of the first scramble value.



第1圖

發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※申請案號：101129234

※申請日：101. 8. 13

※IPC 分類：

G06F 7/58 (2006.01)

一、發明名稱：(中文/英文)

產生雜亂值的系統和產生雜亂值的方法/SYSTEM OF GENERATING
SCRAMBLE DATA AND METHOD OF GENERATING SCRAMBLE
DATA

二、中文發明摘要：

產生雜亂值的系統包含一線性回授位移暫存器和一雜亂引擎。
該線性回授位移暫存器是用以根據一起始值，產生複數個第一雜亂
值；該雜亂引擎是耦接於該線性回授位移暫存器，用以利用該複數
個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的
其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二
雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。

三、英文發明摘要：

A system of generating scramble data includes a linear feedback
shift register and a scramble engine. The linear feedback shift register is
used for generating a plurality of first scramble values according to an
initial value. The scramble engine is coupled to the linear feedback shift
register for utilizing at least one bit of each first scramble value of the
plurality of first scramble values to execute a first logic operation on
other bits of the first scramble value to generate a second scramble



value corresponding to the first scramble value. A bit number of the second scramble value is the same as a bit number of the first scramble value.

四、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：

100	系統
102	線性回授位移暫存器
104	雜亂引擎
106	邏輯閘
108	主機
110	儲存型快閃記憶體
seed	起始值

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種產生雜亂值的系統和產生雜亂值的方法，尤指一種利用雜亂引擎根據線性回授位移暫存器所產生的第一雜亂值，產生低度相關的第二雜亂值的產生雜亂值的系統和產生雜亂值的方法。

【先前技術】

在先前技術中，產生雜亂值的系統是利用一線性回授位移暫存器(linear feedback shift register, LFSR)根據一起始值，產生複數個雜亂值，例如 0x23(0010_0011)、0x47(0100_0111)、0x8F(1000_1111)等。然後，一邏輯閘對上述複數個雜亂值和來自一主機的資料執行一邏輯運算，以產生並輸出對應主機的資料的雜亂資料至一儲存型快閃記憶體(NAND flash)。

線性回授位移暫存器是往左移位一雜亂值的位元，以產生下一雜亂值。例如，線性回授位移暫存器是往左移位雜亂值 0x23(0010_0011)的位元，以產生下一雜亂值 0x47(0100_0111)。但值得注意的是，因為線性回授位移暫存器是往左移位雜亂值 0x23(0010_0011)的位元，以產生雜亂值 0x47(0100_0111)，所以雜亂值 0x23(0010_0011)與雜亂值 0x47(0100_0111)之間具有 7 個相同位元，亦即雜亂值 0x23(0010_0011)與雜亂值 0x47(0100_0111)高度相

關。因此，邏輯閘根據線性回授位移暫存器產生的雜亂值而產生的相鄰雜亂資料亦會高度相關。如此，邏輯閘所產生的高度相關的相鄰雜亂資料可能無法滿足儲存型快閃記憶體的規範。

【發明內容】

本發明的一實施例提供一種產生雜亂值的系統。該系統包含一線性回授位移暫存器和一雜亂引擎。該線性回授位移暫存器(linear feedback shift register, LFSR)是用以根據一起始值，產生複數個第一雜亂值；該雜亂引擎是耦接於該線性回授位移暫存器，用以利用該複數個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。

本發明的另一實施例提供一種產生雜亂值的方法。該方法包含根據一起始值，產生複數個第一雜亂值；利用該複數個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。

本發明提供一種產生雜亂值的系統和產生雜亂值的方法。該系統和該方法是利用一雜亂引擎根據一線性回授位移暫存器所產生的一第一雜亂值，產生一第二雜亂值，其中相鄰第二雜亂值是低度相

關。因此，本發明透過一邏輯閘所產生的相鄰雜亂資料亦會低度相關。如此，相較於先前技術，本發明所產生的低度相關的相鄰雜亂資料可滿足一儲存型快閃記憶體的規範。

【實施方式】

請參照第 1 圖，第 1 圖是為本發明的一實施例說明一種產生雜亂值的系統 100 的示意圖。系統 100 包含一線性回授位移暫存器 (linear feedback shift register, LFSR) 102 和一雜亂引擎 (scramble engine) 104。線性回授位移暫存器 102 是用以根據一起始值 seed，產生複數個第一雜亂值；雜亂引擎 104 是耦接於線性回授位移暫存器 102。

請參照第 2 圖，第 2 圖是為說明雜亂引擎 104 的示意圖。如第 2 圖所示，雜亂引擎 104 是用以利用複數個第一雜亂值中的每一第一雜亂值的一第一位元對第一雜亂值的其他位元執行一第一邏輯運算，以產生對應第一雜亂值的一第二雜亂值，其中第二雜亂值的位元數和第一雜亂值的位元數相同。例如當雜亂引擎 104 接收到一第一雜亂值 0x23(0010_0011)時，雜亂引擎 104 是利用第一雜亂值 0x23(0010_0011)的一第一位元 1 對第一雜亂值 0x23(0010_0011)的其他位元 0、0、1、0、0、0、1 執行一第一邏輯運算，以產生對應第一雜亂值 0x23(0010_0011)的一第二雜亂值 0xDD(1101_1101)，其中第二雜亂值 0xDD(1101_1101)的位元數和第一雜亂值 0x23(0010_0011)的位元數是為相同，且第一邏輯運算是可為一互斥

或邏輯運算。但本發明並不受限於第一雜亂值的位元數是為 8，亦即第一雜亂值亦可具有其他位元數。另外，本發明亦不受限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。同理，當雜亂引擎 104 接收到一第一雜亂值 0x47(0100_0111) 時，雜亂引擎 104 是利用 0x47(0100_0111) 的一第一位元 1 對第一雜亂值 0x47(0100_0111) 的其他位元 0、1、0、0、0、1、1 執行第一邏輯運算，以產生對應 0x47(0100_0111) 的一第二雜亂值 0xB9(1011_1001)。因此，透過雜亂引擎 104 產生的第二雜亂值 0xDD(1101_1101) 和第二雜亂值 0xB9(1011_1001) 之間的關聯性並不高。

如第 1 圖所示，系統 100 另包含一邏輯閘 106，其中邏輯閘 106 是可為一互斥或閘，且第二邏輯運算是為一互斥或邏輯運算。邏輯閘 106 是耦接於雜亂引擎 104，用以對一第二雜亂值和來自一主機 108 的一資料執行第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至一儲存型快閃記憶體(NAND flash)110，其中資料的位元數、第二雜亂值的位元數和雜亂資料的位元數相同。例如，當邏輯閘 106 接收到一第二雜亂值 0xDD(1101_1101) 和來自主機 108 的一資料 0x20(0010_0000) 時，邏輯閘 106 會對第二雜亂值 0xDD(1101_1101) 和資料 0x20(0010_0000) 執行第二邏輯運算，以產生並輸出對應資料 0x20(0010_0000) 的一雜亂資料 0xFD(1111_1101) 至儲存型快閃記憶體 110。

請參照第 3 圖，第 3 圖是為本發明的另一實施例說明一雜亂引擎 304 的示意圖，其中雜亂引擎 304 可取代第 1 圖中的雜亂引擎 104。如第 3 圖所示，雜亂引擎 304 是利用一第一雜亂值的每一奇數位元對第一雜亂值的每一奇數位元的下一位元執行一第一邏輯運算，以產生一第二雜亂值，其中第一邏輯運算是可為一互斥或邏輯運算，但本發明並不受限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。例如，雜亂引擎 304 是利用一第一雜亂值 0x23(0010_0011)的第一奇數位元 1 對第一雜亂值 0x23(0010_0011)的第一奇數位元 1 的下一位元 1 執行第一邏輯運算，產生一第二雜亂值的第一偶數位元 0；利用第一雜亂值 0x23(0010_0011)的第二奇數位元 0 對第一雜亂值 0x23(0010_0011)的第二奇數位元 0 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第二偶數位元 0；利用第一雜亂值 0x23(0010_0011)的第三奇數位元 0 對第一雜亂值 0x23(0010_0011)的第三奇數位元 0 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第三偶數位元 1；以及利用第一雜亂值 0x23(0010_0011)的第四奇數位元 0 對第一雜亂值 0x23(0010_0011)的第四奇數位元 0 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第四偶數位元 0。如第 3 圖所示，第二雜亂值的第一奇數位元、第二奇數位元、第三奇數位元和第四奇數位元分別為 1、0、0、0，以及第二雜亂值的第一偶數位元、第二偶數位元、第三偶數位元和第四偶數位元分別為 0、0、1、0。因此，雜亂引擎 304 即可透過上述過程，產生第二雜亂值 0x21(0010_0001)。另外，本發明並不受限於第一雜亂值的位元數是為 8，亦即第一雜亂

