I639948

(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 I639948 B**

(45)公告日： 中華民國 107 (2018) 年 11 月 01 日

(21)申請案號：103139795 (22)申請日： 中華民國 103 (2014) 年 11 月 17 日

(51)Int. Cl.： *G06F7/58 (2006.01)*

(30)優先權：2013/11/29 美國 14/093,040

(71)申請人：密西根大學董事會 (美國) THE REGENTS OF THE UNIVERSITY OF MICHIGAN (US)

美國

(72)發明人：楊開原 YANG, KAIYUAN (CN) ；西爾維斯特丹尼斯麥可 SYLVESTER, DENNIS MICHAEL (US) ；布洛烏大衛西歐朵爾 BLAAUW, DAVID THEODORE (US) ；菲克大衛艾倫 FICK, DAVID ALAN (US) ；亨利麥可 B HENRY, MICHAEL B. (US) ；李允銘 LEE, YOONMYUNG (KR)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

TW	200400463A	TW	200408922A
DE	102008048292B3	US	8346832B2
US	8410857B2	US	2008/0091755A1

審查人員：李國福

申請專利範圍項數：20 項 圖式數：14 共 40 頁

(54)名稱

產生真實亂數之方法與真實亂數產生器

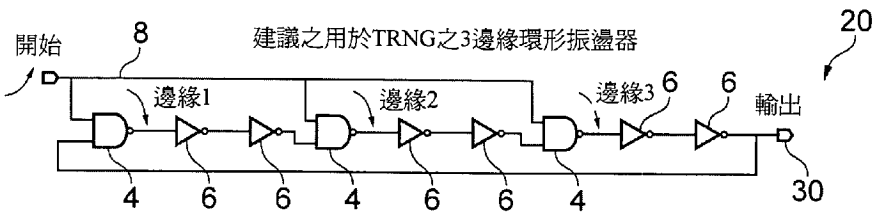
METHOD OF GENERATING TRUE RANDOM NUMBER AND TRUE RANDOM NUMBER GENERATOR

(57)摘要

一種真實亂數產生器包含環形振盪器，該環形振盪器經觸發以在振盪開始時間在第一振盪模式中開始振盪。視熱雜訊而定，第一振盪模式最終將崩潰至第二振盪模式。量測從振盪開始時間至振盪器崩潰至第二模式的時間之崩潰時間，且此崩潰時間可用於決定一亂數。TRNG 可使用標準數位技術完全合成，且該 TRNG 能夠提供高隨機性、良好的產量及能量效率。

A true random number generator comprises a ring oscillator which is triggered to start oscillating in a first mode of oscillation at an oscillation start time. The first mode of oscillation will eventually collapse to a second mode of oscillation dependent on thermal noise. A collapse time from the oscillation start time to the time at which the oscillator collapses to the second mode is measured, and this can be used to determine a random number. The TRNG can be synthesized entirely using standard digital techniques and is able to provide high randomness, good throughput and energy efficiency.

指定代表圖：



第2圖

符號簡單說明：

4・・・輸入反向級

6・・・反向級

8・・・開始信號

20・・・環形振盪器

30・・・輸出節點

以除去偏壓。SiN MOSFET 利用較大的熱雜訊，但是要求後處理以達成充分的隨機性。基於氧化物分解之 TRNG 顯示高熵值，但遭受低效能及高能/位元。基於環形振盪器(Ring oscillator; RO)之 TRNG 提供設計簡化之優點，但是使用慢速抖動時鐘取樣快速時鐘之上述方法提供低隨機性且易受電源攻擊。此外，大多數上述方法不能通過國家標準技術局(National Institute of Standards and Technology; NIST)之所有的隨機性測試。

【0004】 本技術力圖提供可同時達成簡化設計、高隨機性、良好產量、良好能效及抗攻擊性的 TRNG。

【發明內容】

【0005】 自一個態樣可見，本技術提供真實亂數產生器(TRNG)，該真實亂數產生器包含：

環形振盪器；

控制電路，該控制電路經設置以觸發環形振盪器，以在振盪開始時間在第一振盪模式中開始振盪；以及

時間量測電路，該時間量測電路經設置以量測崩潰時間值，該崩潰時間值指示從振盪開始時間至振盪崩潰時間之時間長度，在該振盪崩潰時間，環形振盪器從第一振盪模式切換至第二振盪模式。

【0006】 本技術提供可在第一振盪模式與第二振盪模式中振盪之環形振盪器。第一振盪模式可能不穩定，且因此經過一段時間後，環形振盪器可能崩潰至第二振盪模式。從第一振盪模式崩潰至第二振盪模式所用的時間長度可能取決於熱雜

訊，且因此，藉由量測崩潰時間值（該時間值指示從第一振盪模式中振盪開始至崩潰至第二振盪模式之時間長度），崩潰時間值可用於導出真實亂數。此與習知的基於環形振盪器之 TRNG 形成對比，該環形振盪器使用單模振盪內的抖動作爲隨機性源，而不是從一種振盪模式崩潰至另一種振盪模式。與上述方法不同，根據本技術之 TRNG 完全可使用標準數位合成技術（例如使用標準單元庫及習知的置放及選路工具）合成，同時仍可提供高度隨機性，使得該 TRNG 建構時更經濟且更簡單。此外，產量（每秒產生之隨機位元數）、能效（每產生之隨機位元的能耗）及電路區域相對於上述技術得以改良。

【0007】 在一個實例中，在第一振盪模式中，環形振盪器可在高於第二振盪模式中之頻率下振盪。隨後，從環形振盪器之輸出頻率的減少可偵測第二振盪模式之崩潰。

【0008】 例如，在第一振盪模式中，環形振盪器可傳播環形振盪器周圍之多個邊緣，各邊緣之間具有相位差。例如，環形振盪器可具有多個級，多個輸入節點位於環形振盪器之不同級處。控制電路可將開始信號供給至多個輸入節點，且回應於開始信號，各輸入節點可將各別邊緣注入環形振盪器中。隨後各邊緣將以與單邊緣環形振盪器相同之方式圍繞該環傳播。各邊緣具有與單邊緣振盪器相同之週期，但是邊緣相對於彼此經相移，且在給定輸出點的整體頻率較高。各邊緣將隨時間獨立地積累來自熱雜訊之抖動，引起各自具有完整週期之兩個相鄰邊緣之間的脈寬之遞增變化。最後，兩個

相鄰邊緣將緊密結合在一起，以致彼等邊緣崩潰及相互抵消，使得剩餘一或更多個其他邊緣。此時，因爲當前第二振盪模式中的邊緣少於第一振盪模式中的邊緣，所以環形振盪器之頻率下降。自第一模式中開始振盪至崩潰至第二模式所用的時間反映各邊緣處抖動的積累，且可因此將該時間用作亂數產生之熵源。又，崩潰時間將獨立於環形振盪器的任何過程變化，因爲各邊緣通過同一環形振盪器之級，使各級之切換時間中的任何失配變得均衡。

【0009】 一般而言，第二振盪模式比第一模式具有更少的圍繞環形振盪器傳播之邊緣。然而，當第二振盪模式僅傳播單邊緣時，偵測崩潰可爲最簡單。

【0010】 第一振盪模式可傳播任何數目之邊緣。然而，可較佳地提供一種振盪模式，在該振盪模式中，大於一個的奇數個邊緣圍繞環形振盪器傳播。在偶數個邊緣的情況下，第一振盪模式對過程變化更敏感，因爲環形振盪器之給定級將僅作用於脈衝之上升邊緣或下降邊緣，如此可能降低崩潰時間的隨機性。藉由使用奇數個邊緣，可消除此過程變化，因爲環形振盪器之各級將作用於上升及下降邊緣兩者。儘管已發現具有三個邊緣之振盪模式係足夠的，但是第一振盪模式中可使用任何奇數數目之邊緣。在此實例中，環形振盪器可具備用於回應於開始信號注入該等個別邊緣之三個輸入節點，且隨後此等邊緣之兩個邊緣可隨時間緊密結合在一起且相互抵消，使得第三個邊緣作爲在該第二振盪模式中振盪之單邊緣。

【0011】 在第一模式中開始振盪時，有可能將具有不同相位差之邊緣注入每一連續對之相鄰邊緣之間。因此，與各邊緣有關之輸入節點不必均勻地分散在環的周圍。然而，可較佳地在第一振盪模式開始時提供具有相等的相位差之邊緣，因爲如此可能增加隨機性量。當初始邊緣平均同相分佈時，則將無法預期哪一對邊緣將一起首先崩潰且該崩潰取決於熱雜訊，且因此該整體隨機性將取決於每一邊緣所經歷之熱雜訊。相反，若一些邊緣比其他邊緣更緊密地、同相地接合在一起，則開始更緊密接合在一起的邊緣更可能爲一起崩潰的邊緣，且因此隨機性將受到此等邊緣中之抖動的影響多於其他邊緣中之抖動的影響。因此，可較佳地在環周圍均勻分佈之點處注入邊緣。

【0012】 在一些實施例中，開始信號包含脈衝，該脈衝具有重置該環形振盪器之第一邊緣；及第二邊緣，該第二邊緣觸發環形振盪器以起動第一振盪模式中的振盪。

【0013】 可以多種方式實施用於量測崩潰時間值之時間量測電路。例如，時間量測電路可具有週期計數器，該週期計數器維持週期計數值，該週期計數值指示自振盪開始時間已經過的週期次數。崩潰偵測器可回應於偵測環形振盪器從第一模式切換至第二振盪模式而輸出崩潰信號。藉由從週期計數器俘獲週期計數值之當前值，俘獲電路可回應於來自崩潰偵測器之崩潰信號。因此，俘獲值將指示崩潰至第二振盪模式所用的週期次數，且此次數可經輸出及用於導出真實亂數。

