Generator fizycznie niekopiowalnych kluczy kryptograficznych

[0001] Przedmiotem wynalazku jest generator fizycznie niekopiowalnych kluczy kryptograficznych przeznaczony zwłaszcza do generacji fizycznie pozyskiwanych, nieklonowalnych i unikalnych kluczy kryptograficznych.

[0002] Generator fizycznie niekopiowalnych kluczy (ang. *physically unclonable functions* lub *physically unclonable cryptographic keys*) ma za zadanie generować nieprzewidywalne ciągi liczb losowych ale, co ważne, powtarzalne dla konkretnego egzemplarza układu. Ważne jest by rozrzuty technologiczne prowadziły do takich różnic układowych, które wykluczą generację tych samych kluczy przez dwa układy wykonane według tego samego projektu, w tej samej serii technologicznej. Tak wygenerowane losowe lecz powtarzalne ciągi są przeznaczone do zastosowania jako klucze m.in. do szyfrowania i autoryzacji.

[0003] Znane są w stanie techniki, np. z wynalazków US2011169580 lub WO0161854, generatory losowe, zawierające generatory pierścieniowe, które nie są i nie mogą być generatorami fizycznie niekopiowalnych kluczy kryptograficznych, ponieważ nie generują powtarzalnych ciągów liczbowych dla konkretnych egzemplarzy układów.

[0004] Znany jest w stanie techniki, np. z publikacji Chi-En Yin, Gang Qu, "Temperature-aware cooperative ring oscillator PUF", 2009 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '09), Francisco, CA, USA, 2009, pp. 36-42, DOI: 10.1109/HST.2009.5225055, generator fizycznie niekopiowalnych kluczy kryptograficznych, który zawiera generatory pierścieniowe, których wyjścia dołączone są do dwóch liczników przez multipleksery. Wyjścia liczników dołączone są do komparatora, którego wyjście jest wyjściem generatora fizycznie niekopiowalnych kluczy kryptograficznych.

[0005] Celem wynalazku jest uwydatnienie międzyegzemplarzowych rozrzutów technologicznych elementów i połączeń przekładających się na różnice w działaniu.

[0006] Istota wynalazku polega na tym, że generator fizycznie niekopiowalnych kluczy kryptograficznych zawierający przynajmniej dwa generatory pierścieniowe zgodnie z wynalazkiem cechuje się tym, że posiada przynajmniej jeden detektor fazy, którego wejścia dołączone są do wyjść generatorów pierścieniowych, oraz tym że przynajmniej jeden generator pierścieniowy jest generatorem pierścieniowym z regulowaną szybkością, zaś wyjście detektora fazy dołączone jest do przynajmniej jednego wejścia sterującego przynajmniej jednego generatora pierścieniowego z regulowaną szybkością oraz do wyjścia generatora fizycznie niekopiowalnych kluczy kryptograficznych. Taka konstrukcja sprawia, że układ ten staje się układem chaotycznym, który uwydatnienia międzyegzemplarzowe rozrzuty technologiczne elementów i połączeń – tzw. warunki początkowe.

[0007] Przynajmniej jeden generator pierścieniowy korzystnie posiada wejście inicjalizacji dołączone do wejścia generatora fizycznie niekopiowalnych kluczy kryptograficznych. Dzięki temu można łatwo wielokrotnie rozpoczynać pracę układu chaotycznego od początku.

[0008] Korzystnie wyjście detektora fazy dołączone jest do przynajmniej jednego wejścia sterującego przynajmniej jednego generatora pierścieniowego z regulowaną szybkością za pośrednictwem układu sterującego. Zastosowanie układu sterującego umożliwia wprowadzanie zmian do sygnału sprzężenia zwrotnego, a w konsekwencji poprawę pracy układu chaotycznego.

[0009] Korzystnie wyjście detektora fazy dołączone jest do wyjścia generatora fizycznie niekopiowalnych kluczy kryptograficznych przez układ rejestrująco-porównujący. Układ ten pozwala na przykład zignorować ciągi nietypowe i przypadkowe, które utrudniają wygenerowanie klucza kryptograficznego.

