RZECZPOSPOLITA POLSKA

Urząd Patentowy Rzeczypospolitej Polskiej

(12) **OPIS PATENTOWY** (19) **PL** (11) **237196**

(13) **B1**

(21) Numer zgłoszenia: **422490**

(22) Data zgłoszenia: **08.08.2017**

(51) Int.Cl.
G06F 7/58 (2006.01)
H03K 3/84 (2006.01)

(54) **Generator losowy**

(43) Zgłoszenie ogłoszono:
11.02.2019 BUP 04/19

(45) O udzieleniu patentu ogłoszono:
22.03.2021 WUP 06/21

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

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

(74) Pełnomocnik:
rzecz. pat. Oliwia Czarnocka

PL 237196 B1

Opis wynalazku

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

Znany jest w technice, 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.

Znane są z opisu patentowego WO0161854A1 generator losowych impulsów i układy generujące wykorzystujące co najmniej trzy oscylatory. Sygnały wyjściowe co najmniej dwóch oscylatorów są łączone, aby zakłócać sygnał wyjściowy końcowego oscylatora. W przypadku jednej konfiguracji połączone sygnały wyjściowe co najmniej dwóch oscylatorów przesunięcia fazowego są wykorzystywane do modyfikacji sygnału sprzężenia zwrotnego końcowego oscylatora przesunięcia fazowego, zakłócając w ten sposób sygnał wyjściowy końcowego oscylatora. W innej konfiguracji sygnały wyjściowe co najmniej dwóch oscylatorów z przesunięciem fazowym są używane do napędzania subtraktora, którego sygnał wyjściowy jest łączony z sygnałem wyjściowym z końcowego oscylatora z przesunięciem fazowym do napędzania kolejnego subtraktora, zakłócając w ten sposób sygnał wyjściowy z końcowego oscylatora.

Znane jest z amerykańskiego opisu patentowego US2009077147A1 wielobitowe próbkowanie drgań oscylatora do generowania liczb losowych, w którym układ zawiera oscylator, licznik do zliczania impulsów i zatrzask do blokowania licznika w odpowiedzi na zmiany poziomu logicznego wyjścia oscylatora. Urządzenie może ponadto zawierać detektor krawędzi do wytwarzania sygnału zatrzaskowego w odpowiedzi na zmiany poziomu logicznego wyjścia oscylatora.

Celem wynalazku jest niedeterministyczna inicjalizacja procesu metastabilnościowego, wywołanie procesu chaotycznego oraz uzyskanie losowego zaburzenia działania procesu chaotycznego.

Istota układu według wynalazku polega na tym, że generator losowy posiada detektor fazy, którego wejścia dołączone ma do wyjść generatorów pierścieniowych, oraz że przynajmniej jeden generator pierścieniowy jest generatorem pierścieniowym z przełączaną ścieżką propagacji, oraz że wyjście detektora fazy dołączone ma do przynajmniej jednego wejścia sterującego generatorów pierścieniowych z przełączanymi ścieżkami propagacji, że to wyjście dołączone jest przez układ sterujący, że do wejścia układu sterującego dołączone jest wyjście układu metastabilnościowego.

Generator pierścieniowy ma przynajmniej jedną linię opóźniającą, której wejście i wyjście ma ze sobą połączone i dołączone do wyjścia generatora pierścieniowego oraz że linia opóźniająca ma elementy opóźniające połączone w szereg. Generator pierścieniowy z przełączaną ścieżką propagacji ma 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. Linie opóźniające mają elementy opóźniające połączone w szeregi. Generator pierścieniowy z przełączaną ścieżką propagacji ma multiplekser, którego wejście sterujące ma dołączone do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji, wyjście ma dołączone do wejścia jednej linii opóźniającej, a wejścia ma dołączone do wejścia i wyjścia innej linii opóźniającej.

Układ sterujący ma przynajmniej jeden element opóźniający, a elementy opóźniające połączone są w szereg. Układ sterujący stanowi bramka dodawania losowości, której pierwsze wejście stanowi wejście danych losowych układu sterującego, drugie wejście stanowi wejście sygnałowe układu sterującego, a wyjście bramki dodawania losowości stanowi wyjście układu sterującego. Układ sterujący ma pierwsze wejście bramki dodawania losowości dołączone do wejścia danych losowych układu sterującego przez układ bramkujący, a do układu bramkującego dołączony jest układ sterowania bramkowaniem. Układ sterujący ma drugie wejście bramki dodawania losowości i jej wyjście połączone w szereg z co najmniej jednym elementem opóźniającym, przy czym wejście pierwszego w szeregu elementu dołączone jest do wejścia sygnałowego układu sterującego, a wyjście ostatniego w szeregu elementu dołączone jest do wyjścia układu sterującego.

Detektor fazy stanowi przerzutnik o dwóch wejściach stanowiących wejścia detektora fazy i wyjściu stanowiącym wyjście detektora fazy. Detektor fazy ma dwa przerzutniki o dwóch wejściach i dwóch

wyjściach każdy, ma wejścia przerzutników dołączone do wejść detektora fazy, ma wyjścia przerzutników dołączone do wyjść detektora fazy, przy czym pierwsze wejście detektora fazy dołączone ma jednocześnie do pierwszego wejścia pierwszego przerzutnika i drugiego wejścia drugiego przerzutnika, drugie wejście detektora fazy dołączone ma jednocześnie do drugiego wejścia pierwszego przerzutnika i pierwszego wejścia drugiego przerzutnika, a wyjście detektora fazy dołączone ma do wybranych wyjść przerzutników przez układ logiczny.

Układ metastabilnościowy stanowi przerzutnik o dwóch wejściach stanowiących wejścia układu metastabilnościowego i wyjściu stanowiącym wyjście układu metastabilnościowego. Układ metastabilnościowy stanowi układ metastabilnościowy z oscylacyjną odpowiedzią impulsową o dwóch wejściach stanowiących wejścia układu metastabilnościowego i wyjściu stanowiącym wyjście układu metastabilnościowego. Układ metastabilnościowy z oscylacyjną odpowiedzią impulsową ma wyjście dołączone do wyjścia układu metastabilnościowego przez sumator oraz ma układ liczący, którego wyjścia dołączone są do kolejnych wejść sumatora, a którego wejście dołączone jest do wyjścia układu metastabilnościowego z oscylacyjną odpowiedzią impulsową. Układ metastabilnościowy ma generator metastabilnościowych interwałów czasowych o wejściach dołączonych do wejść układu metastabilnościowego oraz wyjściach dołączonych do wejść arbitra, którego wyjścia dołączone ma do wyjść układu metastabilnościowego przez układ logiczny. Układ metastabilnościowy ma generator metastabilnościowych interwałów czasowych, który ma dwa przerzutniki o dwóch wejściach i pojedynczych wyjściach, ma arbiter, który ma dwa przerzutniki o dwóch wejściach i dwóch wyjściach każdy, oraz ma układ logiczny. 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. 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, natomiast wyjście układu metastabilnościowego dołączone jest do wybranych wyjść przerzutników arbitra przez układ logiczny.

Wynalazek umożliwia generację liczb i ciągów losowych dzięki niestabilności rozwiązania procesu metastabilnościowego oraz dzięki korekcji i niestabilności korekcji fazy generatorów pierścieniowych.