值亦可具有其他位元數。另外，雜亂引擎 304 的其餘操作原理皆和雜亂引擎 104 相同，在此不再贅述。

請參照第 4 圖，第 4 圖是為本發明的另一實施例說明一雜亂引擎 404 的示意圖，其中雜亂引擎 404 可取代第 1 圖中的雜亂引擎 104。如第 4 圖所示，雜亂引擎 404 是利用一第一雜亂值的第一奇數位元對第一雜亂值的其他奇數位元執行一第一邏輯運算以及利用第一雜亂值的第一偶數位元對第一雜亂值的其他偶數位元執行第一邏輯運算，以產生一第二雜亂值，其中第一邏輯運算是可為一互斥或邏輯運算，但本發明並不受限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。如第 4 圖所示，雜亂引擎 404 是利用一第一雜亂值 0x23(0010_0011)的第一奇數位元 1 對第一雜亂值 0x23(0010_0011)的其他奇數位元 0、0、0 執行第一邏輯運算，產生一第二雜亂值的第一奇數位元 1、第二奇數位元 1、第三奇數位元 1 及第四奇數位元 1，以及利用第一雜亂值 0x23(0010_0011)的第一偶數位元 1 對第一雜亂值 0x23(0010_0011)的其他偶數位元 0、1、0 執行第一邏輯運算，產生第二雜亂值的第一偶數位元 1、第二偶數位元 1、第三偶數位元 0 及第四偶數位元 1。因此，雜亂引擎 404 即可透過上述過程，產生第二雜亂值 0xDF(1101_1111)。另外，本發明並不受限於第一雜亂值的位元數是為 8，亦即第一雜亂值亦可具有其他位元數。另外，雜亂引擎 404 的其餘操作原理皆和雜亂引擎 104 相同，在此不再贅述。

請參照第 5 圖，第 5 圖是為本發明的另一實施例說明一雜亂引擎 504 的示意圖，其中雜亂引擎 504 可取代第 1 圖中的雜亂引擎 104。如第 5 圖所示，雜亂引擎 504 是先利用一第一雜亂值的第一位元對第一雜亂值的第二位元執行一第三邏輯運算，以產生一運算值。然後，雜亂引擎 504 利用運算值對第一雜亂值的第一位元與第二位元之外的其他位元執行一第一邏輯運算，以產生一第二雜亂值，其中第一邏輯運算是可為一互斥或邏輯運算，但本發明並不限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。另外，第三邏輯運算和第一邏輯運算可相同或不同。如第 5 圖所示，雜亂引擎 504 是先利用一第一雜亂值 0x21(0010_0001) 的第一位元 1 對第一雜亂值 0x21(0010_0001) 的第二位元 0 執行第三邏輯運算(例如互斥或邏輯運算)，以產生一運算值 1。然後，雜亂引擎 504 再利用運算值 1 對第一雜亂值 0x21(0010_0001) 的第一位元 1 與第二位元 0 之外的其他位元執行第一邏輯運算，以產生一第二雜亂值的其他位元 1、1、0、1、1、1。因此，雜亂引擎 504 即可透過上述過程，產生第二雜亂值 0xDD(1101_1101)。另外，本發明並不限於第一雜亂值的位元數是為 8，亦即第一雜亂值亦可具有其他位元數。另外，雜亂引擎 504 的其餘操作原理皆和雜亂引擎 104 相同，在此不再贅述。

請參照第 6 圖，第 6 圖是為本發明的另一實施例說明一雜亂引擎 604 的示意圖，其中雜亂引擎 604 可取代第 1 圖中的雜亂引擎 104。如第 6 圖所示，雜亂引擎 604 是先利用一第一雜亂值的第一位

元對第一雜亂值的其他位元執行一第三邏輯運算，以產生一預雜亂值。然後，雜亂引擎 604 再利用預雜亂值的每一奇數位元對每一奇數位元的下一位元執行一第一邏輯運算，以產生一第二雜亂值，其中第一邏輯運算是可為一互斥或邏輯運算，但本發明並不受限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。另外，第三邏輯運算和第一邏輯運算可相同或不同。如第 6 圖所示，雜亂引擎 604 是先利用一第一雜亂值 0x23(0010_0011)的第一位元 1 對第一雜亂值 0x23(0010_0011)的其他位元 0、0、1、0、0、0、1 執行第三邏輯運算(例如互斥或邏輯運算)，以產生對應第一雜亂值 0x23(0010_0011)的一預雜亂值 0xDD(1101_1101)。然後，雜亂引擎 604 是利用預雜亂值 0xDD(1101_1101)的第一奇數位元 1 對預雜亂值 0xDD(1101_1101)的第一奇數位元 1 的下一位元 0 執行第一邏輯運算，產生一第二雜亂值的第一偶數位元 1；利用預雜亂值 0xDD(1101_1101)的第二奇數位元 1 對預雜亂值 0xDD(1101_1101)的第二奇數位元 1 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第二偶數位元 0；利用預雜亂值 0xDD(1101_1101)的第三奇數位元 1 對預雜亂值 0xDD(1101_1101)的第三奇數位元 1 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第三偶數位元 1；以及利用預雜亂值 0xDD(1101_1101)的第四奇數位元 1 對預雜亂值 0xDD(1101_1101)的第四奇數位元 1 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第四偶數位元 0。如第 6 圖所示，第二雜亂值的第一奇數位元、第二奇數位元、第三奇數位元和第四奇數位元分別為 1、1、1、1，以及第二雜亂值的第一偶數位元、第二偶數位

元、第三偶數位元和第四偶數位元分別為 1、0、1、0。因此，雜亂引擎 604 即可透過上述過程，產生第二雜亂值 0x77(0111_0111)。另外，本發明並不受限於第一雜亂值的位元數是為 8，亦即第一雜亂值亦可具有其他位元數。另外，雜亂引擎 604 的其餘操作原理皆和雜亂引擎 104 相同，在此不再贅述。

請參照第 1 圖、第 2 圖和第 7 圖，第 7 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。第 7 圖的方法是利用第 1 圖的系統 100 和第 2 圖的雜亂引擎 104 說明，詳細步驟如下：

- 步驟 700： 開始；
- 步驟 702： 線性回授位移暫存器 102 根據一起始值 seed，產生複數個第一雜亂值；
- 步驟 704： 雜亂引擎 104 利用一第一雜亂值的第一位元對第一雜亂值的其他位元執行一第一邏輯運算，以產生一第二雜亂值；
- 步驟 706： 邏輯閘 106 對第二雜亂值和來自主機 108 的一資料執行一第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至儲存型快閃記憶體 110，跳至步驟 704。

在步驟 702 中，線性回授位移暫存器 102 根據起始值 seed，產生複數個第一雜亂值，例如 0x23(0010_0011)、0x47(0100_0111)等。

在步驟 704 中，雜亂引擎 104 是用以利用第一雜亂值的第一位元對第一雜亂值的其他位元執行第一邏輯運算，以產生對應第一雜亂值的第二雜亂值，其中第二雜亂值的位元數和第一雜亂值的位元數相同。例如，如第 2 圖所示，當雜亂引擎 104 接收到一第一雜亂值 0x23(0010_0011)時，雜亂引擎 104 是利用第一雜亂值 0x23(0010_0011)的一第一位元 1 對第一雜亂值 0x23(0010_0011)的其他位元 0、0、1、0、0、0、1 執行第一邏輯運算，以產生對應第一雜亂值 0x23(0010_0011)的一第二雜亂值 0xDD(1101_1101)，其中第二雜亂值 0xDD(1101_1101)的位元數和第一雜亂值 0x23(0010_0011)的位元數是為相同，且第一邏輯運算是可為一互斥或邏輯運算。但本發明並不受限於第一雜亂值的位元數是為 8，亦即第一雜亂值亦可具有其他位元數。另外，本發明亦不受限於第一邏輯運算是為互斥或邏輯運算，亦即第一邏輯運算亦可為其他邏輯運算。同理，當雜亂引擎 104 接收到第一雜亂值 0x47(0100_0111)時，雜亂引擎 104 是利用 0x47(0100_0111)的一第一位元 1 對第一雜亂值 0x47(0100_0111)的其他位元 0、1、0、0、0、1、1 執行第一邏輯運算，以產生對應 0x47(0100_0111)的一第二雜亂值 0xB9(1011_1001)。因此，透過雜亂引擎 104 產生的第二雜亂值 0xDD(1101_1101)和第二雜亂值 0xB9(1011_1001)之間的關聯性並不高。在步驟 706 中，邏輯閘 106 是用以對第二雜亂值和來自主機 108 的資料執行第二邏輯運算，以產生並輸出對應來自主機 108 的資料的雜亂資料至儲存型快閃記憶體 110，其中來自主機 108 的資料的位元數、第二雜亂值的位元數和雜亂資料的位元數相同。例如，當

邏輯閘 106 接收到第二雜亂值 0xDD(1101_1101)和來自主機 108 的一資料 0x20(0010_0000)時，邏輯閘 106 會對第二雜亂值 0xDD(1101_1101)和資料 0x20(0010_0000)執行第二邏輯運算，以產生並輸出對應資料 0x20(0010_0000)的一雜亂資料 0xFD(1111_1101)至儲存型快閃記憶體 110。

請參照第 1 圖、第 3 圖和第 8 圖，第 8 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。第 8 圖的方法是利用第 1 圖的系統 100 和第 3 圖的雜亂引擎 304 說明，詳細步驟如下：

