(19) URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ

(10) **PL 242251 B1**

(12) # Opis patentowy

(21) Numer zgłoszenia: **426575**
(22) Data zgłoszenia: **2018.08.07**
(43) Data publikacji o zgłoszeniu: **2020.02.10 BUP 04/2020**
(45) Data publikacji o udzieleniu patentu: **2023.02.06 WUP 06/2023**

(51) MKP:
H03K 3/84 *(2006.01)*

(73) Uprawniony z patentu:
POLITECHNIKA WARSZAWSKA, Warszawa, PL

(72) Twórca(-y) wynalazku:
KRZYSZTOF GOŁOFIT, Warszawa, PL
PIOTR WIECZOREK, Warszawa, PL

(74) Pełnomocnik:
Oliwia Czarnocka, Warszawa, PL

(54) Tytuł:
Generator losowy

PL 242251 B1

Opis wynalazku

Przedmiotem wynalazku jest generator losowy przeznaczony zwłaszcza do generacji liczb i ciągów liczbowych prawdziwie losowych.

Znany jest w stanie techniki, np. z publikacji Piotra Z. Wieczorka i Krzysztofa Gołofita, „True Random Number Generator Based on Flip-Flop Resolve Time Instability Boosted by Random Chaotic Source", IEEE Transactions on Circuits and Systems I: Regular Papers, Volume 65, Issue 4, pp. 1279–1292, 2018, DOI: 10.1109/TCSI.2017.2751144, generator losowy, który zawiera dwa generatory pierścieniowe z przełączanymi ścieżkami propagacji, do których wyjść dołączony jest detektor fazy, którego wyjście dołączone jest do wejść sterujących generatorów pierścieniowych z przełączanymi ścieżkami propagacji przez układ sterujący w postaci szeregu inwerterów. Do wyjść generatorów pierścieniowych z przełączanymi ścieżkami propagacji dołączony jest także układ metastabilnościowy, którego wyjście stanowi wyjście generatora losowego. Generator pierścieniowy z przełączaną ścieżką propagacji zawierają multiplekser i dwie linie opóźniające połączone ze sobą tak, że wyjście pierwszej linii opóźniającej dołączone jest do wejścia drugiej linii opóźniającej, a wyjście drugiej linii dołączone jest do wyjścia generatora pierścieniowego z przełączaną ścieżką propagacji. Multiplekser ma wejście sterujące dołączone do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji, wyjście dołączone do wejścia pierwszej linii opóźniającej, a wejścia dołączone do wejścia i wyjścia drugiej linii opóźniającej. Linie opóźniające zawierają elementy opóźniające połączone w szeregi.

Znany jest w stanie techniki, np. z publikacji Piotra Z. Wieczorka, „Secure TRNG with Random Phase Stimulation", XL-th IEEE-SPIE Joint Symposium on Photonics, Web Engineering, Electronics for Astronomy and High Energy Physics Experiments, Wilga 2017, SPIE volume 10445, ISBN: 9781510613546, Electronic ISBN: 9781510613553, generator losowy, który zawiera dwa generatory pierścieniowe oraz układ metastabilnościowy. Wyjścia generatorów pierścieniowych dołączone są do wejść układu metastabilnościowego, natomiast wyjście układu metastabilnościowego jest wyjściem generatora losowego. Generator pierścieniowy składa się z linii opóźniającej zamkniętej w pętlę, której wejście i wyjście są ze sobą połączone i dołączone do wyjścia generatora losowego. Linia opóźniająca składa się z elementów opóźniających połączonych w szereg i włączonych pomiędzy wejściem i wyjściem tej linii. Wadą takiego generatora losowego jest jego mała szybkość związana z rzadko występującymi zdarzeniami mogącymi zainicjować metastabilną pracę układu metastabilnościowego, co wynika z wolno kroczących przypadkowych zmian fazy (ang. *random walk in phase* lub *phase walk*).

Z publikacji niemieckiego zgłoszenia patentowego nr DE19618098 oraz z publikacji amerykańskiego zgłoszenia patentowego nr US2011169580, znane są generatory losowe, w których wyjścia dwóch generatorów pierścieniowych dołączone są do wejść detektora fazy, natomiast wyjście detektora fazy jest wyjściem generatora losowego. Wadą takich generatorów losowych jest mała losowość i mała szybkość działania takich układów związana z wolnymi przypadkowymi zmianami fazy.

Ze stanu techniki, np. z publikacji amerykańskich zgłoszeń patentowych nr US5153532, US2002156819 i US2006069706, znane są generatory losowe, w których zastosowano sumowanie – przy użyciu bramki XOR – sygnałów wyjściowych z dwóch lub wielu generatorów pierścieniowych.

Z publikacji patentu amerykańskiego nr US5007087, znana jest konstrukcja generatora losowego oparta na analogowym układzie chaotycznym z ciągłymi zmiennymi. Wadą takich generatorów jest to, że nie da się ich zaimplementować w cyfrowych układach programowalnych, a w związku z tym trudno jest wykorzystać do ich produkcji współczesne linie technologiczne.

Z publikacji amerykańskiego zgłoszenia patentowego o numerze US2014101217, znana jest konstrukcja generatora losowego oparta na cyfrowym układzie chaotycznym, w którym sprzężenie zwrotne ma charakter dyskretny. Wadą takich generatorów jest to, że mają skończoną liczbę stanów układu.

Z publikacji amerykańskiego zgłoszenia patentowego o numerze US2004264233, znany jest generator pierścieniowy z przełączaną ścieżką propagacji, który zawiera dwie linie opóźniające połączone ze sobą tak, że wyjście pierwszej linii dołączone jest do wejścia drugiej linii, której wejście i wyjście dołączone są do sterowanego klucza przełączającego, którego wyjście dołączone jest do wejścia pierwszej linii. Linie opóźniające zawierają elementy opóźniające połączone w szeregi.

