公告本

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：93141121

※ 申請日期：93-12-29　※IPC 分類：G06F 7/58 (2006.01)

一、發明名稱：（中文/英文）

複合多項式之亂數產生方法及其裝置

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

國立清華大學

代表人：（中文/英文）

徐遐生

住居所或營業所地址：（中文/英文）

(300)新竹市光復路二段１０１號

國　籍：（中文/英文）

中華民國

三、發明人：（共 3 人）

姓　名：（中文/英文）

1. 吳誠文 、2. 葉人傑 、3. 區弘勳

國　籍：（中文/英文）

1.~3. 中華民國

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：　年　月　日。

☐ 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：

☐ 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】

本發明是有關於一種亂數產生方法及其裝置(Random Number Generator)，特別是指一種使用複合多項式(Multiple Polynomial-based)之線性反饋位移暫存器技術的亂數產生方法及其裝置。

【先前技術】

目前一般加密/解密(Encryption/ Decryption)系統之傳送端在傳送一文件的過程中，常需要將該文件內容以一亂數產生器產生之亂碼重新編排使資料傳輸時其內容不致於外洩，因此如何產生無週期性之高隨機度(Random)的亂碼序列(Sequence)便顯得格外重要。常見的亂碼產生方法有使用例如熱雜訊(Thermal Noise)或相位/頻率之變動(Jitter)原理來產生一真實隨機序列(Truly Random Sequence)，或是利用線性反饋位移暫存器(Linear Feedback Shift Register；簡稱LFSR)、混沌模式(Chaos model)等原理來產生一虛擬亂數序列(Pseudo Random Sequence)。

如圖 1 所示，說明使用一線性反饋位移暫存器 6 的原理，其中，位移暫存器 6 可視同使用一單次多項式方程式，所使用公式如公式 1 所示：

$$x^{30}+x^5+x^4+x^2+x \qquad \text{公式 1}$$

首先，將一輸入樣本(Input Pattern)61 中填入一序列 b_0~b_{31}，並依公式 1 所示將序列的第 31、6、5、3、2 位元輸出給一 XOR 運算子 62 作 XOR 邏輯運算，最後 XOR 運

九、發明說明：

【發明所屬之技術領域】

本發明是有關於一種亂數產生方法及其裝置(Random Number Generator)，特別是指一種使用複合多項式(Multiple Polynomial-based)之線性反饋位移暫存器技術的亂數產生方法及其裝置。

【先前技術】

目前一般加密/解密(Encryption/ Decryption)系統之傳送端在傳送一文件的過程中，常需要將該文件內容以一亂數產生器產生之亂碼重新編排使資料傳輸時其內容不致於外洩，因此如何產生無週期性之高隨機度(Random)的亂碼序列(Sequence)便顯得格外重要。常見的亂碼產生方法有使用例如熱雜訊(Thermal Noise)或相位/頻率之變動(Jitter)原理來產生一真實隨機序列(Truly Random Sequence)，或是利用線性反饋位移暫存器(Linear Feedback Shift Register；簡稱LFSR)、混沌模式(Chaos model)等原理來產生一虛擬亂數序列(Pseudo Random Sequence)。

如圖 1 所示，說明使用一線性反饋位移暫存器 6 的原理，其中，位移暫存器 6 可視同使用一單次多項式方程式，所使用公式如公式 1 所示：

$$x^{30}+x^5+x^4+x^2+x \qquad \text{公式 1}$$

首先，將一輸入樣本(Input Pattern)61 中填入一序列 b_0~b_{31}，並依公式 1 所示將序列的第 31、6、5、3、2 位元輸出給一 XOR 運算子 62 作 XOR 邏輯運算，最後 XOR 運

算子 62 計算出一種子(Seed)位元 601，並將該種子位元 601 重新輸入至輸入樣本 61 序列中的最小位元(Least Significant Bit; LSB)b_0 以該種子位元 601 取代。如此循環地將各位元資料以串列(Serial)的方式作 XOR 邏輯運算，直到輸入樣本 61 的序列內容被加密/解密完成。

就使用 LFSR 之技術來產生亂數而言，現今共有三種實現方式：一、將單次多項式 LFSR 所產生之近似隨機之亂數結果輸出給複雜的數位電路，用來自我測試(Build-in Self Test)數位電路的輸出入結果是否符合設計需求。二、使用細胞陣列(Cell Array; CA)的方式實現 LFSR 電路，用以產生亂度較大的隨機亂數。三、使用類比式電路來實現 LFSR 電路，此種方式相較於前述二種方式可產生較大亂度的亂數，然而類比式電路具有不易設計的缺點。

綜上所述，目前的 LFSR 具有下述的缺點：

1. 由於單次多項式 LFSR 以串列的方式作 XOR 邏輯運算只能輸出一位元，導致輸出資料的轉換速率(Transmission Rate)低，無法應用在需要多位元輸出的高速系統之中。

