dr hab. inż. Andrzej Borys, prof. nadzw. AMG
Akademia Morska w Gdyni, Wydział Elektryczny
Katedra Telekomunikacji Morskiej
ul. Morska 81-87
81-225 Gdynia

Gdynia, 15.02.2017 r.

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY WYDZIAŁU ELEKTRONIKI I TELEKOMUNIKACJI POLITECHNIKI POZNAŃSKIEJ W POZNANIU

Tytuł rozprawy: **Wykorzystanie zasobów FPGA do budowy szybkich generatorów pseudolosowych**

Autor rozprawy: **mgr inż. Michał Jaworski**

1. ***Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez autora?***

Tematem przedłożonej mi do recenzji pracy doktorskiej jest wykorzystanie technologii FPGA (ang. *field programmable gate array*) do budowy szybkich generatorów liczb pseudolosowych. Ogólnie ujmując, autor rozprawy przeanalizował w niej i zbadał eksperymentalnie przydatność układów programowalnych FPGA w konstrukcji sprzętowych generatorów liczb pseudolosowych, które umożliwiają osiąganie przepływności większych od 10 Gbit/s.

Na przeprowadzoną analizę i badania składają się: poszukiwania odpowiednich algorytmów implementacyjnych wśród opublikowanych w literaturze, sprawdzenie ich własności statystycznych, implementacja w technologii FPGA wybranych rodzin algorytmów, algorytmów łączonych oraz z dołączanym przetwarzaniem (dla poprawy własności statystycznych generowanych ciągów), przeprowadzenie odnośnych testów oraz interpretacja ich wyników.

Teza rozprawy została sformułowana w rozdz. 1 *Wstęp* następująco: układy FPGA pozwalają na skonstruowanie sprzętowych generatorów liczb losowych, które spełniają testy statystyczne organizacji NIST (ang. *National Institute of Standards and Technology*) i umożliwiają pracę w swoich komunikacyjnych zastosowaniach z przepływnościami powyżej 10 Gbit/s.

Powyższa teza została sformułowana dostatecznie jasno.

2. ***Jaka jest przydatność rozprawy z punktu widzenia nauk technicznych, czy założenia przyjęte przez autora są uzasadnione?***

Ocenianą rozprawę można zakwalifikować jako pracę o charakterze aplikacyjnym, co znajduje również odzwierciedlenie w jej tytule. Jej przydatność dla nauk technicznych, a w szczególności dla takich dyscyplin jak: elektronika, informatyka i telekomunikacja, można ocenić po zebranych i przedstawionych w niej przyczynkach. Są to przyczynki natury głównie praktycznej (aplikacyjnej). Zebrałem je i scharakteryzowałem w poniższych punktach:

a) Opracowanie, uzasadnienie i dobór kryteriów oceny przydatności opublikowanych w literaturze algorytmów generacji ciągów pseudolosowych dla konstrukcji uniwersalnego,

skalowalnego generatora, realizowanego sprzętowo w technologii FPGA. Kryteria te zostały omówione w rozdz. 6 rozprawy (zatytułowanym *Metoda*).

b) Przeprowadzenie eksperymentów programowych w celu wydzielenia ze zbioru rodzin algorytmów generacji liczb pseudolosowych opublikowanych w literaturze podzbioru takich, które posiadają cechy użyteczne w sensie kryteriów z pkt. a) powyżej. W wyniku wzmiankowanych eksperymentów stwierdzono, że w dalszej analizie i poszukiwaniach należy wziąć pod uwagę tylko następujące rodzaje generatorów:
   - kongruencyjne generatory multiplikatywne, będące przedstawicielami szerszej klasy tzw. liniowych generatorów kongruencyjnych,
   - generatory w postaci rejestrów przesuwnych z liniowym sprzężeniem zwrotnym (w wersji podstawowej),
   - generatory występujące pod nazwą Xorshift (bazują one na algorytmach zaproponowanych przez Marsaglię w roku 2003; wykorzystują operację przesunięcia bitowego i operację logiczną XOR),
   - zmodyfikowane generatory komórkowe nazywane liniowymi hybrydowymi automatami komórkowymi.