Celem wynalazku jest wywołanie pracy chaotycznej i odpowiedzi metastabilnościowej, jak również zmniejszenie liczby elementów i kosztów implementacyjnych układu.

Istota wynalazku polega na tym, że generator losowy zawierający układ metastabilnościowy, którego wyjście jest dołączone do wyjścia generatora losowego oraz zawierający przynajmniej dwa gene-

ratory pierścieniowe, których wyjścia dołączone są do wejść układu metastabilnościowego oraz przynajmniej jeden z generatorów pierścieniowych stanowi generator pierścieniowy z przełączaną ścieżką propagacji z wejściem sterującym, zgodnie z wynalazkiem cechuje się tym, że wyjście układu metastabilnościowego dołączone jest do wejścia sterującego przynajmniej jednego generatora pierścieniowego z przełączaną ścieżką propagacji. Takie rozwiązanie zapewnia trzy korzystne skutki. Po pierwsze, dla przesunięć fazowych nie mieszczących się w oknie metastabilnościowym układ metastabilnościowy realizuje detekcję fazy i służy do korekcji fazy dołączonych do jego wejść generatorów pierścieniowych. Po drugie, dla przesunięć fazowych mieszczących się w oknie metastabilnościowym układ metastabilnościowy zapewnia losową wartość na swoim wyjściu i wskutek tego wprowadza przypadkową zmianę fazy, czym różni się od detektora fazy. Po trzecie, układ metastabilnościowy wprowadza do pętli sprzężenia zwrotnego opóźnienie, co rozszerza zakres występujących przesunięć fazowych w dołączonych do jego wejść generatorach pierścieniowych.

Korzystnie wyjście układu metastabilnościowego dołączone jest do przynajmniej jednego wejścia sterującego generatorów pierścieniowych z przełączaną ścieżką propagacji przez układ sterujący. Układ sterujący modyfikuje sygnał sprzężenia zwrotnego, co poprawia pracę układu chaotycznego.

Korzystnie, przynajmniej jeden generator pierścieniowy zawiera przynajmniej jedną linię opóźniającą, której wejście i wyjście są ze sobą połączone i dołączone do wyjścia generatora pierścieniowego, przy czym linia opóźniająca zawiera elementy opóźniające połączone w szereg.

Korzystnie, generator pierścieniowy z przełączaną ścieżką propagacji zawiera przynajmniej dwie linie opóźniające połączone ze sobą tak, że wyjście pierwszej linii opóźniającej dołączone jest do wejścia drugiej linii opóźniającej, a wyjście jednej z tych linii opóźniających dołączone jest do wyjścia generatora pierścieniowego z przełączaną ścieżką propagacji, przy czym linie opóźniające zawierają elementy opóźniające połączone w szeregi.

Korzystnie, generator pierścieniowy z przełączaną ścieżką propagacji zawiera przynajmniej jeden multiplekser, którego wejście sterujące dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji, oraz którego wyjście dołączone jest do wejścia jednej linii opóźniającej, oraz którego wejścia dołączone są wejścia i wyjścia innej linii opóźniającej.

Korzystnie, układ sterujący zawiera przynajmniej jeden element opóźniający. Opóźnienie w pętli sprzężenia zwrotnego, wprowadzane łącznie przez układ sterujący oraz układ metastabilnościowy, powoduje szerszy zakres przesunięć fazowych między generatorami pierścieniowymi.

Korzystnie, układ metastabilnościowy stanowi przerzutnik o dwóch wejściach stanowiących wejścia układu metastabilnościowego i wyjściu stanowiącym wyjście układu metastabilnościowego.

Alternatywnie, układ metastabilnościowy zawiera układ metastabilnościowy z oscylacyjną odpowiedzią impulsową o dwóch wejściach stanowiących wejścia układu metastabilnościowego i wyjściu stanowiącym wyjście układu metastabilnościowego.

Korzystnie, wyjście układu metastabilnościowego z oscylacyjną odpowiedzią impulsową dołączone jest do wyjścia układu metastabilnościowego przez sumator.

Korzystnie, układ metastabilnościowy zawiera układ liczący, którego wyjścia dołączone są do kolejnych wejść sumatora, a którego wejście dołączone jest do wyjścia układu metastabilnościowego z oscylacyjną odpowiedzią impulsową.

Alternatywnie, układ metastabilnościowy zawiera generator metastabilnościowych interwałów czasowych o wejściach dołączonych do wejść układu metastabilnościowego oraz wyjściach dołączonych do wejść arbitra, którego wyjścia dołączone są do wyjść układu metastabilnościowego przez układ logiczny.

Korzystnie, generator metastabilnościowych interwałów czasowych zawiera dwa przerzutniki o dwóch wejściach i pojedynczych wyjściach, przy czym wejścia przerzutników generatora metastabilnościowych interwałów czasowych dołączone są do wejść układu metastabilnościowego w taki sposób, że pierwsze wejście układu metastabilnościowego dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika i pierwszego wejścia drugiego przerzutnika, drugie wejście układu metastabilnościowego dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika i drugiego wejścia drugiego przerzutnika, natomiast arbiter zawiera dwa przerzutniki o dwóch wejściach i dwóch wyjściach każdy, przy czym wyjścia przerzutników generatora metastabilnościowych interwałów czasowych dołączone są do wejść przerzutników arbitra w taki sposób, że wyjście pierwszego przerzutnika generatora metastabilnościowych interwałów czasowych dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika arbitra i drugiego wejścia drugiego przerzutnika arbitra, wyjście drugiego przerzutnika

generatora metastabilnościowych interwałów czasowych dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika arbitra i pierwszego wejścia drugiego przerzutnika arbitra, zaś układ logiczny stanowi bramka koniunkcji, przez którą wybrane wyjścia przerzutników arbitra dołączone są do wyjścia układu metastabilnościowego.

