Generator liczb prawdziwie losowych oraz sposób generowania liczb prawdziwie losowych z wykorzystaniem tego generatora liczb prawdziwie losowych

Przedmiotem wynalazku jest generator liczb prawdziwie losowych oraz sposób generowania liczb prawdziwie losowych z wykorzystaniem tego generatora liczb prawdziwie losowych, właściwy zwłaszcza dla struktur programowalnych FPGA.

Generatory liczb prawdziwie losowych – True Random Number Generators – znajdują obecnie szczególne zastosowanie w systemach kryptograficznych, w których nie mogą być wykorzystywane powszechnie spotykane generatory liczb pseudolosowych, które z natury są deterministyczne.

Z literatury naukowo-technicznej znane są sposoby wytwarzania liczb prawdziwie losowych oraz układy cyfrowe realizujące te sposoby z wykorzystaniem struktur programowalnych FPGA.

Z publikacji M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo pt.: „A high-speed oscillator – based truly random numer source for cryptographic applications on a smart card IC", IEEE Transactions on Computers, vol. 52, No. 4, pp. 403 – 409, znany jest generator liczb losowych, który wykorzystuje zewnętrzny oscylator zbudowany z elementów dyskretnych. Jako źródło oscylacji obarczonych drżeniem fazy wykorzystano w nim zjawisko szumu termicznego rezystora. Natomiast w publikacji Ł. Matuszewski, M. Jessa pt.: „A digital true random number generator implemented in different Xilinx FPGAs", PAK, vol. 59, nr 8, str. 742-744, 2013 został przedstawiony generator liczb losowych składający się z 50 oscylatorów pierścieniowych oraz dodatkowego źródła przebiegów losowych

wykorzystującego oscylator pierścieniowy wraz z wielomianem Galois 31-stopnia. W publikacji D. Li, Z. Lu, X. Zou, Z. Liu pt.: „PUFKEY: A High-Security and High Throughput Hardware True Random Number Generator for Sensoe Networks", Sensors, Vol. 15, pp. 26251-26266, 2015 został przedstawiony złożony generator liczb losowych, który składa się z pamięci SRAM będącej źródłem entropii, co oznacza, że po włączeniu zasilania zawartość pamięci jest losowa, wraz z blokiem realizującym odpowiedni algorytm kondycjonujący, który zapewnia prawdziwie losowy zarodek dla niedeterministycznego generatora liczb losowych, który jest zasadniczym elementem rozwiązania konstrukcyjnego przedstawionego w tej publikacji. Z publikacji Y. Yiu, R. C. Cheung, H. Wong pt.: „A Bias-Bounded Digital True Random Number Generator Architecture", IEEE Transactions on Circuits and System I: Regular Papers, Vol. 64, No. 1, pp. 133-144, 2017, znany jest generator liczb losowych oparty na pewnej odmianie oscylatorów pierścieniowych, zawierających komponenty asynchroniczne, czyli C-elementy Müllera. Ten znany generator minimalizuje zjawisko nierównomiernej ilości „0" i „1" w generowanym ciągu losowym. Źródłem losowości generatora, zaprezentowanego w publikacji A. P. Johnson, R. S. Chakraborty, D. Mukhopadyay pt.: „An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA", IEEE Transactions on Circuits and System II: Express Briefs, Vo. 64, Issue 4, pp. 452-456, 2017, jest zjawisko drżenia fazy dwóch oscylatorów zbudowanych z wykorzystaniem specjalnych układów zarządzania sygnałem zegarowym, znajdujących się wewnątrz układów FPGA Xilinx. Ten znany generator liczb losowych posiada również możliwość strojenia „w locie" pewnych parametrów bez konieczności ponownej syntezy całego projektu dla FPGA, ale przeznaczony jest wyłącznie dla układów FPGA firmy Xilinx. Z publikacji, G. P. Stanchieri, A. Marcellis, M. Paccio, E. Palange pt.: „An FPGA-Based Architecture of True Random Number Generator for Network Security Applications", IEEE International Symposium on Circuits and Systems (ISCAS), 2018, znany jest sposób wykorzystania wybudowanych w FPGA specjalnych bloków wytwarzających przebiegi zegarowe. Jako źródło oscylacji obarczonych

drżeniem fazy wykorzystany jest blok pętli synchronizacji fazowej w układzie FPGA Xilinx Kintex Ultrascale.