[0010] Korzystnie układ rejestrująco-porównujący posiada przynajmniej jedno wejście dołączone do wejścia generatora fizycznie niekopiowalnych kluczy kryptograficznych. Takie połączenie ułatwia wykrycie momentu startu układu.

[0011] Korzystnie układ rejestrująco-porównujący posiada przynajmniej jedno wejście dołączone do przynajmniej jednego wyjścia generatora pierścieniowego. Takie połączenie pozwala na synchronizację układu rejestrująco-porównującego z układem chaotycznym.

[0012] Korzystnie przynajmniej jeden generator pierścieniowy zawiera przynajmniej jedną linię opóźniającą, której wyjście dołączone jest do wyjścia generatora pierścieniowego, zaś wyjście linii opóźniającej dołączone jest do jej wejścia przez klucz startowy, którego wejście sterujące dołączone jest do wejścia inicjalizacji generatora pierścieniowego, przy czym linia opóźniająca zawiera elementy opóźniające połączone w szereg.

[0013] Korzystnie przynajmniej jeden generator pierścieniowy z regulowaną szybkością zawiera przynajmniej jedną linię opóźniającą, zawierającą elementy opóźniające połączone w szereg, której wyjście dołączone jest do wyjścia generatora z regulowaną szybkością oraz, za pośrednictwem klucza startowego do wejścia tej linii opóźniającej, przy czym, wejście sterujące klucza startowego dołączone jest do wejścia inicjalizacji generatora pierścieniowego z regulowaną szybkością.

[0014] Korzystnie przynajmniej jeden generator pierścieniowy z regulowaną szybkością zawiera przynajmniej jeden dodatkowy element wprowadzający opóźnienie, dołączany do linii opóźniającej do wyjścia jednego elementu opóźniającego za pomocą klucza, którego wejście sterujące dołączone jest do wejścia sterującego generatora pierścieniowego z regulowaną szybkością. Takie rozwiązanie pozwala na regulację częstotliwości generatora pierścieniowego z regulowaną szybkością, a co za tym idzie na regulację fazy względem innego generatora.

[0015] Korzystnie przynajmniej jeden generator pierścieniowy z regulowaną szybkością zawiera przynajmniej jeden sterowany element opóźniający włączony szeregowo w linię opóźniającą między wyjściem jednego elementu opóźniającego i wejściem następnego, zaś wejście sterujące sterowanego elementu opóźniającego dołączone jest do wejścia sterującego generatora pierścieniowego z regulowaną

szybkością. Takie rozwiązanie pozwala na regulację częstotliwości generatora pierścieniowego z regulowaną szybkością, a co za tym idzie na regulację fazy względem innego generatora.

[0016] Korzystnie sterowany element opóźniający zawiera przynajmniej dwa tranzystory polowe o przeciwnym typie przewodnictwa, których dreny i źródła są parami połączone i jedna para dołączona jest do wejścia sterowanego elementu opóźniającego, druga para dołączona jest do wyjścia sterowanego elementu opóźniającego, a wejście sterujące sterowanego elementu opóźniającego dołączone jest do bramek obydwu tranzystorów polowych. Takie rozwiązanie pozwala na zróżnicowanie opóźnień wprowadzanych przez sterowany element opóźniający bardzo małym kosztem, gdyż tranzystory o przeciwnym typie przewodnictwa włączają się przy przeciwnych stanach logicznych na ich bramkach.

[0017] Korzystnie w tranzystorach polowych stosunek długości do szerokości kanału jednego tranzystora przewyższa stosunek długości do szerokości kanału drugiego tranzystora. Takie rozwiązanie zapewnia regulację opóźnień wprowadzanych przez sterowany element opóźniający przez regulację geometrią kanałów tranzystorów.

[0018] Korzystnie w szereg z przynajmniej jednym z tranzystorów polowych włączony jest przynajmniej jeden element opóźniający. Takie rozwiązanie zapewnia dodatkowe opóźnienie wprowadzane w linii wybranego tranzystora.

