【19】中華民國　　【12】專利公報　（U）

【11】證書號數：M574715
【45】公告日： 中華民國 108 (2019) 年 02 月 21 日
【51】Int. Cl.：　*G06F7/58 (2006.01)*　*G06F7/10 (2006.01)*
G06F7/483 (2006.01)　*G06F8/76 (2018.01)*
G06F9/22 (2006.01)

新型　　全 5 頁

【54】名　稱：　真亂數產生器裝置

【21】申請案號：　107215762　　【22】申請日： 中華民國 107 (2018) 年 11 月 20 日

【72】新型創作人：李易青 (TW) LI, YI-CING；萬培彥 (TW) WAN, PEI-YEN；廖德祿 (TW) LIAO, TEH-LU；顏錦柱 (TW) YAN, JUN-JUH
【71】申 請 人：　樹德科技大學　SHU-TE UNIVERSITY
高雄市燕巢區橫山路 59 號
【74】代 理 人：　葉大慧

(NOTE)備註：　相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

【57】申請專利範圍

1. 一種真亂數產生器裝置，所述真亂數產生器裝置以一微控制器為主要架構，該微控制器可產生一真亂數序列，該真亂數產生器裝置包括：一種子模組，具有一混合函數以及一混沌系統方程式，用以產生一第一擬隨機亂數序列；一運算模組，具有該混沌系統方程式，用以產生一第二擬隨機亂數序列；一處理模組，連接該種子模組以及該運算模組，具有該混合函數，將該種子模組以及該運算模組輸入之該第一擬隨機亂數序列以及該第二擬隨機亂數序列進行一動態調變，藉以得到該真亂數序列。
2. 如申請專利範圍第 1 項所述的真亂數產生器裝置，其中，該混沌系統方程式為 Henon map 混沌系統的差分動態方程，以及該第二擬隨機亂數序列為 Henon map 混沌系統 x_2之狀態序列。
3. 如申請專利範圍第 1 項所述的真亂數產生器裝置，其中，該動態調變使用一浮點數數位化的方式，進行放大及混勻輸入之隨機序列，其至少包括下列步驟：(a) 隨機選用一個質數 p, $p \in Z_q^*$; (b) 從中選擇質數 g, $g \in Z_q^*$; (c) 由一擬隨機亂數序列，經一浮點數數位化的方式，取得隨機動態正整數對 (r，x) ; (d) 計算金鑰 $y = g^x \bmod p$; (e) 由另一擬隨機亂數序列取得 S_R，進行調變後序列函數 $S_{RI} = S_R \cdot y^r \bmod p$。
4. 如申請專利範圍第 3 項所述的真亂數產生器裝置，其中，該浮點數數位化的方式為依照 IEEE754 格式，將取得浮點數拆分為 8Bytes，選用第六個 Bytes 作為 r 的來源，利用 r 的大小來對應 x 的範圍，使得 x 的範圍侷限在 $(1 \le x \le p-1)$。
5. 如申請專利範圍第 3 項所述的真亂數產生器裝置，其中，Z_p^*表示以質數 p 及 q 以 $g^i \bmod p$，$i = 1,2,\ldots,p$所形成之集合，所以 p,g的選擇為選擇一質數 p，再從 Z_p^*中選擇 $g \in Z_p^*$。
6. 如申請專利範圍第 1 項所述的真亂數產生器裝置，其中，該真亂數產生器裝置具有卡方測試 (Chi-square test) 測試合格。
7. 如申請專利範圍第 1 項所述的手持式膠帶裝置，其中，該真亂數產生器裝置具有美國國家標準與技術研究院 NIST 測試合格。

圖式簡單說明

圖 1 係本創作之真亂數產生器裝置之架構示意圖。 圖 2 係本創作之動態調變之步驟流程圖。 圖 3 係本創作之浮點數數位化之對應圖。 圖 4 係本創作之卡方測試之分類運算表。 圖 5 係本創作之 NIST 測試結果表。