Najczęściej stosowanym źródłem losowości dla generatorów liczb prawdziwie losowych jest wykorzystanie zjawiska niestabilności częstotliwości lub drżenia fazy wielu swobodnie drgających oscylatorów. Najczęściej wykorzystywanymi oscylatorami są oscylatory pierścieniowe, które stanowią kaskadowe połączenie nieparzystej liczby elementów logicznych realizujących negację logiczną, przy czym wyjście ostatniego elementu połączone jest z wejściem pierwszego elementu, co zostało przedstawione w publikacji Ł. Matuszewskiego, M. Jessa pt.: „A digital true random number generator implemented in different Xilinx FPGAs", PAK, vol. 59, nr 8, str. 742-744, 2013 oraz w publikacji Y. Yiu, R. C. Cheung, H. Wong pt.: „A Bias-Bounded Digital True Random Number Generator Architecture", IEEE Transactions on Circuits and System I: Regular Papers, Vol. 64, No. 1, pp. 133-144, 2017. W publikacjach A. P. Johnson, R. S. Chakraborty, D. Mukhopadyay pt.: „An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA", IEEE Transactions on Circuits and System II: Express Briefs, Vo. 64, Issue 4, pp. 452-456, 2017 oraz G. P. Stanchieri, A. Marcellis, M. Paccio, E. Palange pt.: „An FPGA-Based Architecture of True Random Number Generator for Network Security Applications", IEEE International Symposium on Circuits and Systems (ISCAS), 2018 jako źródło oscylacji obarczonych drżeniem fazy zostały przedstawione generatory zbudowane z wykorzystaniem pewnych dedykowanych bloków cyfrowych wewnątrz układów FPGA. Te znane rozwiązania znajdują jednak zastosowanie tylko w strukturach programowalnych jednego producenta – firmy Xilinx.

Znane generatory liczb prawdziwie losowych, zbudowane są zwłaszcza w oparciu o oscylatory pierścieniowe, przy czym zazwyczaj wykorzystywanych jest co najmniej kilkadziesiąt oscylatorów. Generatory takie mają złożoną budowę i wymagają dużej liczby zasobów logicznych danego układu programowalnego FPGA.

Celem wynalazku było opracowanie nowego generatora liczb prawdziwie

losowych oraz sposobu generowania liczb prawdziwie losowych z wykorzystaniem tego nowego generatora, który będzie stanowił rozwiązanie proste, a jednocześnie uniwersalne, wymagające niewielkiej liczny zasobów logicznych i które będzie możliwe do zaimplementowania w strukturach FPGA dowolnego producenta.

Generator liczb prawdziwie losowych zawierający dwa oscylatory pierścieniowe, według wynalazku charakteryzuje się tym, że zawiera cztery moduły zatrzaskujące, z których każdy zawiera oscylator pojemnościowy z wejściem głównym połączonym z portami wejścia/wyjścia do łączenia z zewnętrznymi końcówkami wejścia/wyjścia układu FPGA oraz wyjściem oscylatorowym oraz zawiera bufor wejścia/wyjścia, który zawiera bufor wejściowy oraz bufor trójstanowy, przy czym wejście bufora wejściowego jest połączone z dwukierunkowym portem bufora wejścia/wyjścia, z którym połączone jest wyjście bufora trójstanowego, a ponadto wyjście bufora wejściowego jest połączone z wyjściem oscylatorowym, zaś przed dwukierunkowym portem bufora wejścia/wyjścia podłączone jest źródło prądowe dostarczające, zaś wyjście bufora wejściowego jest połączone z wejściem końcówki sterującej bufora trójstanowego poprzez bramkę NOT, a ponadto każdy moduł zatrzaskujący zawiera dwuwejściową bramkę logiczną XOR oraz cztery przerzutniki flip-flop typu D, przy czym czwarty przerzutnik flip-flop typu D posiada asynchroniczne wejście zerujące, zaś wejście zegarowe pierwszego przerzutnika flip-flop typu D oraz drugiego przerzutnika flip-flop typu D są połączone z wyjściem oscylatora pojemnościowego, a wejścia danych pierwszego przerzutnika flip-flop typu D oraz drugiego przerzutnika flip-flop typu D są wejściami zewnętrznymi modułu zatrzaskującego, zaś wyjście pierwszego przerzutnika flip-flop typu D oraz wyjście drugiego przerzutnika flip-flop typu D są połączone z wejściami bramki logicznej XOR, zaś wyjście tej bramki logicznej XOR jest połączone z wejściem trzeciego przerzutnika flip-flop typu D, którego wyjście jest wyjściem bitowym modułu zatrzaskującego, zaś wejścia zegarowe trzeciego przerzutnika flip-flop typu D oraz czwartego przerzutnika flip-flop typu D są połączone z wejściem bramki NOT oscylatora pojemnościowego, a ponadto asynchroniczne wejście zerujące

