"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Projektowanie kryptograficznych układów cyfrowych	Designing cryptographic digital circuits
Kod przedmiotu	WCYKSCSI_.....	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	studia pierwszego stopnia	
Rodzaj przedmiotu		
Obowiązuje od naboru	2021/2022	

Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS

semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS
	razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium	
VI	60x	20		40+			5.0
razem		20		40			5.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 6 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne
Autor	dr inż. Piotr Bora
Jednostka odpowiedzialna za przedmiot	WCY/IMiK/ZK
Skrócony opis przedmiotu	• Wykład i ćwiczenia laboratoryjne z wykorzystaniem platform sprzętowych z układami FPGA.

Pełny opis przedmiotu (treści programowe)

lp.	Semestr VI temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Wprowadzenie do przedmiotu: ewolucja i stan obecny układów programowalnych: architektury, techniki programowania, narzędzia i metodologia projektowania	2				
2	Klasyfikacja układów cyfrowych, układy specjalizowane ASIC, struktury programowalne FPGA i CPLD - przegląd architektur bloków logicznych, topologii połączeń i technik programowania	3				
3	Przegląd rodzin układów PLD firmy INTEL (dawniej ALTERA); omówienie architektur, parametrów technicznych, możliwości funkcjonalnych i implementacyjnych	3				
4	Analiza problemu wyboru układu pod kątem aplikacji zapewnienie specyficznych wymagań co do parametrów elektrycznych, charakterystyk dynamicznych, aspektów strategicznych, ekonomicznych itp.	2				
5	Wprowadzenie do narzędzi komputerowego projektowania: proces opracowania układu od opisu do jego realizacji, języki opisu układów i systemów, struktura projektu, biblioteki funkcji standardowych i specjalizowanych, megafunkcje, wirtualne megafunkcje. Charakterystyka systemu QUARTUS II : proces tworzenia projektu	10				
6	Zapoznanie ze środowiskiem Quartus Prime i ModelSim: kompilacja i symulacja gotowego projektu w języku opisu sprzętu wraz z zapoznaniem się z podstawowymi możliwościami oprogramowania			4		
7	Język Verilog HDL: projektowanie układów kominacyjnych oraz sekwencyjnych (rejestrowych, liczników, sterowania, pamięciowych) oraz układów arytmetycznych ze szczególnym naciskiem na efektywność układową i wydajnościową implementacji sprzętowej			10		
8	Koprocesor algorytmu Trivium: propozycja architektury koprocesora, zapoznanie się z typową architekturą, implementacja elementów kombinacyjnych i sekwencyjnych na podstawie wzorca projektowego i proste testowanie symulacyjne			4		
9	Koprocesor algorytmu SHA2-256: propozycja architektury koprocesora, zapoznanie się z typową architekturą, implementacja elementów kombinacyjnych i sekwencyjnych na podstawie wzorca projektowego i testowanie symulacyjne			8		

	lp.	Semestr VI temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
	10	Koprocesor algorytmu AES-256: propozycja architektury koprocesora, zapoznanie się z typową architekturą, implementacja elementów kombinacyjnych i sekwencyjnych na podstawie wzorca projektowego, integracja wielu elementów i zaawansowane testowanie symulacyjne			14		
		Razem	20		40		

Literatura

podstawowa:
- T.Łuba, et al., Specjalizowane układy cyfrowe w strukturach programowalnych PLD i FPGA, 1997
- Z.Salcic, A.Smailagic, Digital System Design and Prototyping Using Field Programmable Logic, 1997

uzupełniająca:
- Jean-Pierre Deschamps, Jose Luis Imana, Gustavo D. Sutter, "Hardware Implementation of Finite-Field Arithmetic", 2009
- Jean-Pierre Deschamps, Gustavo D. Sutter, Enrique Cantó, "Guide to FPGA implementation of Arithmetic Functions", 2012
- Henri Cohen, Gerhard Frey, "Handbook of Elliptic and Hyperelliptic Curve Cryptography", 2005

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
U1	Umie formułować i analizować problemy, znajdować ich rozwiązania oraz przeprowadzać eksperymenty, interpretować ich wyniki i wyciągać wnioski, umie konstruować implementacje algorytmów kryptograficznych oraz analizować i oceniać bezpieczeństwo systemów kryptograficznych.	K_U12, K_U18
W1	Zna i rozumie pojęcia, zasady i metody z zakresu teorii liczb i matematycznych podstaw i koncepcji kryptologii w zakresie rozwiązań obliczeniowych realizowanych sprzętowo.	K_W22
W2	Zna i rozumie pojęcia oraz zasady i metody konstrukcji i analizy poprawności implementacji sprzętowych protokołów i algorytmów kryptograficznych i kryptoanalitycznych	K_W23

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Moduł zaliczany jest na podstawie egzaminu;
- Warunkiem koniecznym dopuszczenia do zaliczenia modułu jest zaliczenie zajęć laboratoryjnych;
- Obecność na wszystkich zajęciach laboratoryjnych jest obowiązkowa. Nieobecność na zajęciach powoduje konieczność opanowania omawianego materiału we własnym zakresie;
- Do zajęć laboratoryjnych uruchamiany jest moduł zdalnego nauczania na platformie Microsoft Teams w celu: udostępniania materiałów do zajęć, przekazywania rozwiązań zadań indywidualnych, oraz zapewnienia sprawnego kontaktu i konsultacji. Każdy ze studentów ma obowiązek zapisać się jako uczestnik modułu zdalnego nauczania;
- Przed każdymi zajęciami na platformie Microsoft Teams udostępniane są materiały do przygotowania do zajęć. Po każdych zajęciach na platformie Microsoft Teams udostępniana jest treść zadania indywidualnego do pracy własnej. Zajęcia laboratoryjne zaliczane są na podstawie zadań indywidualnych, odpowiedzi ustnych oraz pisemnych;
- Szczegółowe warunki zaliczenia zajęć laboratoryjnych podaje prowadzący zajęcia na pierwszych zajęciach laboratoryjnych;
- Egzamin jest przeprowadzany w formie pisemnej lub ustnej;
- Szczegółowe warunki egzaminu podaje prowadzący zajęcia na pierwszym wykładzie.

Bilans ECTS (nakład pracy studenta)

SEMESTR 6 Aktywność	Obciążenie studenta Liczba godzin	Liczba ECTS
Udział w wykładach	20	0.5
Udział w laboratoriach	40	1.5
Udział w ćwiczeniach	0	0
Udział w projektach	0	0
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	30	0.25
Samodzielne przygotowanie do laboratoriów	40	1.25
Samodzielne przygotowanie do ćwiczeń		
Samodzielna realizacja projektu	20	1.5
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu		
Przygotowanie do zaliczenia		
Udział w egzaminie / kolokwium		
Sumaryczne obciążenie pracą studenta	150	5
Zajęcia z udziałem nauczycieli	60	2

	SEMESTR 6		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Zajęcia powiązane z działalnością naukową	150	5
	Zajęcia o charakterze praktycznym	100	4.25

autor

dr inż. Piotr Bora
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. Kojdecki Marek
tytuł, stopień naukowy, imię, NAZWISKO, podpis