Przedmiot wynalazku jest przedstawiony w przykładzie wykonania na rysunku, na którym fig. 1 przedstawia schemat blokowy generatora losowego z generatorem pierścieniowym i generatorem pierścieniowym z przełączaną ścieżką propagacji, układem metastabilnościowym oraz detektorem fazy, fig. 2 przedstawia schemat blokowy generatora losowego z dwoma generatorami pierścieniowymi z przełączanymi ścieżkami propagacji, układem metastabilnościowym, detektorem fazy oraz układem sterującym o pojedynczym wejściu, fig. 3 przedstawia schemat blokowy generatora losowego z generatorem pierścieniowym i generatorem pierścieniowym z przełączaną ścieżką propagacji, układem metastabilnościowym, detektorem fazy oraz układem sterującym o dwóch wejściach, fig. 4 przedstawia schemat blokowy generatora losowego z dwoma generatorami pierścieniowymi z przełączanymi ścieżkami propagacji, układem metastabilnościowym, detektorem fazy oraz układem sterującym o dwóch wejściach, fig. 5 przedstawia schemat blokowy generatora pierścieniowego, fig. 6 przedstawia schemat blokowy pierwszego generatora pierścieniowego z przełączaną ścieżką propagacji, fig. 7 przedstawia schemat blokowy drugiego generatora pierścieniowego z przełączaną ścieżką propagacji, fig. 8 przedstawia schemat blokowy układu sterującego zbudowanego z elementów opóźniających, fig. 9 przedstawia schemat blokowy układu sterującego zbudowanego z bramki dodawania losowości, fig. 10 przedstawia schemat blokowy układu sterującego zbudowanego z bramki dodawania losowości oraz układu bramkującego, fig. 11 przedstawia schemat blokowy układu sterującego zbudowanego z bramki dodawania losowości oraz elementów opóźniających, fig. 12 przedstawia schemat blokowy układu sterującego zbudowanego z bramki dodawania losowości, układu bramkującego i elementów opóźniających, fig. 13 przedstawia schemat blokowy detektora fazy zbudowanego z jednego przerzutnika, fig. 14 przedstawia schemat blokowy detektora fazy zbudowanego z dwóch przerzutników, fig. 15 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z przerzutnika, fig. 16 przedstawia schemat

blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową, fig. 17 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową oraz sumatora, fig. 18 przedstawia schemat blokowy układu metastabilnościowego zbudowanego z układu metastabilnościowego z oscylacyjną odpowiedzią impulsową, sumatora i układu liczącego, a fig. 19 – 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-DF i i2-DF detektora fazy DF oraz do wejść i1-UM i i2-UM układu metastabilnościowego UM. Wyjście detektora fazy o-DF dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji s-GPSP. Wyjście o-UM układu metastabilnościowego UM dołączone jest do wyjścia o-GL generatora losowego GL.

Detektor fazy DF przełącza częstotliwość generatora pierścieniowego z przełączaną ścieżką propagacji GPSP cyklicznie zmieniając lub synchronizując fazę obydwu generatorów GP i GPSP. Bliskość faz generatorów oznacza czasową bliskość zboczy generowanych sygnałów, które służą do pobudzenia układu metastabilnościowego UM, który wytwarza zjawisko losowe. Układ złożony z generatorów GP i GPSP oraz detektora fazy DF jest układem chaotycznym.

Generator losowy przedstawiony na fig. 2 zawiera dwa generatory pierścieniowe z przełączanymi ścieżkami propagacji GPSP i GPSP', których wyjścia o-GPSP i o-GPSP' dołączone są do wejść i1-DF i i2-DF detektora fazy DF oraz do wejść i1-UM i i2-UM układu metastabilnościowego UM. Wyjście detektora fazy o-DF dołączone jest do wejścia i-US układu sterującego US, a wyjście układu sterującego o-US dołączone jest do wejść sterujących generatorów pierścieniowych z przełączanymi ścieżkami propagacji s-GPSP i s-GPSP' cyklicznie zmieniając lub synchronizując fazę obydwu generatorów. Wyjście o-UM układu metastabilnościowego UM dołączone jest do wyjścia o-GL generatora losowego GL.

Opóźnienie wprowadzane przez układ sterujący US do pętli sterowania fazą generatorów poprawia chaotyczne właściwości działania układu. Zastosowanie drugiego generatora pierścieniowego z przełączaną ścieżką propagacji GPSP', pracującego przeciwnie w stosunku do pierwszego generatora pierścieniowego z przełączaną ścieżką propagacji GPSP, poprawia chaotyczne właściwości działania układu oraz zbieżność faz generatorów.

Generator losowy przedstawiony na fig. 3 zawiera generator pierścieniowy GP oraz generator pierścieniowy z przełączaną ścieżką propagacji GPSP, których wyjścia o-GP i o-GPSP dołączone są do wejść i1-DF i i2-DF detektora fazy DF oraz do wejść i1-UM i i2-UM układu metastabilnościowego UM. Wyjście detektora fazy o-DF dołączone jest do głównego wejścia i-US' układu sterującego US', wyjście układu metastabilnościowego o-UM dołączone jest do dodatkowego wejścia układu sterującego r-US', a wyjście układu sterującego o-US' dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji s-GPSP. Wyjście o-UM układu metastabilnościowego UM dołączone jest do wyjścia o-GL generatora losowego GL.

Dzięki zastosowaniu dodatkowego wejścia układu sterującego r-US' do układu chaotycznego złożonego z generatorów GP i GPSP, detektora fazy DF i układu sterującego US' może być dodawany sygnał losowy wytwarzany przez układ metastabilnościowy UM.

Generator losowy przedstawiony na fig. 4 zawiera dwa generatory pierścieniowe z przełączanymi ścieżkami propagacji GPSP i GPSP', których wyjścia o-GPSP i o-GPSP' dołączone są do wejść i1-DF i i2-DF detektora fazy DF oraz do wejść i1-UM i i2-UM układu metastabilnościowego UM. Wyjście detektora fazy o-DF dołączone jest do głównego wejścia i-US' układu sterującego US', wyjście układu metastabilnościowego o-UM dołączone jest do dodatkowego wejścia układu sterującego r-US', a wyjście układu sterującego o-US' dołączone jest do wejść sterujących generatorów pierścieniowych z przełączanymi ścieżkami propagacji s-GPSP i s-GPSP'. Wyjście o-UM układu metastabilnościowego UM dołączone jest 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 chaotyczne właściwości działania układu oraz zbieżność faz generatorów.

Generator pierścieniowy przedstawiony na fig. 5 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. 6 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. 7 ma budowę taką jak układ z fig. 6, z tą różnicą, że wejścia i0-MUX i i1-MUX multipleksera MUX są dołączone są 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. 8 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 poprawia chaotyczne właściwości działania układu.

Układ sterujący przedstawiony na fig. 9 stanowi bramka dodawania losowości XOR', której pierwsze wejście stanowi wejście danych losowych r-US' układu sterującego US', drugie wejście bramki stanowi wejście sygnałowe układu sterującego i-US', a wyjście bramki stanowi wyjście układu sterującego o-US'.

Bramka XOR' wprowadza opóźnienie dla sygnału przekazywanego pomiędzy wejściem i-US' i wyjściem o-US' oraz dodaje do tego sygnału wartość losową dostarczaną do wejścia danych losowych układu sterującego r-US'.