【0014】 儘管通常週期計數器可使用任何參考時鐘計算週期

次數，計算環形振盪器自身之振盪週期對於週期計數器而言可能係有利的。首先，此舉減少了用於提供計數參考時鐘之另外振盪器之需要。又，因爲第一模式中之環形振盪器之頻率可能高於第二模中的頻率，當環形振盪器崩潰至第二模式時，連續週期之間的時間段將增加，且因此存在用於俘獲電路（例如鎖存電路）之更多時間，以在週期計數回應於環形振盪器之另一週期而再次增加之前俘獲週期計數之當前值。

【0015】 在一個實例中，崩潰偵測器可包含相位頻率偵測器(PFD)，該相位頻率偵測器基於環形振盪器之輸出與參考環形振盪器之輸出的相位比較產生崩潰信號，該參考環形振盪器在預定頻率處振盪。其中該環形振盪器之第一振盪模式具有第一頻率，該第一頻率大於第二振盪模式之第二頻率，參考環形振盪器可經設置以便預定頻率在第一與第二頻率之間。因此，當環形振盪器在第一振盪模式中時，該環形振盪器將比參考環形振盪器振盪的更快；而當該環形振盪器在第二振盪模式中時，該環形振盪器將比參考環形振盪器振盪的更慢。相位頻率偵測器可輸出指示兩個振盪器之相對頻率的信號，且此信號可用於決定該環形振盪器何時已崩潰至第二振盪模式。

【0016】 此可用於提供故障移除電路，以過濾掉由崩潰偵測器產生之崩潰信號中的故障。例如，當使用相位頻率偵測器時，即使環形振盪器之振盪模式無變化，在崩潰信號返回崩潰信號之上述值之前短期改變值時可能會出現奇怪的故障。故障移除電路可過濾掉此等短期故障，以便在崩潰信號狀態

中存在更長期的變化時僅偵測崩潰。例如，故障移除電路可包含 AND 閘極，該 AND 閘極在輸入崩潰信號及該崩潰信號之延遲版本時接收。此舉確保若崩潰信號將狀態改變較短時段（短於通過延遲緩衝器/反相器之延遲），則此故障不會引起崩潰偵測。

【0017】 除故障移除電路之外或替代故障移除電路，可在時間量測電路中提供移位暫存器，用於增加對崩潰偵測的信任。移位暫存器可具有數個移位級，各移位級接收各時脈週期中之先前級的輸出。可在移位暫存器之第一級輸入崩潰信號，且隨後可將移位暫存器之最終級的輸出發送至俘獲元件。此舉有效地延遲了崩潰信號，以便俘獲元件在比實際產生崩潰信號稍遲的數個週期後偵測崩潰信號狀態中的變化。若在較早之過渡之後不久崩潰偵測器之狀態中有變化，則移位暫存器可經重置以防止上述之過渡影響該俘獲元件。此舉確保若崩潰信號改變且保持在崩潰信號之新值中達等於移位暫存器之移位級數的週期次數，則俘獲元件將僅俘獲週期計數值之當前值。

【0018】 在一些實施例中，TRNG 可包含亂數決定單元，該亂數決定單元基於由量測電路量測之崩潰時間值決定亂數值。然而，此舉並非必須的，因爲在其他實施例中，可將崩潰時間值輸出至並非 TRNG 自身之部分的外部元件，且該外部元件可隨後決定亂數值。

【0019】 有可能直接將崩潰時間值映射至亂數值。然而，因爲崩潰時間值取決於將傾向於展示常態分佈之熱雜訊，該時

間崩潰值將比其他值更經常地取用一些數值。爲了產生具有均勻概率分佈之亂數，可基於由時間量測電路量測之崩潰時間值之位元的子集決定亂數值。例如，崩潰時間值可經截斷以產生對應於崩潰時間值之數個最低有效位元的截斷值，且隨後可基於該截斷值決定亂數值。總體上，取用不同數值之崩潰時間值之最低有效位元的概率分佈傾向於比作爲整體之崩潰時間值之概率分佈更均勻，且因此截斷崩潰時間值可改良 TRNG 之隨機性。

【0020】 在一些實例中，在決定亂數值時，亦可能需要排除截斷值之最低有效位元。此舉可用於消除亂數之敏感性，以使取樣該週期計數器之俘獲元件失配。

【0021】 所有硬體 TRNG 應解決來自潛在雜訊環境之干擾，以及試圖減少產生之亂數之隨機性的專屬攻擊。眾所熟知，若環形振盪器之電源有雜訊或攻擊者有意將一些高頻雜訊引入於電源軌道上，則環形振盪器可能對頻率注入敏感。已發現，使用本技術之 TRNG，包含 TRNG 之積體電路的元件（可具有內阻或電容）自身可提供充分的雜訊過濾，以防止環境雜訊及專屬攻擊。然而，要改良雜訊防護且減少對攻擊的敏感度，可將低通濾波器耦接在環形振盪器及該環形振盪器之電源軌道之間。低通濾波器可具備比預期頻率低之截止頻率，在該預期頻率下，可預期雜訊將影響產生之數的隨機性。以此方式，可生產穩固的 TRNG，該 TRNG 難以攻擊且更可靠地產生真實的亂數。

【0022】 自另一態樣可見，本技術提供真實亂數產生器，該

真實亂數產生器包含：

環形振盪器構件，該環形振盪器構件在第一振盪模式及第二振盪模式之一者中振盪；

控制構件，該控制構件用於觸發環形振盪器在振盪開始時間之第一振盪模式中開始振盪；以及

時間量測構件，該時間量測構件用於量測崩潰時間值，該崩潰時間值指示從振盪開始時間至振盪崩潰時間之時間長度，在該振盪崩潰時間，環形振盪器構件從第一振盪模式切換至第二振盪模式。

【0023】 自另一態樣可見，本技術提供一種產生真實亂數之方法，該方法包含以下步驟：

在振盪開始時間，觸發環形振盪器以在第一振盪模式中開始振盪；

量測崩潰時間值，該崩潰時間值指示從振盪開始時間至振盪崩潰時間之時間長度，在該振盪崩潰時間，環形振盪器從第一振盪模式切換至第二振盪模式；以及

基於崩潰時間值決定真實亂數。

【0024】 從結合附圖閱讀之實例之以下詳細描述中將顯而易見本技術之其他態樣、特徵及優點。

【圖式簡單說明】

【0025】 第 1 圖圖示習知的環形振盪器；

【0026】 第 2 圖圖示根據本技術之環形振盪器，該環形振盪器可經觸發以在崩潰至第二振盪模式之前於第一振盪模式中

振盪；

【0027】 第 3 圖爲時序圖，該時序圖比較在第一振盪模式中時的第 1 圖之環形振盪器與第 2 圖之環形振盪器的振盪；

【0028】 第 4 圖爲相位圖，該相位圖圖示環形振盪器之各別邊緣之間的相位差；

【0029】 第 5 圖圖示環形振盪器至第二振盪模式之崩潰；

【0030】 第 6 圖圖示數學分析，該數學分析指示預期本技術之環形振盪器所受熱雜訊的影響比習知的環形振盪器更強烈；

【0031】 第 7 圖圖示 TRNG，該 TRNG 包含環形振盪器及用於量測崩潰至第二振盪模式之時間的時間量測電路；

【0032】 第 8 圖爲時序圖，該時序圖圖示第 7 圖之 TRNG 的操作；

【0033】 第 9 圖圖示用於測試 TRNG 抗雜訊之穩固度的設定以及 TRNG 之實例，該 TRNG 具備在 TRNG 之電源線上的濾波器；

【0034】 第 10 圖爲指示 TRNG 之兩個示例性實施之隨機性測試結果的表格；

【0035】 第 11 圖圖示實驗結果，該時間結果指示 TRNG 之隨機性及 TRNG 抗攻擊之穩固度；

【0036】 第 12 圖爲比較本技術之 TRNG 與先前技術之 TRNG 之表格；

【0037】 第 13 圖圖示產生真實亂數之方法；以及

【0038】 第 14 圖示意性地圖示將由時間量測電路量測之崩

潰時間值映射至隨機數值之實例。

【實施方式】

【0039】 第 1 圖圖示具有奇數個反向級 4、6 之習知的環形振盪器 2。反向級之一者爲以 NAND 閘極形式之輸入反向級 4，輸入反向級 4 接收較早反向級 6 之輸出及開始信號 8。在重置振盪器 2 之後，NAND 閘極 4 之兩個輸入均在邏輯 0 處，且因此 NAND 閘極之輸出在邏輯 1 處。當開始信號 8 上升至邏輯 1 時，隨後 NAND 閘極 4 下落，且此舉將一邊緣注入至環形振盪器中，該邊緣隨後圍繞該環形振盪器傳播。因爲各反向級 6 具有相關延遲，隨後邊緣需要一些時間以在環周圍傳播。因爲存在奇數個反向級，如第 3 圖之頂部中所示，輸出節點 10 處的信號作爲具有給定振盪器頻率之一系列脈衝出現。

【0040】 第 2 圖圖示根據本技術之環形振盪器 20。與習知的環形振盪器不同，在第 2 圖之環形振盪器 20 中，在三個不同的輸入反向級（輸入節點）4（各輸入反向級包含 NAND 閘極）處輸入開始信號。各輸入反向級 4 經安置位於環周圍之不同點處，且因此回應於開始信號 8 之上升邊緣，此舉將觸發第一振盪模式，在第一振盪模式中環形振盪器 20 圍繞該環傳播三個邊緣，各邊緣藉由給定相位差與其他邊緣分離。第 3 圖之下部分顯示時序圖，該時序圖圖示在輸出節點 30 處偵測時的各別邊緣。如在習知的環形振盪器 2 中，各邊緣具有相同的脈寬，但是各別邊緣之間存在相移。在輸出節點 30 處偵測到第二邊緣時，該第二邊緣相對於第一及第三邊緣經反向，