czwartego przerzutnika flip-flop typu D jest połączone z trzecim wejściem zewnętrznym modułu zatrzaskującego, zaś wyjście czwartego przerzutnika flip-flop typu D jest wyjściem informacyjnym modułu zatrzaskującego do informowania o dostępności bitu danych na wyjściu bitowym, a ponadto do dwóch wejść zewnętrznych przyłączone są dwa oscylatory pierścieniowe, a ponadto porty wejścia/wyjścia oscylatorów pojemnościowych modułów zatrzaskujących połączone są z końcówkami wejścia/wyjścia układu FPGA, zaś pierwsze wejścia zewnętrzne modułów zatrzaskujących są ze sobą połączone oraz drugie wejścia zewnętrzne modułów zatrzaskujących są ze sobą połączone, a ponadto trzecie wejścia zewnętrzne modułów zatrzaskujących są ze sobą połączone, a ponadto pierwsze wejścia zewnętrzne są połączone z wyjściem pierwszego oscylatora pierścieniowego, zaś drugie wejścia zewnętrzne są połączone z wyjściem drugiego oscylatora pierścieniowego, zaś trzecie wejścia zewnętrzne są połączone z asynchronicznym wejściem zerującym, a ponadto wyjścia bitowe modułów zatrzaskujących są połączone z wejściem czterowejściowej bramki XOR, której wyjście połączone jest z zespołem dwóch kaskadowo połączonych ze sobą pierwszego przerzutnika synchronizującego oraz drugiego przerzutnika synchronizującego, przy czym wyjście drugiego przerzutnika synchronizującego jest jednocześnie wyjściem końcowym, a ponadto wyjścia informacyjne modułów zatrzaskujących są połączone z czterema wejściami bramki czterowejściowej, której wyjście jest połączone z wejściem zespołu kaskadowo połączonych ze sobą trzeciego przerzutnika synchronizującego oraz czwartego przerzutnika synchronizującego, przy czym wyjście tego zespołu jest jednocześnie wyjściem informacyjnym zewnętrznym, a ponadto wejścia zegarowe pierwszego przerzutnika synchronizującego, drugiego przerzutnika synchronizującego, trzeciego przerzutnika synchronizującego oraz czwartego przerzutnika synchronizującego są połączone ze sobą i są połączone z wejściem zegarowym.

Korzystnie oscylator pierścieniowy zawiera tablice LUT, które są ze sobą połączone kaskadowo, przy czym tablic LUT jest trzy i mają one taką samą wartość

słowa inicjującego, zaś rodzaj funkcji kombinacyjnej, określany jest jako logiczna negacja albo tablice LUT są dwie, przy czym pierwsza tablica LUT jest negatorem, zaś druga tablica LUT jest buforem.

Dalsze korzyści uzyskiwane są, jeżeli oscylator pierścieniowy ma częstotliwość od 390 MHz do 600 MHz, zaś bramka czterowejściowa jest C-elementem Müllera albo jest bramką AND.

Sposób generowania liczb prawdziwie losowych z wykorzystaniem generatora liczb prawdziwie losowych, według wynalazku charakteryzuje się tym, że sygnały z oscylatorów pierścieniowych dostarcza się do wejść zewnętrznych modułów zatrzaskujących, które w każdym module zatrzaskującym próbkuje się sygnałem z oscylatora pojemnościowego, a następnie dostarcza się je do pierwszego przerzutnika flip-flop typu D oraz do drugiego przerzutnika flip-flop typu D, po czym wartość bitów na wyjściach pierwszego przerzutnika flip-flop typu D oraz drugiego przerzutnika flip-flop typu D prowadzi się poprzez bramkę XOR, na której redukuje się dwie losowe wartości bitów do pojedynczego bitu i poprawia się właściwości statystyczne losowego ciągu bitów, a następnie wartość bitu zapisuje się na trzecim przerzutniku flip-flop typu D oraz za pomocą czwartego przerzutnika flip-flop typu D ustawia się wyjście informacyjne modułu zatrzaskującego i poprzez to wyjście informacyjne informuje się o pojawieniu się nowej wartości bitu wyjściowego na wyjściu bitowym modułów zatrzaskującego oraz wskazuje się możliwość odczytu tej wartości, następnie po odczytaniu tej wartości bitu aktywuje się trzecie wejście zewnętrzne modułu zatrzaskującego i zeruje się czwarty przerzutnik flip-flop typu D, następnie bity odczytane na wyjściach bitowych modułów zatrzaskujących przekazuje się poprzez czterowejściową bramkę XOR kolejno do pierwszego przerzutnika synchronizującego oraz do drugiego przerzutnika synchronizującego, a następnie na wyjście końcowe, zaś poprzez bramkę czterowejściową informację o dostępności bitu na wyjściu końcowym przekazuje się do wyjścia informacyjnego zewnętrznego poprzez drugi przerzutnik synchronizujący, a następnie poprzez

trzeci przerzutnik synchronizujący, a następnie po odczytaniu wartości bitu z wyjścia końcowego ustawia się asynchroniczne wejście zerujące w stan wysoki i zeruje się wyjście informacyjne zewnętrzne, po czym asynchroniczne wejście zerujące przeprowadza się w stan niski.

Korzystnie jako bramkę czterowejściową stosuje się C-element Müllera albo stosuje się bramkę AND.

Nowy generator liczb prawdziwie losowych jest uniwersalny i ma prostą budowę, a ponadto wymaga on niewielkiej liczby zasobów logicznych i może być zaimplementowany w strukturach FPGA dowolnego producenta.