- 步驟 800： 開始；
- 步驟 802： 線性回授位移暫存器 102 根據一起始值 seed，產生複數個第一雜亂值；
- 步驟 804： 雜亂引擎 304 利用一第一雜亂值的每一奇數位元對每一奇數位元的下一位元執行一第一邏輯運算，以產生一第二雜亂值；
- 步驟 806： 邏輯閘 106 對第二雜亂值和來自主機 108 的一資料執行一第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至儲存型快閃記憶體 110，跳至步驟 804。

第 8 圖的實施例和第 7 圖的實施例的差別在於在步驟 804 中，雜亂引擎 304 是利用第一雜亂值的每一奇數位元對第一雜亂值的每

一奇數位元的下一位元執行第一邏輯運算，以產生對應第一雜亂值的第二雜亂值。例如，如第 3 圖所示，當雜亂引擎 304 接收到一第一雜亂值 $0x23(0010_0011)$ 時，雜亂引擎 304 是利用第一雜亂值 $0x23(0010_0011)$ 的第一奇數位元 1 對第一雜亂值 $0x23(0010_0011)$ 的第一奇數位元 1 的下一位元 1 執行第一邏輯運算，產生一第二雜亂值的第一偶數位元 0；利用第一雜亂值 $0x23(0010_0011)$ 的第二奇數位元 0 對第一雜亂值 $0x23(0010_0011)$ 的第二奇數位元 0 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第二偶數位元 0；利用第一雜亂值 $0x23(0010_0011)$ 的第三奇數位元 0 對第一雜亂值 $0x23(0010_0011)$ 的第三奇數位元 0 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第三偶數位元 1；以及利用第一雜亂值 $0x23(0010_0011)$ 的第四奇數位元 0 對第一雜亂值 $0x23(0010_0011)$ 的第四奇數位元 0 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第四偶數位元 0。如第 3 圖所示，第二雜亂值的第一奇數位元、第二奇數位元、第三奇數位元和第四奇數位元分別為 1、0、0、0，以及第二雜亂值的第一偶數位元、第二偶數位元、第三偶數位元和第四偶數位元分別為 0、0、1、0。因此，雜亂引擎 304 即可透過上述過程，產生第二雜亂值 $0x21(0010_0001)$ 。另外，第 8 圖的實施例的其餘操作原理皆和第 7 圖的實施例相同，在此不再贅述。

請參照第 1 圖、第 4 圖和第 9 圖，第 9 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。第 9 圖的方法是利用第 1 圖的系統 100 和第 4 圖的雜亂引擎 404 說明，詳細步驟如下：

- 步驟 900： 開始；
- 步驟 902： 線性回授位移暫存器 102 根據一起始值 seed，產生複數個第一雜亂值；
- 步驟 904： 雜亂引擎 404 利用一第一雜亂值的第一奇數位元對第一雜亂值的其他奇數位元執行一第一邏輯運算以及利用第一雜亂值的第一偶數位元對第一雜亂值的其他偶數位元執行第一邏輯運算，以產生一第二雜亂值；
- 步驟 906： 邏輯閘 106 對第二雜亂值和來自主機 108 的一資料執行一第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至儲存型快閃記憶體 110，跳至步驟 904。

第 9 圖的實施例和第 7 圖的實施例的差別在於在步驟 904 中，雜亂引擎 404 是利用第一雜亂值的第一奇數位元對第一雜亂值的其他奇數位元執行第一邏輯運算以及利用第一雜亂值的第一偶數位元對第一雜亂值的其他偶數位元執行第一邏輯運算，以產生第二雜亂值。例如，如第 4 圖所示，當雜亂引擎 404 接收到一第一雜亂值 0x23(0010_0011)時，雜亂引擎 404 是利用第一雜亂值 0x23(0010_0011)的第一奇數位元 1 對第一雜亂值 0x23(0010_0011)的其他奇數位元 0、0、0 執行第一邏輯運算，產生一第二雜亂值的第一奇數位元 1、第二奇數位元 1、第三奇數位元 1 及第四奇數位元

1，以及利用第一雜亂值 0x23(0010_0011)的第一偶數位元 1 對第一雜亂值 0x23(0010_0011)的其他偶數位元 0、1、0 執行第一邏輯運算，產生第二雜亂值的第一偶數位元 1、第二偶數位元 1、第三偶數位元 0 及第四偶數位元 1。因此，雜亂引擎 404 即可透過上述過程，產生第二雜亂值 0xDF(1101_1111)。另外，第 9 圖的實施例的其餘操作原理皆和第 7 圖的實施例相同，在此不再贅述。

請參照第 1 圖、第 5 圖和第 10 圖，第 10 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。第 10 圖的方法是利用第 1 圖的系統 100 和第 5 圖的雜亂引擎 504 說明，詳細步驟如下：

步驟 1000： 開始；

步驟 1002： 線性回授位移暫存器 102 根據一起始值 seed，產生複數個第一雜亂值；

步驟 1004： 雜亂引擎 504 利用一第一雜亂值的第一位元對第一雜亂值的第二位元執行一第三邏輯運算，以產生一運算值；

步驟 1006： 雜亂引擎 504 利用運算值對第一雜亂值的第一位元與第二位元之外的其他位元執行一第一邏輯運算，以產生一第二雜亂值；

步驟 1008： 邏輯閘 106 對第二雜亂值和來自主機 108 的一資料執行一第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至儲存型快閃記憶體 110，跳至

步驟 1004。

第 10 圖的實施例和第 7 圖的實施例的差別在於在步驟 1004 中，雜亂引擎 504 是先利用第一雜亂值的第一位元對第一雜亂值的第二位元執行第三邏輯運算，以產生運算值；在步驟 1006 中，雜亂引擎 504 利用運算值對第一雜亂值的第一位元與第二位元之外的其他位元執行第一邏輯運算，以產生第二雜亂值，其中第三邏輯運算是可為一互斥或邏輯運算，但本發明並不受限於第三邏輯運算是為互斥或邏輯運算，亦即第三邏輯運算亦可為其他邏輯運算。另外，第三邏輯運算和第一邏輯運算可相同或不同。例如，如第 5 圖所示，當雜亂引擎 504 接收到一第一雜亂值 0x23(0010_0011)時，雜亂引擎 504 是先利用第一雜亂值 0x21(0010_0001)的第一位元 1 對第一雜亂值 0x21(0010_0001)的第二位元 0 執行第三邏輯運算，以產生一運算值 1。然後，雜亂引擎 504 再利用運算值 1 對第一雜亂值 0x21(0010_0001)的第一位元 1 與第二位元 0 之外的其他位元執行第一邏輯運算，以產生一第二雜亂值的其他位元 1、1、0、1、1、1。因此，雜亂引擎 504 即可透過上述過程，產生第二雜亂值 0xDD(1101_1101)。另外，第 10 圖的實施例的其餘操作原理皆和第 7 圖的實施例相同，在此不再贅述。

請參照第 1 圖、第 6 圖和第 11 圖，第 11 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。第 11 圖的方法是利用第 1 圖的系統 100 和第 6 圖的雜亂引擎 604 說明，詳細步驟如下：

- 步驟 1100： 開始；
- 步驟 1102： 線性回授位移暫存器 102 根據一起始值 seed，產生複數個第一雜亂值；
- 步驟 1104： 雜亂引擎 604 利用一第一雜亂值的第一位元對第一雜亂值的其他位元執行一第三邏輯運算，以產生一預雜亂值；
- 步驟 1106： 雜亂引擎 604 利用預雜亂值的每一奇數位元對每一奇數位元的下一位元執行一第一邏輯運算，以產生一第二雜亂值；
- 步驟 1108： 邏輯閘 106 對第二雜亂值和來自主機 108 的一資料執行一第二邏輯運算，以產生並輸出對應來自主機 108 的資料的一雜亂資料至儲存型快閃記憶體 110，跳至步驟 1104。

第 11 圖的實施例和第 7 圖的實施例的差別在於在步驟 1104 中，雜亂引擎 604 是先利用第一雜亂值的第一位元對第一雜亂值的其他位元執行第三邏輯運算，以產生預雜亂值；在步驟 1106 中，雜亂引擎 604 再利用預雜亂值的每一奇數位元對每一奇數位元的下一位元執行第一邏輯運算，以產生第二雜亂值，其中第三邏輯運算是可為一互斥或邏輯運算，但本發明並不受限於第三邏輯運算是為互斥或邏輯運算，亦即第三邏輯運算亦可為其他邏輯運算。另外，第三邏輯運算和第一邏輯運算可相同或不同。例如，如第 6 圖所示，當雜