Układ sterujący przedstawiony na fig. 10 ma budowę taką jak układ z fig. 9, w którym pierwsze wejście bramki dodawania losowości XOR' dołączone jest do wejścia danych losowych układu sterującego r-US' przez układ bramkujący AND' oraz do układu bramkującego AND' dołączony jest układ sterowania bramkowaniem LCZ'.

Układ bramkujący AND' wraz z układem sterowania bramkowaniem LCZ' dopuszczają jedynie wybrane wartości losowe dostarczane do wejścia danych losowych układu sterującego r-US'. Na przykład układ sterowania bramkowaniem LCZ' może być wykonany w postaci licznika, który będzie dopuszczał jedynie co którąś wartość losową.

Układ sterujący przedstawiony na fig. 11 ma budowę taką jak układ z fig. 10, w którym wyjście bramki dodawania losowości XOR' dołączone jest do wyjścia układu sterującego o-US' przez dwuelementowy szereg złożony z elementów opóźniających EO.

Szereg elementów opóźniających EO wraz z bramką dodawania losowości XOR' wprowadzają dodatkowe opóźnienie dla sygnału przekazywanego pomiędzy wejściem i-US' i wyjściem o-US' układu sterującego. Opóźnienie to wpływa na charakterystykę chaotycznego zachowania układu. Miejsce dołączenia bramki dodawania losowości XOR' względem elementów opóźniających EO, będące miejscem w szeregu elementów pomiędzy wejściem sygnałowym i-US' a wyjściem układu sterującego o-US', wpływa na moment wprowadzenia losowości do układu chaotycznego.

Układ sterujący przedstawiony na fig. 12 jest połączeniem układów sterujących z fig. 10 oraz fig. 11, za wyjątkiem miejsca dołączenia bramki dodawania losowości XOR' względem elementów opóźniających EO, która w tym układzie znajduje się pomiędzy elementami opóźniającymi.

Detektor fazy przedstawiony na fig. 13 stanowi przerzutnik P o dwóch wejściach D i C stanowiących wejścia i1-DF i i2-DF detektora fazy DF i wyjściu Q stanowiącym wyjście detektora fazy o-DF.

W zależności od tego, czy narastające zbocze na wejściu D przerzutnika nadejdzie przed czy po narastającym zboczu na wejściu C przerzutnika, na wyjściu Q pojawi się logiczna jedynka lub logiczne zero.

Detektor fazy przedstawiony na fig. 14 zawiera układ logiczny AND o dwóch wejściach i jednym wyjściu oraz dwa przerzutniki P1 i P2, każdy o dwóch wejściach D1 i C1 oraz D2 i C2 jak również dwóch wyjściach Q1 i nQ1 oraz Q2 i nQ2. Wejścia przerzutników dołączone są do wejść detektora fazy DF, natomiast wyjścia przerzutników dołączone do wyjść detektora fazy przez układ logiczny AND. Pierwsze wejście detektora fazy i1-DF dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika D1 i drugiego wejścia drugiego przerzutnika C2. Drugie wejście detektora fazy i2-DF dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika C1, i pierwszego wejścia drugiego przerzutnika D2. Wejścia układu logicznego AND dołączone są do drugiego wyjścia pierwszego przerzutnika nQ1 oraz pierwszego wyjścia drugiego przerzutnika Q2. Wyjście układu logicznego AND dołączone jest do wyjścia detektora fazy o-DF.

Detektor fazy zbudowany z dwóch przerzutników pozwala na symetryczną detekcję ujemnych i dodatnich przesunięć fazowych.

Układ metastabilnościowy przedstawiony na fig. 15 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 jest 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.

Układ metastabilnościowy przedstawiony na fig. 16 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. 17 ma budowę taką jak układ z fig. 16, 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. 18 ma budowę taką jak układ z fig. 17, 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. 19 zawiera generator metastabilnościowych interwałów czasowych GMIC, arbiter ARB oraz układ logiczny AND. Generator metastabilnościowych interwałów czasowych GMIC zawiera dwa przerzutniki Pb i Pe, 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.

Zastrzeżenia patentowe

1. Generator losowy zawierający układ metastabilnościowy, którego wyjście jest dołączone do wyjścia generatora losowego oraz zawierający dwa generatory pierścieniowe, których wyjścia dołączone są do wejść układu metastabilnościowego, **znamienny tym**, że posiada detektor fazy (DF), którego wejścia (i1-DF, i2-DF) dołączone są do wyjść generatorów pierścieniowych (o-GP, o-GPSP, o-GPSP'), oraz że przynajmniej jeden generator pierścieniowy jest generatorem pierścieniowym z przełączaną ścieżką propagacji (GPSP, GPSP'), oraz że wyjście detektora fazy (o-DF) dołączone jest do przynajmniej jednego wejścia sterującego generatorów pierścieniowych z przełączanymi ścieżkami propagacji (s-GPSP).
2. Generator losowy według zastrz. 1, **znamienny tym**, że wyjście detektora fazy (o-DF) dołączone jest do przynajmniej jednego wejścia sterującego generatorów pierścieniowych z przełączanymi ścieżkami propagacji (s-GPSP, s-GPSP') przez układ sterujący (US).
3. Generator losowy według zastrz. 1, **znamienny tym**, że wyjście detektora fazy (o-DF) dołączone jest do przynajmniej jednego wejścia sterującego generatorów pierścieniowych z przełączanymi ścieżkami propagacji (s-GPSP, s-GPSP') przez układ sterujący (US'), oraz że do wejścia (r-US') układu sterującego (US') dołączone jest wyjście (o-UM) układu metastabilnościowego (UM).
4. Generator losowy według zastrz. 1, **znamienny tym**, że 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.
5. Generator losowy według zastrz. 1, **znamienny tym**, że generator pierścieniowy z przełączaną ścieżką propagacji (GPSP, GPSP') zawiera przynajmniej dwie linie opóźniające (LO1, LO2) połączone ze sobą tak, że wyjście pierwszej linii opóźniającej (o-LO1) dołączone jest do wejścia drugiej linii opóźniającej (i-LO2), oraz że wyjście jednej z tych linii opóźniających (o-LO2) dołączone jest do wyjścia generatora pierścieniowego z przełączaną ścieżką propagacji (o-GPSP, o-GPSP'), przy czym linie opóźniające (LO1, LO2) zawierają elementy opóźniające (EO) połączone w szeregi.
6. Generator losowy według zastrz. 5, **znamienny tym**, że generator pierścieniowy z przełączaną ścieżką propagacji (GPSP, GPSP') zawiera multiplekser (MUX), którego wejście sterujące (s-MUX) dołączone jest do wejścia sterującego generatora pierścieniowego z przełączaną ścieżką propagacji (s-GPSP, s-GPSP'), oraz którego wyjście (o-MUX) dołączone jest do wejścia jednej linii opóźniającej (i-LO1), oraz którego wejścia (i0-MUX, i1-MUX) dołączone są wejścia i wyjścia innej linii opóźniającej (o-LO2, i-LO2).
7. Generator losowy według zastrz. 2, **znamienny tym**, że układ sterujący (US) zawiera przynajmniej jeden element opóźniający (EO), oraz elementy opóźniające (EO) połączone są w szereg.
8. Generator losowy według zastrz. 3, **znamienny tym**, że układ sterujący (US') stanowi bramka dodawania losowości (XOR'), której pierwsze wejście stanowi wejście danych loso-

wych układu sterującego (r-US'), drugie wejście stanowi wejście sygnałowe układu sterującego (i-US'), a wyjście bramki dodawania losowości (XOR') stanowi wyjście układu sterującego (o-US').