Dzięki zastosowaniu konstrukcji generatora według wynalazku uzyskuje się zaburzenie pracy chaotycznej losowymi zdarzeniami, co stanowi synergistyczny rezultat jednoczesnej realizacji detekcji fazy i generacji liczb losowych wynikających z rozwiązania procesu metastabilnościowego.

Przedmiot wynalazku jest przedstawiony w przykładzie wykonania na rysunku, na którym fig. 1 przedstawia schemat blokowy generatora losowego z generatorem pierścieniowym, generatorem pierścieniowym z przełączaną ścieżką propagacji i układem metastabilnościowym, fig. 2 przedstawia schemat blokowy generatora losowego z dwoma generatorami pierścieniowymi z przełączaną ścieżką propagacji, układem sterującym i układem metastabilnościowym, fig. 3 przedstawia schemat blokowy generatora pierścieniowego, fig. 4 przedstawia schemat blokowy pierwszego generatora pierścieniowego z przełączaną ścieżką propagacji, fig. 5 przedstawia schemat blokowy drugiego generatora pierścieniowego z przełączaną ścieżką propagacji, fig. 6 przedstawia schemat blokowy układu sterującego zbudowanego z elementów opóźniających, fig. 7 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z przerzutnika, fig. 8 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową, fig. 9 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową oraz sumatora, fig. 10 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową, sumatora i układu liczącego, natomiast fig. 11 – schemat blokowy układu metastabilnościowego zbudowanego z generatora metastabilnościowych interwałów czasowych oraz arbitra.

Generator losowy przedstawiony na fig. 1 zawiera generator pierścieniowy GP oraz generator pierścieniowy z przełączaną ścieżką propagacji GPSP, których wyjścia o-GP i o-GPSP dołączone są do wejść i1-UM i i2-UM układu metastabilnościowego UM. Wyjście układu metastabilnościowego o-UM dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji s-GPSP oraz do wyjścia o-GL generatora losowego GL.

Dla większych niż małe przesunięć fazowych sygnałów pochodzących z generatora pierścieniowego GP i generatora pierścieniowego z przełączaną ścieżką propagacji GPSP, układ metastabilnościowy realizuje funkcję detekcji znaku fazy pomiędzy sygnałami tych generatorów. W zależności od tego znaku układ metastabilnościowy UM przełącza częstotliwość generatora pierścieniowego z przełączaną ścieżką propagacji GPSP cyklicznie synchronizując fazę obydwu generatorów pierścieniowych GP i GPSP. Dzięki takiemu sprzężeniu zwrotnemu układ złożony z generatorów pierścieniowych GP i GPSP oraz układu metastabilnościowego UM może pracować w sposób chaotyczny. Natomiast dla małych przesunięć fazowych sygnałów pochodzących z generatora pierścieniowego GP i generatora pierścieniowego z przełączaną ścieżką propagacji GPSP – tj. dla zboczy sygnałów generatora pojawiających się równocześnie lub prawie równocześnie, układ metastabilnościowy generuje na swoim wyjściu wartość losową, przez co korekcja fazy ma charakter także losowy. Im wolniejszy jest układ metastabilnościowy, tym większe przesunięcia fazowe inicjują powstanie zjawisk metastabilnych, które wpływają na losowość działania układu chaotycznego. Dodatkowo, z racji tego, że typowy układ metastabilnościowy używany do detekcji fazy jest wolniejszy od typowego detektora fazy, układ metastabilnościowy wprowadza do pętli sprzężenia zwrotnego opóźnienie, co rozszerza zakres możliwych do uzyskania różnic fazowych pomiędzy dołączonymi do jego wejść generatorami pierścieniowymi.

Generator losowy przedstawiony na fig. 2 zawiera dwa generatory pierścieniowe z przełączaną ścieżką propagacji GPSP i GPSP', których wyjścia o-GPSP i o-GPSP' dołączone są do wejść i1- UM i i2-UM układu metastabilnościowego UM. Wyjście układu metastabilnościowego o-UM dołączone jest do wejścia i-US układu sterującego US, a wyjście układu sterującego o-US dołączone jest do wejść sterujących generatorów pierścieniowych z przełączaną ścieżką propagacji s-GPSP i s-GPSP'. Wyjście o-UM układu metastabilnościowego UM dołączone jest także do wyjścia o-GL generatora losowego GL.

Zastosowanie drugiego generatora pierścieniowego z przełączaną ścieżką propagacji GPSP', pracującego przeciwnie w stosunku do pierwszego generatora pierścieniowego z przełączaną ścieżką propagacji GPSP, poprawia zbieżność korekcji fazy sygnałów pochodzących z tych generatorów. Natomiast dodatkowe opóźnienie wprowadzane przez układ sterujący US do pętli sterowania fazą generatorów powoduje dodatkowe opóźnienie w korekcji fazy, a przez to większy zakres możliwych do uzyskania różnic fazowych sygnałów pochodzących z tych generatorów.

Generator pierścieniowy przedstawiony na fig. 3 zawiera linię opóźniającą LO, której wejście i-LO i wyjście o-LO są ze sobą połączone i dołączone do wyjścia o-GP generatora pierścieniowego GP. Linia opóźniająca LO zawiera elementy opóźniające EO połączone w szereg.

Liczba elementów opóźniających oraz opóźnienie wprowadzane przez każdy element opóźniający determinują podstawową częstotliwość pracy generatora pierścieniowego GP. Częstotliwość podstawowa jest obarczona niestałością, wynikającą ze zjawisk fizycznych – typowych dla układów elektronicznych (zjawiska szumowe, termiczne, jitter itp.).