c) Przeprowadzenie testów statystycznych rodzin generatorów wymienionych w pkt. b) powyżej dla różnych wartości parametrów je definiujących i różnych warunków początkowych. Wyniki tych obszernych testów przedstawiono w tabelach zamieszczonych w rozprawie w podrozdz. 7.1.1 – 7.1.4, a ich analizę porównawczą, podsumowanie i wnioski w podrozdziale następnym, 7.1.5. Stwierdzono, że w świetle powyższej analizy statystycznej oraz przy uwzględnieniu innych uwarunkowań, najlepszymi kandydatami na uniwersalne, skalowalne generatory liczb pseudolosowych w implementacji przy pomocy technologii FPGA są kongruencyjne generatory multiplikatywne i generatory typu Xorshift.

d) Implementacja sprzętowa w technologii FPGA przykładowych kongruencyjnych generatorów multiplikatywnych i generatorów typu Xorshift – z zastosowaniem, w razie konieczności, metody poprawy ich własności statystycznych.

e) Opracowanie i implementacja różnych wariantów skalowalnych (w sensie definicji skalowalności generatora podanej w podrozdz. 7.1 pracy) generatorów liczb losowych i ich przebadanie. Wyniki w tym zakresie zostały przedstawione w podrozdz. 7.2.5.

f) Opracowanie, przy wykorzystaniu uprzednio uzyskanych wyników badań, uniwersalnego modułu skalowalnego generatora liczb pseudolosowych. Kod informatyczny opisujący ten moduł został przedstawiony w podrozdz. 7.3 rozprawy. W tym ostatnim podrozdziale dokonano również porównania zaproponowanej implementacji z innymi rozwiązaniami opublikowanymi w literaturze (patrz: tabela 7.79). Zaproponowane w tej rozprawie rozwiązanie charakteryzuje się zestawem parametrów będących jednymi z najlepszych.

Liczba i ranga przyczynków wymienionych powyżej pozwala stwierdzić, że składająca się z nich rozprawa wnosi istotny wkład do wiedzy o implementacjach generatorów liczb losowych. Jest to nowa wiedza, która będzie przydatna w dalszych badaniach naukowych i praktycznych weryfikacjach w ww. obszarze nauk technicznych. Nowe jest zaproponowane w podrozdz. 7.3 rozwiązanie - wieńczące wysiłki i trud włożony w przeprowadzone badania - uniwersalnego, skalowalnego modułu generatora liczb pseudolosowych. Moduł ten może być od zaraz zastosowany w wielu systemach elektronicznych, telekomunikacyjnych i informatycznych w celu polepszenia ich parametrów użytkowych.

Projektowanie złożonych układów, jakimi niewątpliwie są uniwersalne, skalowalne generatory ciągów pseudolosowych, jest zadaniem niestandardowym, skomplikowanym i wymagającym rozwiązania wielu problemów z zakresu elektroniki i informatyki. Z tego powodu jest to zawsze zadanie na miarę pracy doktorskiej.

Poczynione w pracy założenia są słuszne. Zostały one zweryfikowane przez autora w przeprowadzonych eksperymentach programowych, symulacjach, badaniach statystycznych i pomiarach generatorów ciągów pseudolosowych wykonanych w technologii FPGA.

3. ***Czy autor rozwiązał postawione zagadnienie i czy użył właściwej do tego metody?***

Autor rozwiązał postawione zagadnienie i użył w tym celu właściwych narzędzi matematycznych i programistycznych, metod badań statystycznych, projektowych oraz metod pomiarowych. Nie ustrzegł się jednakże przed różnymi potknięciami i usterkami, których dotyczą następujące uwagi szczegółowe:

a) Oferowana przepływność projektowanych i implementowanych, skalowalnych generatorów liczb losowych jest wymieniona przez autora jako jeden z podstawowych parametrów projektowych tych generatorów. W pracy nie podano jednakże żadnego wzoru, który by ją określał, np. w zależności od częstotliwości sygnału zegara, liczby generatorów składowych, parametrów we wzorze (wzorach) opisujących zastosowany algorytm generacji, szybkości przetwarzania sygnałów w części poprawiającej wybrane charakterystyki statystyczne generatorów itp. Z tego też powodu w treści pracy trudno znaleźć informację, jak wzmiankowaną wielkość: wartość oferowanej przepływności bitowej wprowadzał do każdego ze swoich projektów (ustalał w projekcie) autor rozprawy.