因爲在輸出節點 30 與輸入邊緣 2 的第二輸入節點之間存在奇數個反向級，而在輸出節點 30 與輸入邊緣 1 及邊緣 3 的第一/第三輸入節點之間存在偶數個反向級。第 3 圖之下曲線顯示在輸出節點 30 處偵測之整體信號具有習知環形振盪器信號之三倍的頻率。

【0041】 第 4 圖爲相位圖，該圖圖示振盪器 20 之第一振盪模式中各別邊緣之間的相位差。因爲輸入反向級 4 藉由同一數目之非輸入反向級 6 與相鄰之反向級 4 彼此分離，則入口之各對之間的相位差係相同的（在此實例中爲 120 度）。然而，在其他實施例中，在各別對邊緣之間將可能提供不等的相位差。此外，藉由包括接收開始信號 8 之不同數目的輸入反向級 4，有可能提供具有超過三個邊緣之環形振盪器。

【0042】 如第 4 圖中所示，在第一振盪模式中，邊緣之每一者將獨立地積累來自熱雜訊之抖動，引起各自具有完整週期之兩個相鄰邊緣之間脈寬的遞增變化。在第 5 圖中圖示此現象，在該圖中脈寬開始相對均勻，但依熱雜訊而定逐漸變化。兩個相鄰的邊緣隨時間最終變得密集，以致彼等邊緣崩潰且相互抵消，僅留下一個剩餘邊緣，且使得環形振盪器進入第二振盪模式（對應於第 1 圖中振盪器之習知的振盪模式）。從第一振盪模式（3 倍頻率模式）開始振盪至在第二振盪模式（1 倍頻率模式）中崩潰所用的時間反映抖動之積累，且該時間用作亂數產生之熵源。固有地取消過程變化，因爲所有的三個邊緣通過同一環振盪級 4、6，取消了由於過程變化所引起的級之間的任何失配。

【0043】 第 6 圖圖示對預期抖動的分析。儘管在習知的環形振盪器中，脈寬的方差與環形振盪器已振盪之週期次數 n 無關，但是對於第 2 圖至第 5 圖之三邊緣環形振盪器，方差隨週期次數 N 線性地增加，此意味存在大很多的熵。此意味著脈寬之隨機性比在習知的振盪器中要大得多，導致崩潰至第二振盪模式之量測時間中的高隨機度。

【0044】 第 7 圖示意性地圖示包括第 2 圖之環形振盪器 20 之真實亂數產生器(TRNG) 50 之實例。TRNG 50 包含控制電路 55，控制電路 55 包含產生主時脈信號之主環形振盪器。控制電路 55 產生用於環形振盪器 20 之開始信號。使用包含下降邊緣（後接上升邊緣）之脈衝產生開始信號。下降邊緣重置該環形振盪器 20，而上升邊緣觸發環形振盪器 20 以在振盪開始時間在第一振盪模式中開始振盪。提供時間量測電路 60 用於量測從振盪開始時間至振盪崩潰時間所用的時間，在該振盪崩潰時間處，環振盪崩潰至第二振盪模式。藉由時間量測電路 60 將崩潰時間值 62 輸出至亂數決定單元 70，亂數決定單元 70 基於所量測之崩潰時間值 62 決定亂數。

【0045】 在此實例中，時間量測電路包含相位頻率偵測器(PFD) 80，相位頻率偵測器 80 比較環形振盪器 20 之輸出與參考環形振盪器 82 之輸出的相位，參考環形振盪器 82 以預定頻率振盪，該預定頻率處在環形振盪器之第一振盪模式中的振盪頻率與第二振盪模式中的頻率之間。例如，參考環形振盪器 82 之頻率可爲第二振盪模式中之環形振盪器 20 之頻率的 1.5 倍（第一振盪模式中之環形振盪器 20 之頻率的一半）。

此舉可藉由提供具有三分之二數目之級 4、6 的參考環形振盪器 82 作爲環形振盪器 20 達成。任何習知的相位頻率偵測器設計可用於 PFD 80。在第 7 圖中圖示示例性 PFD 設計。PFD 80 輸出崩潰信號 83，該崩潰信號 83 指示環形振盪器 20 之頻率是大於還是小於參考環形振盪器 82 之頻率。同時，週期計數器 86 計算環形振盪器 20 之輸出的週期，及週期計數器 86 基於經過之週期輸出計數值。當 PFD 80 產生之崩潰信號 83 切換狀態，以指示環形振盪器 20 已從第一模式切換至第二振盪模式時，則俘獲暫存器 90 經觸發以俘獲週期計數器 86 產生之計數值的當前值。隨後，亂數決定單元 70 可將該俘獲之計數值讀取爲崩潰時間值 62。回應於控制信號 55 產生之開始信號 8 的下降邊緣，環形振盪器 20、參考環形振盪器 82 及俘獲暫存器 90 全部經重置。

【0046】 可將 PFD 80 輸出之崩潰信號 83 直接輸出至俘獲暫存器 90，以觸發俘獲來自週期計數器 86 之計數值。然而，環形振盪器不可能僅在極少量的週期後崩潰至第二模式。要防止崩潰信號 83 中之故障在最初幾個週期期間觸發對計數值的俘獲（很可能不正確且可能偏斜亂數分配），計數器之中間位元（此實例中的位元[3]）用於防止在最初幾個週期中對崩潰的錯誤觸發。鎖存器 92、94 及 NOR 閘極 96 防止俘獲暫存器 90 俘獲週期計數，直至計數值之位元 3 已切換至邏輯 1。俘獲暫存器 90 由從鎖存器 94 輸出之閘控崩潰信號 84 觸發，而不是由 PFD 輸出之崩潰信號 83 觸發。此舉確保不可在操作之最初的八個週期中偵測崩潰事件。若初始週期需要不同的

週期次數，則週期計數值之不同位元可用於閘控崩潰偵測。

【0047】 第 7 圖之下半部圖示 PFD 80 之示例性電路佈置。因爲環形振盪器 20 之第一與第二振盪模式之間的頻率變化較大（三倍的頻率差異），可使用 PFD 80 之習知的數位實施，該實施使完全可整合之設計成爲可能。PFD 80 包括標準 PFD 設計 100，PFD 設計 100 接收來自環形振盪器 20 之輸出 CLKA 及來自參考環形振盪器 82 之輸出 CLKB。PFD 100 產生信號上 UP（上）、DOWN（下），以使得若環形振盪器 20 之頻率大於參考環形振盪器 82 之頻率，則 UP 信號在大部分時間內將係高的，而 DOWN 信號在大部分時間內將係低的，除存在參考環形振盪器 82 之脈衝時的奇怪故障之外。另一方面，若環形振盪器 20 之頻率低於參考環形振盪器 82 之頻率，則 UP 信號在大部分時間內將係低的，而 DOWN 信號在大部分時間內將係高的，除接收產生環形振盪器 20 之亂數脈衝時的奇怪故障之外。提供故障移除級 104 以移除此等故障。故障移除級 104 包含 UP 及 DOWN 信號路徑兩者上的故障移除電路。各故障移除電路包含 AND 閘極 106 及緩衝器（在其他實施例中可爲反相器）108。緩衝器/反相器 108 延遲接收之信號，且信號之延遲及非延遲版本經輸入至 AND 閘極 106。AND 閘極 106 之輸出將僅在延遲及非延遲信號兩者均爲高時爲高，因此當 UP 或 DOWN 信號過渡高時，則 AND 106 之輸出將僅在上(up)信號之高位值比緩衝器/反相器 108 之閘極延遲的持續更長時間時切換至高位。此舉消除了短期故障，其中該信號暫時切換值。在其他實施例中，可在時間量測電路 60

之其他部分內提供故障移除電路，而不是使故障移除電路作爲如第 7 圖所示之 PFD 80 之部分。

【0048】 此外，PFD 80 可具有移位暫存器級 110，移位暫存器級 110 延遲數個週期之崩潰信號。在此實例中，提供 2 位元移位暫存器，且因此崩潰信號 83 之輸出中存在兩個週期延遲（儘管可視需要提供較多數目之級）。UP 及 DOWN 信號之每一者通過兩級移位暫存器，若 DOWN 信號中存在上升邊緣過渡，則重置 UP 移位暫存器，且若 UP 信號中存在上升邊緣過渡，則重置 DOWN 移位暫存器。移位暫存器級確保 UP/DOWN 信號之值的變化必須維持至少兩個連續週期，以便將該變化記錄爲崩潰事件。因此，僅在較低頻率下偵測環形振盪器 20 之兩個連續週期之後標記崩潰事件。

【0049】 PFD 80 可基於移位暫存器級 110 之 UP 輸出 OUT_A 或 DOWN 輸出 OUT_B 中之任一者輸出崩潰信號 83。在第 7 圖中圖示之實例中，崩潰信號 83 係基於 UP 輸出 OUT_A，但可使用 DOWN 輸出 OUT_B 作爲崩潰信號 83 建構互補時間量測電路 60。在其他實施例中，可將移位暫存器級 110 提供於時間量測電路 60 內之不同的位置中，或可完全的省略移位暫存器級 110。

【0050】 第 8 圖圖示時序圖，該圖圖示第 7 圖之 TRNG 的操作。控制電路 55 中的主時鐘頻率經設置足夠緩慢，使得絕大多數崩潰事件在有效相位持續時間內完成。在測試之設計中，超過 90%之崩潰時間準時完成。通常，在 3 邊緣振盪器的情況下，若控制電路 55 產生之主時鐘的時脈脈衝至少長於