Generator pierścieniowy z przełączaną ścieżką propagacji przedstawiony na fig. 4 zawiera dwie linie opóźniające LO1 i LO2 oraz multiplekser MUX. Linie opóźniające LO1 i LO2 połączone ze sobą w szereg tak, że wyjście pierwszej linii opóźniającej o-LO1 dołączone jest do wejścia drugiej linii opóźniającej i-LO2. Wyjście drugiej linii o-LO2 dołączone jest do wyjścia o-GPSP generatora pierścieniowego z przełączaną ścieżką propagacji GPSP. Każda z linii opóźniających LO1 i LO2 zawiera elementy opóźniające EO połączone w szeregi. Multiplekser MUX ma dwa wejścia i0-MUX i i1-MUX, które dołączone są do wyjść linii opóźniających o-LO1 i O-LO2. Wyjście multipleksera o-MUX dołączone jest do wejścia pierwszej linii opóźniającej i-LO1. Wejście sterujące multipleksera s-MUX dołączone jest do wejścia sterującego generatora s-GPSP.

Generator GPSP posiada dwie podstawowe częstotliwości pracy, a wybór jednej z nich dokonywany jest przez sygnał sterujący generatora s-GPSP. Podstawowe częstotliwości pracy zależą od liczby elementów opóźniających EO składających się na każdą z linii opóźniających LO1 i LO2, od opóźnień wprowadzanych przez każdy element opóźniający EO oraz od opóźnienia wprowadzanego przez multiplekser MUX. Częstotliwości podstawowe są obarczone niestałością, wynikającą ze zjawisk fizycznych – typowych dla układów elektronicznych (zjawiska szumowe, termiczne, jitter itp.).

Generator pierścieniowy z przełączaną ścieżką propagacji przedstawiony na fig. 5 ma budowę taką jak układ z fig. 4, z tą różnicą, że wejścia i0-MUX i i1-MUX multipleksera MUX są dołączone do wyjść linii opóźniających o-LO1 i O-LO2 na odwrót. Odwrotne dołączenie wyjść linii opóźniających do wejść multipleksera powoduje, że wybrana częstotliwość pracy generatora GPSP' jest przeciwna w stosunku do częstotliwości wybranej w generatorze GPSP.

Układ sterujący przedstawiony na fig. 6 zawiera dwuelementowy szereg złożony z elementów opóźniających EO dołączony pomiędzy wejściem i-US i wyjściem o-US układu sterującego US.

Szereg elementów opóźniających EO wprowadza opóźnienie w sprzężeniu zwrotnym, tj. opóźnienie w przekazywaniu sygnału sterowania korekcją fazy, dzięki czemu zwiększa zakres przesunięć fazowych. Opóźnienie to jest dobierane łącznie z opóźnieniem wprowadzanym przez układ metastabilnościowy.

Układ metastabilnościowy przedstawiony na fig. 7 stanowi przerzutnik Pa o dwóch wejściach Da i Ca stanowiących wejścia i1-UM i i2-UM układu metastabilnościowego UM i wyjściu Qa stanowiącym wyjście układu metastabilnościowego o-UM.

Przerzutnik Pa charakteryzuje się tym, że względne nieduże przesunięcia czasu pomiędzy zboczami dostarczanymi do wejść przerzutnika Da i Ca wprowadzają go w pracę w odpowiednim obszarze metastabilności, czego skutkiem jest losowy stan logiczny na wyjściu Qa. Rodzaj przerzutnika – np. przerzutnik typu „D", przerzutnik „RS", przerzutnik „JK" itp. – ma drugorzędne znaczenie dopóki przerzutnik spełnia dwa warunki: po pierwsze wykrywa pierwszeństwo zboczy sygnałów wejściowych, a po drugie zapewnia losową odpowiedź na swoim wyjściu w przypadku odpowiedniej bliskości zboczy sygnałów wejściowych.

Układ metastabilnościowy przedstawiony na fig. 8 stanowi układ metastabilnościowy z oscylacyjną odpowiedzią impulsową UMOO o dwóch wejściach R i S stanowiących wejścia i1-UM i i2-UM układu metastabilnościowego UM i wyjściu wOO stanowiącym wyjście układu metastabilnościowego o-UM.

Przerzutnik UMOO charakteryzuje się tym, że względne nieduże przesunięcia czasu pomiędzy zboczami dostarczanymi do wejść przerzutnika R i S wprowadzają go w pracę w odpowiednim obszarze metastabilności, czego skutkiem jest oscylacyjna odpowiedź przerzutnika o zmiennej liczbie oscylacji, a także losowym stanie logicznym na wyjściu wOO.

Układ metastabilnościowy przedstawiony na fig. 9 ma budowę taką jak układ z fig. 8, przy czym wyjście wOO układu metastabilnościowego z oscylacyjną odpowiedzią impulsową UMOO dołączone jest do wyjścia układu metastabilnościowego o-UM przez sumator SUM.

Sumator SUM pozwala na zsumowanie zmiennej liczby oscylacji pojawiającej się na wyjściu wOO.

Układ metastabilnościowy przedstawiony na fig. 10 ma budowę taką jak układ z fig. 9, przy czym dodatkowo zawiera układ liczący LCZ, którego wyjścia dołączone są do kolejnych wejść sumatora SUM

oraz którego wejście i-LCZ dołączone jest do wyjścia układu metastabilnościowego z oscylacyjną odpowiedzią impulsową wOO.

Licznik LCZ zlicza liczbę oscylacji pojawiającą się na wyjściu wOO, którą następnie sumuje sumator SUM. Dodatkowo w tym układzie uwzględniany jest stan logiczny na wyjściu wOO.