2. 如圖 2 所示，由於單次多項式的硬體邏輯電路並不能任意更改，而在固定方程式的限制之下，使得亂數序列 7 將在一定週期內重複出現，因此其特性便容易被破解。

3. 使用細胞陣列或類比式電路來實現 LFSR 的方式，必須花費較大的硬體成本才能達到不易被破解之亂數需求，而且電路不易設計。

【發明內容】

因此，本發明之目的，即在提供一種使用複合多項式之LFSR技術的數位式亂數產生方法及其裝置。

於是，本發明複合多項式之亂數產生方法，係在一具有複數位移暫存器之亂數產生器內進行運算以輸出一亂數，該方法包含下述步驟：(A) 在該亂數產生器中建立一複合式查表電路，且該複合式查表電路內建有複數輸入多項式之對照表；(B)輸入一選擇訊號以選取該對照表中對應數目之一輸入多項式；及(C)配合步驟(B)所選取之該輸入多項式，在該等位移暫存器中進行線性反饋位移暫存之運算。

本發明亂數產生器包含一選擇單元、一複合式查表電路、一位移暫存電路及一邏輯閘電路，該選擇單元用以輸出一選擇訊號；該複合式查表電路耦接該選擇單元，且內建有一具有複數輸入多項式之對照表；該位移暫存電路具有複數位移暫存器，耦接該複合式查表電路；該邏輯閘電路耦接該等位移暫存器，在該邏輯閘電路中，是分別對各該位移暫存器之輸出作邏輯運算，並將運算得到之一種子序列回授至各該位移暫存器。

藉此，該複合式查表電路接收該選擇單元輸出之選擇訊號，可動態地選取該對照表之一輸入多項式，且該位移暫存電路可對應該所選取之該輸入多項式分別對各該位移暫存器所輸出之該種子序列作邏輯運算。

本發明複合多項式之亂數產生方法及其裝置可用於產生符合美國聯邦資訊處理標準(FIPS140-2)之亂數序列，若是外接例如 AMBA(Advanced Micro-controller Bus

Architecture)中的 AHB(Advanced High-performance Bus)標準 Arbiter 訊號，亦可由該外接之訊號改變其亂數產生規則，更可達到亂度之增加及不可預測性。

【實施方式】

有關本發明之前述及其他技術內容、特點與功效，在以下配合參考圖式之一較佳實施例的詳細說明中，將可清楚的呈現。

在說明本發明複合多項式之亂數產生方法之前，先將本發明亂數產生器 1 的作用說明如下：

如圖 3 所示，亂數產生器 1 具有一控制/分配電路 11、一複合式查表電路 12、一位移暫存電路(LFSR)13、一邏輯閘電路 14 及一選擇單元 15。其中，選擇單元 15 用以輸出一選擇訊號 150；複合式查表電路 12 內建有複數輸入多項式之對照表(Polynomial LUT)；位移暫存電路 13 用以執行位移暫存功能；邏輯閘電路 14 是對位移暫存電路 13 之輸出作邏輯運算，並將運算得到之一種子序列 141 回授至位移暫存電路 13。

其中，控制/分配電路 11 可輸入一時脈訊號(CLK)101、一重置(Reset)訊號 102 及一亂數輸出要求(Request)訊號 103。該等訊號之作用在於：時脈訊號 101 之每次脈衝是用以使位移暫存電路 13 之訊號往右移及對於序列之最小位元(LSB)進行補位；重置訊號 102 則是重新設定系統使其維持系統原先的預設狀態；亂數輸出要求訊號 103 則用以設定控制/分配電路 11 輸出端是否產生一亂數輸出訊號 104，當

亂數輸出訊號 104 輸出完成，則控制/分配電路 11 以輸出一狀態訊號 105 顯示完成亂數輸出訊號 104 之輸出。

而在選擇單元 15 共有三輸入訊號，分別是一多項式/種子值致能訊號 152(Load Polynomial & Seed)、一真實亂數源訊號(Truly Random Source; 以下簡稱 TRS)154 和一取消真實亂數源訊號(Disable Truly Random Source; 以下簡稱 DTRS)156，該等訊號之作用說明如下：

多項式/種子值致能訊號 152 的目的是讓選擇單元 15 按照訊號選取多項式，以及選取種子值(Seed)輸入至位移暫存電路 13。當使用者輸入亂數輸出要求訊號 103 至亂數產生器 1 時，若是第一次運算，種子序列 141 尚未有值(均為 0)之時，多項式/種子值致能訊號 152 會把系統預設的一初始種子值輸入至位移暫存電路 13 中。

TRS 訊號 154 致能時是表示選用一外部訊號產生源，本實施例是使用 AMBA 中的 AHB 標準 Arbiter 訊號，而 DTRS 訊號 156 之目的是取消以真實亂數源來當作決定多項式的因子；假設亂數產生器 1 是致能 TRS 訊號 154 作為決定多項式的因子時，TRS 訊號 154 便接到選擇訊號 150，並以該外部訊號產生源所提供之訊號隨機地選取多項式；若是 DTRS 訊號 156 致能的情況下，則隨機分配起始訊號 153 便接到選擇訊號 150，以亂數產生器 1 本身所產生之隨機亂數來選擇多項式(作用容後再述)。