b) Podobna uwaga, jak w pkt. a) powyżej, odnosi się do długości generowanych słów. Trudno doszukać się w treści pracy, jak tę wielkość zadawał (wprowadzał) w projekcie danego generatora autor pracy.

c) W pracy brakuje opisu zastosowanej metody poprawy wybranych własności statystycznych generatorów liczb losowych. Z tego powodu niektóre fragmenty pracy są niezrozumiałe. Mimo wielu podjętych przeze mnie prób nie udało się mi dokładnie zrozumieć, na czym polegają manipulacje wartościami parametrów R, α i L. (Nie znalazłem w treści pracy precyzyjnych definicji tych parametrów.)

d) Nie podano w rozprawie, czy istnieją jakieś alternatywne metody poprawy własności statystycznych generatorów liczb pseudolosowych – w stosunku do tej, która została zastosowana w pracy.

e) Podany na str. 125 listing kodu informatycznego opracowanego modułu uniwersalnego, skalowalnego generatora liczb losowych jest mało czytelny - z powodu użytego koloru (jasnoniebieski) i wielkości czcionki. Listing ten powinien posiadać podpis i powinien również posiadać objaśnienie, w jakim go sporządzono języku programowania.

f) Podobna uwaga, jak uwaga e) powyżej, odnosi się także do innych miejsc w pracy, w których występują fragmenty kodu informatycznego napisanego z użyciem czcionki w kolorze jasnoczerwonym lub jasnoniebieskim.

g) Symbol F został zdefiniowany w mało widocznym miejscu na str. 73. Ta definicja powinna zostać powtórzona w dalszej części pracy, gdzie zostały zamieszczone tabelki z wynikami badań statystycznych generatorów.

h) Znaczenie parametrów a, b i c generatorów liczb pseudolosowych typu Xorshift można wywieść ze wzoru (4.21) podanego na str. 52. Należało się powołać na ten wzór w tabelach 7.33, 7.34, 7.35, 7.36 i w innych w dalszej części pracy, w których podane zostały wartości wzmiankowanych parametrów dla różnych wersji generatorów typu Xorshift, w szczególności, że parametr a jest używany w pracy na oznaczenie także innych wielkości.

4. ***Jaki charakter ma rozprawa (teoretyczny, doświadczalny, konstrukcyjny), jaka jest jej pozycja w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?***

Rozprawa ma charakter wybitnie aplikacyjny. Jej celem było (jak to sformułowano w rozdz. 1 *Wstęp*): „wykazanie prawdziwości tezy, że układy FPGA można z powodzeniem wykorzystać do budowy szybkich generatorów liczb pseudolosowych oraz zaproponowanie uniwersalnego, skalowalnego generatora pseudolosowego spełniającego wszystkie testy NIST, który w postaci modułu mógłby być dołączony do dowolnego projektu realizowanego w technologii FPGA". Cel ten został w pełni osiągnięty.

Nie ma w ocenianej pracy przyczynków teoretycznych do (zresztą bardzo trudnej) teorii generatorów liczb pseudolosowych.

W zakresie projektowania i realizacji generatorów liczb pseudolosowych przedłożona rozprawa zawiera wiele oryginalnych rozwiązań szczegółowych. Niektóre z nich autor rozprawy już opublikował (jako autor lub współautor) w czasopismach naukowych lub przedstawił w swoich wystąpieniach na liczących się konferencjach.

Oceniana praca nie odbiega od światowego poziomu prac doktorskich w tematyce związanej z technologią FPGA i implementacjami algorytmów generacji ciągów liczb pseudolosowych.

5. ***Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora?***

Na to pytanie można odpowiedzieć tak: Oryginalność rozprawy jest związana z przyczynkami, które wniósł autor do nauki poprzez tę pracę. Wszystkie je wymieniłem już w pkt. 2 mojej recenzji; doliczyłem się tam sześciu takich istotnych, oryginalnych przyczynków. Składają się one na i stanowią o oryginalności bronionej rozprawy. Innymi słowy, można powiedzieć także tak, że osiągnięcia wymienione i krótko przedstawione w pkt. 2 powyżej stanowią samodzielny i oryginalny dorobek autora rozprawy.