Układ metastabilnościowy przedstawiony na fig. 11 zawiera generator metastabilnościowych interwałów czasowych GMIC, arbiter ARB oraz układ logiczny AND. Generator metastabilnościowych interwałów czasowych GMIC zawiera dwa przerzutniki Pb i Pc, każdy o dwóch wejściach Db i Cb oraz Dc i Cc, jak również pojedynczych wyjściach Qb i Qc. Arbiter ARB zawiera dwa przerzutniki Pd i Pe, każdy o dwóch wejściach Dd i Cd oraz De i Ce, jak również dwóch wyjściach Qd i nQd oraz Qe i nQe. Układ logiczny AND posiada dwa wejście i jedno wyjście. Wejścia przerzutników generatora metastabilnościowych interwałów czasowych GMIC dołączone są do wejść układu metastabilnościowego UM w taki sposób, że pierwsze wejście układu metastabilnościowego i1-UM dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika Db i pierwszego wejścia drugiego przerzutnika Dc, a drugie wejście układu metastabilnościowego i2-UM dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika Cb i drugiego wejścia drugiego przerzutnika Cc. Wyjścia przerzutników Qb i Qc dołączone są do wejść przerzutników arbitra ARB w taki sposób, że wyjście pierwszego przerzutnika Qb dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika arbitra Dd i drugiego wejścia drugiego przerzutnika arbitra Ce, a wyjście drugiego przerzutnika Qc dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika arbitra Cd i pierwszego wejścia drugiego przerzutnika arbitra De. Wyjście układu metastabilnościowego o-UM dołączone jest do wyjść przerzutników arbitra nQd i Qe przez układ logiczny AND. Wejścia układu logicznego AND dołączone są do drugiego wyjścia pierwszego przerzutnika arbitra nQd oraz pierwszego wyjścia drugiego przerzutnika arbitra Qe. Wyjście układu logicznego AND dołączone jest do wyjścia układu metastabilnościowego o-UM.

Dostarczenie do przerzutników Pb i Pc generatora metastabilnościowych interwałów czasowych GMIC sygnałów cyfrowych o względne niedużych przesunięciach czasu pomiędzy zboczami dostarczanymi do wejść przerzutników, wywołuje w nich stany metastabilne, których rozwiązaniem są wartości logiczne pojawiające się na wyjściach Qb i Qc w różnych momentach czasu. Zarówno wartości logiczne, jak i interwały czasowe są źródłami losowości o określonych właściwościach tych losowości. Arbiter porównuje czasy odpowiedzi przerzutników Pb i Pc, a wynik tego porównania – który jest wartością losową – jest interpretowany przez układ logiczny AND jako logiczne zero lub logiczna jedynka.

Możliwości zastosowania wynalazku przewiduje się w generowaniu liczb i ciągów liczbowych prawdziwie losowych.

Unikalną cechą wynikającą z zastosowania wynalazku jest to, że bardzo prosta konstrukcja jednocześnie: wywołuje pracę chaotyczną układu, wywołuje sporadyczne losowe odpowiedzi metastabilnościowe, zaburza tymi losowymi zdarzeniami pracę chaotyczną, jak również zmniejsza liczbę potrzebnych elementów opóźniających w układzie sterującym z powodu opóźnień wprowadzanych przez układ metastabilnościowy. Tak synergiczne połączenie elementów układu i zmniejszenie jego kosztów implementacyjnych oraz współdzielona realizacja funkcji detekcji fazy i generacji liczb losowych wynikających z rozwiązania procesu metastabilnościowego przeczy wiedzy znawców z dziedziny generatorów losowych.

Zastrzeżenia patentowe

1. Generator losowy (GL) zawierający układ metastabilnościowy (UM), którego wyjście (o-UM) jest dołączone do wyjścia (o-GL) generatora losowego (GL) oraz zawierający przynajmniej dwa generatory pierścieniowe (GP), których wyjścia dołączone są do wejść (i1-UM, i2-UM) układu metastabilnościowego (UM) oraz przynajmniej jeden z generatorów pierścieniowych (GP) stanowi generator pierścieniowy z przełączaną ścieżką propagacji (GPSP, GPSP') z wejściem sterującym (s-GPSP, s-GPSP'), **znamienny tym**, że wyjście układu metastabilnościowego (o-UM) dołączone jest do wejścia sterującego (s-GPSP, s-GPSP') przynajmniej jednego generatora pierścieniowego z przełączaną ścieżką propagacji (GPSP, GPSP').
2. Generator losowy według zastrz. 1 **znamienny tym**, że wyjście (o-UM) układu metastabilnościowego (UM) dołączone jest do przynajmniej jednego wejścia sterującego (s-GPSP, s-GPSP') generatorów pierścieniowych z przełączaną ścieżką propagacji (GPSP, GPSP') przez układ sterujący (US).