如圖 4 所示，本實施例中，複合式查表電路 12 具有複數查表單元 121~125，位移暫存電路 13 具有位移暫存器

131~135，其中，在各查表單元 121~125 中各內建複數多項式之對照表(LUT)如表一所示：

表一

查表單元				
121	122	123	124	125
$x^7+x^3+x^2+x+1$	$x^7+x^5+x^3+x+1$	x^7+x^3+1	$x^7+x^5+x^4+x^3+1$	$x^7+x^5+x^4+x^3+x^2+x+1$
x^7+x+1	$x^7+x^5+x^4+x^3+x^2+x+1$	$x^7+x^6+x^5+x^4+1$	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	x^7+x^3+1
$x^7+x^5+x^3+x+1$	x^7+x^3+1	$x^7+x^5+x^4+x^3+1$	$x^7+x^3+x^2+x+1$	$x^7+x^3+x^2+x+1$
$x^7+x^5+x^4+x^3+x^2+x+1$	$x^7+x^6+x^5+x^4+1$	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	x^7+x+1	x^7+x+1
x^7+x^3+1	$x^7+x^5+x^4+x^3+1$	$x^7+x^3+x^2+x+1$	$x^7+x^5+x^3+x+1$	$x^7+x^5+x^3+x+1$
$x^7+x^6+x^5+x^4+1$	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	x^7+x+1	$x^7+x^5+x^4+x^3+x^2+x+1$	$x^7+x^6+x^5+x^4+1$
$x^7+x^5+x^4+x^3+1$	$x^7+x^3+x^2+x+1$	$x^7+x^5+x^3+x+1$	x^7+x^3+1	$x^7+x^5+x^4+x^3+1$
$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	x^7+x+1	$x^7+x^5+x^4+x^3+x^2+x+1$	$x^7+x^6+x^5+x^4+1$	$x^7+x^6+x^5+x^4+x^3+x^2+1$

本實施例中，該等位移暫存器 131~135 可為 D 型正反器(Flip-Flop)，各查表單元 121~125 係對應地連接各位移暫存器 131~135，而經過多次測試後，發現該等輸入多項式為 7 位元不可再分解之多項式(7-bit Primitive Polynomial)時，其所產生序列之亂度為最佳，且可通過 FIPS140-2 的測試標

準。因此，令各該位移暫存器 131~135 之位元數為 7，該等查表單元之數目為 M=5，總位元之輸出共為 M*N=35 位元，如此，可從總位元 M*N=35 之輸出中抽取出 k=3 位元作為隨機分配起始訊號 153 之來源；而各查表單元 121~125 中的輸入多項式數量為 2^k=8，因此，若是 DTRS 訊號 156 致能的情況下，則隨機分配起始訊號 153 便接到選擇訊號 150，k=3 位元之選擇訊號 150 可對應地選擇各查表單元 121~125 中 8 個不同多項式的任一輸入多項式。

此外，若判斷輸入至位移暫存器 131~135 之種子序列 s0~s4 其中有任一值為 0 時，則使用預設的初始種子值加入種子序列值為 0 的該位移暫存器 131~135 中，如此便可避免全 0 的種子值讓位移暫存電路 13 計算時落入死值(Dead Value)而無法使用；若判斷輸入至位移暫存器 131~135 之種子序列 s0~s4 中有值(不為 0)時，則是將新的種子序列 141 值輸入至位移暫存電路 13 中。

配合圖 3~5 所示，將本發明複合多項式之亂數產生方法說明如下：

步驟 301：在該亂數產生器 1 中建立如表 1 之該等輸入多項式於各查表單元 121~125 之中。

步驟 302：選擇單元 15 載入多項式/種子值致能訊號 152 以作為進行複合多項式之亂數計算處理及進行隨機分配種子訊號之判斷。

本實施例中，多項式/種子值致能訊號 152 是用以決定是否接收控制/分配電路 11 所分配之隨機起始訊號 153 作為

該選擇訊號 150，其分配方式便是在邏輯閘電路 14 先排除 3 位元，以該 3 位元作為隨機起始訊號 153 之輸出之後，再將排除 3 位元後的剩餘位元作為輸出結果 16。

步驟 303：由選擇單元 15 輸入選擇訊號 150 以選取複合式查表電路 12 中查表單元 121~125 中對應數目之一輸入多項式。

亦即，若是接收控制/分配電路 11 所分配之隨機分配起始訊號 153，則是輸入 k=3 位元之選擇訊號予各查表單元 121~125，例如：選擇訊號之輸入為 000，則為選取如表 1 所示的各查表單元 121~125 同一列位址為 000 之多項式：x7+x3+x2+x+1、x7+x5+x3+x+1、x7+x3+1、x7+x5+x4+x3+1 及 x7+ x5+ x4+x3+x2+x+1。