亂引擎 604 接收到一第一雜亂值 $0x23(0010_0011)$ 時，雜亂引擎 604 是先利用第一雜亂值 $0x23(0010_0011)$ 的第一位元 1 對第一雜亂值 $0x23(0010_0011)$ 的其他位元 0、0、1、0、0、0、1 執行第三邏輯運算，以產生對應第一雜亂值 $0x23(0010_0011)$ 的一預雜亂值 $0xDD(1101_1101)$ 。然後，雜亂引擎 604 是利用預雜亂值 $0xDD(1101_1101)$ 的第一奇數位元 1 對預雜亂值 $0xDD(1101_1101)$ 的第一奇數位元 1 的下一位元 0 執行第一邏輯運算，產生一第二雜亂值的第一偶數位元 1；利用預雜亂值 $0xDD(1101_1101)$ 的第二奇數位元 1 對預雜亂值 $0xDD(1101_1101)$ 的第二奇數位元 1 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第二偶數位元 0；利用預雜亂值 $0xDD(1101_1101)$ 的第三奇數位元 1 對預雜亂值 $0xDD(1101_1101)$ 的第三奇數位元 1 的下一位元 0 執行第一邏輯運算，產生第二雜亂值的第三偶數位元 1；以及利用預雜亂值 $0xDD(1101_1101)$ 的第四奇數位元 1 對預雜亂值 $0xDD(1101_1101)$ 的第四奇數位元 1 的下一位元 1 執行第一邏輯運算，產生第二雜亂值的第四偶數位元 0。如第 6 圖所示，第二雜亂值的第一奇數位元、第二奇數位元、第三奇數位元和第四奇數位元分別為 1、1、1、1，以及第二雜亂值的第一偶數位元、第二偶數位元、第三偶數位元和第四偶數位元分別為 1、0、1、0。因此，雜亂引擎 604 即可透過上述過程，產生第二雜亂值 $0x77(0111_0111)$ 。另外，第 11 圖的實施例的其餘操作原理皆和第 7 圖的實施例相同，在此不再贅述。

綜上所述，本發明所提供的產生雜亂值的系統和產生雜亂值的

方法，是利用雜亂引擎根據線性回授位移暫存器所產生的第一雜亂值，產生第二雜亂值，其中相鄰第二雜亂值是低度相關。因此，本發明透過邏輯閘所產生的相鄰雜亂資料亦會低度相關。如此，相較於先前技術，本發明所產生的低度相關的相鄰雜亂資料可滿足儲存型快閃記憶體的規範。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【圖式簡單說明】

第 1 圖是為本發明的一實施例說明一種產生雜亂值的系統的示意圖。

第 2 圖是為說明雜亂引擎的示意圖。

第 3 圖是為本發明的另一實施例說明雜亂引擎的示意圖。

第 4 圖是為本發明的另一實施例說明雜亂引擎的示意圖。

第 5 圖是為本發明的另一實施例說明雜亂引擎的示意圖。

第 6 圖是為本發明的另一實施例說明雜亂引擎的示意圖。

第 7 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。

第 8 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。

第 9 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程圖。

第 10 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程图。

第 11 圖是為本發明的另一實施例說明一種產生雜亂值的方法的流程图。

【主要元件符號說明】

100	系統
102	線性回授位移暫存器
104、304、404、504、604	雜亂引擎
106	邏輯閘
108	主機
110	儲存型快閃記憶體
seed	起始值
700-706、800-806、900-906、 1000-1008、1100-1108	步驟

七、申請專利範圍：

1. 一種產生雜亂值的系統，包含：
一線性回授位移暫存器(linear feedback shift register, LFSR)，用以根據一起始值，產生複數個第一雜亂值；及
一雜亂引擎，耦接於該線性回授位移暫存器，用以利用該複數個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。
2. 如請求項 1 所述的系統，另包含：
一邏輯閘，耦接於該雜亂引擎，用以對該第二雜亂值和來自一主機的一資料執行一第二邏輯運算，以產生並輸出對應該資料的一雜亂資料至一儲存型快閃記憶體(NAND flash)，其中該資料的位元數、該第二雜亂值的位元數和該雜亂資料的位元數相同。
3. 如請求項 2 所述的系統，其中該邏輯閘是為一互斥或閘，且該第二邏輯運算是為一互斥或邏輯運算。
4. 如請求項 1 所述的系統，其中該雜亂引擎是利用該第一雜亂值的第一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生該第二雜亂值。

5. 如請求項 1 所述的系統，其中該雜亂引擎是利用該第一雜亂值的每一奇數位元對該奇數位元的下一位元執行該第一邏輯運算，以產生該第二雜亂值。
6. 如請求項 1 所述的系統，其中該雜亂引擎是利用該第一雜亂值的第一奇數位元對該第一雜亂值的其他奇數位元執行該第一邏輯運算以及利用該第一雜亂值的第一偶數位元對該第一雜亂值的其他偶數位元執行該第一邏輯運算，以產生該第二雜亂值。
7. 如請求項 1 所述的系統，其中該雜亂引擎是先利用該第一雜亂值的第一位元對該第一雜亂值的第二位元執行一第三邏輯運算，以產生一運算值，再利用該運算值對該第一位元與該第二位元之外的其他位元執行該第一邏輯運算，以產生該第二雜亂值。
8. 如請求項 1 所述的系統，其中該雜亂引擎是先利用該第一雜亂值的第一位元對該第一雜亂值的其他位元執行一第三邏輯運算，以產生一預雜亂值，以及再利用該預雜亂值的每一奇數位元對該奇數位元的下一位元執行該第一邏輯運算，以產生該第二雜亂值。
9. 如請求項 7 或 8 所述的系統，其中該第三邏輯運算和該第一邏

輯運算相同或不同。

10. 如請求項 4、5、6、7 或 8 所述的系統，其中該第一邏輯運算是為一互斥或邏輯運算。

11. 一種產生雜亂值的方法，包含：

根據一起始值，產生複數個第一雜亂值；及

利用該複數個第一雜亂值中的每一第一雜亂值的至少一位元對該第一雜亂值的其他位元執行一第一邏輯運算，以產生對應該第一雜亂值的一第二雜亂值，其中該第二雜亂值的位元數和該第一雜亂值的位元數相同。

12. 如請求項 11 所述的方法，另包含：

對該第二雜亂值和來自一主機的一資料執行一第二邏輯運算，以產生並輸出對應該資料的一雜亂資料至一儲存型快閃記憶體；

其中該資料的位元數、該第二雜亂值的位元數和該雜亂資料的位元數相同。

13. 如請求項 12 所述的方法，其中該第二邏輯運算是為一互斥或邏輯運算。

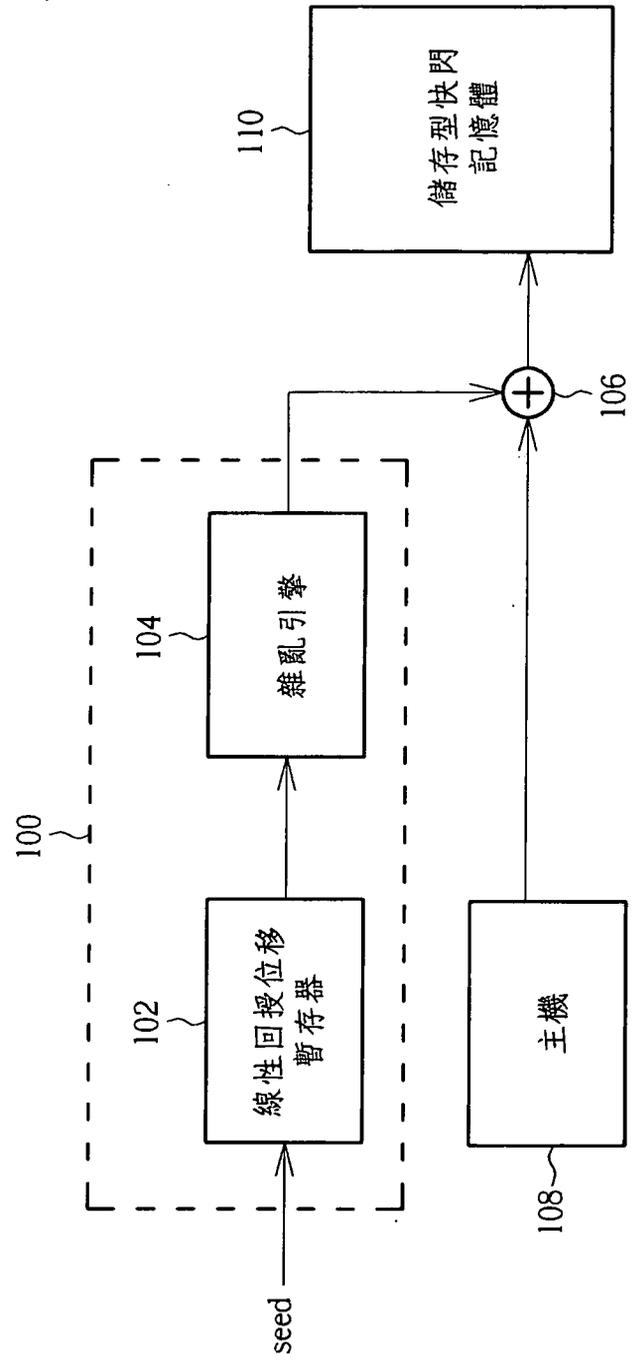
14. 如請求項 11 所述的方法，其中利用該第一雜亂值的至少一位元

對該第一雜亂值的其他位元執行該第一邏輯運算，以產生對應該第二雜亂值，是為利用該第一雜亂值的第一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生該第二雜亂值。