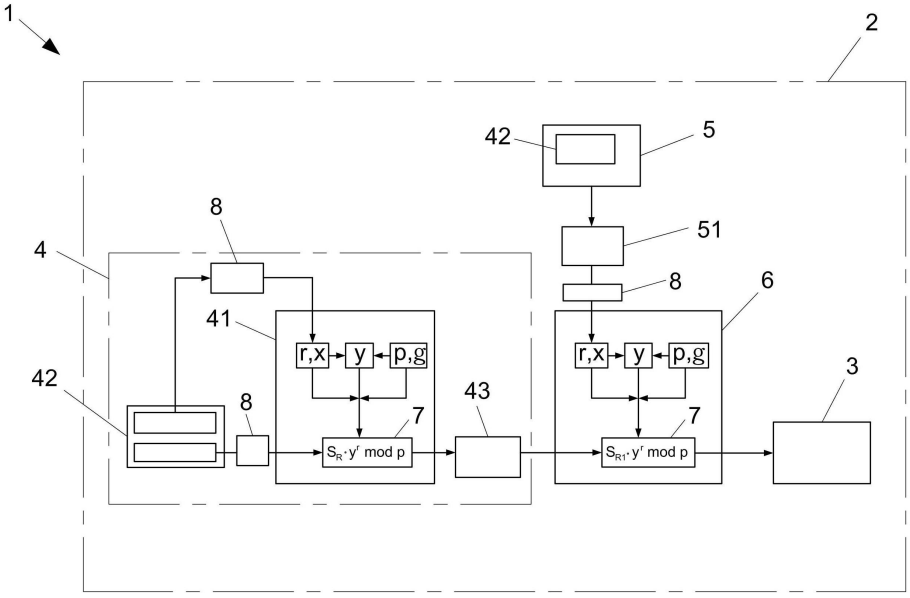

圖1

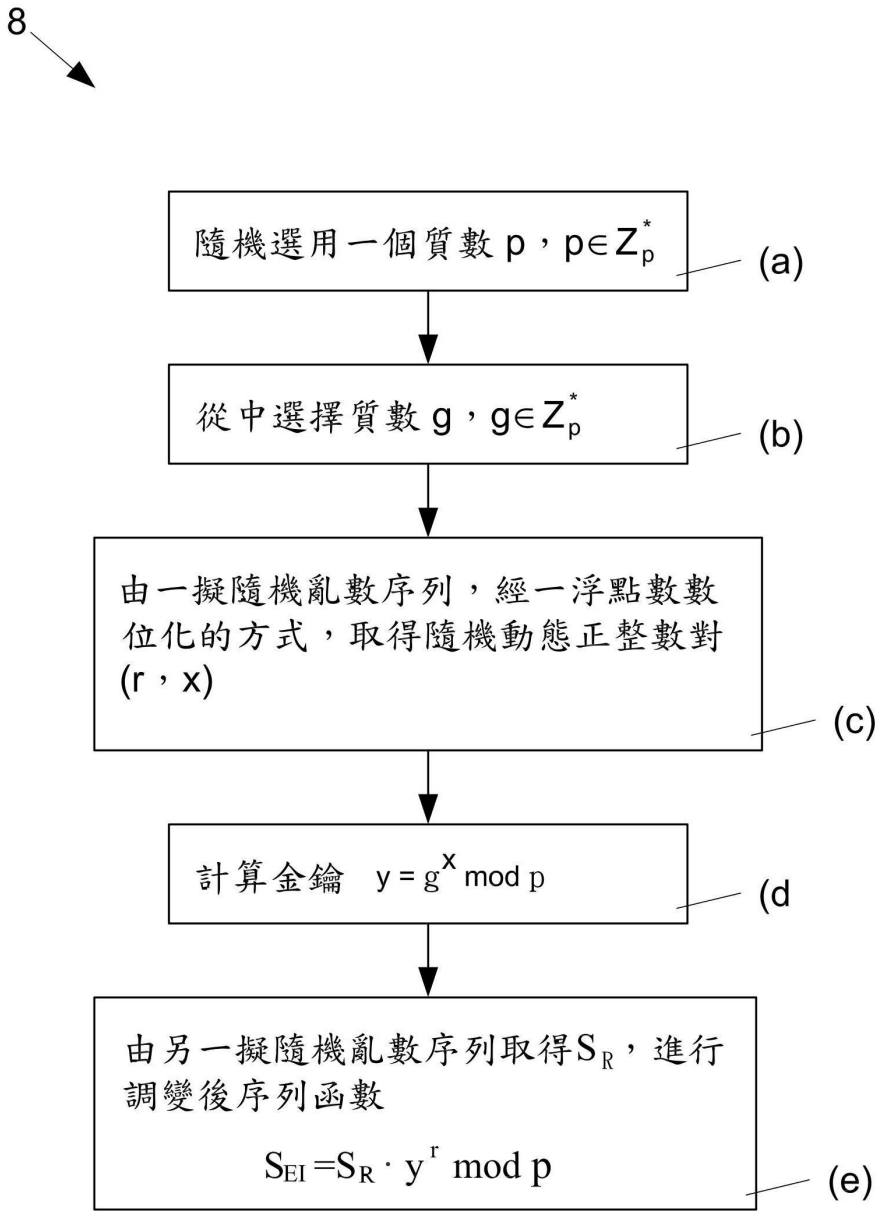
8
隨機選用一個質數 p，$p \in Z_p^*$
(a)
從中選擇質數 g，$g \in Z_p^*$
(b)
由一擬隨機亂數序列，經一浮點數數位化的方式，取得隨機動態正整數對 (r，x)
(c)
計算金鑰 $y = g^x \bmod p$
(d
由另一擬隨機亂數序列取得S_R，進行調變後序列函數
$S_{EI} = S_R \cdot y^r \bmod p$
(e)