步驟 304：配合步驟 303 所選取之各輸入多項式，在該等位移暫存器 131~135 及邏輯閘電路 14 進行線性反饋位移暫存(LFSR)之運算。

本實施例之計算方式，主要是對各位移暫存器 131~135 的輸出結果 16 之字元 0~字元 4 進行 XOR 計算，為方便說明起見，將字元 0~字元 4 分別命名 w0、w1、w2、w3、w4，而在邏輯閘電路 14 中，是分別作 w0⊕w1、w1⊕w3、w2⊕w0、w3⊕w4、w4⊕w2 之邏輯運算(⊕表示 XOR 運算子)並分別得到種子序列 s0~s4，並將各種子序列 s0~s4 回授至各位移暫存器 131~135 以取代各位移暫存器 131~135 各序列的最小位元。

本實施例中，原本輸出結果 16 之位元數應為 5*7=35

位元，但是實際輸出僅取出 32 位元，主要是以該 3 位元作為選擇訊號 150 之來源，例如設定將輸出結果 16 之字元 2 的第 3 位元、字元 3 的第 2 位元，以及字元 4 的第 1 位元為選擇訊號 150，則排除上述 3 位元之輸出即為 32 位元之亂數輸出訊號 104。

如圖 6 所示，概括地說明了使用複數多項式可打破週期性重複的情況，由於本發明之亂數產生方法綜合了複數輸入多項式之設計，並可隨機地選取選取任一輸入多項式，因此可大幅提昇輸出結果之亂度，例如：狀態一~狀態八分別為多項式 1~8 所產生的亂數序列，由於可隨機選取多項式的結果，相較於單次方程式的將在一定週期內重複出現，隨機且動態地選取各輸入多項式的結果，打破了週期的限制，使得不可預測性將可增加。必須說明的是，圖 6 並未真實呈現系統實際的亂數產生結果，因為本發明產生之亂數序列的實際情況將更為複雜。

歸納上述，本發明之亂數產生方法及亂數產生器具有下述優點：

1. 本發明克服了目前單次多項式 LFSR 以串列的方式導致輸出資料的轉換速率過低的缺點，一次便可輸出多位元(32-bit)的亂數，可符合高速系統的需求。

2. 本發明綜合了多數輸入多項式之設計，並可隨機地選取選取任一輸入多項式，不似目前單次多項式的亂數序列容易被破解。

3. 本發明可以使用容易實現的數位式電路設計，有利

於保密系統、晶片測試系統及通訊系統中的任一種產業上之用途。

惟以上所述者，僅為本發明之較佳實施例而已，當不能以此限定本發明實施之範圍，即大凡依本發明申請專利範圍及發明說明內容所作之簡單的等效變化與修飾，皆仍屬本發明專利涵蓋之範圍內。

【圖式簡單說明】

圖 1 是一示意圖，說明使用單次多項式概念之線性反饋位移暫存器的原理；

圖 2 是一示意圖，說明固定方程式的限制之下，使得亂數序列將在一定週期內重複出現；

圖 3 是一電路方塊圖，說明本發明亂數產生器之一較佳實施例；

圖 4 是一電路方塊圖，說明該較佳實施例中，複合式查表電路、位移暫存電路及邏輯閘電路之連接關係；

圖 5 是一流程圖，說明本發明複合多項式之亂數產生方法；及

圖 6 是一示意圖，概略說明使用複合式多項式的情況，使得亂數序列不會在固定週期內重複出現。

【主要元件符號說明】

1 ……亂數產生器

101 ……時脈訊號

102 ……重置訊號

103 ……亂數輸出要求訊號

104 ……亂數輸出訊號

105 ……狀態訊號

11 ……控制/分配電路

12 ……複合式查表電路

121~125 查表單元

13 ……位移暫存電路

131~135 位移暫存器

14 ……邏輯閘電路

141 ……種子序列

15 ……選擇單元

150 ……選擇訊號

152 ……多項式/種子值致能訊號

153 ……隨機分配起始訊號

154 ……真實亂數源訊號

156 ……取消真實亂數源訊號

16 ……輸出結果

301~304 步驟

五、中文發明摘要：

一種複合多項式之亂數產生方法，係在一具有複數位移暫存器之亂數產生器內進行運算以輸出一亂數，該方法包含下述步驟：(A)在該亂數產生器中建立一複合式查表電路，且該複合式查表電路內建有複數輸入多項式之對照表；(B)輸入一選擇訊號以選取該對照表中對應數目之一輸入多項式；及(C)配合步驟(B)所選取之該輸入多項式，在該等位移暫存器中進行線性反饋位移暫存之運算。

六、英文發明摘要：

十、申請專利範圍：

1. 一種複合多項式之亂數產生方法，係在一具有複數位移暫存器之亂數產生器內進行運算以輸出一亂數，該方法包含下述步驟：

(A)在該亂數產生器中建立一複合式查表電路，且該複合式查表電路內建有複數輸入多項式之對照表；

(B)輸入一選擇訊號以選取該對照表中對應數目之一輸入多項式；及

(C)配合步驟(B)所選取之該輸入多項式，在該等位移暫存器中進行線性反饋位移暫存之運算。

2. 依據申請專利範圍第 1 項所述之亂數產生方法，其中，步驟(A)中，該複合式查表電路具有複數查表單元，且各該查表單元係對應地連接一位移暫存器，而該等位移暫存器之數目為 M，該等查表單元之數目為 N，總位元之輸出共為 M*N 位元，步驟(B)中，係從總位元 M*N 之輸出中抽取出 k 位元作為選擇訊號之來源。