9. Generator losowy według zastrz. 8, **znamienny tym**, że pierwsze wejście bramki dodawania losowości (XOR') dołączone jest do wejścia danych losowych układu sterującego (r-US') przez układ bramkujący (AND'), oraz że do układu bramkującego (AND') dołączony jest układ sterowania bramkowaniem (LCZ').
10. Generator losowy według zastrz. 8, **znamienny tym**, że drugie wejście bramki dodawania losowości (XOR') oraz jej wyjście połączone są w szereg z co najmniej jednym elementem opóźniającym (EO'), przy czym wejście pierwszego w szeregu elementu dołączone jest do wejścia sygnałowego układu sterującego (i-US'), a wyjście ostatniego w szeregu elementu dołączone jest do wyjścia układu sterującego (o-US').
11. Generator losowy według zastrz. 8, **znamienny tym**, że pierwsze wejście bramki dodawania losowości (XOR') dołączone jest do wejścia danych losowych układu sterującego (r-US') przez układ bramkujący (AND'), oraz że do układu bramkującego (AND') dołączony jest układ sterowania bramkowaniem (LCZ'), oraz że drugie wejście bramki dodawania losowości (XOR') oraz jej wyjście połączone są w szereg z co najmniej jednym elementem opóźniającym (EO'), przy czym wejście pierwszego w szeregu elementu dołączone jest do wejścia sygnałowego układu sterującego (i-US'), a wyjście ostatniego w szeregu elementu dołączone jest do wyjścia układu sterującego (o-US').
12. Generator losowy według zastrz. 1, **znamienny tym**, że detektor fazy (DF) stanowi przerzutnik (P) o dwóch wejściach (D, C) stanowiących wejścia detektora fazy (i1-DF, i2-DF) i wyjściu (Q) stanowiącym wyjście detektora fazy (o-DF).
13. Generator losowy według zastrz. 1, **znamienny tym**, że detektor fazy (DF) zawiera dwa przerzutniki (P1), (P2) o dwóch wejściach (D1, C1), (D2, C2) i dwóch wyjściach (Q1, nQ1), (Q2, nQ2) każdy, który ma wejścia przerzutników dołączone do wejść detektora fazy i który ma wyjścia przerzutników dołączone do wyjść detektora fazy, przy czym pierwsze wejście detektora fazy (i1-DF) dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika (D1) i drugiego wejścia drugiego przerzutnika (C2), drugie wejście detektora fazy (i2-DF) dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika (C1) i pierwszego wejścia drugiego przerzutnika (D2), a wyjście detektora fazy (o-DF) dołączone jest do wybranych wyjść przerzutników (nQ1, Q2) przez układ logiczny (AND).
14. Generator losowy według zastrz. 1, **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).
15. Generator losowy według zastrz. 1, **znamienny tym**, że układ metastabilnościowy (UM) stanowi 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).
16. Generator losowy według zastrz. 15, **znamienny tym**, że wyjście układu metastabilnościowego z oscylacyjną odpowiedzią impulsową (wOO) dołączone jest do wyjścia układu metastabilnościowego (o-UM) przez sumator (SUM).
17. Generator losowy według zastrz. 16, **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).
18. Generator losowy według zastrz. 1, **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).
19. Generator losowy według zastrz. 18, **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 genera-