Przedmiot wynalazku został przedstawiony w przykładzie wykonania na rysunku, na którym fig. 1 przedstawia oscylator pojemnościowy, fig 2 – moduł zatrzaskujący pojedynczy bit generatora liczb prawdziwie losowych w widoku schematycznym, fig. 3 – generator liczb prawdziwie losowych w widoku schematycznym, fig. 4 – oscylator pierścieniowy z trzema tablicami LUT generatora liczb prawdziwie losowych w widoku schematycznym, fig. 5 – oscylator pierścieniowy z dwoma tablicami LUT generatora liczb prawdziwie losowych w widoku schematycznym, natomiast fig. 6 – C-element Müllera generatora liczb prawdziwie losowych w widoku schematycznym.

Generator liczb prawdziwie losowych, według wynalazku, w pierwszym przykładzie wykonania zawiera cztery moduły zatrzaskujące MZ1, MZ2, MZ3, MZ4, z których każdy zawiera oscylator pojemnościowy, cztery przerzutniki flip-flop typu D DFF1, DFF2, DFF3, DFF4 oraz bramkę logiczną XOR G2. Oscylator pojemnościowy zawiera wejście główne, które połączone jest z portem wejścia/wyjścia EXTPIN, poprzez który łączony jest on z zewnętrznymi końcówkami wejścia/wyjścia PIN1, PIN2, PIN3, PIN4 układu FPGA oraz zawiera wyjście oscylatorowe OSCOUT. Ponadto oscylator pojemnościowy zawiera bufor wejścia/wyjścia IOBUF, który zawiera bufor wejściowy oraz bufor trójstanowy. Wejście bufora wejściowego połączone jest z dwukierunkowym portem IO bufora wejścia/wyjścia IOBUF, przy czym bufor wejściowy odczytuje poziom logiczny

występujący na tym dwukierunkowym porcie IO, który jednocześnie podłączony jest do portu wejścia/wyjścia EXTPIN i przepisuje go na wyjście O bufora wejściowego, które połączone jest z wyjściem oscylatorowym OSCOUT oscylatora pojemnościowego. Bufor trójstanowy, zależnie od poziomu logicznego występującego na końcówce sterującej T, dla T=0, wymusza na dwukierunkowym porcie IO, a jednocześnie na porcie wejścia/wyjścia EXTPIN stan logiczny występujący na wejściu I bufora wejścia/wyjścia IOBUF, albo, dla T=1, jest w stanie wysokiej impedancji. Przed dwukierunkowym portem IO bufora wejścia/wyjścia IOBUF podłączone jest źródło prądowe dostarczające PULLUP niewielki prąd do zewnętrznej końcówki wejścia/wyjścia PIN1, PIN2, PIN3 PIN4 układu FPGA, poprzez port wejścia/wyjścia EXTPIN. Z niepodłączoną końcówką wejścia/wyjścia PIN1, PIN2, PIN3, PIN4 układu FPGA związana jest pewna pojemność pasożytnicza. Aby powstały oscylacje wyjście O bufora wejściowego jest połączone z wejściem końcówki sterującej T bufora trójstanowego poprzez dodatkową bramkę NOT G1. W układzie FPGA dodatkowa bramka NOT realizowana jest z wykorzystaniem tablicy LUT. W stanie początkowym wyjście O bufora wejściowego będące jednocześnie wyjściem bufora wejścia/wyjścia IOBUF, a tym samym wyjście oscylatorowe OSCOUT oscylatora pojemnościowego, jest w stanie niskim. Wymusza to stan wysokiej impedancji na dwukierunkowym porcie IO bufora wejścia/wyjścia IOBUF. Jednocześnie źródło prądowe dostarczające PULLUP prąd o wartości bardzo niewielkiej, ładuje pojemność pasożytniczą skojarzoną z portem wejścia/wyjścia EXTPIN. Jeżeli napięcie występujące na tym porcie wejścia/wyjścia EXTPIN przekroczy wartość progową dla stanu wysokiego VIH dla bufora wejścia/wyjścia IOBUF, wówczas na wyjściu O bufora wejściowego pojawi się stan wysoki. Spowoduje to, poprzez bramkę NOT G1 wymuszenie poziomu niskiego na dwukierunkowym porcie IO bufora wejścia/wyjścia IOBUF i jednocześnie na porcie wejścia/wyjścia EXTPIN, a tym samym rozładowanie pojemności pasożytniczej. Rozładowanie następuje w znacznie krótszym czasie, związanym z faktem możliwości odbioru prądu o dużej wartości poprzez bufor wyjściowy. Spadek napięcia na porcie