[0019] Korzystnie pomiędzy bramki tranzystorów polowych a wejście sterujące sterowanego elementu opóźniającego włączony jest przynajmniej jeden inwerter. Takie rozwiązanie zapewnia przeciwną pracę tranzystorów sterowanych tym samym sygnałem, dzięki czemu wywołuje przeciwną zmianę częstotliwości w dwóch komplementarnych generatorach pierścieniowych z regulowaną szybkością.

[0020] Korzystnie przynajmniej jeden generator pierścieniowy z regulowaną szybkością jest generatorem pierścieniowym z przełączaną ścieżką propagacji. Takie rozwiązanie pozwala na regulację częstotliwości generatora pierścieniowego z przełączaną ścieżką propagacji, a co za tym idzie na regulację fazy względem innego generatora.

[0021] Korzystnie przynajmniej jeden 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, zaś 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.

[0022] Korzystnie przynajmniej jeden generator pierścieniowy z przełączaną ścieżką propagacji zawiera 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 przez klucz startowy, którego wejście sterujące dołączone jest do wejścia inicjalizacji generatora pierścieniowego z przełączaną ścieżką propagacji, a wejścia multipleksera dołączone są wejścia i wyjścia innej linii opóźniającej.

[0023] Korzystnie przynajmniej jeden układ sterujący zawiera przynajmniej jeden element opóźniający, zaś elementy opóźniające połączone są w szereg.

[0024] Korzystnie przynajmniej jeden detektor fazy stanowi przerzutnik o dwóch wejściach stanowiących wejścia detektora fazy stanowiącym wyjście detektora fazy.

[0025] Korzystnie przynajmniej jeden detektor fazy zawiera dwa przerzutniki o dwóch wejściach i dwóch wyjściach 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 dołączone jest jednocześnie do pierwszego wejścia pierwszego przerzutnika i drugiego wejścia drugiego przerzutnika, drugie wejście detektora fazy dołączone jest jednocześnie do drugiego wejścia pierwszego przerzutnika i pierwszego wejścia drugiego przerzutnika, a wyjście detektora fazy dołączone jest do wybranych wyjść przerzutników przez układ logiczny.

[0026] Przedmiot wynalazku jest przedstawiony w przykładzie wykonania na rysunku, na którym fig.1 przedstawia schemat blokowy generatora fizycznie niekopiowalnych kluczy kryptograficznych z generatorem pierścieniowym i generatorem pierścieniowym z regulowaną szybkością oraz detektorem fazy, fig.2 przedstawia schemat blokowy generatora fizycznie niekopiowalnych kluczy kryptograficznych z dwoma generatorami pierścieniowymi z regulowaną szybkością, detektorem fazy, układem sterującym oraz układem rejestrująco-porównującym o jednym wejściu, fig.3 przedstawia schemat blokowy generatora fizycznie niekopiowalnych kluczy kryptograficznych z dwoma generatorami pierścieniowymi z regulowaną szybkością, detektorem fazy, układem sterującym oraz układem rejestrująco-porównującym o trzech wejściach, fig.4 przedstawia schemat blokowy generatora pierścieniowego, fig.5 przedstawia schemat blokowy pierwszego generatora pierścieniowego z regulowaną szybkością, fig.6 przedstawia schemat blokowy drugiego generatora pierścieniowego z regulowaną szybkością, fig.7 przedstawia schemat blokowy trzeciego generatora pierścieniowego z regulowaną szybkością, fig.8 przedstawia schemat blokowy sterowanego elementu opóźniającego zawierającego dwa tranzystory polowe, fig.9 przedstawia schemat blokowy sterowanego elementu opóźniającego zawierającego dwa tranzystory polowe oraz dodatkowe opóźnienia włączone w szereg z jednym tranzystorem polowym, fig.10 przedstawia schemat blokowy sterowanego elementu opóźniającego z inwersją sygnału sterowania, fig.11 przedstawia schemat blokowy pierwszego generatora pierścieniowego z przełączaną ścieżką propagacji, fig.12 przedstawia schemat blokowy drugiego generatora pierścieniowego z przełączaną ścieżką propagacji, fig.13 przedstawia schemat blokowy układu sterującego zbudowanego z elementów opóźniających, fig.14 przedstawia schemat blokowy detektora fazy zbudowanego z jednego przerzutnika, a fig.15 – schemat blokowy detektora fazy zbudowanego z dwóch przerzutników.