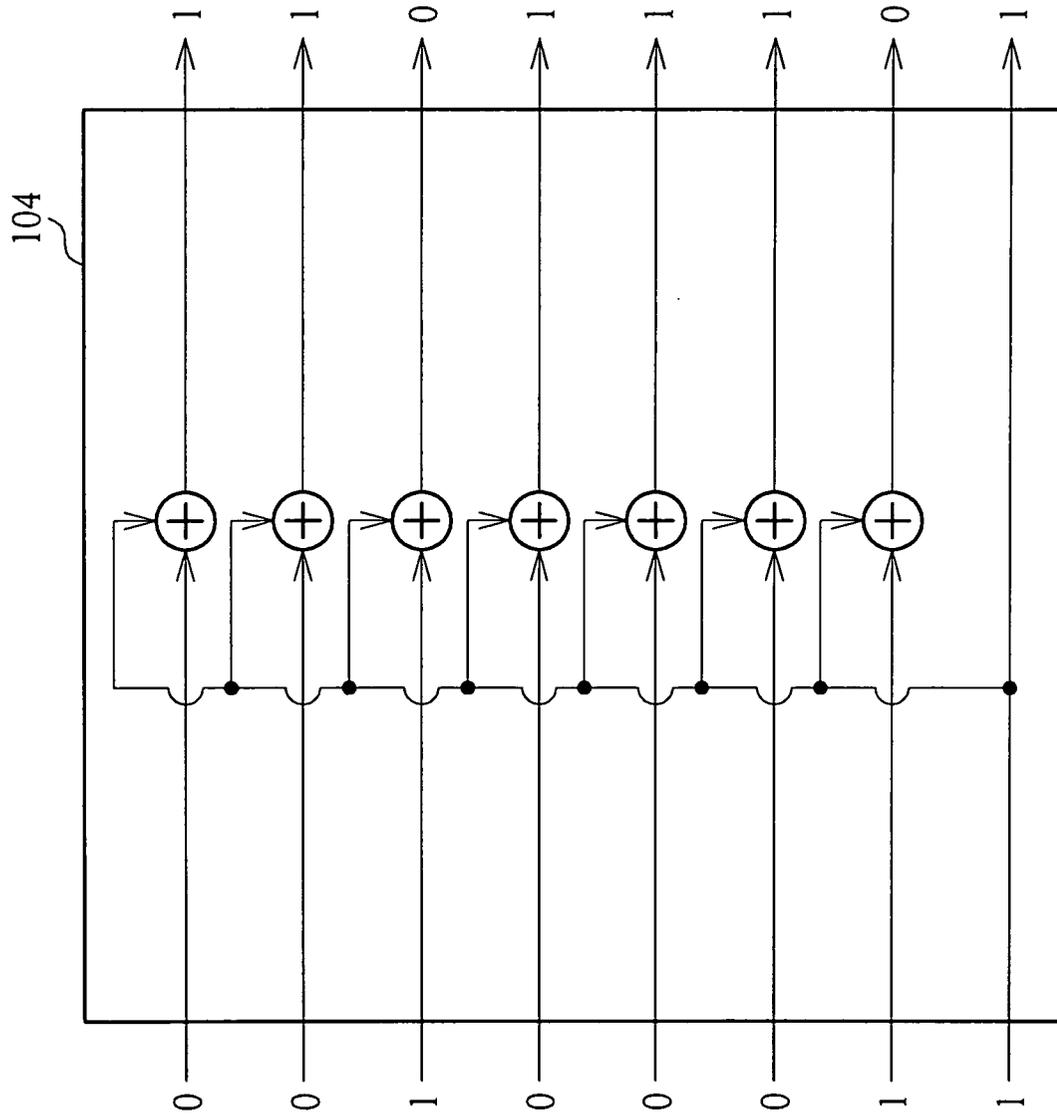
15. 如請求項 11 所述的方法，其中利用該第一雜亂值的至少一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生對應該第二雜亂值，是為利用該第一雜亂值的每一奇數位元對該奇數位元的下一位元執行該第一邏輯運算，以產生該第二雜亂值。
16. 如請求項 11 所述的方法，其中利用該第一雜亂值的至少一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生對應該第二雜亂值，是為利用該第一雜亂值的第一奇數位元對該第一雜亂值的其他奇數位元執行該第一邏輯運算以及利用該第一雜亂值的第一偶數位元對該第一雜亂值的其他偶數位元執行該第一邏輯運算，以產生該第二雜亂值。
17. 如請求項 11 所述的方法，其中利用該第一雜亂值的至少一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生對應該第二雜亂值包含：
利用該第一雜亂值的第一位元對該第一雜亂值的第二位元執行一第三邏輯運算，以產生一運算值；及
利用該運算值對該第一位元與該第二位元之外的其他位元執行該第一邏輯運算，以產生該第二雜亂值。

18. 如請求項 11 所述的方法，其中利用該第一雜亂值的至少一位元對該第一雜亂值的其他位元執行該第一邏輯運算，以產生對應該第二雜亂值包含：
- 利用該第一雜亂值的第一位元對該第一雜亂值的其他位元執行一第三邏輯運算，以產生一預雜亂值；及
- 利用該預雜亂值的每一奇數位元對該奇數位元的下一位元執行該第一邏輯運算，以產生該第二雜亂值。
19. 如請求項 17 或 18 所述的方法，其中該第三邏輯運算和該第一邏輯運算相同或不同。
20. 如請求項 14、15、16、17 或 18 所述的方法，其中該第一邏輯運算是為一互斥或邏輯運算。