wejścia/wyjścia EXTPIN poniżej wartości progowej dla stanu niskiego VIL, będący wynikiem rozładowania pojemności pasożytniczej, powoduje przejście dwukierunkowego portu IO bufora wejścia/wyjścia IOBUF w stan wysokiej impedancji i jednocześnie następuje ponowne ładowanie pojemności pasożytniczej poprzez źródło prądowe dostarczające PULLUP. Następnie cały proces powtarza się. W jego wyniku, na wyjściu oscylatorowym OSCOUT, otrzymuje się bardzo krótkie impulsy, które zdeterminowane są czasem rozładowania pojemności pasożytniczej, oraz długie przerwy między impulsami wynikające z czasu ładowania pojemności pasożytniczej. Wyjścia oscylatora pojemnościowego są połączone z wejściami zegarowymi pierwszego przerzutnika flip-flop typu D DFF1 oraz drugiego przerzutnika flip-flop typu D DFF2. Czwarty przerzutnik flip-flop typu D DFF4 posiada asynchroniczne wejście zerujące CLR. Wejścia danych pierwszego przerzutnika flip-flop typu D DFF1 oraz drugiego przerzutnika flip-flop typu D DFF2 są jednocześnie wejściami zewnętrznymi modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4, do których doprowadzone są sygnały z dwóch oscylatorów pierścieniowych OSC1, OSC2. Wyjście pierwszego przerzutnika flip-flop typu D DFF1 oraz wyjście drugiego przerzutnika flip-flop typu D DFF2 są dołączone do wejść bramki logicznej XOR G2, której wyjście jest połączone z wejściem danych trzeciego przerzutnika flip-flop typu D DFF3. Wyjście tego trzeciego przerzutnika flip-flop typu D DFF3 jest jednocześnie wyjściem bitowym RBIT modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4, na którym pojawia się bit danych, którego wartość ma charakter losowy. Wejścia zegarowe trzeciego przerzutnika flip-flop typu D DFF3 oraz czwartego przerzutnika flip-flop typu D DFF4 są połączone z wyjściem bramki NOT G1 oscylatora pojemnościowego. Wejście danych czwartego przerzutnika flip-flop typu D DFF4 ustawione jest na stałe w stanie wysokim. Asynchroniczne wejście zerujące CLR czwartego przerzutnika flip-flop typu D DFF4 połączone jest z trzecim wejściem zewnętrznym RRST modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4, zaś wyjście tego czwartego przerzutnika flip-flop typu D DFF4 jest jednocześnie wyjściem informacyjnym RY modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4, które informuje o dostępności bitu danych

na wyjściu bitowym RBIT. Porty wejścia/wyjścia EXTPIN oscylatorów pojemnościowych w modułach zatrzaskujących MZ1, MZ2, MZ3, MZ4 są połączone z zewnętrznymi końcówkami wejścia/wyjścia PIN1, PIN2, PIN3, PIN4 układu FPGA, które nie mogą być połączone elektrycznie z żadnymi obwodami zewnętrznymi. Pierwsze wejścia zewnętrzne ROSC1 modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są ze sobą połączone, drugie wejścia zewnętrzne ROSC2 modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są ze sobą połączone oraz trzecie wejścia zewnętrzne RRST modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są ze sobą połączone. Pierwsze wejścia zewnętrzne ROSC1 modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są połączone z wyjściem pierwszego oscylatora pierścieniowego OSC1, zaś drugie wejścia zewnętrzne ROSC2 modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są połączone z wyjściem drugiego oscylatora pierścieniowego OSC2. Trzecie wejścia zewnętrzne RRST modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są natomiast połączone z asynchronicznym wejściem zerującym CLR. Wyjścia bitowe RBIT wszystkich modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są połączone z wejściem czterowejściowej bramki XOR G10, której wyjście połączone jest z zespołem dwóch kaskadowo połączonych ze sobą przerzutników synchronizujących: pierwszego przerzutnika synchronizującego DFF20 oraz drugiego przerzutnika synchronizującego DFF21. Wyjście drugiego przerzutnika synchronizującego DFF21 jest jednocześnie wyjściem końcowym RNDBIT generatora liczb prawdziwie losowych. Wyjścia informacyjne RY modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są połączone z wejściami bramki czterowejściowej G11, której wyjście jest połączone z wejściem zespołu kaskadowo połączonych dwóch przerzutników synchronizujących: trzeciego przerzutnika synchronizującego DFF22 oraz czwartego przerzutnika synchronizującego DFF23, przy czym wyjście tego zespołu jest jednocześnie wyjściem informacyjnym zewnętrznym RDY, na którym pojawienie się poziomu wysokiego informuje o dostępności bitu na wyjściu końcowym RNDBIT. Wejścia zegarowe pierwszego przerzutnika synchronizującego DFF20, drugiego przerzutnika synchronizującego DFF21,