6. ***Jakie są słabe strony rozprawy i jej główne wady?***

Słabą stroną przedstawionej pracy są występujące niekiedy niespójności stylu i we wzorach (np. parametr a użyty w innym sensie we wzorach (4.1) i (4.8) niż we wzorze (4.21)). Według mnie cały materiał z rozdz. 5 (dotyczący własności statystycznych i implementacji wybranych generatorów) powinien być połączony z materiałem z poprzedzającego rozdz. 4 (dotyczącego przeglądu rozwiązań generatorów pseudolosowych) i umieszczony w jednym rozdziale.

Często objaśnienia do rysunków i tabel są niepełne albo umieszczone w miejscach dalekich od nich, co utrudnia pełne zrozumienie tych rysunków i tabel.

7. ***Czy rozprawa świadczy o dostatecznej wiedzy autora i znajomości współczesnej literatury z zakresu dyscypliny naukowej, jakiej rozprawa dotyczy?***

Spis literatury na końcu rozprawy obejmuje 145 pozycji, w tym 3 publikacje autorskie lub współautorskie, na poruszone w niej zagadnienia. Tak bogaty spis cytowanej literatury, a także sposób jej wykorzystania (ujawniający się przy czytaniu rozprawy), świadczą o dużej wiedzy autora i znajomości współczesnej literatury z zakresu dyscypliny naukowej dotyczącej jego rozprawy.

8. ***Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?***

Autor przedstawił osiągnięte wyniki w sposób poprawny i przekonujący. Uzyskał to poprzez dobrą organizację pracy i używając poprawnego języka polskiego. Pewną liczbę różnego rodzaju potknięć, które jednakże nie zmieniają ogólnego, dobrego wrażenia, jakie odnosi się czytając rozprawę, wymieniam poniżej:

a) Skrót Xorshift32 użyty na str. 5 rozprawy powinien się również znaleźć w wykazie skrótów i oznaczeń zamieszczonym na str. 4.

b) Występują drobne błędy języka angielskiego w streszczeniu rozprawy w tym języku na str. 6.
c) Na str. 7 występuje niezręczność językowa „z łatwością powielalny". Proponuję użyć takiego zwrotu: „dający się łatwo powielać".
d) Występują często tzw. literówki (np. na str. 8 u góry napisano „określono generatory oferujący ..", na str. 24 „Spratan-6", na str. 34 „bark", na str. 43 „sterując brakami", w podpisie pod rys. 4.2 „Galios", na str. 59 „w skalowalnym generatorze sprzętowych" oraz w wielu innych miejscach).
e) Czasem szwankuje interpunkcja: najczęściej jest to brak przecinków lub są one postawione w niewłaściwych miejscach.
f) Na str. 15 wielkość U(0,1) nie została zdefiniowana.
g) Niejasne de facto to samo objaśnienie pod wzorami (4.2) i (4.3). Za pierwszym razem mamy: „.. okres ciągu wyjściowego generatora MCG wynosi M-1", natomiast za drugim: „.. znacznie dłuższy maksymalny okres wytwarzanych ciągów wynoszący M-1".
h) Na str. 73, w ostatnim punkcie z listy górnej, użyto niepoprawnego określenia „istnieją bardziej optymalne ustawienia".

9. Czy i jaka jest przydatność rozprawy dla gospodarki narodowej?

Opracowany, zaimplementowany w technologii FPGA i przetestowany przez autora rozprawy moduł uniwersalnego, skalowalnego generatora liczb pseudolosowych - o wyróżniających się parametrach - może być zastosowany w gospodarce narodowej w bardzo wielu systemach elektronicznych, telekomunikacyjnych i informatycznych w celu poprawy ich funkcjonowania. Obszar zastosowań takich generatorów jest naprawdę bardzo szeroki.

10. Czy rozprawa spełnia wymagania stawiane rozprawom doktorskim przez obowiązujące przepisy?

W recenzowanej rozprawie zebrano wiele nowych, wartościowych wyników z zakresu implementacji algorytmów generacji liczb pseudolosowych sprzętowo z wykorzystaniem technologii FPGA. Znaczenie dla nauki tych rezultatów (razem wziętych) jest, według mnie, na miarę rozprawy doktorskiej. Podsumowując zatem, uważam, że przedłożona rozprawa spełnia wymagania stawiane przez stosowne przepisy rozprawom doktorskim i wnioskuję o jej dopuszczenie do publicznej obrony.

Andrzej Borys