第 2 圖中圖示之環中的反相器總數之三分之一的延遲，則應及時重置及重新開始所有節點。回應於主時脈信號之上升邊緣，控制電路 55 產生開始信號 8 之下降脈衝。脈衝之下降邊緣重置環形振盪器 20、參考環形振盪器 82 及時間量測電路 60 內的多個鎖存器/暫存器 92、94、90。脈衝之上升邊緣觸發環形振盪器 20 以第二模式之 3 倍的頻率在第一振盪模式中開始振盪，且觸發參考環形振盪器 20 以預定頻率振盪，該預定頻率爲環形振盪器 20 之第二模式之頻率的 1.5 倍。週期計數器 86 計算環形振盪器 20 之週期次數。在第一振盪模式中時，環形振盪器 20 之頻率高於參考環形振盪器 82 之頻率，且因此 PFD 80 之輸出 83 係高的。最終，來自週期計數器 86 之計算信號之位元（3）過渡爲高，且從此時開始，PFD 輸出 83 中的的變化將觸發閘控崩潰信號 84（停止信號）中的變化。當環形振盪器 20 切換至第二振盪模式時，PFD 崩潰信號 83 過渡爲低，引起閘控崩潰信號 84 過渡爲高。此舉觸發計數暫存器 90 從週期計數器 86 俘獲當前計數值。亂數決定單元 70 可隨後讀取或輸出及使用此值以決定亂數。

【0051】 在一些實施例中，可能不能將亂數決定單元 70 提供至 TRNG 50 中，且反而可將計數值 62 輸出至外部元件，該外部元件隨後決定一亂數。

【0052】 所有硬體 TRNG 必須解決來自潛在雜訊環境以及專屬攻擊之干擾。已知環形振盪器對頻率注入敏感，在基於環形振盪器之 TRNG 中已將此情況報告以引入誤差。爲量測 3 邊緣 TRNG 對惡意攻擊之敏感度，吾人使用晶片外雜訊源測

試該 3 邊緣 TRNG 之穩固度。此外，吾人形成注入及量測雜訊兩者的晶載測試結構，及防止受該雜訊影響之展示構件（參見第 9 圖）。爲了量測頻率注入之敏感度，由晶載電壓控制振盪器 102 控制之可程式化雜訊產生器 100 將大量雜訊引入 TRNG 電源軌道 104（或至少環形振盪器 20 之電源軌道）上，鎖定振盪及影響崩潰事件時間。爲了量測晶載雜訊振幅，提供雜訊監控器 106，在雜訊監控器 106 中，異步時鐘取樣雜訊電源電壓，並將雜訊電源電壓與外部參考電壓比較且因此增量計數器 108。使用充足的樣品（吾人之量測中的 2^{14} 個），可從計數器值決定雜訊振幅。

【0053】 此外，具有 210 MHz 的角（截止）頻率之 RC 雜訊濾波器 110 經設計，以緩和電源雜訊之影響。如第 9 圖之右手部分所示，可在 TRNG 50 之電源軌道或環形振盪器 20 上提供 RC 濾波器 110，且 RC 濾波器用作低通濾波器，以便消除相對高頻雜訊。如以下討論，已發現此舉可足以防止受電源雜訊攻擊。在一些實施例中，可能不要求濾波器作爲積體電路內之 RC 元件，該積體電路自身可提供充足的雜訊過濾。然而，要增加 TRNG 穩固地抗攻擊之信心，可提供濾波器。

【0054】 使用兩個測試晶片評估建議的 3 邊緣 TRNG；一個測試晶片位於具有 8 個不同環之 28 nm 的 CMOS 中；另一測試晶片位於具有 48 個不同的 TRNG 之 65 nm 的 CMOS 中。NIST Pub 800-200 RNG 測試套用於評估產生之位元的隨機性。如第 10 圖所示，28 nm 及 65 nm 之 TRNG 兩者通過全部 15 個 NIST 測試。

【0055】 使用 RF 信號產生器，在電源上注入高達 600mVpp 之雜訊（在移除去耦基座的板之後），以測試 TRNG 抗晶片外攻擊的穩固度。65 nm 之 TRNG 在沒有濾波器的情況下對高達 360mVpp 之雜訊保持隨機性，且在具有濾波器的情況下對高達 600mVpp 的產生器限制保持隨機性。爲了補償濾波器 IR 下降，在增加 5%之電源電壓下操作具有濾波器之 TRNG，此導致少量的功率損失。因爲 28 nm 之 TRNG 中之 RO 在更高頻率下操作，彼等 TRNG 對外部攻擊的靈敏度較低；即使未經過濾之版本並未遭受產生器限制下的隨機性減低。天線注入之 EMI 雜訊亦未引起任何隨機性測試之故障。

【0056】 第 11 圖圖示電源雜訊對使用晶載雜訊產生之 TRNG 效能的影響。即使惡意攻擊者不可存取該雜訊源，此測試可展示 3 邊緣之 TRNG 如何輕易地與晶片上系統中之其他雜訊電路整合。TRNG 顯示對接近 1 倍及 4 倍之標稱 RO 頻率之頻率的電源雜訊的敏感性，減少崩潰時間均值及方差。在無濾波器的情況下，隨機性在>125mV 之雜訊振幅及 4 倍頻率條件下降低，但在使用濾波器後該隨機性恢復。藉由增加濾波器 R 及/或 C，以額外的功率及/或區域爲代價可改良抗攻擊防護。當 TRNG 歸因於外部影響不能產生輸出位元時發生服務拒絕。此僅在具有恰好在 3 倍標稱頻率下晶載雜訊產生之未受防護的 TRNG 中觀察到（參看第 11 圖之右下角的曲線），因爲該環鎖定至 TRNG 之 3 倍頻率模式，從而防止崩潰。在此情況下，良率（產生輸出位元之主週期的百分比）下降至 7.37%。使用濾波器 110 可防止此情況。然而，即使在 3 倍頻

率雜訊產生時，產生之位元亦保持隨機性（通過所有測試），顯示了建議之 TRNG 的穩固度。

【0057】 第 12 圖之表格總結與較早的 TRNG 相比之 28 nm 及 65 nm 之設計兩者的量測結果。將本技術與以下系統比較：

【0058】 [1] M. Bucci 等人所著的「A High Speed Oscillator Based True Random Number Generator for Cryptographic Applications on a Smart Card IC」，IEEE Trans. Computers，2003 年 4 月。

【0059】 [3] R. Brederlow 等人所著的「A Low-Power True Random Number Generator using Random Telegraph Noise of Single Oxide Traps」，ISSCC，2006。

【0060】 [4] C. Tokunaga 等人所著的「True Random Number Generator with a Metastability-Based Quality Control」，ISSCC，2007。

【0061】 [5] S. Mathew 等人所著的「2.4Gbps, 7mW All-Digital PVT-variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors」，IEEE JSSC，2012 年 11 月。

【0062】 [6] M. Matsumoto 等人所著的「1200 μ m2 Physical Random-Number Generators Based on SiN MOSFET for Secure Smart-Card Application」，ICCC，2008。

【0063】 [7] N. Liu 等人所著的「A true random number generator using time-dependent dielectric breakdown」，Symp VLSI Circuits，2001。

【0064】 如第 12 圖中所示，本技術比大多數其他技術提供更高的位元率（產量），能夠通過所有的 NIST 隨機測試且與其他技術相比提供增加的能量效率(nJ/bit)及抗攻擊性。此外，本技術提供更易於設計之 TRNG，因爲第 7 圖中圖示之完全的數位電路佈置使得標準數位合成技術能夠與習知的置放及選路算法一起使用，例如使用標準單元庫以提供 TRNG 50 的所有元件。

【0065】 第 13 圖示意性地圖示產生真實亂數之方法。在步驟 200 處，環形振盪器 20 開始在第一振盪模式中振盪，在該第一振盪模式中，多個邊緣同時在環周圍傳播。週期計數器 86 開始計算環形振盪器 20 之週期。在步驟 202 處，崩潰偵測器 80 決定環形振盪器 20 是否已崩潰至第二振盪模式，在該第二振盪模式中，較少的邊緣在該環周圍傳播。若未崩潰至第二振盪模式，則該崩潰偵測器繼續檢查崩潰。當環形振盪器崩潰至第二振盪模式時，該方法進行至步驟 204，在步驟 204 處，將來自週期計數器 86 之週期計數值俘獲至俘獲暫存器 90 中。俘獲之週期計數值表示第一模式中振盪開始與崩潰至第二模式之間的時間。此時間取決於以熱雜訊形式之熵值，且因此該時間高度隨機。在步驟 206 處，基於俘獲之週期計數由亂數決定單元 70 或外部元件產生亂數。

【0066】 第 14 圖圖示從俘獲之週期計數產生隨機值的實例。如第 11 圖右上角之圖所示，俘獲之計數值將展示常態分佈，且因此若直接將此計數值映射至亂數值，則產生之亂數的概率分佈將是不均勻的。要提供更均勻之分佈，可取用俘

獲之計數值之位元的子集且可丟棄其他位元。通常，計數值之最低有效位元將顯示最均勻的變化，且因此可截斷計數值之上位元。第 14 圖顯示一實例，在該實例中，高於計數值之位元[M]的位元被截斷。又，計數值之最低有效位元 0 可能對逆取樣(counter sampling)正反器 90 中的失配敏感。因此，藉由降低此位元，位元[M:1]之剩餘子集提供具有更均勻分佈之亂數。若需要比此子集具有更多數目之位元的亂數，則可並行提供多個 TRNG 50，各 TRNG 產生隨機值之一部分，且該等部分隨後經串聯形成整體隨機值。替代地，同一 TRNG 50 可在連續週期中產生若干隨機位元串，且隨後在不同週期中產生之值可經串聯產生較大的隨機值。

【0067】 儘管本文已參閱附圖詳細描述本發明之說明性實施例，但是應瞭解，本發明不限於彼等精確的實施例，且在不脫離如由附加申請專利範圍所定義的本發明之範疇及精神的情況下，熟習此項技術者可在實施例中實現多種變化及修改。

【符號說明】

【0068】

2 習知的環形振盪器

4 輸入反向級

6 反向級

8 開始信號

10 輸出節點

20 環形振盪器

30 輸出節點

50 真實亂數產生器(TRNG)