3. Generator losowy według zastrz. od 1 albo 2 **znamienny tym**, że przynajmniej jeden generator pierścieniowy (GP) zawiera przynajmniej jedną linię opóźniającą (LO), której wejście (i-LO) i wyjście (o-LO) są ze sobą połączone i dołączone do wyjścia generatora pierścieniowego (o-GP), przy czym linia opóźniająca (LO) zawiera elementy opóźniające (EO) połączone w szereg.
4. Generator losowy według zastrz. 1 albo 2, albo 3 **znamienny tym**, że generator pierścieniowy z przełączaną ścieżką propagacji (GPSP, GPSP') zawiera przynajmniej dwie linie opóźniające (LO1, LO2, LO1', LO2') połączone ze sobą tak, że wyjście pierwszej linii opóźniającej (o-LO1, o-LO1') dołączone jest do wejścia drugiej linii opóźniającej (i-LO2, i-LO2'), oraz że wyjście jednej z tych linii opóźniających (o-LO2, o-LO2') dołączone jest do wyjścia generatora pierścieniowego z przełączaną ścieżką propagacji (o-GPSP, o-GPSP'), przy czym linie opóźniające (LO1, LO2, LO1', LO2') zawierają elementy opóźniające (EO) połączone w szeregi.
5. Generator losowy według zastrz. 4 **znamienny tym**, że generator pierścieniowy z przełączaną ścieżką propagacji (GPSP, GPSP') zawiera przynajmniej jeden multiplekser (MUX, MUX'), którego wejście sterujące (s-MUX, s-MUX') dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji (s-GPSP, s-GPSP'), oraz którego wyjście (o-MUX, o-MUX') dołączone jest do wejścia jednej linii opóźniającej (i-LO1, i-LO1'), oraz którego wejścia (i0-MUX, i1-MUX, i1-MUX', i0-MUX') dołączone są wejścia i wyjścia innej linii opóźniającej (o-LO2, i-LO2, o-LO2', i-LO2').
6. Generator losowy według zastrz. od 2 do 5 **znamienny tym**, że przynajmniej jeden układ sterujący (US) przynajmniej jeden element opóźniający (EO).
7. Generator losowy według zastrz. od 1 do 6 **znamienny tym**, że układ metastabilnościowy (UM) stanowi przerzutnik (Pa) o dwóch wejściach (Da, Ca) stanowiących wejścia układu metastabilnościowego (i1-UM, i2-UM) i wyjściu (Qa) stanowiącym wyjście układu metastabilnościowego (o-UM).
8. Generator losowy według zastrz. od 1 do 6 **znamienny tym**, że układ metastabilnościowy (UM) zawiera układ metastabilnościowy z oscylacyjną odpowiedzią impulsową (UMOO) o dwóch wejściach (R, S) stanowiących wejścia układu metastabilnościowego (i1-UM, i2-UM) i wyjściu (wOO) stanowiącym wyjście układu metastabilnościowego (o-UM).
9. Generator losowy według zastrz. 8 **znamienny tym**, że wyjście układu metastabilnościowego z oscylacyjną odpowiedzią impulsową (wOO) dołączone jest do wyjścia układu metastabilnościowego (o-UM) przez sumator (SUM).
10. Generator losowy według zastrz. 9 **znamienny tym**, że zawiera układ liczący (LCZ), którego wyjścia dołączone są do kolejnych wejść sumatora (SUM), a którego wejście (i-LCZ) dołączone jest do wyjścia układu metastabilnościowego z oscylacyjną odpowiedzią impulsową (wOO).
11. Generator losowy według zastrz. od 1 do 6 **znamienny tym**, że układ metastabilnościowy (UM) zawiera generator metastabilnościowych interwałów czasowych (GMIC) o wejściach dołączonych do wejść układu metastabilnościowego (i1-UM, i2-UM) oraz wyjściach dołączonych do wejść arbitra (ARB), którego wyjścia dołączone są do wyjść układu metastabilnościowego (o-UM) przez układ logiczny (AND).
12. Generator losowy według zastrz. 11 **znamienny tym**, że generator metastabilnościowych interwałów czasowych (GMIC) zawiera dwa przerzutniki (Pb), (Pc) o dwóch wejściach (Db, Cb), (Dc, Cc) i pojedynczych wyjściach (Qb), (Qc), przy czym wejścia przerzutników generatora metastabilnościowych interwałów czasowych (GMIC) dołączone są do wejść układu metastabilnościowego (UM) w taki sposób, że pierwsze wejście układu metastabilnościowego (i1-UM) dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika (Db) i pierwszego wejścia drugiego przerzutnika (Dc), drugie wejście układu metastabilnościowego (i2-UM) dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika (Cb) i drugiego wejścia drugiego przerzutnika (Cc), oraz że arbiter (ARB) zawiera dwa przerzutniki (Pd), (Pe) o dwóch wejściach (Dd, Cd), (De, Ce) i dwóch wyjściach (Qd, nQd), (Qe, nQe) każdy, przy czym wyjścia przerzutników generatora metastabilnościowych interwałów czasowych (GMIC) dołączone są do wejść przerzutników arbitra (ARB) w taki sposób, że wyjście pierwszego przerzutnika generatora metastabilnościowych interwałów czasowych (Qb) dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika arbitra (Dd) i drugiego wejścia drugiego przerzutnika arbitra (Ce), wyjście drugiego przerzutnika generatora metastabilnościowych interwałów czasowych (Qc) dołączone jest jednocześnie do drugiego

wejścia pierwszego przerzutnika arbitra (Cd) i pierwszego wejścia drugiego przerzutnika arbitra (De), oraz że układ logiczny (AND) stanowi bramka koniunkcji, przez którą wybrane wyjścia przerzutników arbitra (nQd, Qe) dołączone są do wyjścia układu metastabilnościowego (o-UM).