tora 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

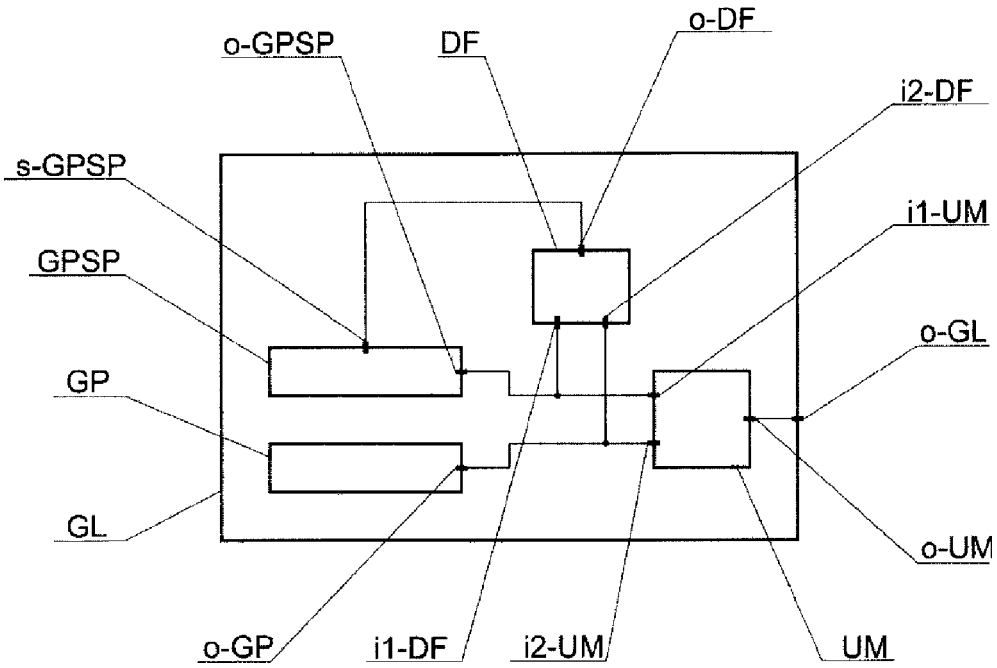

Fig. 1

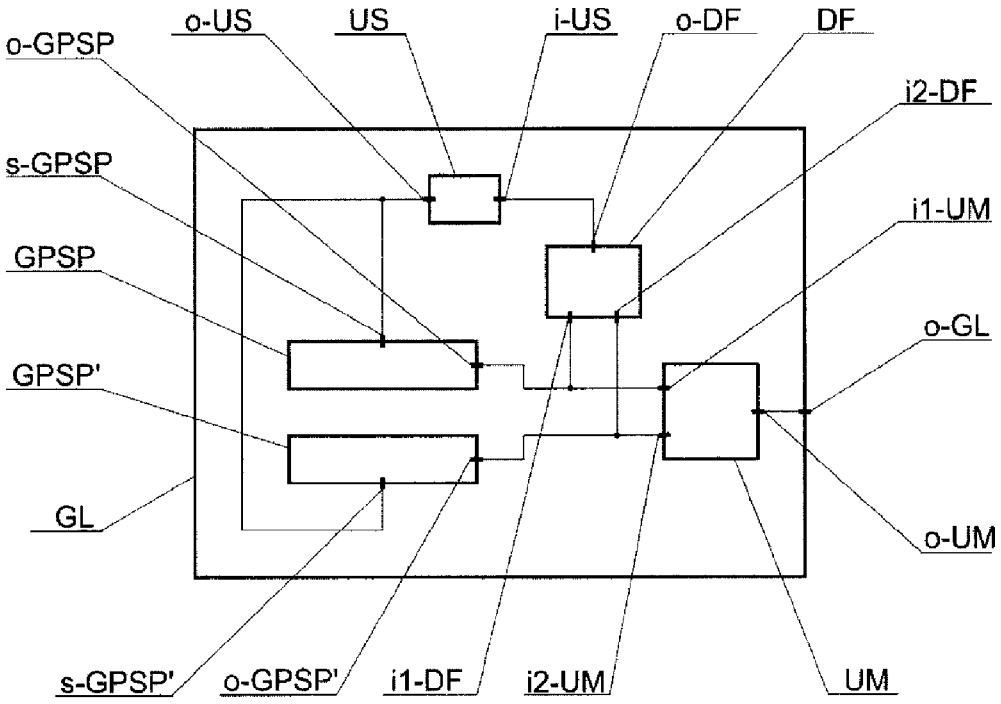

Fig. 2

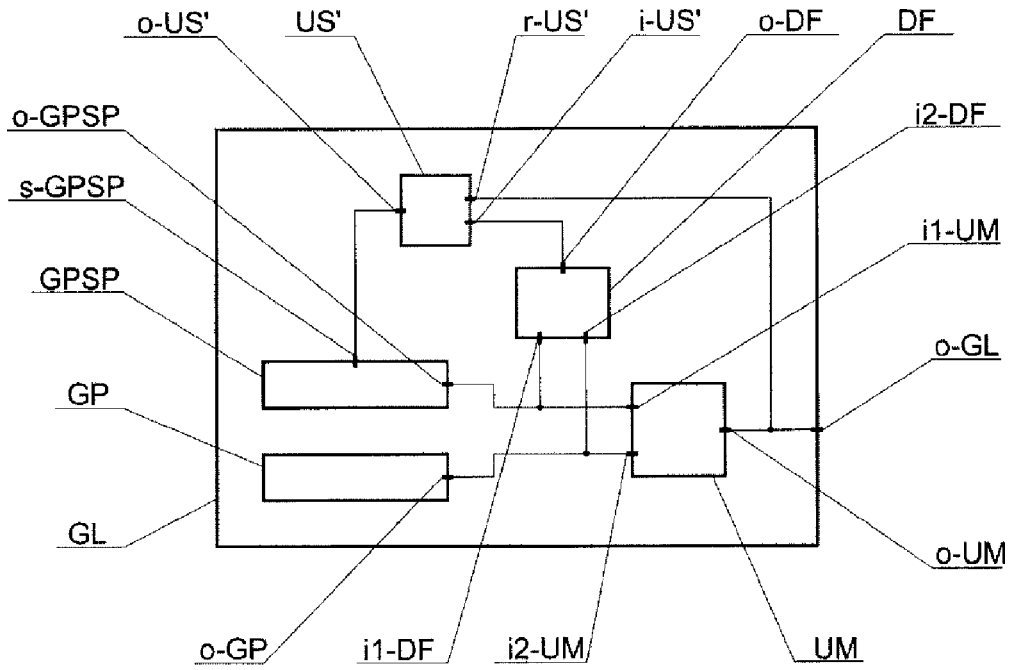
o-US'
US'
r-US'
i-US'
o-DF
DF
o-GPSP
i2-DF
s-GPSP
i1-UM
GPSP
o-GL
GP
GL
o-UM
o-GP
i1-DF
i2-UM
UM

Fig. 3

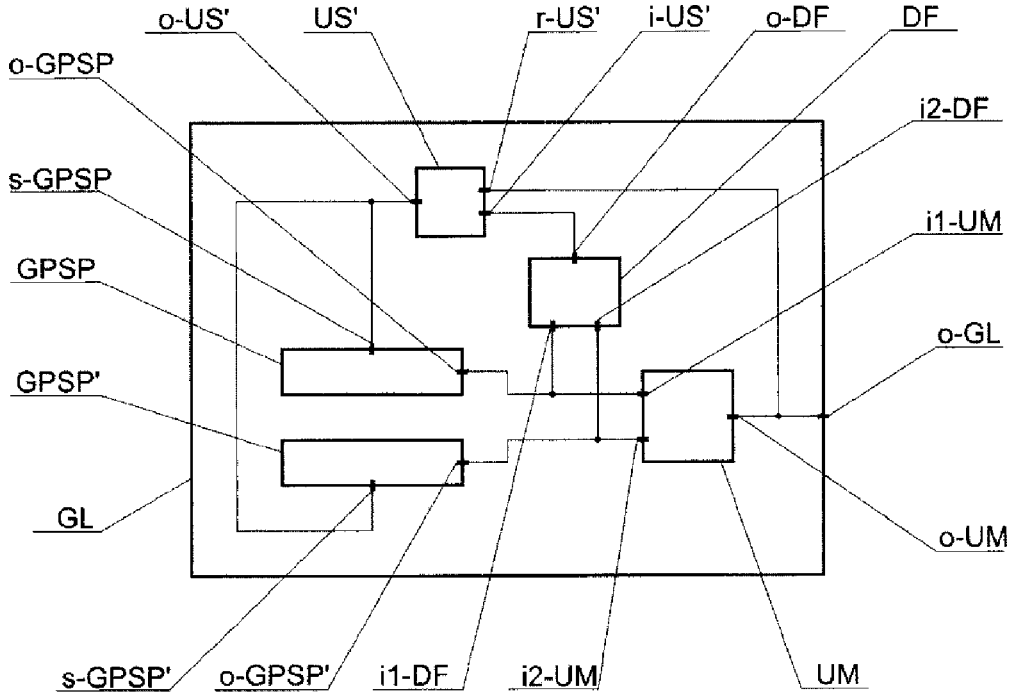
o-US'
US'
r-US'
i-US'
o-DF
DF
o-GPSP
i2-DF
s-GPSP
i1-UM
GPSP
o-GL
GPSP'
GL
o-UM
s-GPSP'
o-GPSP'
i1-DF
i2-UM
UM