3. 依據申請專利範圍第 1 項所述之亂數產生方法，其中，步驟(B)中，該選擇訊號之來源可為外接一符合 AMBA AHB 之 Arbiter 訊號。

4. 一種亂數產生器，包含：

一選擇單元，用以輸出一選擇訊號；

一複合式查表電路，耦接該選擇單元，且內建有一具有複數輸入多項式之對照表；

一位移暫存電路，具有複數位移暫存器，耦接該複

合式查表電路；及

一邏輯閘電路，耦接該等位移暫存器，在該邏輯閘電路中，是分別對各該位移暫存器之輸出作邏輯運算，並將運算得到之一種子序列回授至各該位移暫存器；

藉此，該複合式查表電路接收該選擇單元輸出之選擇訊號，可動態地選取該對照表之一輸入多項式，且該位移暫存電路可對應該所選取之該輸入多項式分別對各該位移暫存器所輸出之該種子序列作邏輯運算。

5. 依據申請專利範圍第 4 項所述之亂數產生器，其中，該複合式查表電路具有複數查表單元，且各該查表單元係對應地連接一位移暫存器，而該等位移暫存器之數目為 M，該等查表單元為 N 位元，總位元之輸出共為 M*N 位元，而從總位元之輸出中可抽取出 k 位元作為選擇訊號之來源。

6. 依據申請專利範圍第 5 項所述之亂數產生器，其中，各該查表單元中的輸入多項式數量為 2^k，該選擇訊號係 k 位元可對應地選擇各該查表單元中的任一輸入多項式。