55 控制電路

60 時間量測電路

62 崩潰時間值/計數值

70 亂數決定單元

80 相位頻率偵測器

82 參考環形振盪器

83 PFD 崩潰信號

84 閘控崩潰信號

86 週期計數器

90 鎖存器/暫存器

92 鎖存器/暫存器

94 鎖存器/暫存器

96 NOR 閘極

100 標準 PFD 設計

102 晶載電壓控制振盪器

104 TRNG 電源軌道

106 AND 閘極/雜訊監控器

108 緩衝器/反相器

110 移位暫存器級

200 步驟

202 步驟

204 步驟

206 步驟

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

measured, and this can be used to determine a random number. The TRNG can be synthesized entirely using standard digital techniques and is able to provide high randomness, good throughput and energy efficiency.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

4 輸入反向級

6 反向級

8 開始信號

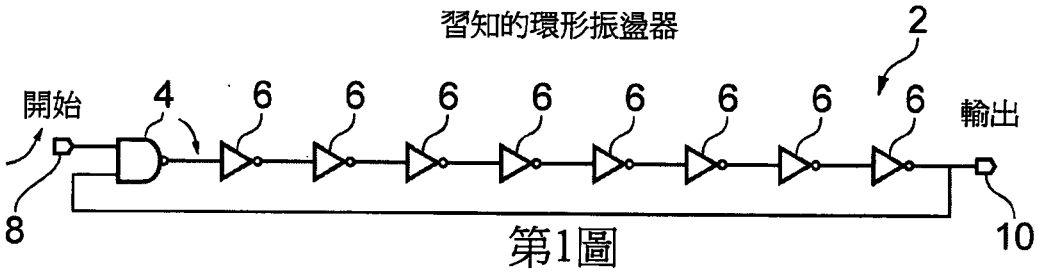
20 環形振盪器

30 輸出節點

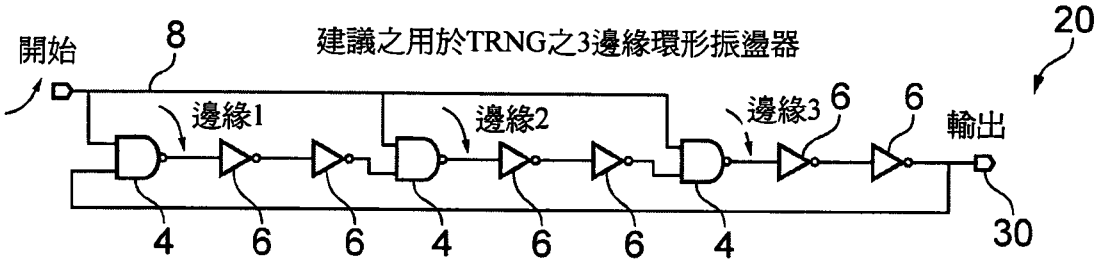
【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