Fig. 4

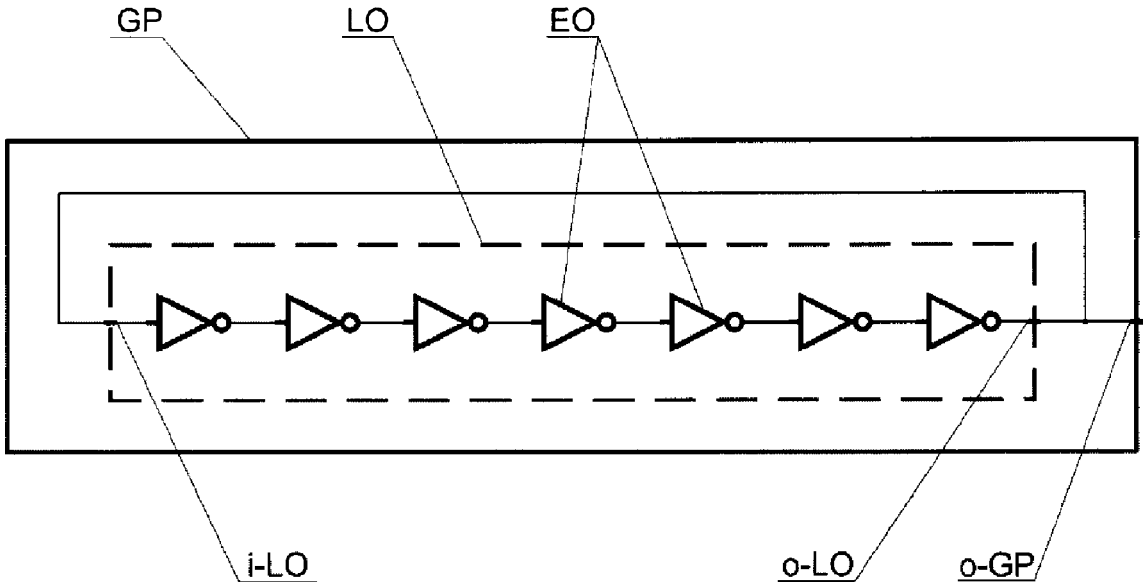
GP
LO
EO
i-LO
o-LO
o-GP

Fig. 5

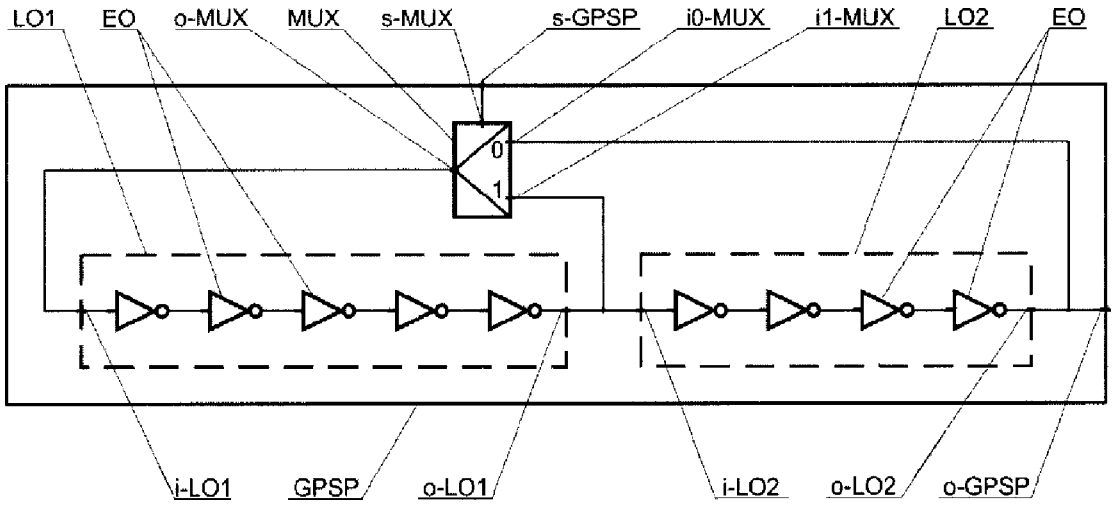
LO1
EO
o-MUX
MUX
s-MUX
s-GPSP
i0-MUX
i1-MUX
LO2
EO
0
1
i-LO1
GPSP
o-LO1
i-LO2
o-LO2
o-GPSP

Fig. 6

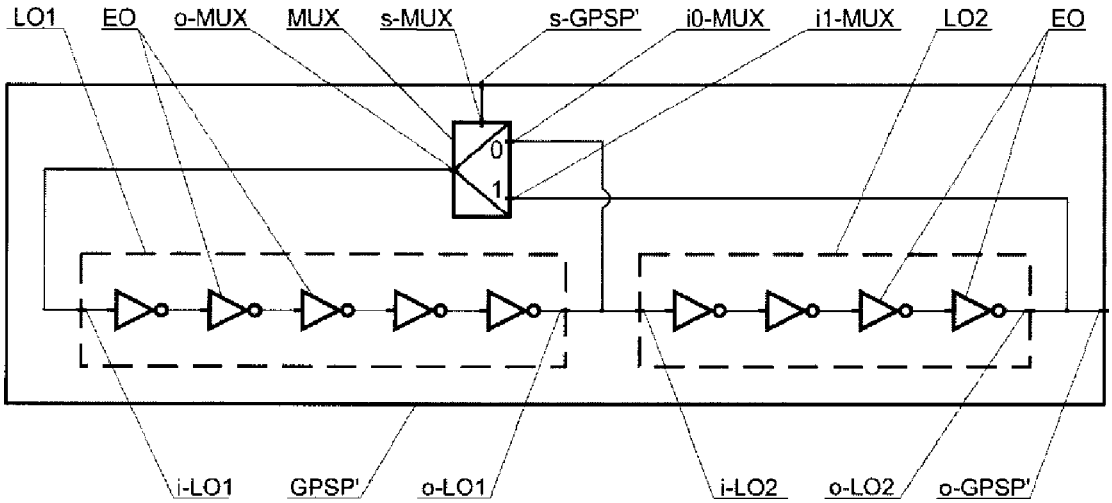
LO1
EO
o-MUX
MUX
s-MUX
s-GPSP'
i0-MUX
i1-MUX
LO2
EO
0
1
i-LO1
GPSP'
o-LO1
i-LO2
o-LO2
o-GPSP'