trzeciego przerzutnika synchronizującego DFF22 oraz czwartego przerzutnika synchronizującego DFF23 są ze sobą połączone i jednocześnie połączone są one z wejściem zegarowym CLK. Pierwszy oscylator pierścieniowy OSC1 i drugi oscylator pierścieniowy OSC2 zawierają kaskadowo połączone ze sobą tablice LUT LUT5, które są podstawowymi elementami logicznymi wewnątrz układu FPGA, realizującymi dowolną funkcję kombinacyjną pięciu zmiennych wejściowych. Wyjście ostatniej w szeregu tablicy LUT LUT5 jest połączone z wejściem pierwszej w szeregu tablicy LUT LUT5. Tablica LUT LUT5 pod względem funkcjonalnym jest utożsamiana z multiplekserem o pięciu wejściach adresowych I0, I1, I2, I3, I4 i trzydziestu dwóch wejściach danych, na które podaje się odpowiednie wartości zer i jedynek stanowiących słowo inicjujące INIT tablicy LUT LUT5. Wartość tego słowa podaje się stosując zapis szesnastkowy. Wyjście multipleksera jest jednocześnie wyjściem O tablicy LUT LUT5, na którym pojawia się wartość logiczna funkcji kombinacyjnej zmiennych wejść adresowych I0, I1, I2, I3, I4, zdeterminowana postacią słowa inicjującego INIT. W pierwszym oscylatorze pierścieniowym OSC1 są trzy tablice LUT LUT5, które zawierają taką samą wartość słowa inicjującego INIT, która określa rodzaj funkcji kombinacyjnej jako logiczną negację. Drugi oscylator pierścieniowy OSC2 zawiera dwie tablice LUT LUT5, z których pierwsza tablica LUT LUT5 pełni również funkcję negatora, zaś druga tablica LUT LUT5 pełni funkcję bufora i nie zmienia wartości logicznej sygnału występującego na swoim wejściu. Każda z tablic LUT LUT5 charakteryzuje się określonym czasem propagacji, a ich kaskadowe połączenie wraz z połączeniem wyjścia ostatniej w szeregu tablicy LUT LUT5 z wejściem pierwszej w szeregu tablicy LUT LUT5, powoduje, że cały układ oscyluje z częstotliwością zależną od czasu opóźnienia sygnału wnoszonego przez kaskadę połączonych tablic LUT LUT5. Dla układów FPGA Xilinx z rodziny Artix-7 pierwszy oscylator pierścieniowy OSC1 umożliwia uzyskanie częstotliwości o wartości 392 MHz, zaś drugi oscylator pierścieniowy OSC2 umożliwia uzyskanie częstotliwości o wartości 590 MHz. Bramka czterowejściowa G11 jest C-elementem Müllera, który jest asynchronicznym elementem sekwencyjnym, który

stanowi pojedyncza tablica LUT LUT5, której wyjście Y jest połączone z wejściem I4 tej bramki oraz z odpowiednim słowem inicjującym INIT. Na wyjściu tego C-elementu Müllera pojawia się wartość logiczna „1" od momentu gdy wszystkie wejścia C-elementu Müllera zostaną ustawione w stan wysoki, aż do momentu, gdy wszystkie wejścia elementu zostaną wyzerowane. Przy zastosowaniu C-elementu Müllera, gdy wyjście informacyjne zewnętrzne RDY przejdzie w stan niski, wówczas trzeci przerzutnik synchronizujący DFF22 oraz czwarty przerzutnik synchronizujący DFF23, jak również wszystkie wyjścia informacyjne RY modułów zatrzaskujących MZ1, MZ2, MZ3, MZ4 są wyzerowane.

Generator liczb prawdziwie losowych, według wynalazku, w drugim przykładzie wykonania, jest taki jak w przykładzie pierwszym, z tym, że bramkę czterowejściową G11 stanowi zwykła bramka AND.

Sposób generowania liczb prawdziwie losowych z wykorzystaniem generatora liczb prawdziwie losowych, według wynalazku, w pierwszym przykładzie realizacji realizuje się tak, że sygnały z dwóch oscylatorów pierścieniowych OSC1, OSC2 dostarcza się do wejść zewnętrznych ROSC1, ROSC2 modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4 i próbkuje się je sygnałem z oscylatora pojemnościowego. Wartość częstotliwości sygnałów dostarczanych do wejść zewnętrznych ROSC1, ROSC2 musi być znacznie większa od częstotliwości sygnału oscylatora pojemnościowego. Zadaniem modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4 jest wygenerowanie bitu, którego wartość będzie miała charakter możliwie jak najbardziej losowy. Źródłem losowości jest zjawisko drżenia fazy oscylatora pojemnościowego oraz dwóch oscylatorów pierścieniowych OSC1, OSC2, a także potencjalnie mogące wystąpić zjawisko niestabilności w pierwszym przerzutniku flip-flop typu D DFF1 oraz drugim przerzutniku flip-flop typu D DFF2. Sygnał z pierwszego wejścia zewnętrznego ROSC1 jest kierowany do pierwszego przerzutnika flip-flop typu D DFF1, zaś sygnał z drugiego wejścia zewnętrznego ROSC2 jest kierowany do drugiego przerzutnika flip-flop typu D DFF2. Ponieważ faza sygnału zegarowego, pochodzącego z oscylatora pojemnościowego, ma charakter losowy, jak również fazy sygnałów na wejściach