Rysunki

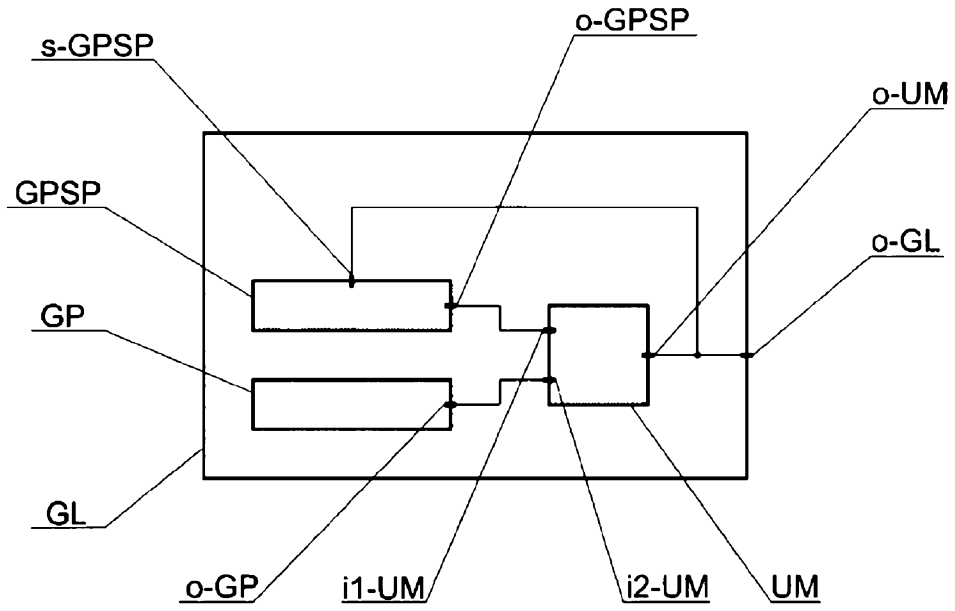

Fig. 1

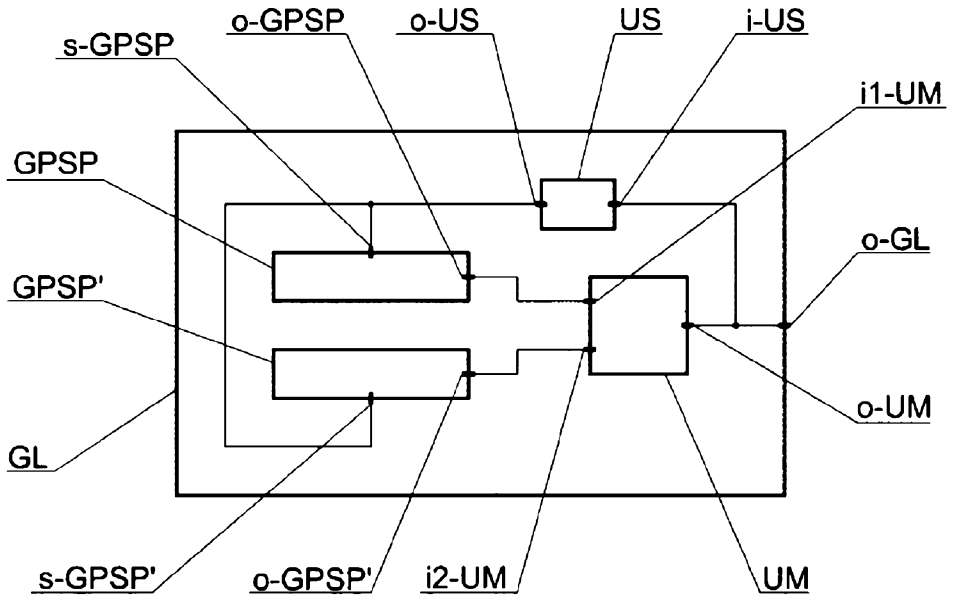

Fig. 2

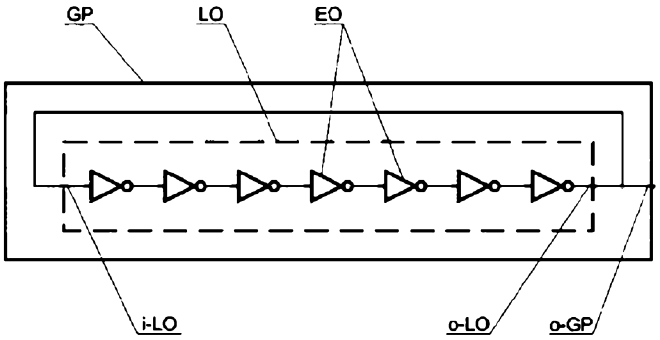

Fig. 3

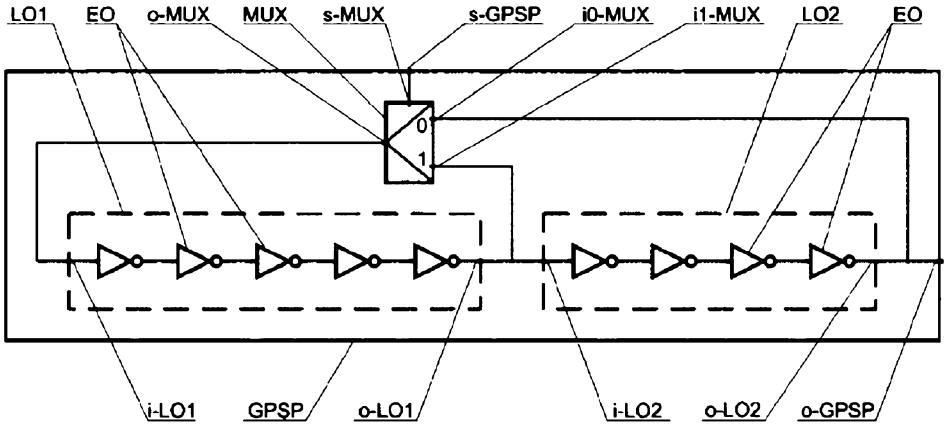

Fig. 4

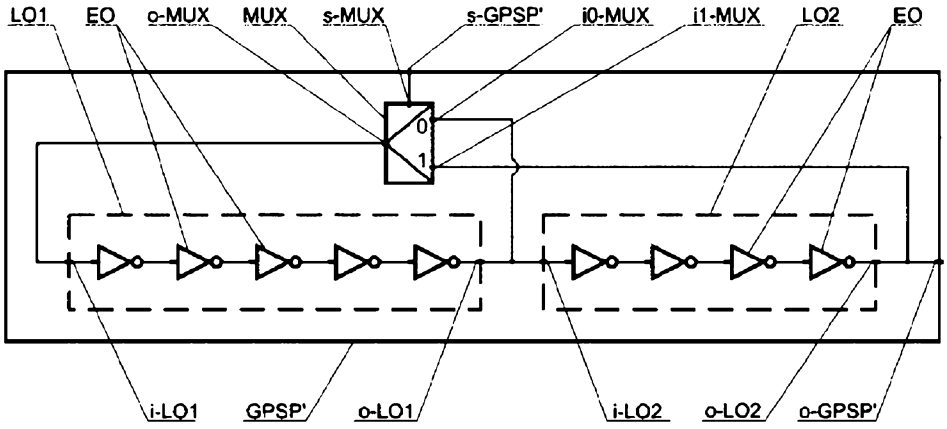

Fig. 5