Fig. 7

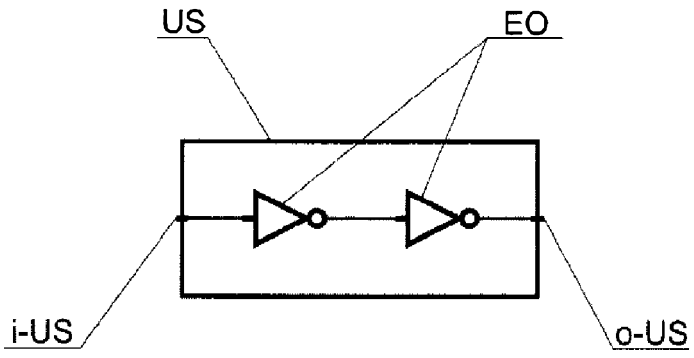
US
EO
i-US
o-US

Fig. 8

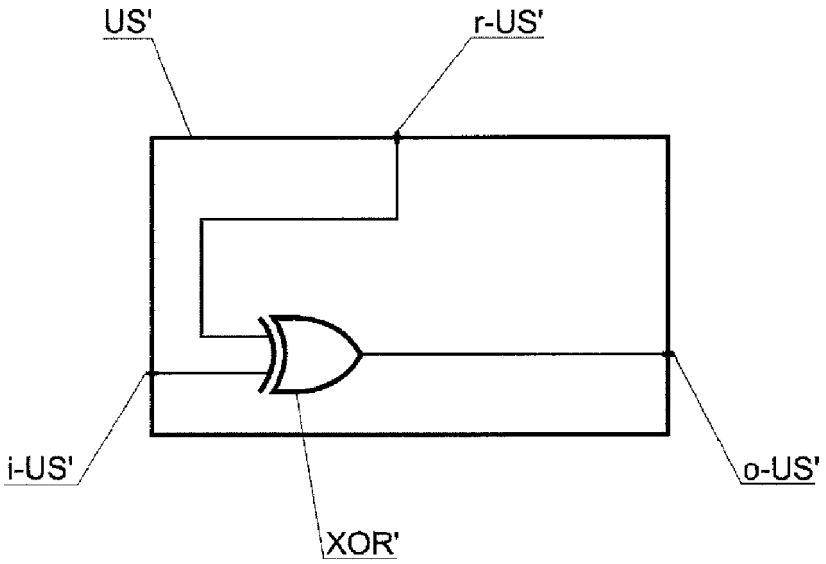

Fig. 9

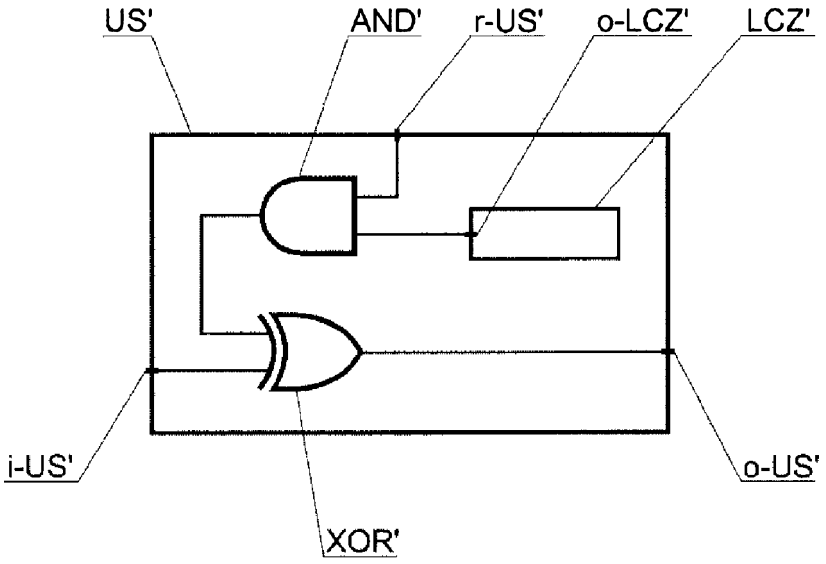

Fig. 10

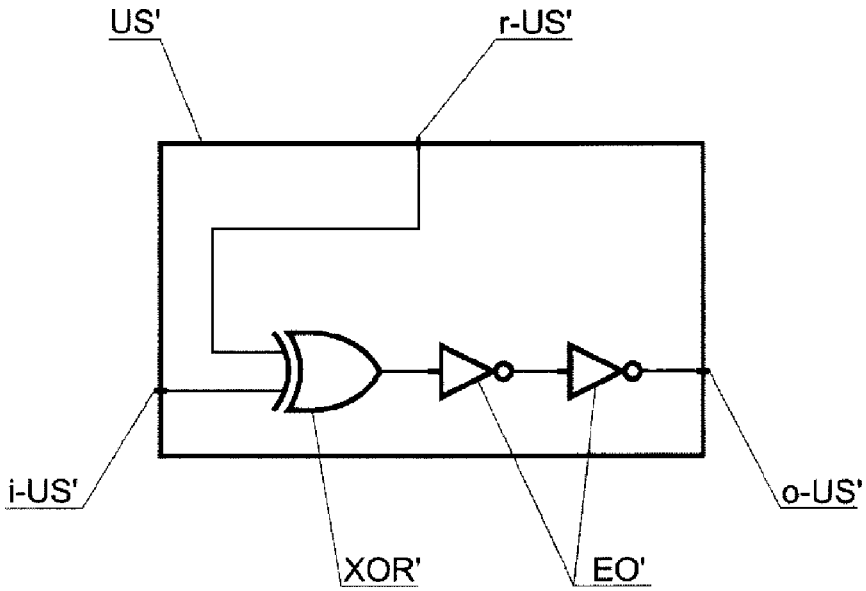

Fig. 11

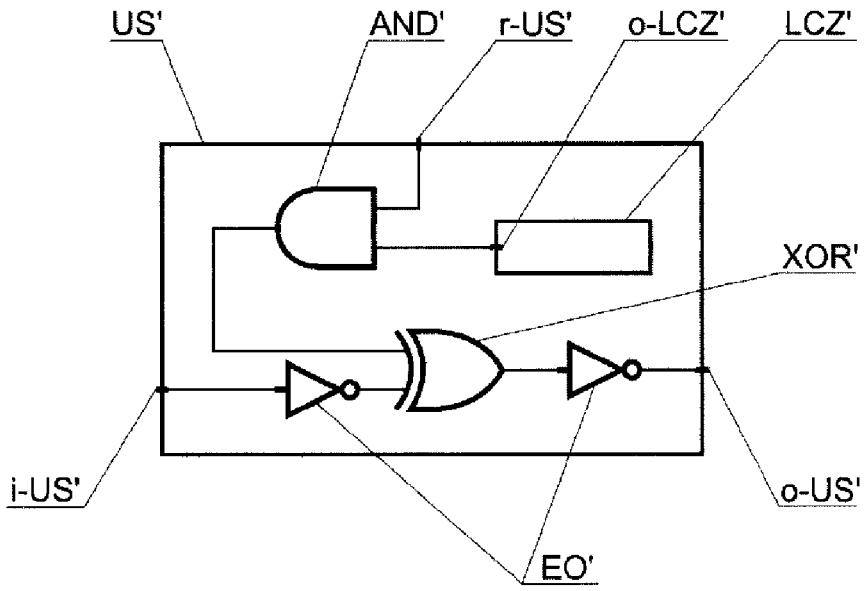

Fig. 12

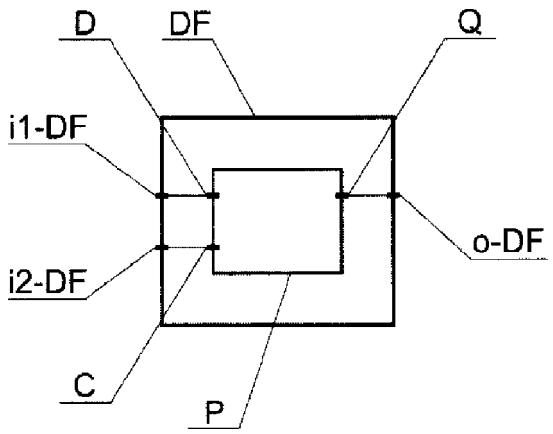
D
DF
Q
i1-DF
o-DF
i2-DF
C
P

Fig. 13

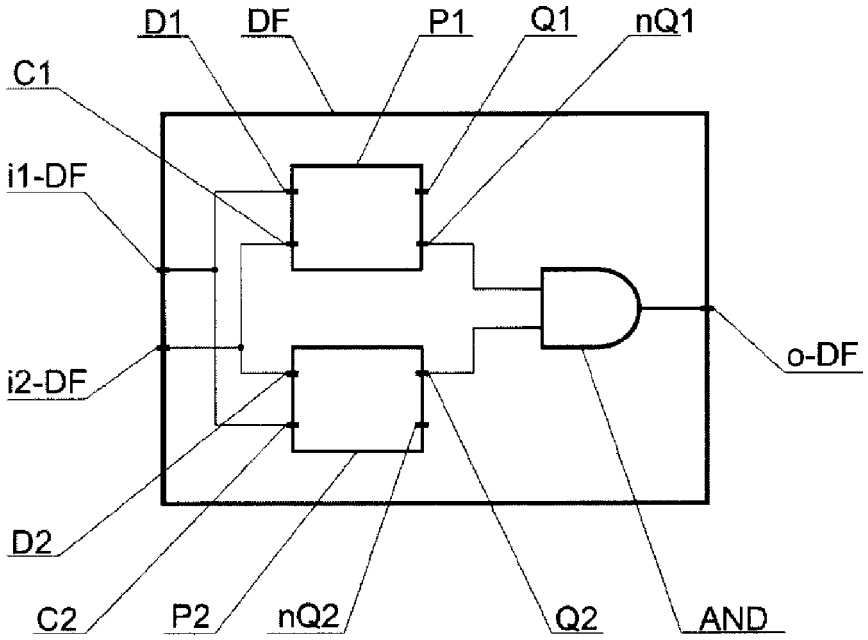
D1
DF
P1
Q1
nQ1
C1
i1-DF
o-DF
i2-DF
D2
C2
P2
nQ2
Q2
AND