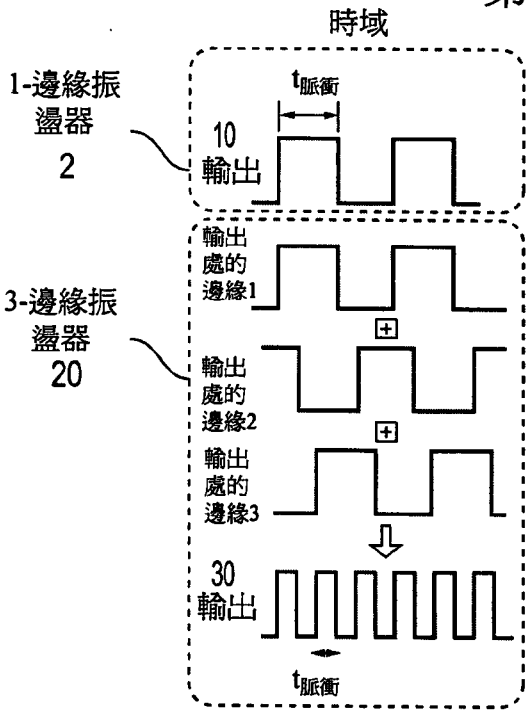
圖 式



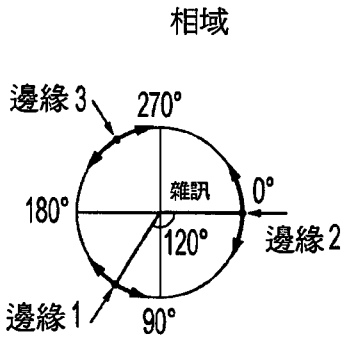
第1圖



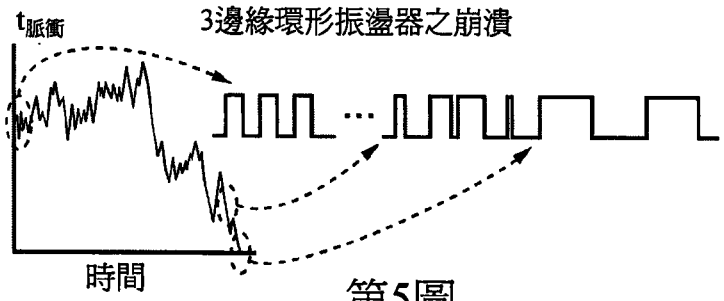
第2圖



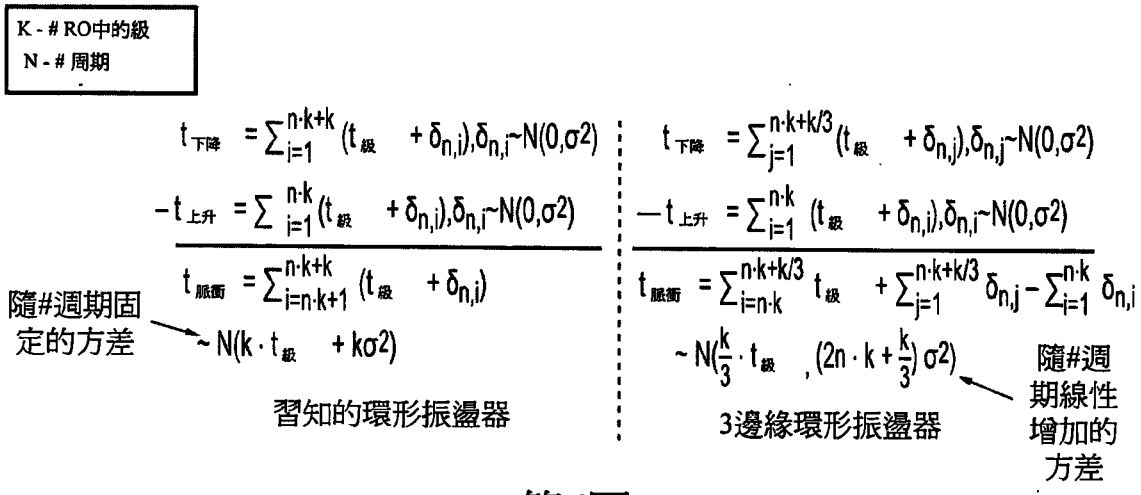
第3圖



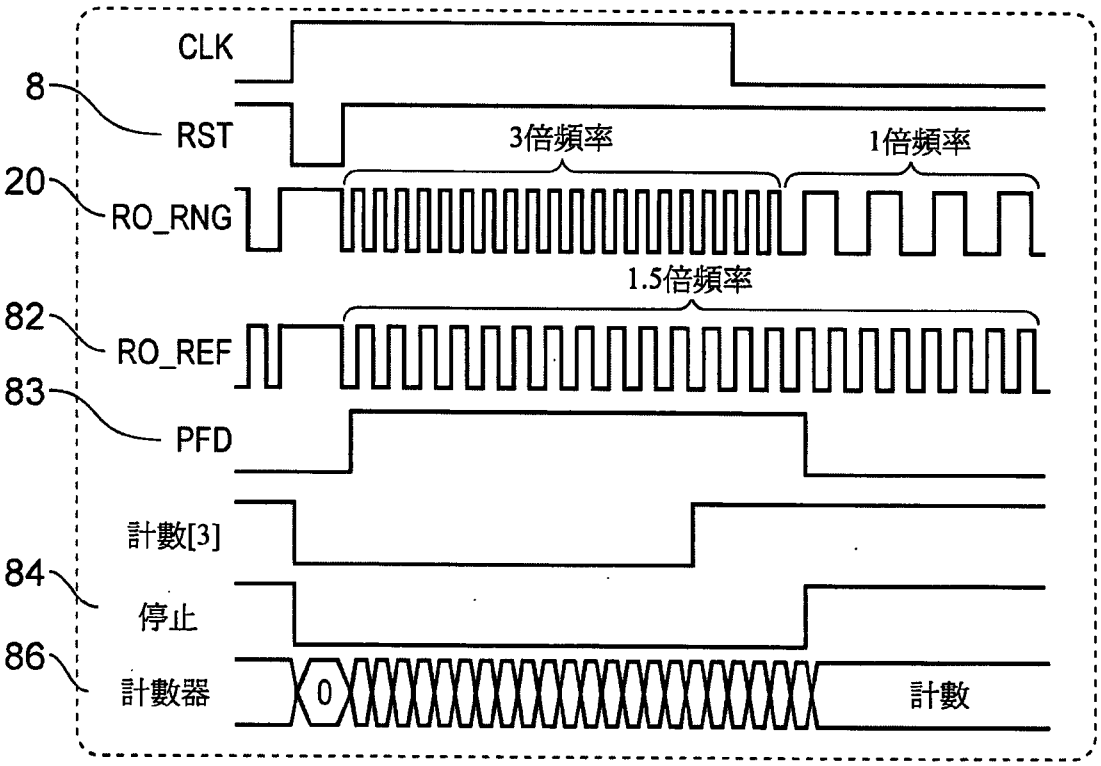
第4圖



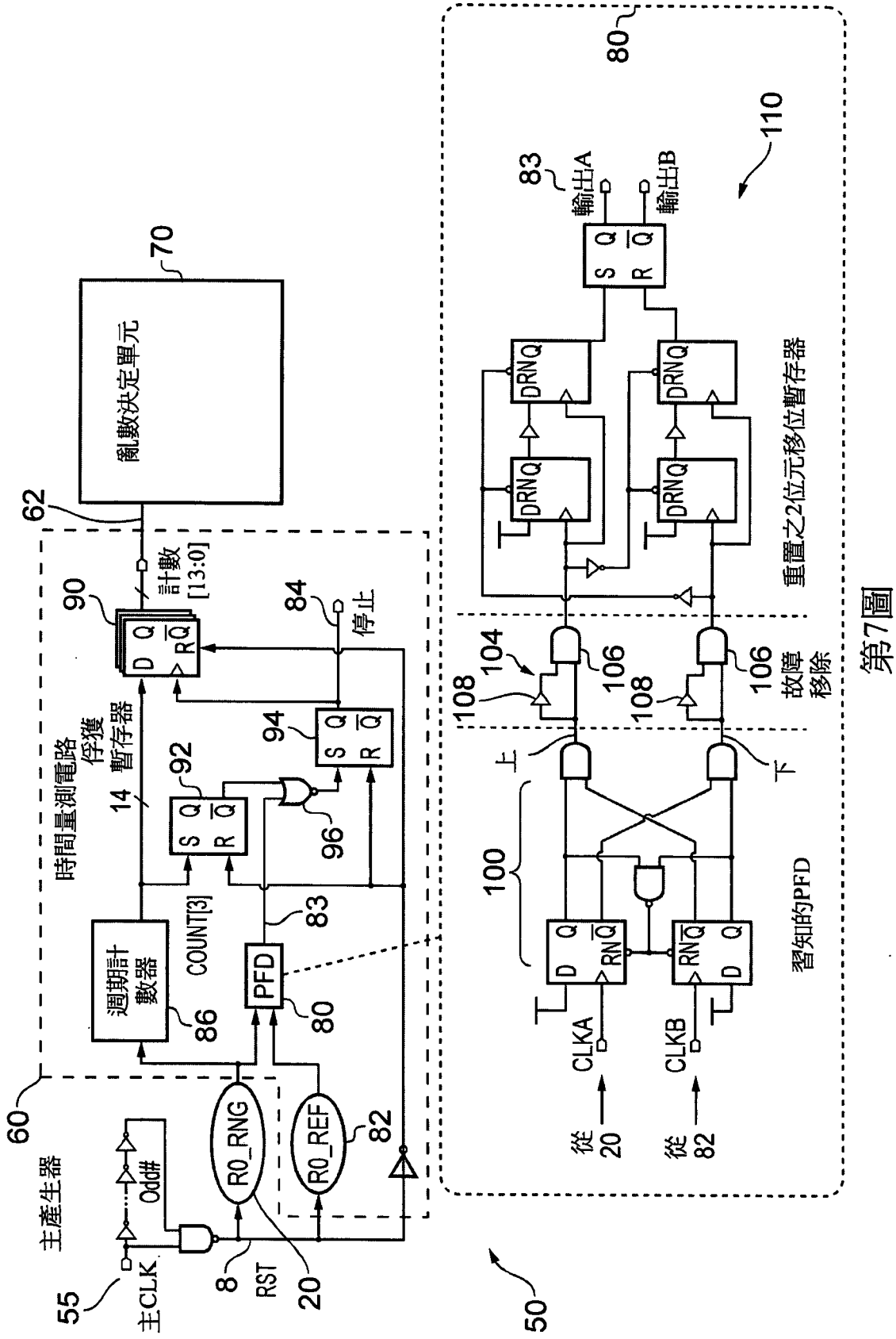
第5圖


K - # RO中的級
N - # 周期
$t_{下降} = \sum_{i=1}^{n\cdot k+k}(t_{級} + \delta_{n,i}), \delta_{n,i} \sim N(0,\sigma^2)$
$-t_{上升} = \sum_{i=1}^{n\cdot k}(t_{級} + \delta_{n,i}), \delta_{n,i} \sim N(0,\sigma^2)$
$t_{脈衝} = \sum_{i=n\cdot k+1}^{n\cdot k+k}(t_{級} + \delta_{n,i})$
隨#週期固定的方差
$\sim N(k \cdot t_{級} + k\sigma^2)$
習知的環形振盪器
$t_{下降} = \sum_{j=1}^{n\cdot k+k/3}(t_{級} + \delta_{n,j}), \delta_{n,j} \sim N(0,\sigma^2)$
$-t_{上升} = \sum_{i=1}^{n\cdot k}(t_{級} + \delta_{n,i}), \delta_{n,i} \sim N(0,\sigma^2)$
$t_{脈衝} = \sum_{i=n\cdot k}^{n\cdot k+k/3} t_{級} + \sum_{j=1}^{n\cdot k+k/3} \delta_{n,j} - \sum_{i=1}^{n\cdot k} \delta_{n,i}$
$\sim N(\frac{k}{3} \cdot t_{級}, (2n \cdot k + \frac{k}{3})\sigma^2)$
隨#週期線性增加的方差
3邊緣環形振盪器

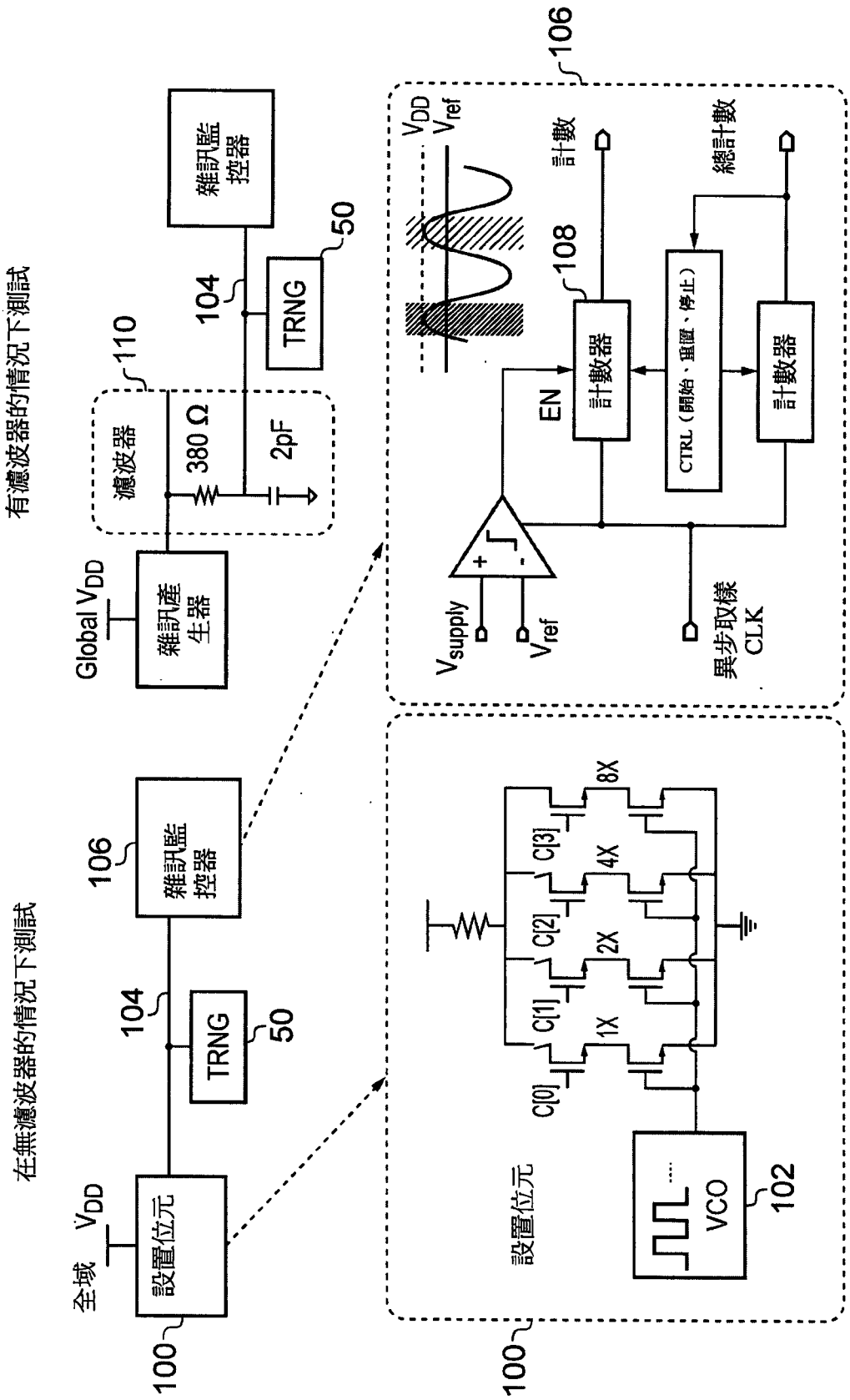
第6圖


CLK
8
RST
3倍頻率
1倍頻率
20
RO_RNG
1.5倍頻率
82
RO_REF
83
PFD
計數[3]
84
停止
86
計數器
0
計數

第8圖


50
60
主產生器
55
主CLK
Od#
8
RST
R0_RNG
20
R0_REF
82
時間量測電路
14
停獲暫存器
週期計數器
86
COUNT[3]
PFD
80
83
92
96
94
90
計數[13:0]
62
亂數決定單元
70
84
停止
80
110
83
輸出A
輸出B
DRNQ
重置之2位元移位暫存器
104
106
108
故障移除
上
下
100
CLKA
CLKB
從20
從82
習知的PFD