7. 依據申請專利範圍第 4 項所述之亂數產生器，其中，該等輸入多項式係 7 位元不可再分解之多項式。

8. 依據申請專利範圍第 4 項所述之亂數產生器，可用於產生符合美國聯邦資訊處理標準(FIPS140-2)之亂數序列。

十一、圖式

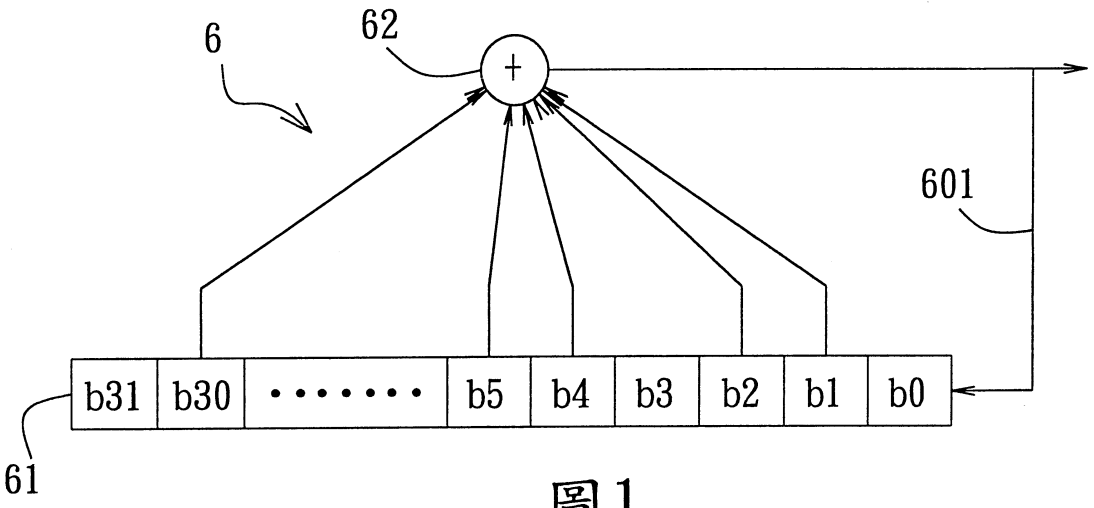

圖1

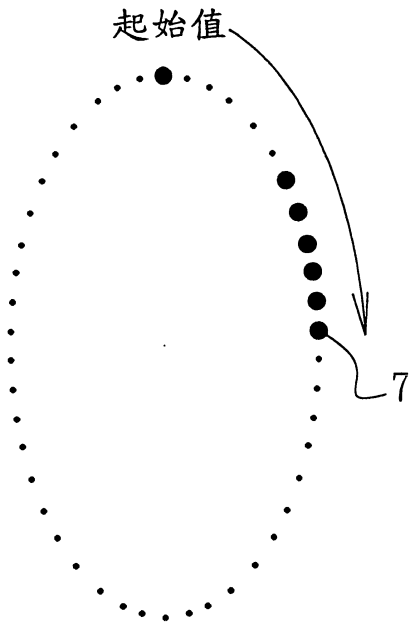

圖2

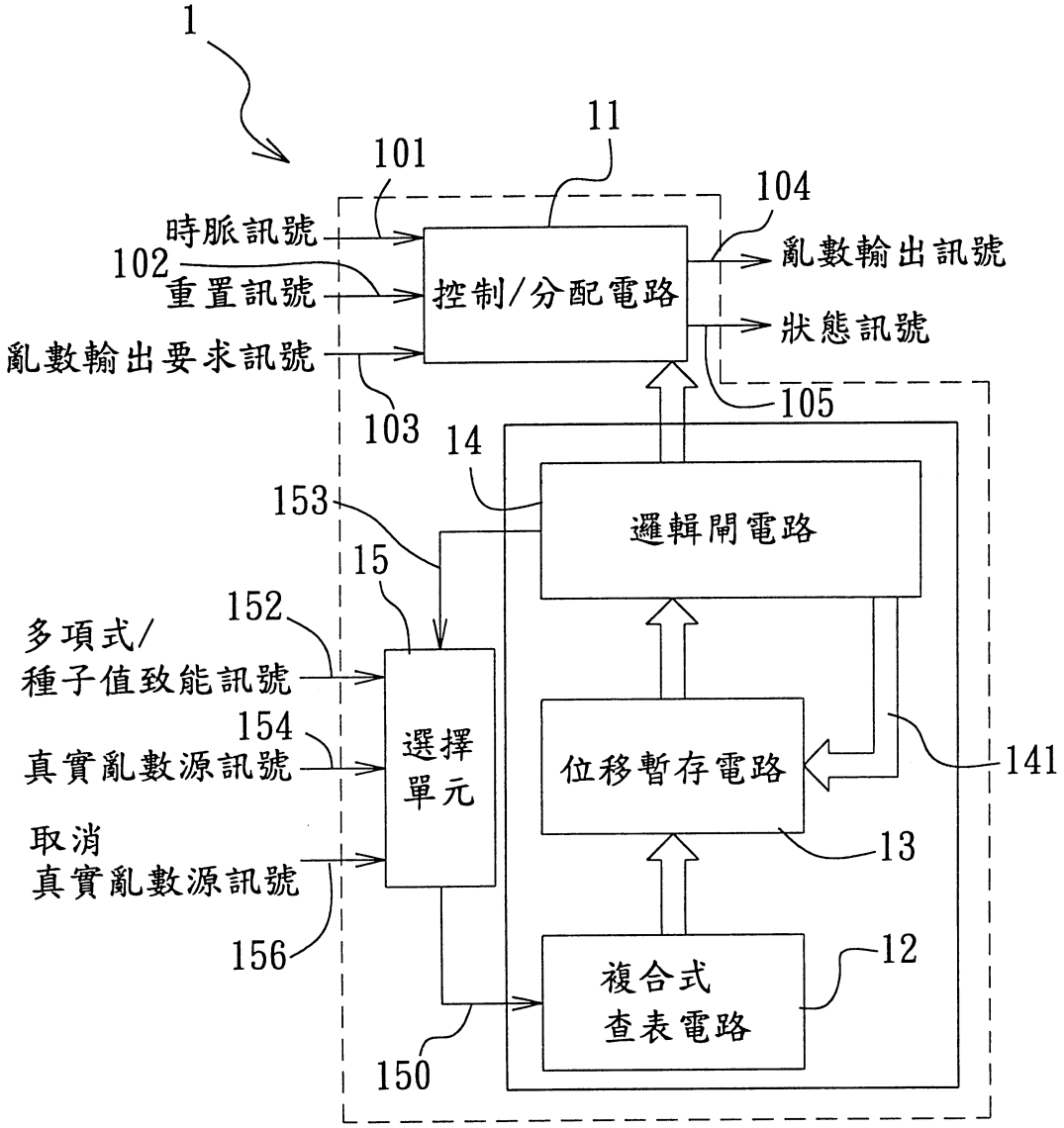
1
11
101
104
時脈訊號
102
重置訊號
控制/分配電路
亂數輸出訊號
狀態訊號
亂數輸出要求訊號
103
105
14
153
邏輯閘電路
15
152
多項式/
種子值致能訊號
154
真實亂數源訊號
選擇
單元
位移暫存電路
141
取消
真實亂數源訊號
13
156
12
複合式
查表電路
150