[0027] Generator fizycznie niekopiowalnych kluczy kryptograficznych przedstawiony na fig.1 zawiera generator pierścieniowy GP oraz generator pierścieniowy z regulowaną

szybkością GPRS, których wyjścia o-GP i o-GPRS dołączone są do wejść i1-DF i i2-DF detektora fazy DF. Wyjście detektora fazy o-DF dołączone jest do wejścia sterującego generatora pierścieniowego z regulowaną szybkością s-GPRS. Wyjście o-DF detektora fazy DF dołączone jest także do wyjścia o-PUF generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF. Wejście inicjalizacji i-UCH generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF dołączone jest jednocześnie do wejść inicjalizujących generatora pierścieniowego oraz generatora pierścieniowego z regulowaną szybkością i-GP i i-GPRS.

[0028] Detektor fazy DF przełącza częstotliwość generatora pierścieniowego z regulowaną szybkością GPRS cyklicznie zmieniając lub synchronizując fazę obydwu generatorów GP i GPRS - czego efektem jest chaotyczne zachowanie układu. Różnice międzyegzemplarzowe w budowie generatorów pierścieniowych powodują, że chaos deterministyczny staje się chaosem niedeterministycznym jednak do pewnego stopnia specyficznym dla elementów użytych do budowy układu. Dzięki temu ciągi generowane przez układ chaotyczny zapewniają unikalność związaną z konkretnym egzemplarzem. Podłączenie wejść inicjalizujących generatora pierścieniowego oraz generatora pierścieniowego z regulowaną szybkością i-GP i i-GPRS do wejścia inicjalizacji i-UCH generatora pozwala na łatwe, cykliczne uruchamianie układu. Brak tych połączeń powoduje, że układ musi być inicjalizowany w inny sposób - na przykład przez cykliczne włączanie zasilania generatora pierścieniowego oraz generatora pierścieniowego z regulowaną szybkością.

[0029] Generator fizycznie niekopiowalnych kluczy kryptograficznych przedstawiony na fig.2 zawiera dwa generatory pierścieniowe z regulowaną szybkością GPRS i GPRS', których wyjścia o-GPRS i o-GPRS' dołączone są do wejść i1-DF i i2-DF detektora fazy DF. 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 regulowaną szybkością s-GPRS i s-GPRS'. Wyjście

o-DF detektora fazy DF dołączone jest do wejścia u-URP układu rejestrująco-porównującego URP, a wyjście tego układu o-URP dołączone jest do wyjścia o-PUF generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF. Wejście inicjalizacji i-UCH generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF dołączone jest jednocześnie do wejść inicjalizujących generatorów pierścieniowych z regulowaną szybkością i-GPRS i i-GPRS'.

[0030] Generatory pierścieniowe z regulowaną szybkością GPRS i GPRS', detektor fazy DF oraz układ sterujący US stanowią układ chaotyczny, który zapewnia wrażliwość na międzyegzemplarzowe rozrzuty parametrów elementów składających się na ten układ. Układ rejestrująco-porównujący zapewnia możliwość rejestracji ciągów i porównywania ich między sobą. Rejestracja kolejnych ciągów generowanych przez układ chaotyczny i porównanie ich między sobą pozwalają stwierdzić, w którym momencie zachodzą między tymi ciągami różnice. Zastosowanie drugiego generatora pierścieniowego z regulowaną szybkością GPRS', pracującego przeciwnie w stosunku do pierwszego generatora pierścieniowego z regulowaną szybkością GPRS, poprawia chaotyczne właściwości działania układu. Dołączenie wejść inicjalizujących generatorów pierścieniowych z regulowaną szybkością i-GPRS i i-GPRS' do wejścia inicjalizującego i-UCH generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF ułatwia wielokrotną inicjalizację pracy generatorów pierścieniowych z regulowaną szybkością GPRS i GPRS'.