第7圖


有濾波器的情況下測試
在無濾波器的情況下測試
全域 V_{DD}
設置位元
100
106
雜訊監控器
104
TRNG
50
雜訊監控器
104
TRNG
50
110
濾波器
380 Ω
2pF
Global V_{DD}
雜訊產生器
106
V_{DD}
V_{ref}
計數
108
EN
計數器
CTRL（開始、重置、停止）
總計數
計數器
V_{supply}
V_{ref}
異步取樣 CLK
100
設置位元
C[0]
C[1]
C[2]
C[3]
1X
2X
4X
8X
VCO
102

第9圖

測試名稱	65nm，21級RO，0.9V，2.80Mb/s		28nm，21級RO，0.9V，23.16Mb/s	
	P-valueχ^2	通過率	P-valueχ^2	通過率
頻率	0.785562	296/300	0.872947	297/300
阻斷頻率	0.082177	297/300	0.746572	297/300
累積和	0.462245	294/300	0.955835	296/300
累積和	0.942895	295/300	0.329332	294/300
流量	0.220931	296/300	0.574903	297/300
最長流量	0.329332	296/300	0.81047	298/300
矩陣秩	0.046668	294/300	0.000682	296/300
FFT	0.03013	295/300	0.224821	295/300
非重疊模板	通過 *	通過 *	通過 *	通過 *
重疊模板	0.878107	297/300	0.329332	296/300
線性複雜性	0.487885	297/300	0.304126	295/300
通用	0.935716	98/100	0.719747	99/100
隨機偏移	PASS*	PASS*	PASS*	PASS*
隨機偏移變體	通過 *	通過 *	通過 *	通過 *
近似熵	0.514124	100/100	0.275709	100/100
串列	0.304126	99/100	0.897763	99/100
串列	0.867692	99/100	0.595549	100/100

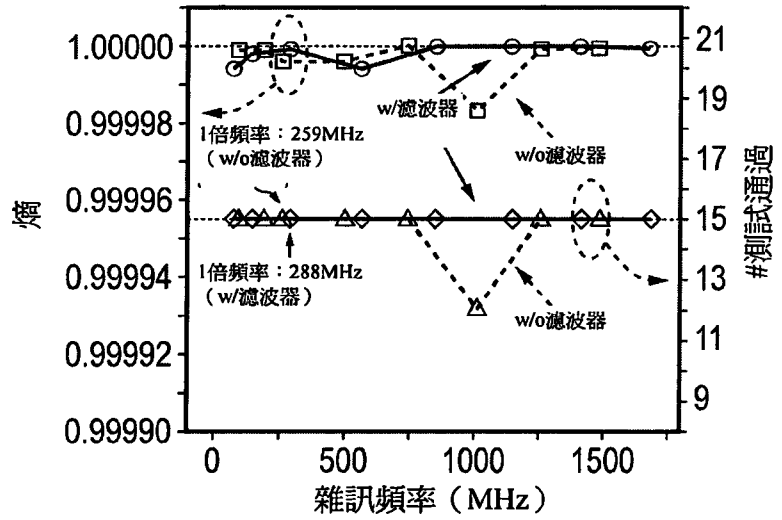
* 非重疊、隨機偏移及隨機偏移變體測試分別具有148個、8個及18個子測試。「通過」意味所有子測試通過最低要求

** 最低的 p-valueχ^2 爲0.001

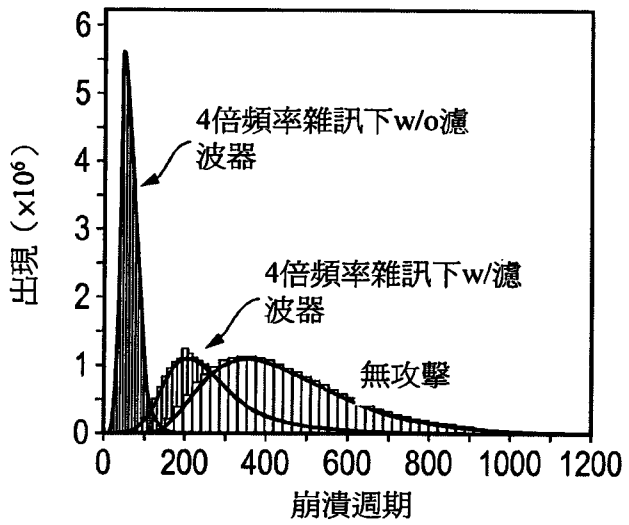
*** 最初10個測試的最低通過率爲291/300，且其他5個測試的通過率爲90/100。

第10圖

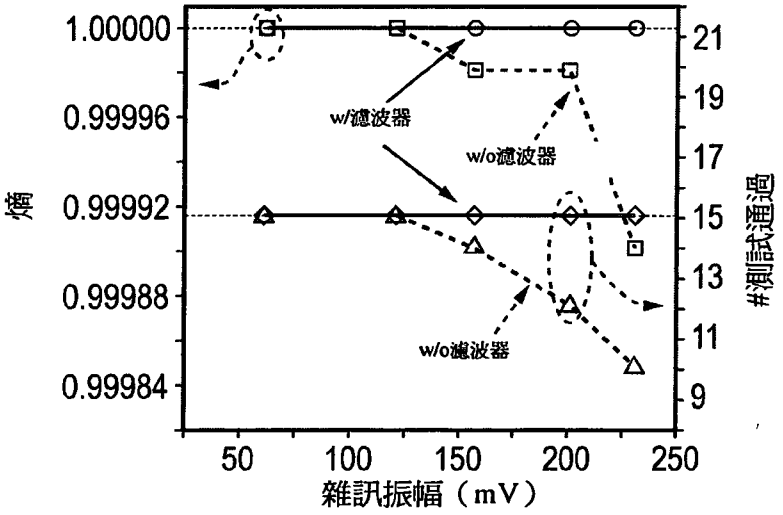
攻擊下的隨機性（雜訊振幅=200mV）



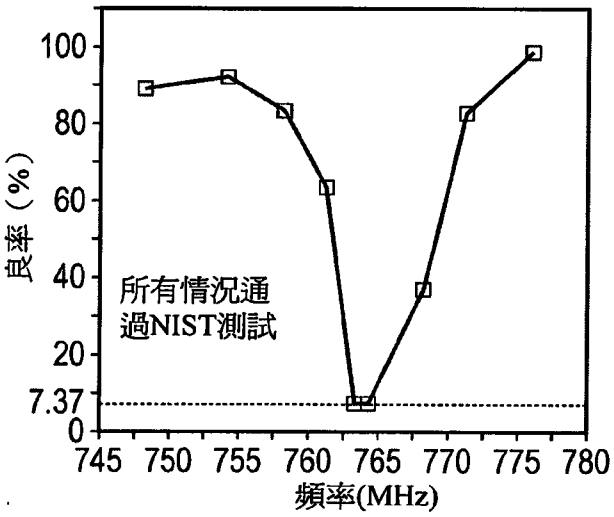
攻擊下崩潰之週期的分佈（雜訊振幅=200mV）



攻擊下的隨機性（雜訊頻率=4倍標稱頻率）



3倍標稱頻率下的服務拒絕（雜訊振幅=200mV）



第11圖

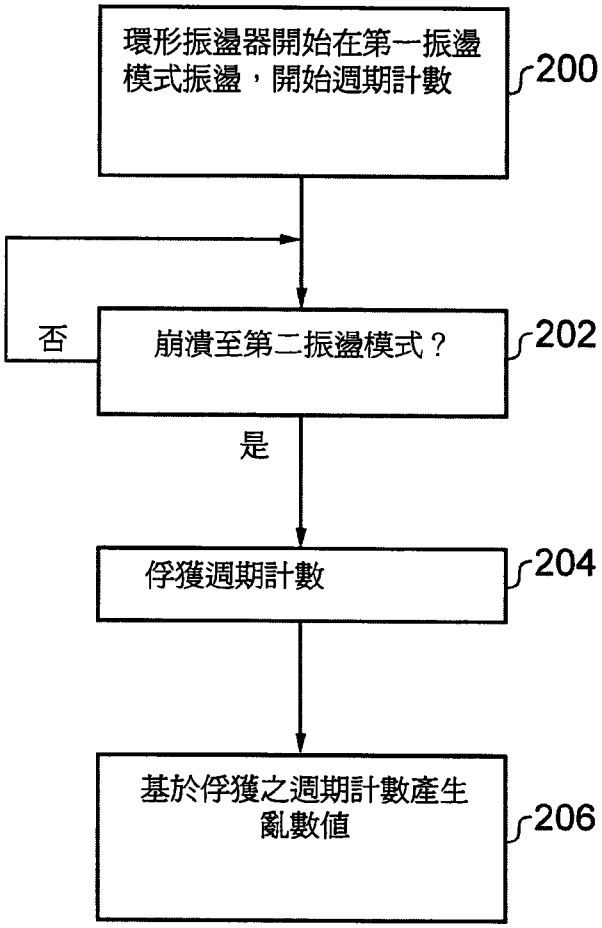
	此工作 (25°C, 0.9V 核心電源)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers '03 [1]
技术	28nm	65nm	45nm	65nm	0.25μm	0.13μm	0.12μm	0.18μm
熵源	3邊緣RO中的抖動		亞穩度	氧化物分解	SiN MOSFET 雜訊	亞穩度	亞穩度	振盪器抖動
位元率(Mb/s)	23.16	2.8	2400	0.011	2	0.2	0.2	10
NIST通过	所有	所有	所有	所有	未報告 b	5	未報告	未報告 b
TRNG核心区域 (μm^2)	375	960 (1080a)	4004	1200	1200	36300	9000	16000
功率(mW)	0.54	0.159	7	2	1.9	1	0.05	2.3
效率(nJ/bit)	0.023	0.057	0.0029	181.81	0.95	5	0.25	0.23
后处理	否	否	否	否	是	否	是	否
抗攻击性	是	是	未報告	未報告	未報告	未報告	未報告	否 c

a 包括過濾區域的1/8（MIM蓋和多晶電阻器）；8個TRNG共享1個濾波器且MIM蓋經安置於TRNG之上

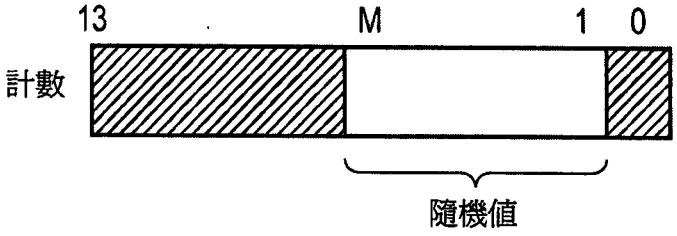
b 提供NIST FIPS 140-2測試結果，該測試結果比具有4個測試之NISTPub|800-22較舊且較不嚴謹，且僅需要20000個位元

c 在[8]中成功攻擊基於類似RO方法之市售的TRNG

第12圖


環形振盪器開始在第一振盪模式振盪，開始週期計數
200
否
崩潰至第二振盪模式？
202
是
俘獲週期計數
204
基於俘獲之週期計數產生亂數值
206

第13圖


13
M
1
0
計數
隨機值

第14圖

measured, and this can be used to determine a random number. The TRNG can be synthesized entirely using standard digital techniques and is able to provide high randomness, good throughput and energy efficiency.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