zewnętrznych ROSC1, ROSC2 mają charakter losowy i nie są w żaden sposób skorelowane z sygnałem z oscylatora pojemnościowego, to również wartość zatrzaskiwana w pierwszym przerzutniku flip-flop typu D DFF1 oraz w drugim przerzutniku flip-flop typu D DFF2 ma charakter losowy. Ponadto losowość może zostać pogłębiona przez zjawisko metastabilności mogące wystąpić w pierwszym przerzutniku flip-flop typu D DFF1 oraz drugim przerzutniku flip-flop typu D DFF2. Zjawisko metastabilności może mieć miejsce, gdy zmieni się wartość pojawiająca się na wejściach danych przerzutników flip-flop typu D DFF1, DFF2 tuż przed lub tuż po nadejściu aktywnego, narastającego zbocza na wejściu zegarowym pierwszego przerzutnika flip-flop typu D DFF1 oraz drugiego przerzutnika flip-flop typu D DFF2, których zachowanie w stanie metastabilnym ma z natury charakter nieprzewidywalny. Następnie wartość bitów uzyskanych na wyjściach pierwszego przerzutnika flip-flop typu D DFF1 oraz drugiego przerzutnika flip-flop typu D DFF2 prowadzi się poprzez bramkę XOR G2 do trzeciego przerzutnika flip-flop typu D DFF3, na którym jest zapamiętywana. Użycie bramki XOR G2, w której redukuje się dwie losowe wartości bitów do pojedynczego bitu, dodatkowo poprawia właściwości statystyczne losowego ciągu bitów. Zapamiętanie losowego bitu w trzecim przerzutniku flip-flop typu D DFF3 następuje w momencie pojawienia się zbocza opadającego sygnału z oscylatora pojemnościowego. Jest więc ono opóźnione w stosunku do momentu zatrzaskiwania bitów w pierwszym przerzutniku flip-flop typu D DFF1 oraz w drugim przerzutniku flip-flop typu D DFF2, które następuje podczas zbocza narastającego. W momencie zapisywania wartości bitu w trzecim przerzutniku flip-flop typu D DFF3, ustawia się również wyjście informacyjne RY czwartego przerzutnika flip-flop typu D DFF4, przez które informuje się o pojawieniu się nowej wartości bitu wyjściowego na wyjściu bitowym RBIT i jednocześnie wskazuje się moment, kiedy tę wartość można odczytać. Po odczytaniu tej wartości bitu czwarty przerzutnik flip-flop typu D DFF4 zeruje się poprzez aktywowanie na krótką chwilę trzeciego wejścia zewnętrznego RRST modułu zatrzaskującego MZ1, MZ2, MZ3, MZ4. Odczytany na wyjściu bitowym RBIT bit wyjściowy

przekazuje się, poprzez czterowejściową bramkę XOR G10 do zespołu przerzutników: pierwszego przerzutnika synchronizującego DFF20 oraz drugiego przerzutnika synchronizującego DFF21. Następnie bit kieruje się na wyjście końcowe RNDBIT. Informację o dostępności bitu na wyjściu końcowym RNDBIT przekazuje się poprzez bramkę czterowejściową G11, będącą C-elementem Müllera do zespołu trzeciego przerzutnika synchronizującego DFF22 oraz czwartego przerzutnika synchronizującego DFF23, a następnie kieruje się ją na wyjście informacyjne zewnętrzne RDY. Zadaniem zespołu pierwszego przerzutnika synchronizującego DFF20 i drugiego przerzutnika synchronizującego DFF21 oraz zespołu trzeciego przerzutnika synchronizującego DFF22 oraz czwartego przerzutnika synchronizującego DFF23 jest synchronizacja wewnętrznych sygnałów generatora liczb prawdziwie losowych z zewnętrznym synchronicznym systemem, który odczytuje i przetwarza ciąg bitów wytwarzanych przez ten generator. Obecność wartości bitu wytworzonego przez ten generator liczb prawdziwie losowych jest sygnalizowana ustawieniem wyjścia informacyjnego zewnętrznego RDY. Po dokonaniu, przez system zewnętrzny, odczytu wartości bitu występującego na wyjściu końcowym RNDBIT, asynchroniczne wejście zerujące CLR generatora liczb prawdziwie losowych ustawia się w stan wysoki, zaś aktywacja tego asynchronicznego wejścia zerującego CLR powoduje wyzerowanie wyjścia informacyjnego zewnętrznego RDY, a następnie powrót asynchronicznego wejścia zerującego CLR do nieaktywnego poziomu niskiego. Wyjście informacyjne zewnętrzne RDY ustawia się ponownie, gdy gotowy do odczytu będzie kolejny bit udostępniony na wyjściu końcowym RNDBIT.