Fig. 14

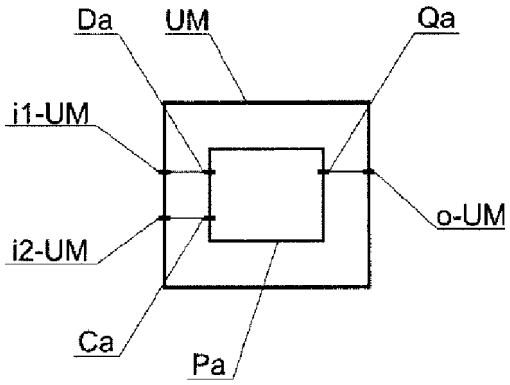

Fig. 15

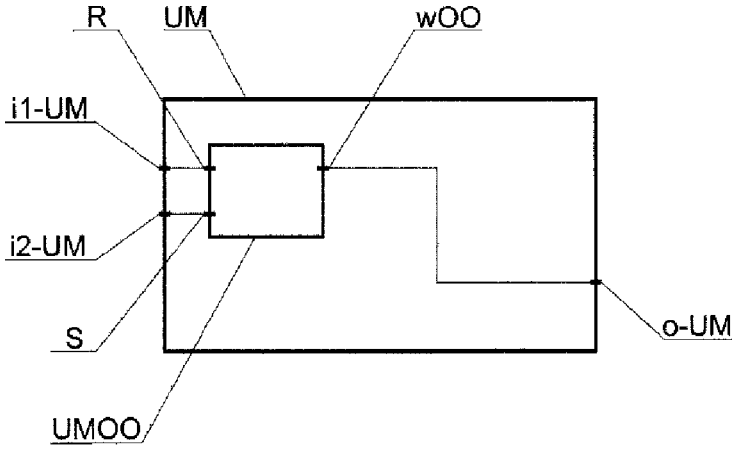

Fig. 16

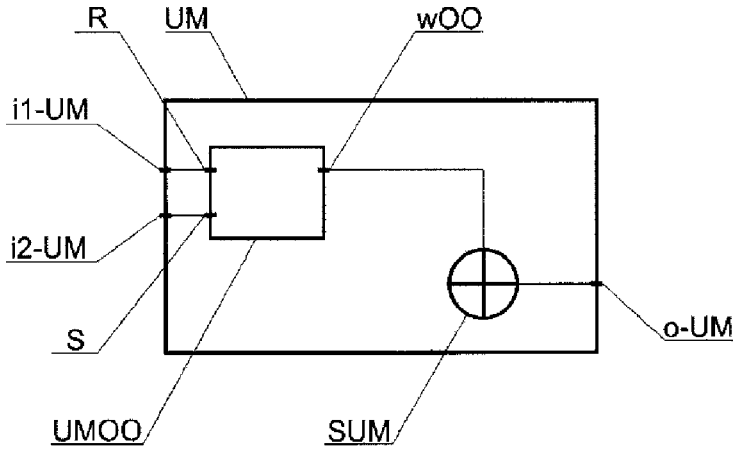

Fig. 17

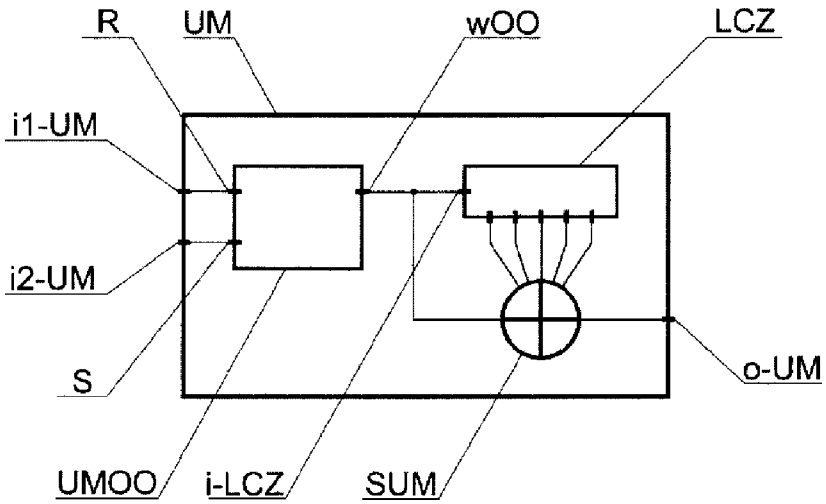
R
UM
wOO
LCZ
i1-UM
i2-UM
S
o-UM
UMOO
i-LCZ
SUM

Fig. 18

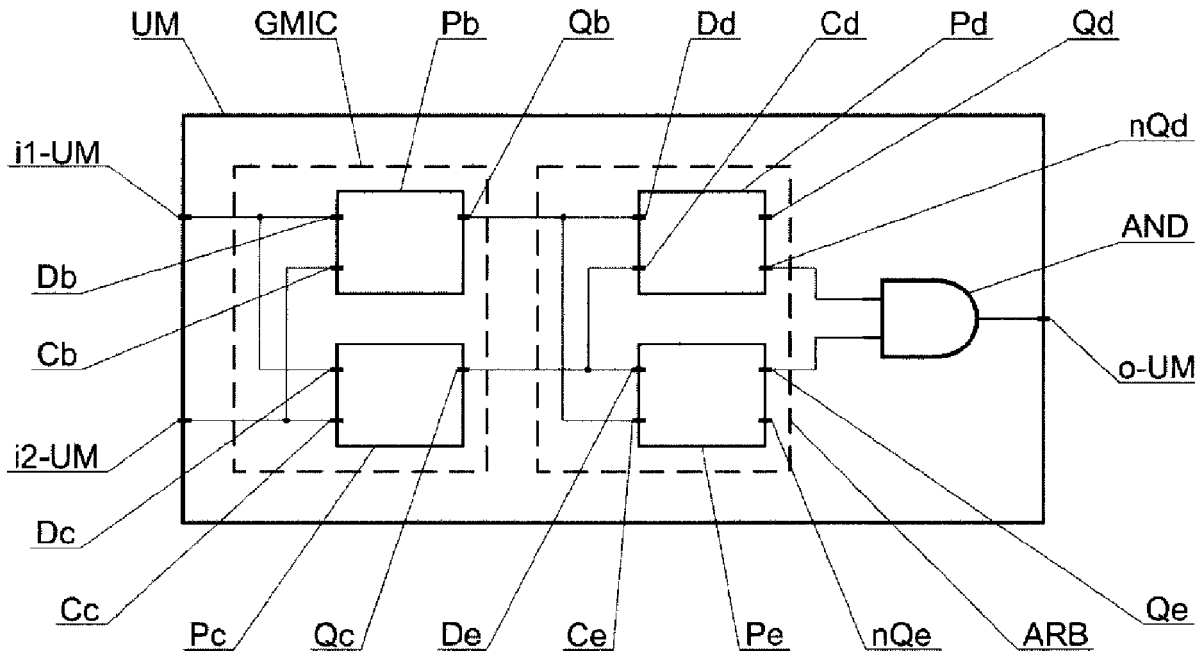
UM
GMIC
Pb
Qb
Dd
Cd
Pd
Qd
nQd
i1-UM
AND
Db
Cb
o-UM
i2-UM
Dc
Cc
Qe
Pc
Qc
De
Ce
Pe
nQe
ARB

Fig. 19