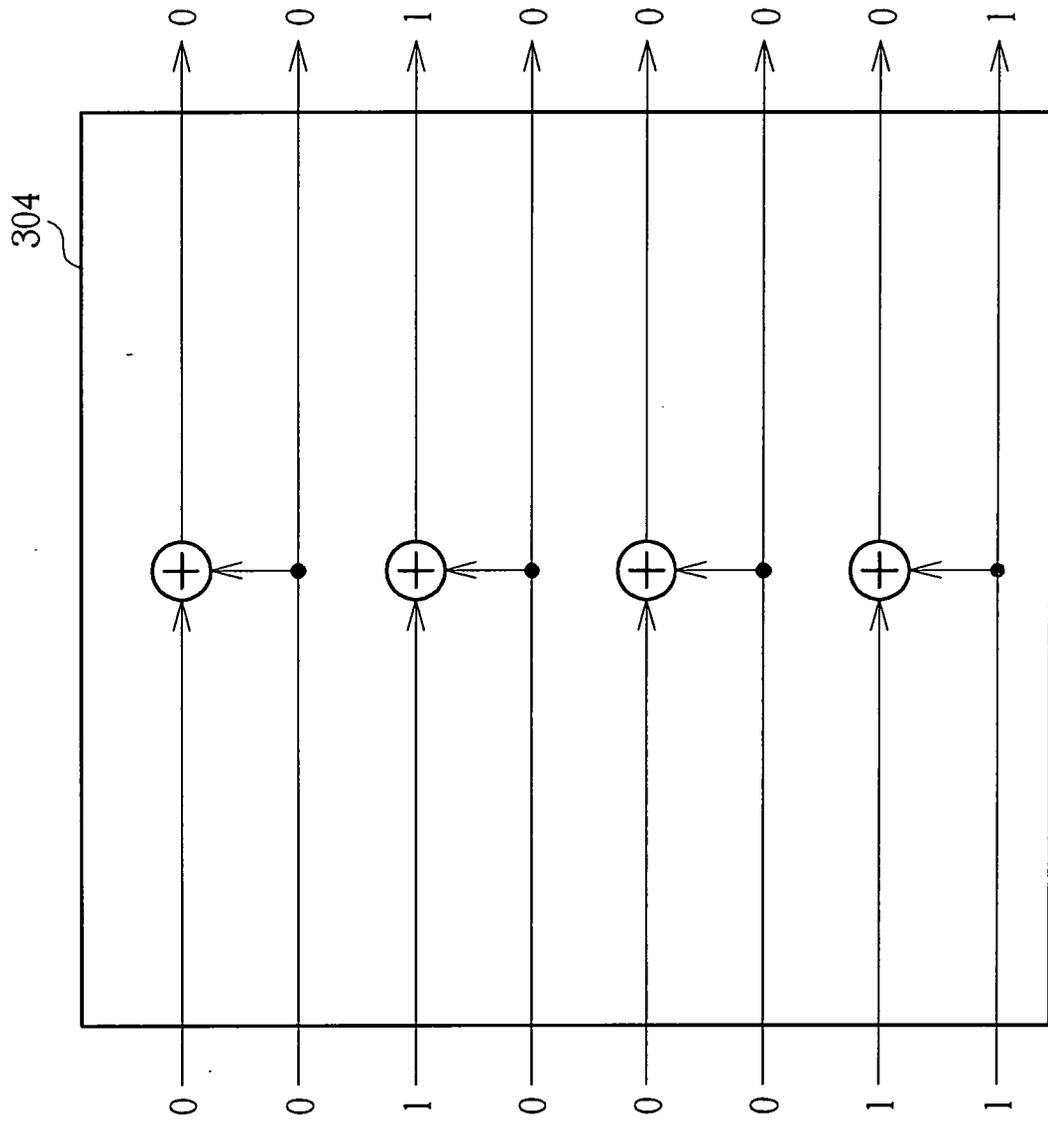
八、圖式：



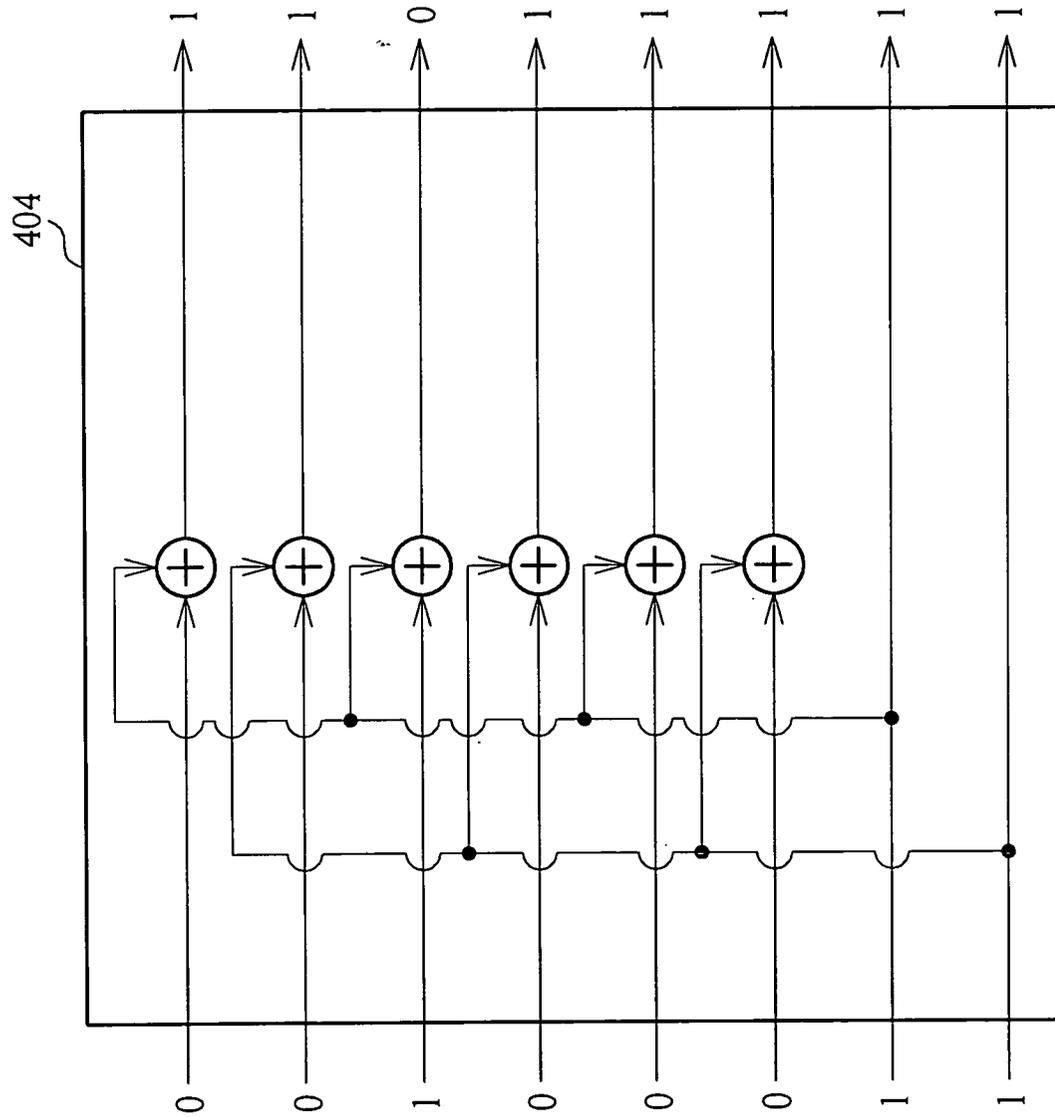
第1圖



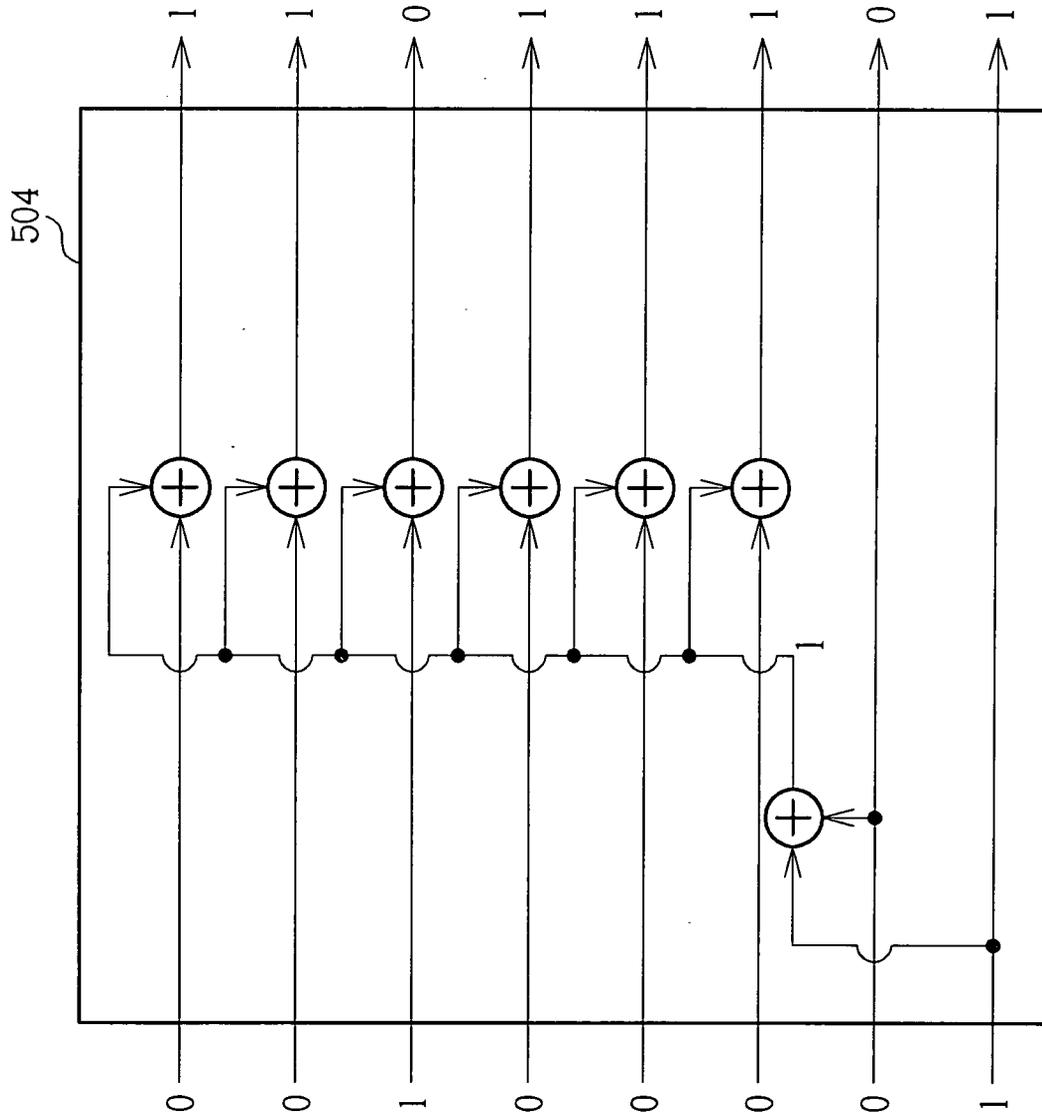
第2圖



第3圖