圖3

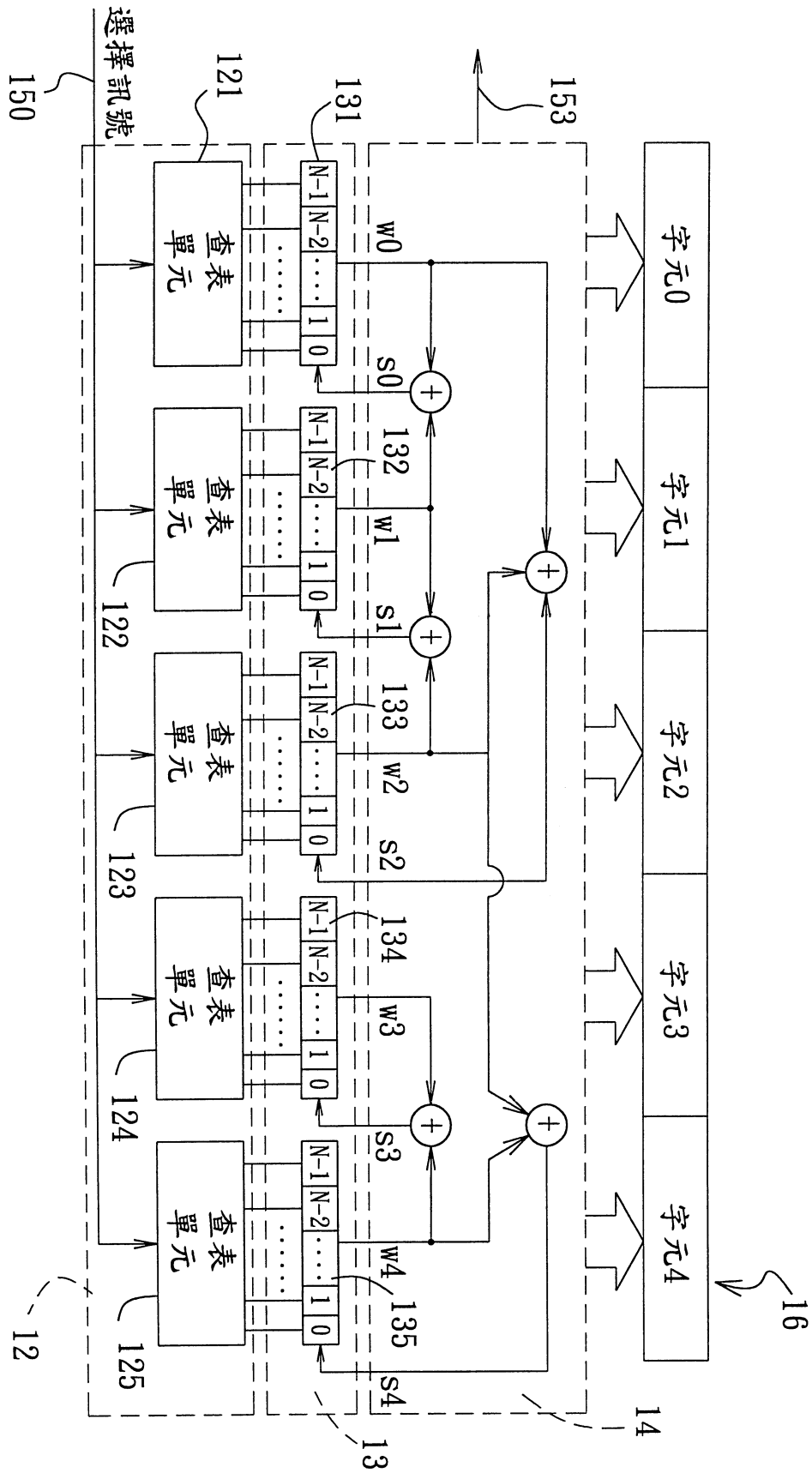
字元0
字元1
字元2
字元3
字元4
16
14
153
選擇訊號
150
121
131
查表單元
N-1
N-2
1
0
w0
s0
132
w1
s1
133
w2
s2
134
w3
s3
135
w4
s4
13
122
123
124
125
12

圖4

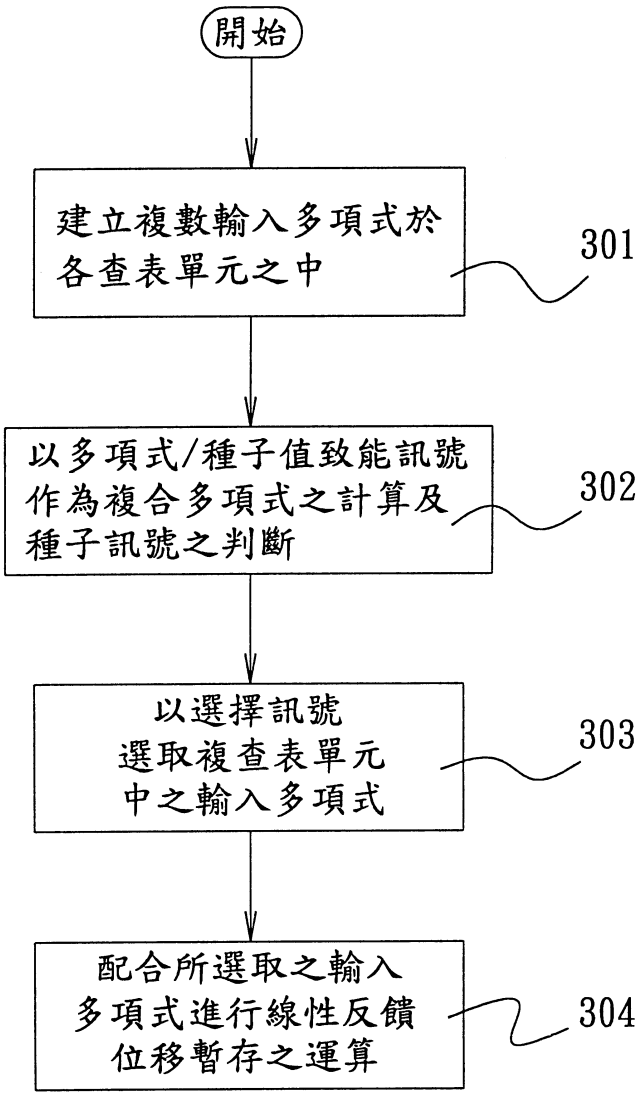
開始
建立複數輸入多項式於各查表單元之中
301
以多項式/種子值致能訊號作為複合多項式之計算及種子訊號之判斷
302
以選擇訊號選取複查表單元中之輸入多項式
303
配合所選取之輸入多項式進行線性反饋位移暫存之運算
304