圖2

(4)

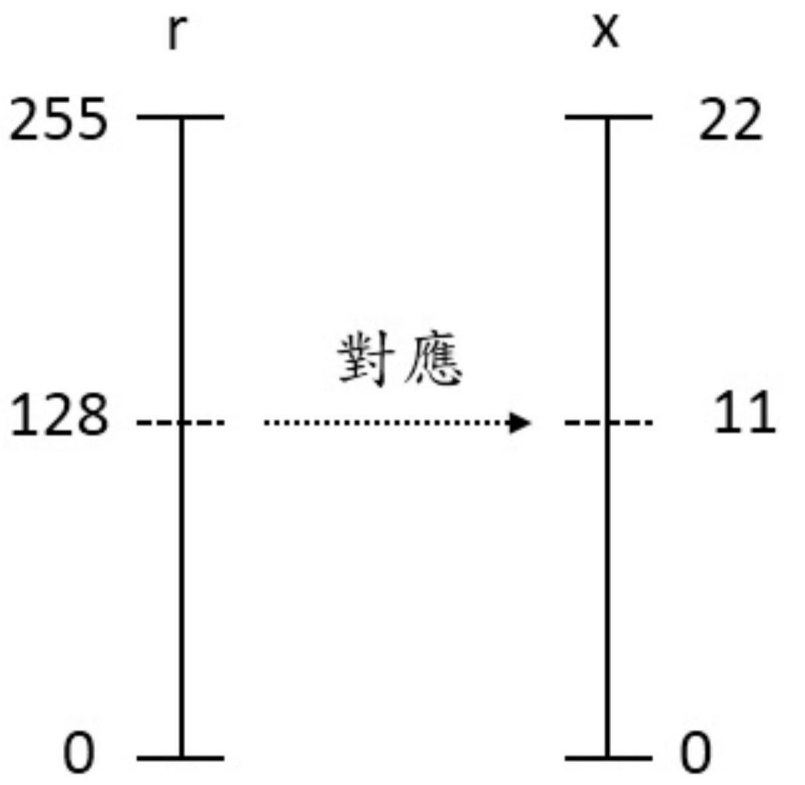

圖3

interval	O_i	E_i	O_i-E_i	$(O_i-E_i)^2$	$(O_i-E_i)^2/E_i$
間隔1　範圍(0,17]	7	6.666	0.334	0.111	0.016
間隔2　範圍(17,34]	6	6.666	-0.666	0.443	0.066
間隔3　範圍(34,51]	6	6.666	-0.666	0.443	0.066
間隔4　範圍(51,68]	9	6.666	2.334	5.447	0.817
間隔5　範圍(68,85]	6	6.666	-0.666	0.443	0.066
間隔6　範圍(85,102]	6	6.666	-0.666	0.443	0.066
間隔7　範圍(102,119]	7	6.666	0.334	0.111	0.016
間隔8　範圍(119,136]	7	6.666	0.334	0.111	0.016
間隔9　範圍(136,153]	6	6.666	-0.666	0.443	0.066
間隔10 範圍(153,170]	7	6.666	0.334	0.111	0.016
間隔11 範圍(170,187]	6	6.666	-0.666	0.443	0.066
間隔12 範圍(187,204]	6	6.666	-0.666	0.443	0.066
間隔13 範圍(204,221]	6	6.666	-0.666	0.443	0.066
間隔14 範圍(221,238]	9	6.666	2.334	5.447	0.817
間隔15 範圍(238,256]	6	6.666	-0.666	0.443	0.066

圖4

TRN		
test	P-value	是否通過測試
frequency	0.739918	Pass
BlockFrequency	0.739918	Pass
CumulativeSums	0.739918	Pass
Runs	0.350485	Pass
LongestRun	0.739918	Pass
Rank	0.213309	Pass
FFT	0.739918	Pass
NonOverlappingTemplate	0.911413	Pass
OverlappingTemplate	0.999271	Pass
Universal	0.534146	Pass
ApproximateEntropy	0.887706	Pass
RandomExcursions	0.993519	Pass
RandomExcursionsVariant	0.213309	Pass
Serial	0.534146	Pass
LinearComplexity	0.739918	Pass

圖5