Sposób generowania liczb prawdziwie losowych z wykorzystaniem generatora liczb prawdziwie losowych, według wynalazku, w drugim przykładzie realizacji, taki jak w przykładzie pierwszym z tym, że jako bramkę czterowejściową G11, stosuje się czterowejściową bramkę AND.

Jakość generatora liczb prawdziwie losowych według wynalazku zbadano zgodnie z wytycznymi dokumentu NIST SP 800-22 za pomocą dostarczonego przez instytut NIST specjalistycznego oprogramowania. Badanie przeprowadzono

z wykorzystaniem odpowiednio przygotowanego zintegrowanego systemu cyfrowego zaimplementowanego w układzie FPGA znajdującego się na płycie ewaluacyjnej Nexys Video Artix-7, który zawiera mikroprocesor MicroBlaze oraz moduły towarzyszące takie jak generator częstotliwości taktującej, pamięć lokalna, pamięć DDR3 oraz moduł generatora liczb prawdziwie losowych, które połączone były za pomocą standardowej magistrali AXI4. Zadaniem systemu jest odczyt kolejnych bitów wytwarzanych przez generator liczb prawdziwie losowych i zapisywanie ich w zewnętrznej pamięci DDR3. Po zgromadzeniu odpowiedniej liczby bitów, są one przesyłane za pomocą łącza szeregowego UART-USB do komputera PC, gdzie mogą być poddane odpowiednim testom statystycznym. Przy pomocy systemu cyfrowego gromadzi się i przekazuje do komputera PC ciągi bitów z generatora liczb prawdziwie losowych o długości 128Mbit – 134217728 bitów. Następnie za pomocą oprogramowania opracowanego przez instytut NIST dany ciąg analizuje się statystycznie dokonując jego podziału na 1000 sekwencji o długości 134271 bitów każda. W tabeli 1 pokazano wynik analizy ciągu losowego pochodzącego z generatora liczb prawdziwie losowych. Kolumny od C1 do C10 zawierają częstotliwości wystąpień p-wartości w jednostkowym przedziale podzielonym na 10 dyskretnych wartości, kolumna P-Value zawiera p-wartość, która obliczana jest poprzez zastosowanie formuły chi-square, kolumna Proportion zawiera proporcje ilości sekwencji, które pozytywnie przeszły testy, zaś kolumna Statistical Test zawiera nazwę zastosowanego testu. Kolumny od C1 do P-Value zawierają informacje o tym, czy p-wartości rozłożone są w sposób jednolity wewnątrz podziału jednostkowego. Próg zaliczenia danego testu statystycznego sprawdzającego losowość wynosił 980, z wyjątkiem testów: Random Excurions oraz Random Excurions Variant, dla których próg zaliczenia wynosił 161. Przeprowadzone badanie wykazało, że generator liczb prawdziwie losowych według wynalazku spełnia wszystkie testy statystyczne według instytutu NIST. Badania polegające na gromadzeniu 128 Mbit ciągów danych z generatora i ich analizie powtarzano wielokrotnie. Za każdym razem uzyskiwano pozytywny wynik badań co świadczy o tym, że ciągi są rzeczywiście losowe i ich zawartość jest

nieprzewidywalna.

Tabela 1

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-Value	Proportion	Statistical Test
87	90	118	101	91	86	100	114	100	113	0.193767	992/1000	Frequency
97	96	104	103	94	121	109	83	84	109	0.194813	991/1000	BlockFrequency
96	88	94	111	91	104	95	109	114	98	0.616305	987/1000	CumulativeSums
87	90	120	108	97	97	107	92	91	111	0.299736	994/1000	CumulativeSums
102	99	95	95	81	94	88	100	121	125	0.055010	992/1000	Runs
89	102	103	97	103	91	108	108	93	106	0.878618	989/1000	LongestRun
116	84	95	106	109	85	127	81	102	95	0.018036	993/1000	Rank
93	97	99	108	98	112	94	82	109	108	0.558502	992/1000	FFT
89	95	86	113	110	109	103	104	93	98	0.564639	990/1000	NonOverlappingTemplate
97	86	113	89	99	112	102	95	92	115	0.385543	981/1000	OverlappingTemplate
95	125	116	99	99	81	99	93	107	86	0.074791	991/1000	AproximateEntropy
17	26	15	21	8	21	9	16	17	17	0.053841	166/167	RandomExcursions
15	20	23	9	18	19	9	20	18	16	0.196260	165/167	RandomExcurionsVariant

110	90	114	98	101	87	88	110	102	100	0.516113	989/1000	Serial
102	89	94	103	86	111	105	110	106	94	0.653773	991/1000	Serial
90	98	72	105	102	111	113	106	102	101	0.187581	988/1000	LinearComplexity

000001749
POLITECHNIKA RZESZOWSKA
im. Ignacego Łukasiewicza
35-959 Rzeszów, Al. Powstańców Warszawy 12
tel. 17 865-11-00
NIP 8130266999

RZECZNIK PATENTOWY
Piotr Okarmus