[0031] Generator fizycznie niekopiowalnych kluczy kryptograficznych przedstawiony na fig.3 zawiera dwa generatory pierścieniowe z regulowaną szybkością GPRS i GPRS', których wyjścia o-GPRS i o-GPRS' dołączone są do wejść i1-DF i i2-DF detektora fazy DF. 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 regulowaną szybkością s-GPRS i s-GPRS'. Wyjście o-DF detektora fazy DF dołączone jest do wejścia u-URP układu rejestrująco-porównującego URP, a wyjście tego układu o-URP

dołączone jest do wyjścia o-PUF generatora fizycznie niekopiowalnych kluczy kryptograficznych PUF. Wejście generatora fizycznie niekopiowalnych kluczy kryptograficznych i-UCH dołączone jest jednocześnie do wejść inicjalizujących generatorów pierścieniowych z regulowaną szybkością i-GPRS i i-GPRS' oraz do drugiego wejścia układu rejestrująco-porównującego i-URP. Trzecie wejście układu rejestrująco-porównującego z-URP dołączone jest do wyjścia drugiego generatora pierścieniowego z regulowaną szybkością o-GPRS'.

[0032] Dołączenie wejść i-URP i z-URP układu rejestrująco-porównującego URP do wejścia inicjalizującego i-UCH generatora fizycznie niekopiowalnych kluczy kryptograficznych UCH oraz do wyjścia o-GPRS' jednego z generatorów pierścieniowych z regulowaną szybkością GPRS' poprawia i upraszcza rejestrację i wzajemne porównanie ciągów liczbowych.

[0033] Generator pierścieniowy przedstawiony na fig.4 zawiera linię opóźniającą LO, której wyjście o-LO jest jednocześnie dołączone do wyjścia o-GP generatora pierścieniowego GP oraz do wejścia i-LO linii opóźniającej LO przez klucz startowy KS, którego wejście sterujące dołączone jest do wejścia inicjalizacji i-GP generatora pierścieniowego GP. Linia opóźniająca LO zawiera elementy opóźniające EO połączone w szereg.

[0034] 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, jak również właściwościami specyficznymi dla konkretnego układu. Klucz startowy KS sterowany przez wejście inicjalizacji i-GP generatora pierścieniowego GP pozwala na zatrzymanie pracy generatora i ponowne jego uruchomienie w wybranym momencie.

[0035] Generator pierścieniowy z regulowaną szybkością przedstawiony na fig.5 zawiera linię opóźniającą LO, której wyjście o-LO jest jednocześnie dołączone do wyjścia o-GPRS generatora pierścieniowego z regulowaną szybkością GPRS oraz do

jej wejścia i-LO przez klucz startowy KS, którego wejście sterujące dołączone jest do wejścia inicjalizacji generatora i-GPRS. Linia opóźniająca LO zawiera elementy opóźniające EO połączone w szereg. Pomiędzy wybranymi elementami opóźniającymi EO linia opóźniająca LO ma element wprowadzający opóźnienie w postaci kondensatora C, który jedną końcówką jest dołączany do tej linii przy pomocy klucza KL. Druga końcówka kondensatora C dołączona jest do masy układu GND. Wejście sterujące klucza KL dołączone jest do wejścia sterującego generatora s-GPRS.

[0036] Generator GPRS posiada dwie podstawowe częstotliwości pracy, a wybór jednej z nich dokonywany jest przez sygnał sterujący generatora s-GPRS. Podstawowe częstotliwości pracy zależą od liczby elementów opóźniających EO składających się na linię opóźniającą LO, od opóźnienia wprowadzanego przez każdy element opóźniający EO oraz od opóźnienia wprowadzanego przez dołączenie kondensatora C powodujące wolniejsze przełączanie się sąsiadujących z nim elementów opóźniających EO. Częstotliwości podstawowe są obarczone niestałością, wynikającą ze zjawisk fizycznych, jak również właściwościami specyficznymi dla konkretnego układu. Klucz startowy KS sterowany przez wejście inicjalizacji generatora i-GPRS pozwala na zatrzymanie pracy generatora i ponowne jego uruchomienie w wybranym momencie.