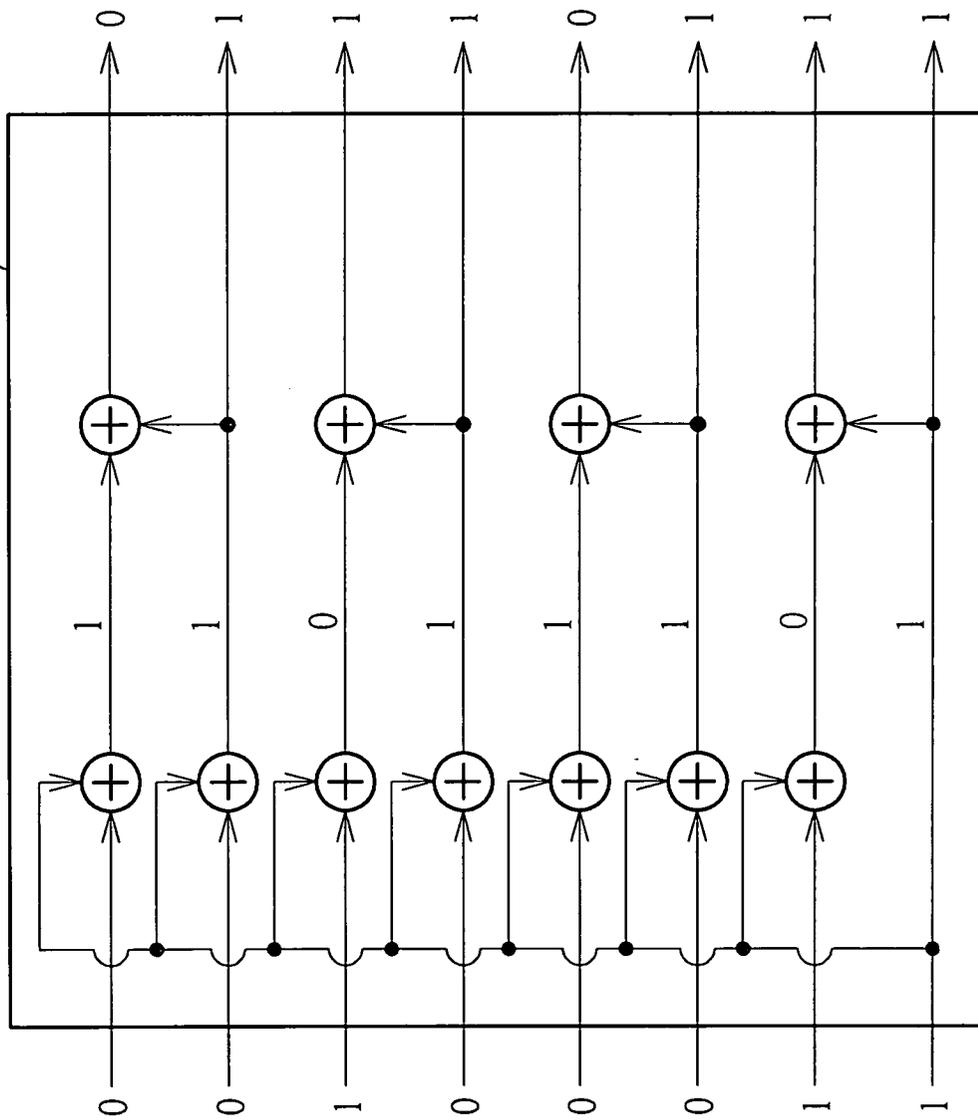


第4圖

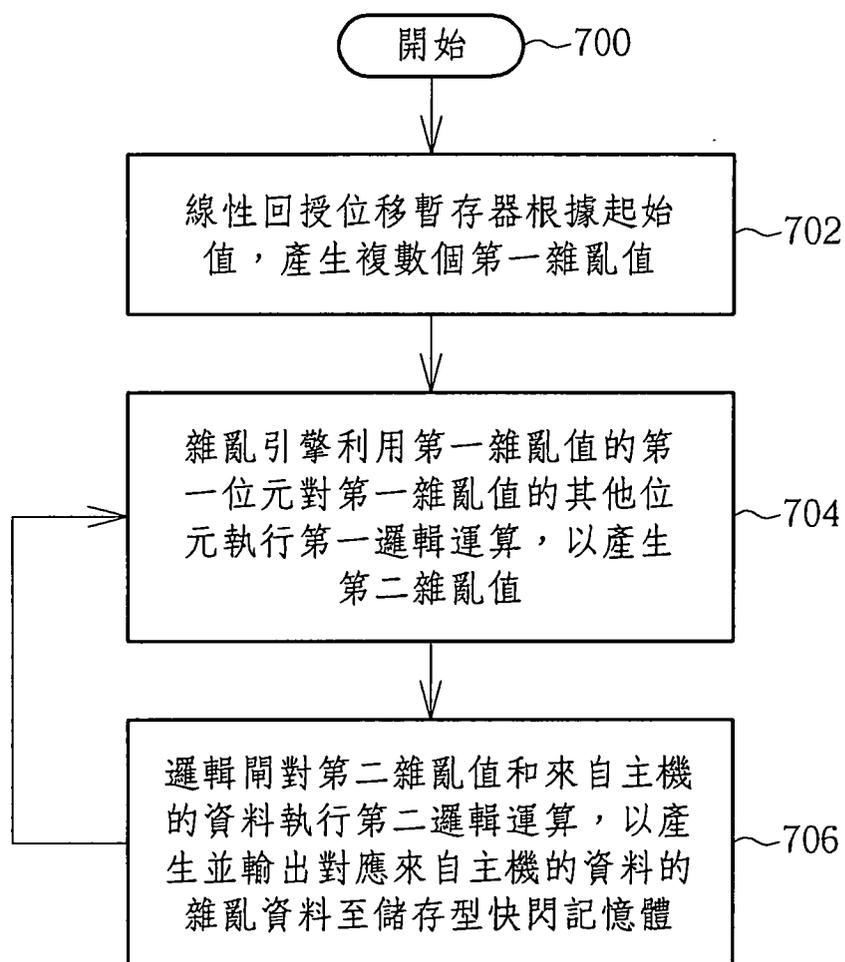


第5圖

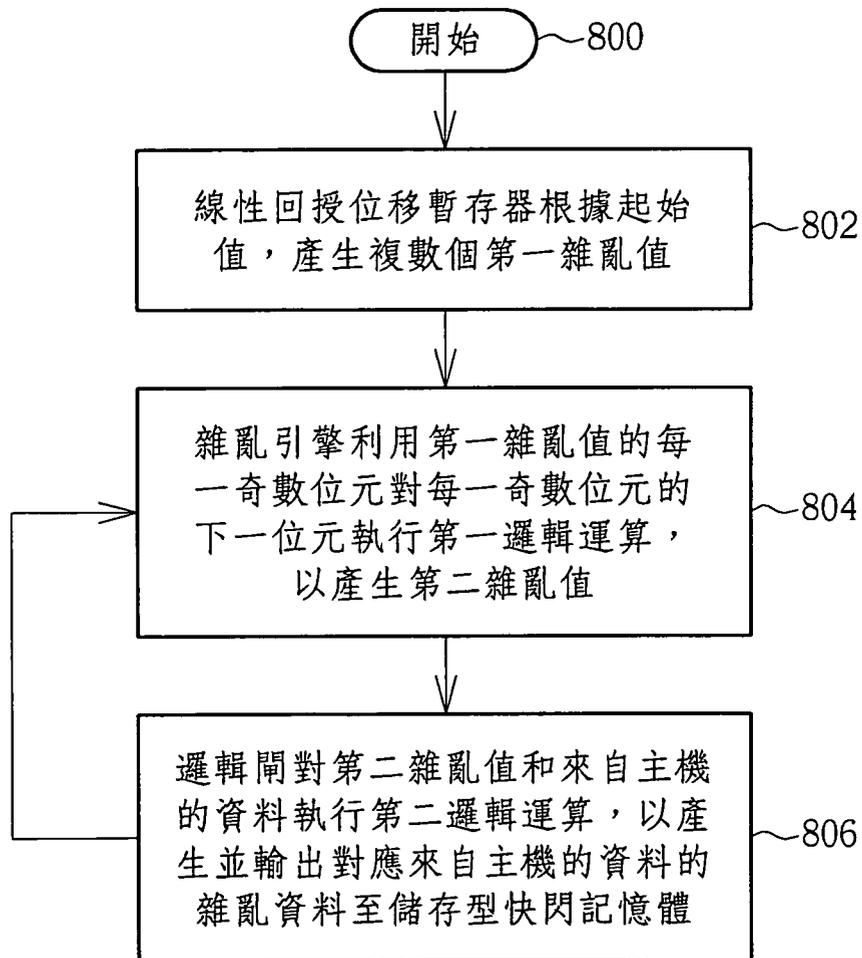
604