圖5

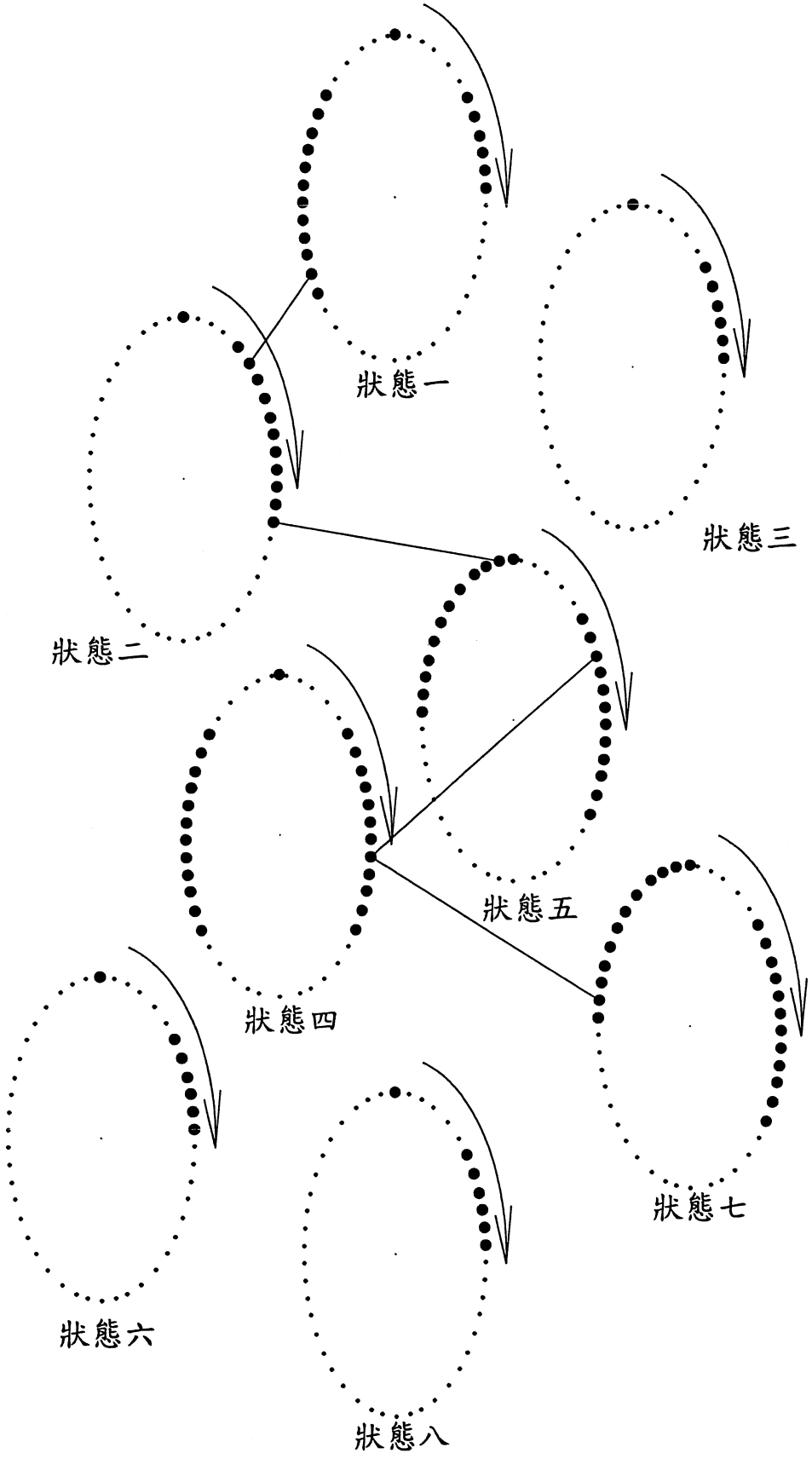

圖6

七、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明：

1 ……亂數產生器

101 ……時脈訊號

102 ……重置訊號

103 ……亂數輸出要求訊號

104 ……亂數輸出訊號

105 ……狀態訊號

11 ……控制/分配電路

12 ……複合式查表電路

13 ……位移暫存電路

14 ……邏輯閘電路

141 ……種子序列

15 ……選擇單元

150 ……選擇訊號

152 ……多項式/種子值致能訊號

153 ……隨機分配起始訊號

154 ……真實亂數源訊號

156 ……取消真實亂數源訊號

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：