[0037] Generator pierścieniowy z regulowaną szybkością przedstawiony na fig.6 ma budowę taką jak układ z fig.5, z tą różnicą, że klucz KL’ ma działanie przeciwne do klucza KL. Odwrotne działanie klucza powoduje, że wybrana częstotliwość pracy generatora GPRS’ jest przeciwna w stosunku do częstotliwości wybranej w generatorze GPRS.

[0038] Generator pierścieniowy z regulowaną szybkością przedstawiony na fig.7 zawiera linię opóźniającą LO, której wyjście o-LO jest jednocześnie dołączone do wyjścia o-GPRS generatora pierścieniowego z regulowaną szybkością GPRS oraz do jej wejścia i-LO przez klucz startowy KS, którego wejście sterujące dołączone jest do wejścia inicjalizacji generatora i-GPRS. Linia opóźniająca LO zawiera elementy opóźniające EO połączone w szereg.

Pomiędzy wybranymi elementami opóźniającymi EO linia opóźniająca LO ma włączony sterowany element opóźniający T, którego wejście sterujące s-T dołączone jest do wejścia sterującego s-GPRS generatora pierścieniowego z regulowaną szybkością GPRS.

[0039] Generator GPRS posiada dwie podstawowe częstotliwości pracy, a wybór jednej z nich dokonywany jest przez sygnał sterujący generatora s-GPRS. Podstawowe częstotliwości pracy zależą od liczby elementów opóźniających EO składających się na linię opóźniającą LO, od opóźnienia wprowadzanego przez każdy element opóźniający EO oraz od opóźnienia wprowadzanego przez sterowany element opóźniający T, które wybierane jest przy pomocy sygnału logicznego doprowadzonego do wejścia sterującego s-GPRS generatora pierścieniowego z regulowaną szybkością GPRS, a zatem i do wejścia sterującego s-T sterowanego elementu opóźniającego T.

[0040] Klucz startowy KS sterowany przez wejście inicjalizacji generatora i-GPRS pozwala na zatrzymanie pracy generatora i ponowne jego uruchomienie w wybranym momencie - w szczególności równoczesne uruchomienie wszystkich generatorów. Binarne ciągi liczbowe pojawiające się na wyjściu detektora fazy po określonym czasie działania układu pozwalają odróżnić fizyczne układy zawierające identyczne implementacje. Rozróżnienie to jest możliwe dzięki występowaniu rozrzutów technologicznych w układach elektronicznych.

[0041] Sterowany element opóźniający przedstawiony na fig.8 zawiera dwa tranzystory polowe o przeciwnym typie przewodnictwa P, N. Źródła tranzystorów są ze sobą połączone i dołączone do wejścia i-T sterowanego elementu opóźniającego T, dreny tranzystorów są ze sobą połączone i dołączone do wyjścia o-T sterowanego elementu opóźniającego T, natomiast bramki tranzystorów są ze sobą połączone i dołączone do wejścia sterującego s-T sterowanego elementu opóźniającego T.

[0042] Symetryczność budowy tranzystora polowego pozwala na zamianę miejscami jego końcówek, drenu i źródła. Przeciwny typ przewodnictwa tranzystorów, sterowanych tym samym sygnałem logicznym dołączonym do bramek obydwu tranzystorów, powoduje że

zero logiczne wyłącza jeden tranzystor N i włącza drugi P, podczas gdy jedynka logiczna czyni odwrotnie. Przy identycznej geometrii tranzystorów, jeden z nich P wprowadza nieco większe opóźnienie pomiędzy wejściem i-T a wyjściem o-T sterowanego elementu opóźniającego T. Zmiana geometrii kanałów tranzystorów, w szczególności istotne wydłużenie jednego z kanałów, wprowadza silnie asymetryczną pracę tranzystorów pod względem wprowadzanego opóźnienia. Odwrócenie długości kanałów w innej parze tranzystorów, zawartych w innym sterowanym elemencie opóźniającym, włączonym w szereg elementów opóźniających innego generatora pierścieniowego z regulowaną szybkością, zapewnia komplementarne sterowanie parą takich generatorów, w których ten sam sygnał sterujący wywołuje przeciwny skutek w każdym z nich.