4 輸入反向級

6 反向級

8 開始信號

20 環形振盪器

30 輸出節點

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

產生真實亂數之方法與真實亂數產生器

METHOD OF GENERATING TRUE RANDOM NUMBER AND TRUE RANDOM NUMBER GENERATOR

【技術領域】

【0001】 本技術係關於真實亂數產生器之領域。

【先前技術】

【0002】 真實亂數產生器(True random number generator; TRNG)基於預期為隨機的物理現象（諸如大氣雜訊、熱雜訊或放射性衰變）量測亂數。因為用作 TRNG 之熵源的物理現象是無法預期的，所以產生之亂數係真實隨機的。如此與偽亂數產生器(Pseudo random number generator; PRNG)形成對比，偽亂數產生器使用數學公式或亂數預計算表以生成隨機出現之數列，但該數列在給定用於產生偽亂數之初始條件下實際上為可預測及確定的。對於許多應用，PRNG 係足夠的且實施此等偽亂數產生器比實施 TRNG 更經濟。然而，對於其他應用，TRNG 產生之真實隨機性係必要的，而 PRNG 則可能係不充分的。

【0003】 上述工作已展示基於電阻器-放大器-ADC 鏈、振盪器抖動、亞穩度及其他元件雜訊的 TRNG。然而，類比設計遭受變化及雜訊，使得彼等設計難以與數位電路整合。新近之基於亞穩度方法提供卓越的效能，但是經常要求細緻的校準

專利案號：103139795

公告本 107年06月01日 修正

I639948

發明摘要

※ 申請案號：103139795

※ 申請日：2014 年 11 月 17 日　　※IPC 分類：G06F 7/58 (2006.01)

【發明名稱】（中文/英文）

產生真實亂數之方法與真實亂數產生器

METHOD OF GENERATING TRUE RANDOM NUMBER AND TRUE RANDOM NUMBER GENERATOR

【中文】

一種真實亂數產生器包含環形振盪器，該環形振盪器經觸發以在振盪開始時間在第一振盪模式中開始振盪。視熱雜訊而定，第一振盪模式最終將崩潰至第二振盪模式。量測從振盪開始時間至振盪器崩潰至第二模式的時間之崩潰時間，且此崩潰時間可用於決定一亂數。TRNG 可使用標準數位技術完全合成，且該 TRNG 能夠提供高隨機性、良好的產量及能量效率。

【英文】

A true random number generator comprises a ring oscillator which is triggered to start oscillating in a first mode of oscillation at an oscillation start time. The first mode of oscillation will eventually collapse to a second mode of oscillation dependent on thermal noise. A collapse time from the oscillation start time to the time at which the oscillator collapses to the second mode is

申請專利範圍

1. 一種真實亂數產生器，該真實亂數產生器包含：

一環形振盪器；

一控制電路，該控制電路經設置以觸發該環形振盪器，以在一振盪開始時間在一第一振盪模式中開始振盪；以及

一時間量測電路，該時間量測電路經設置以量測一崩潰時間值，該崩潰時間值指示從該振盪開始時間至一振盪崩潰時間之一時間長度，在該振盪崩潰時間，該環形振盪器從該第一振盪模式切換至一第二振盪模式。

2. 如請求項 1 所述之真實亂數產生器，其中在該第一振盪模式中，該環形振盪器經設置以在高於該第二振盪模式中之一頻率下振盪。

3. 如請求項 1 所述之真實亂數產生器，其中在該第一振盪模式中，該環形振盪器經設置以在該環形振盪器周圍傳播複數個邊緣，各邊緣之間具有一相位差；以及

在該第二振盪模式中，該環形振盪器經設置以在該環形振盪器周圍傳播少於該第一振盪模式中之邊緣。

4. 如請求項 3 所述之真實亂數產生器，其中在該第二振盪模式中，該環形振盪器經設置以在該環形振盪器周圍傳播一單一邊緣。

5. 如請求項 3 所述之真實亂數產生器，其中在該第一振盪模式中，該環形振盪器經設置以在該環形振盪器周圍傳播一奇數個邊緣。

6. 如請求項 3 所述之真實亂數產生器，其中在該第一振盪模式中開始振盪時，該環形振盪器經設置以傳播該複數個邊緣，在各連續對邊緣之間具有一相等的相位差。

7. 如請求項 1 所述之真實亂數產生器，其中該環形振盪器包含位於該環形振盪器之不同級處的複數個輸入節點；

該控制電路經設置以在該振盪開始時間將一開始信號供給至該複數個輸入節點；以及

回應於該開始信號，各輸入節點經設置以將一各別邊緣注入至該環形振盪器中。

8. 如請求項 1 所述之真實亂數產生器，其中該時間量測電路包含：

一週期計數器，該週期計數器經設置以維持一週期計數值，該週期計數值指示自該振盪開始時間已經過的週期次數；

一崩潰偵測器，該崩潰偵測器經設置以回應於偵測該環形振盪器從該第一振盪模式切換至該第二振盪模式而輸出一崩潰信號；以及

一俘獲電路，該俘獲電路經設置以回應於該崩潰信號俘獲該週期計數值的一當前值。

9. 如請求項 8 所述之真實亂數產生器，其中該週期計數器經設置以計算該環形振盪器之一輸出的振盪週期。

10. 如請求項 8 所述之真實亂數產生器，其中該時間量測電路包含一參考環形振盪器，該參考環形振盪器經設置以在一預定頻率下振盪；以及

該崩潰偵測器包含一相位頻率偵測器，該相位頻率偵測器經設置以基於該環形振盪器之一輸出與該參考環形振盪器之一輸出的一相位比較產生該崩潰信號。

11. 如請求項 10 所述之真實亂數產生器，其中該環形振盪器經設置以在該第一振盪模式中以一第一頻率振盪，且經設置以在該第二振盪模式中以一第二頻率振盪，該第二頻率小於該第一頻率；以及

該參考環形振盪器之該預定頻率在該第一頻率與該第二頻率之間。

12. 如請求項 8 所述之真實亂數產生器，其中該時間量測電路包含一故障移除電路，該故障移除電路經設置以過濾掉該崩潰偵測器產生之該崩潰信號中的故障。

13. 如請求項 8 所述之真實亂數產生器，其中該時間量測電路包含具有複數個移位級之一移位暫存器；

該移位暫存器經設置以接收該移位暫存器之一第一級處由該崩潰偵測器產生之該崩潰信號；以及

該俘獲電路經設置以回應於該移位暫存器之一最終級之一輸出俘獲該週期計數值之該當前值。

14. 如請求項 1 所述之真實亂數產生器，該真實亂數產生器包含一亂數決定單元，該亂數決定單元經設置以基於由該量測電路量測之該崩潰時間值決定一亂數值。

15. 如請求項 14 所述之真實亂數產生器，其中該亂數決定單元經設置以基於由該時間量測電路量測之該崩潰時間值之位元的一子集決定該亂數值。

16. 如請求項 14 所述之真實亂數產生器，其中該亂數決定單元經設置以截斷該崩潰時間值，以產生對應於該崩潰時間值之複數個最低有效位元之一截斷值，且以基於該截斷值決定該亂數值。

17. 如請求項 16 所述之真實亂數產生器，其中該亂數決定單元經設置以基於排除該截斷值之該最低有效位元的該截斷值決定該亂數值。

18. 如請求項 1 所述之真實亂數產生器，該真實亂數產生器包含耦接在該環形振盪器與該環形振盪器之一電源軌道之間

的一低通濾波器。

19. 一種真實亂數產生器，該真實亂數產生器包含：

環形振盪器構件，該環形振盪器構件在一第一振盪模式及一第二振盪模式之一者中振盪；

控制構件，該控制構件用於觸發該環形振盪器在一振盪開始時間之該第一振盪模式中開始振盪；以及

時間量測構件，該時間量測構件用於量測一崩潰時間值，該崩潰時間值指示從該振盪開始時間至一振盪崩潰時間之一時間長度，在該振盪崩潰時間，該環形振盪器構件從該第一振盪模式切換至該第二振盪模式。

20. 一種產生一真實亂數之方法，該方法包含以下步驟：

在一振盪開始時間，觸發一環形振盪器以在一第一振盪模式中開始振盪；

量測一崩潰時間值，該崩潰時間值指示從該振盪開始時間至一振盪崩潰時間之一時間長度，在該振盪崩潰時間，該環形振盪器從該第一振盪模式切換至一第二振盪模式；以及

基於該崩潰時間值決定該真實亂數。