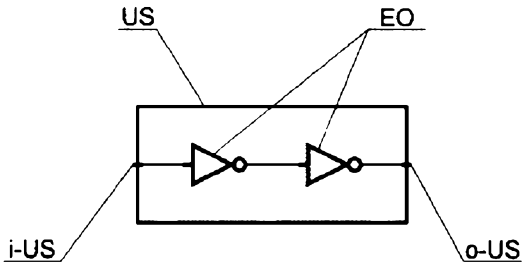

Fig. 6

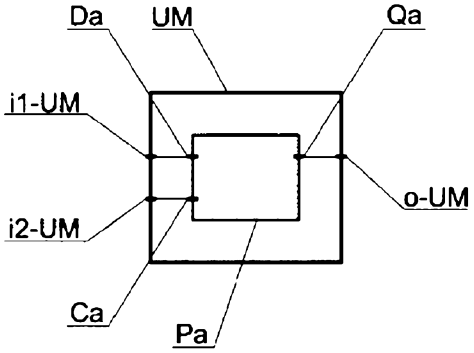

Fig. 7

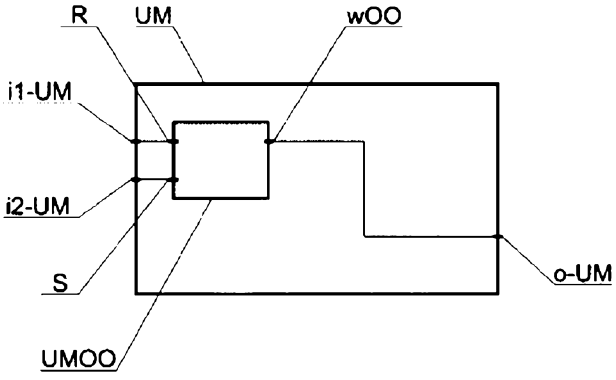

Fig. 8

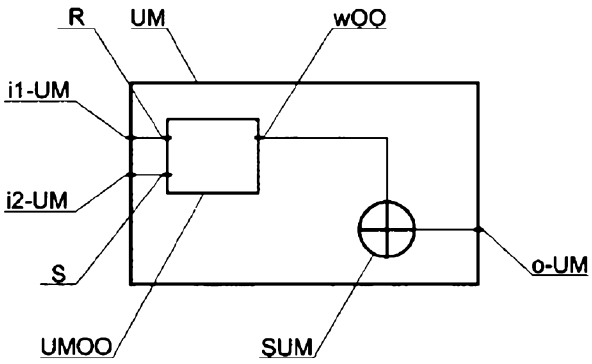

Fig. 9

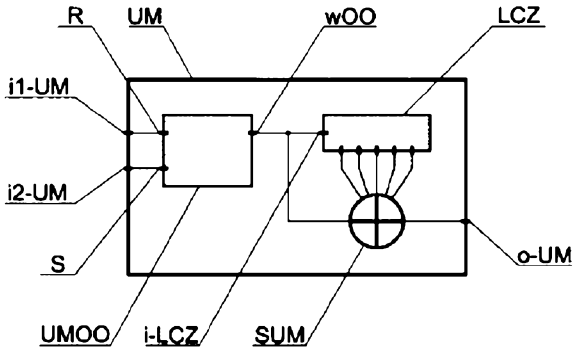

Fig. 10

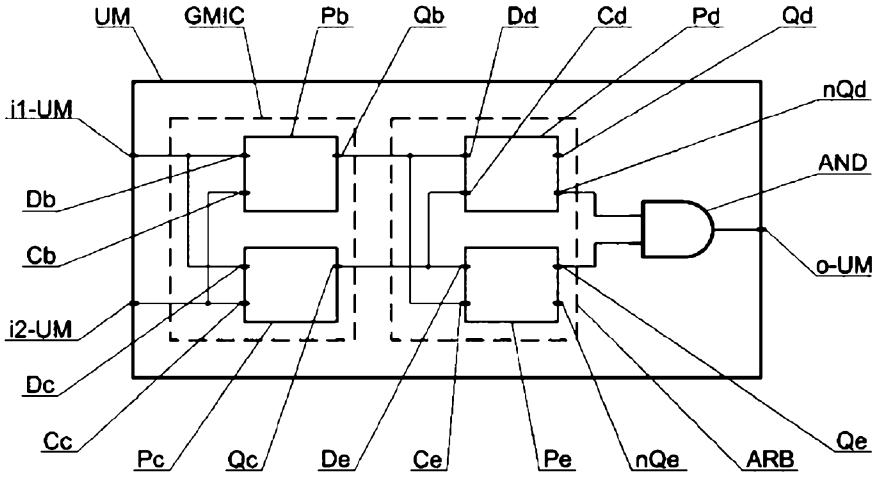

Fig. 11