[0043] Sterowany element opóźniający przedstawiony na fig.9 ma budowę taką jak układ z fig.8, z tą różnicą, że w szereg z jednym tranzystorem P, to znaczy pomiędzy tym tranzystorem P a wyjściem o-T sterowanego elementu opóźniającego T, włączone zostały szeregowo dwa elementy opóźniające EO.

[0044] Włączenie dodatkowych elementów opóźniających EO zapewnia dodatkowe opóźnienie pomiędzy wejściem i-T a wyjściem o-T sterowanego elementu opóźniającego T jedynie dla jednego stanu logicznego sygnału sterującego s-T. Takie same elementy opóźniające włączone w szereg z drugim tranzystorem w innej parze tranzystorów, zawartych w innym sterowanym elemencie opóźniającym, włączonym w szereg elementów opóźniających innego generatora pierścieniowego z regulowaną szybkością, zapewniają komplementarne sterowanie parą takich generatorów, w których ten sam sygnał sterujący wywołuje przeciwny skutek w każdym z nich.

[0045] Sterowany element opóźniający przedstawiony na fig.10 ma budowę taką jak układ z fig.8, z tą różnicą, że pomiędzy bramki tranzystorów polowych P i N a wejście sterujące s-T sterowanego elementu opóźniającego T włączony został inwerter Inv.

[0046] Zastosowanie inwertera Inv w tylko jednym z dwóch sterowanych elementów opóźniających, posiadających identyczną budowę wewnętrzną, włączonych w szeregi elementów opóźniających

linii opóźniających dwóch generatorów pierścieniowych z regulowaną szybkością, zapewnia komplementarne sterowanie parą takich generatorów, w których ten sam sygnał sterujący wywołuje przeciwny skutek w każdym z nich.

[0047] Generator pierścieniowy z przełączaną ścieżką propagacji przedstawiony na fig.11 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 przez klucz startowy KS, którego wejście sterujące dołączone jest do wejścia inicjalizacji generatora i-GPSP. Wejście sterujące multipleksera s-MUX dołączone jest do wejścia sterującego generatora s-GPSP.

[0048] 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, jak również właściwościami specyficznymi dla konkretnego układu. Klucz startowy KS sterowany przez wejście inicjalizacji generatora i-GPSP pozwala na zatrzymanie pracy generatora i ponowne jego uruchomienie w wybranym momencie.

[0049] Generator pierścieniowy z przełączaną ścieżką propagacji przedstawiony na fig.12 ma budowę taką jak układ z fig.11, 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.

[0050] Układ sterujący przedstawiony na fig.13 zawiera dwuelementowy szereg złożony z elementów opóźniających EO dołączony pomiędzy wejściem i-US i wyjściem o-US układu sterującego US.

[0051] Szereg elementów opóźniających EO wprowadza opóźnienie w sprzężeniu zwrotnym, tj. opóźnienie w przekazywaniu sygnału sterowania korekcją fazy, dzięki czemu poprawia chaotyczne właściwości działania układu.

[0052] Detektor fazy przedstawiony na fig.14 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.

[0053] 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. Rodzaj przerzutnika – np. przerzutnik typu „D", przerzutnik „RS", przerzutnik „JK" itp. – ma drugorzędne znaczenie dopóki przerzutnik wykrywa pierwszeństwo zboczy sygnałów wejściowych.

[0054] Detektor fazy przedstawiony na fig.15 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.

[0055] Detektor fazy zbudowany z dwóch przerzutników pozwala na symetryczną detekcję ujemnych i dodatnich przesunięć fazowych.

[0056] Możliwości zastosowania wynalazku przewiduje się bezpośrednio w układach chaotycznych i układach korekcji fazy, a pośrednio w generowaniu niekopiowalnych kluczy kryptograficznych unikalnych dla konkretnego urządzenia.