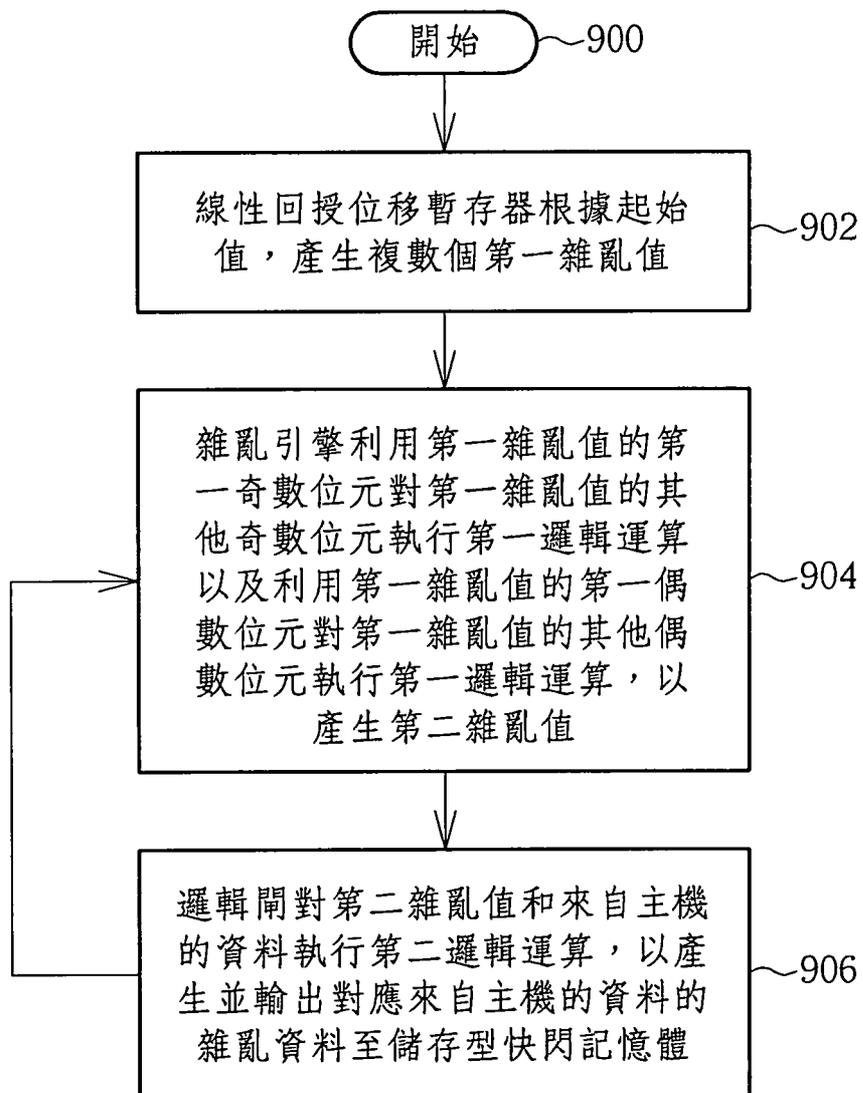
第6圖



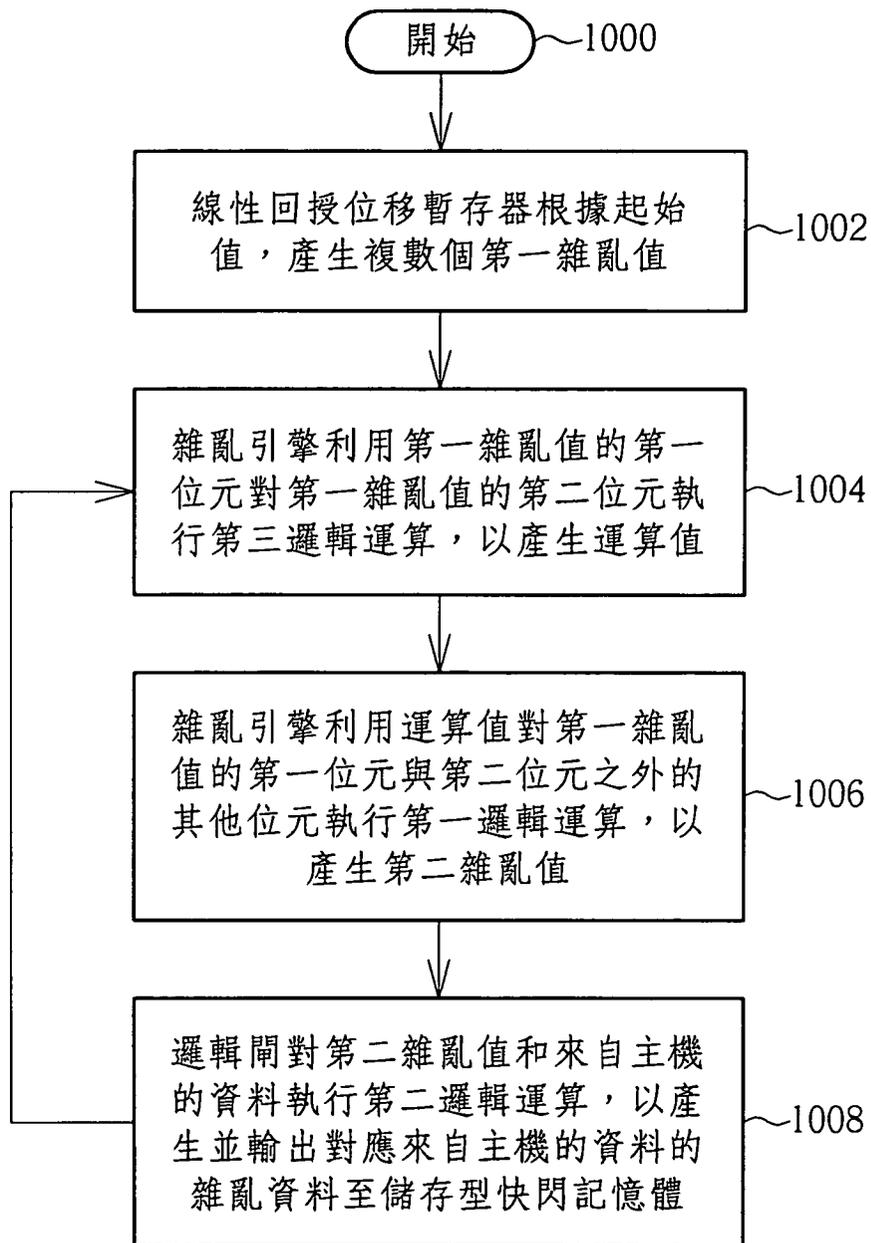
第7圖



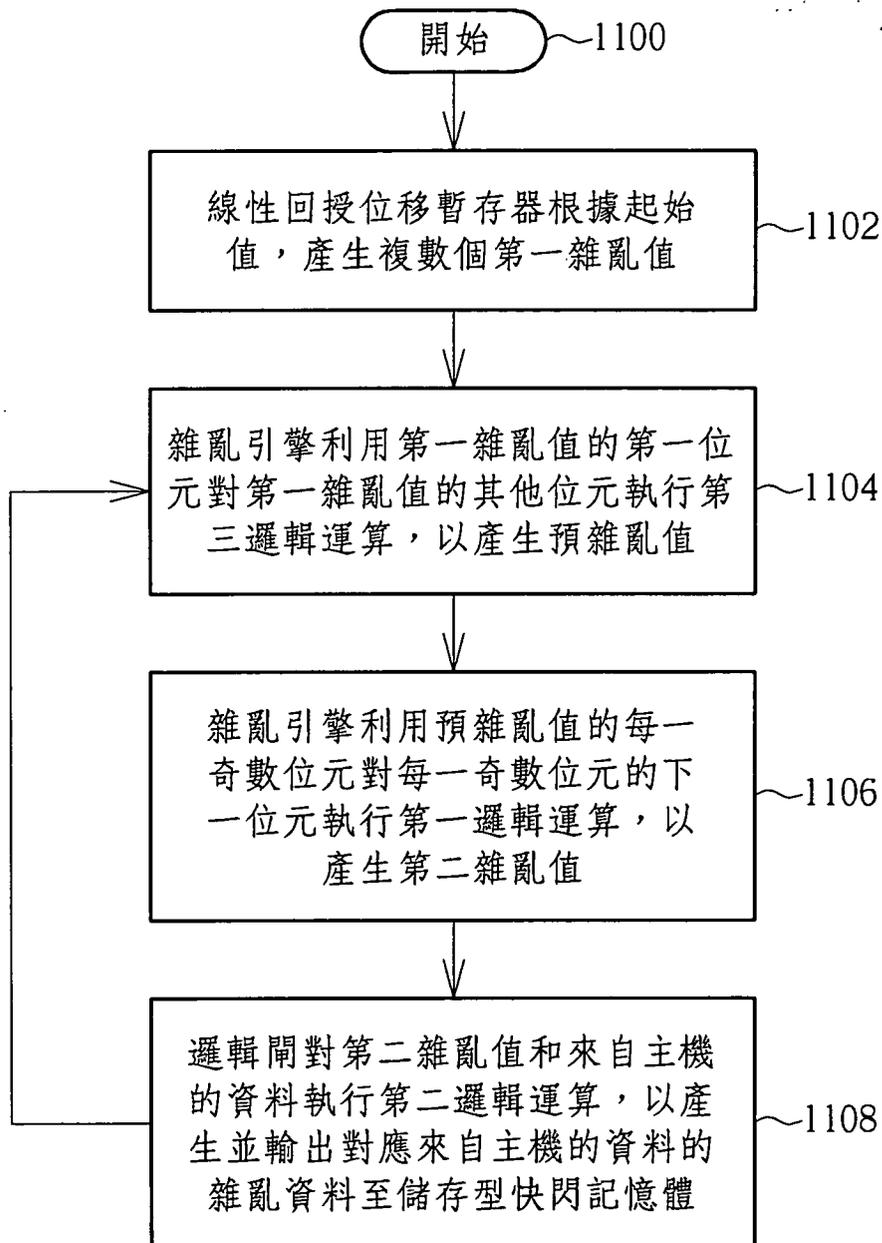
第8圖



第9圖



第10圖



第11圖