**Nazwa przedmiotu:**

Implementacja algorytmów w reprogramowalnych strukturach FPGA

**Koordynator przedmiotu:**

Piotr Sapiecha

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Telekomunikacja

**Grupa przedmiotów:**

Przedmioty techniczne - zaawansowane

**Kod przedmiotu:**

IMAS

**Semestr nominalny:**

2 / rok ak. 2018/2019

**Liczba punktów ECTS:**

5

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

118

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

2

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

1

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 0h |
| Laboratorium: | 0h |
| Projekt: | 15h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

- podstawowe wiadomości z teorii układów logicznych,
- podstawowe wiadomości z algorytmów

**Limit liczby studentów:**

50

**Cel przedmiotu:**

- zapoznanie i zainteresowanie słuchaczy z zaawansowanymi metodami syntezy logicznej,
- pokazanie szeregu zastosowań omawianych metod, na przykładach projektów: szybkich układów arytmetycznych, układów DSP, układów komutacyjnych,
tablic routingu i filtrów pakietów,
- przedstawienie aparatu matematycznego stosowanego podczas projektowania wymienionych algorytmów i układów.

**Treści kształcenia:**

[1] Wykład wprowadzający.  Motywacje i cele wykładu.
[2-3] Szybkie algorytmy i układy arytmetyczne programowe i sprzętowe algorytmy dodawania: z szybkim obliczaniem przeniesień, mnożenia: Karatsuby, na drzewach Wallace’a,  realizacje potokowe.
[4-5] Szybkie algorytmy sortowania programowe i sprzętowe algorytmy: MergeSort, Quicksort, i sieci: Bitoniczne i Batchera, zastosowania pola komutacyjne: crossbar, knockout, Banyan.
[6-7] Arytmetyka modularna , twierdzenia Eulera, Chińskie o resztach , szyfrowanie RSA i ElGamala.
[8] Szybka transformata Fouriera (FFT),  twierdzenie o splocie, szybkie mnożenie wielomianów, filtry typu FIR, IIR.
[9] Algorytmy faktoryzacji liczb naturalnych - bezpieczeństwo szyfru RSA , metody: Pollarda, sito kwadratowe.
[10-11] Arytmetyka ciał skończonych,  kody korygujące typu: BCH, Reeda-Salomona, algorytm AES, szyfry na krzywych eliptycznych.
[12-14] Problemy NP-trudne, problem SAT i twierdzenie Stephena Cooka,  algorytmy dokładne i aproksymacyjne,  zastosowania w syntezie logicznej: redukcja zmiennych wejściowych do układu logicznego, dekompozycja funkcjonalna układu logicznego.
[15] Budowa tablic routingu typu LC-trie, wyszukiwanie wzorców, algorytmy KMP, KR, filtry Blooma, zastosowania w IDS'ach .

**Metody oceny:**

egzamin pisemny i ustny, projekt, referat, prezentacja

**Egzamin:**

tak

**Literatura:**

[1] Uwe Meyer-Baese, Digital Signal Processing with Field Programmable Gate Arrays
[2] Łuba T.(et al.), Programowalne układy przetwarzania sygnałów i informacji
[3] F. Rodríguez-Henríquez, N.A. Saqib, A. Díaz-Pèrez, and C. K. Koc, Cryptographic Algorithms on Reconfigurable Hardware

**Witryna www przedmiotu:**

http://www.zpt.tele.pw.edu.pl/didactics.html

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka imas\_w01:**

Szybkie i potokowe układy arytmetyczne. Technika sum prefiksowych: układy sumujące i odejmujące, komparatory, drzewa Wallace’a, sumator n liczb, układy mnożące, metoda Karaczuby, metoda Newtona, układy dzielące.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W01

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Szybkie sieci sortujące Zasada 0/1. Sieci bitoniczne, oraz sieci Batchera typu odd-even.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W01

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Układy sprzętowe realizyjące transformatę FFT oraz filtry Implementacja szybkiej transformaty Fouriera w sprzęcie, zastosowanie twierdzenia o splocie, filtry: implementacja filtrów FIR, IIR, arytmetyka rozproszona.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Pola komutacyjne Pola typu: crossbar, knockout, Banyan, Closa, Sunshine, komutatory współdzielące medium.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W06, K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Kryptograficzne układy sprzętowe Obliczenia w ciałach skończonych, potęgowanie Montgomerego. Algorytmy asymetryczne: Dieffiego-Hellmana i RSA. Algorytmy symetryczne AES.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Tablice routingu Budowa tablic routingu z wykorzystaniem struktur LC-trie.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Kodery i dekodery Kody korygujące błędy. Kody typu: BCH , Reeda-Salomona, oraz Reeda-Mullera.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W06, K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka imas\_w01:**

Sprzętowe systemy IDS Wyszukiwanie wielu wzorców, algorytmy KMP, Aho-Corasica, algorytm KR, filtry Blooma.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_W07

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka imas\_u01:**

Kodery i dekodery Kody korygujące błędy. Kody typu: BCH , Reeda-Salomona, oraz Reeda-Mullera.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U05

**Powiązane charakterystyki obszarowe:** I.P7S\_UW

**Charakterystyka imas\_u01:**

Sprzętowe systemy IDS Wyszukiwanie wielu wzorców, algorytmy KMP, Aho-Corasica, algorytm KR, filtry Blooma.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U01

**Powiązane charakterystyki obszarowe:** I.P7S\_UK

**Charakterystyka imas\_u01:**

Szybkie i potokowe układy arytmetyczne Technika sum prefiksowych: układy sumujące i odejmujące, komparatory, drzewa Wallace’a, sumator n liczb, układy mnożące, metoda Karaczuby, metoda Newtona, układy dzielące.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U01

**Powiązane charakterystyki obszarowe:** I.P7S\_UK

**Charakterystyka imas\_u01:**

Szybkie sieci sortujące Zasada 0/1. Sieci bitoniczne, oraz sieci Batchera typu odd-even.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.1.o, III.P7S\_UW.3.o

**Charakterystyka imas\_u01:**

Układy sprzętowe realizyjące transformatę FFT oraz filtry Implementacja szybkiej transformaty Fouriera w sprzęcie, zastosowanie twierdzenia o splocie, filtry: implementacja filtrów FIR, IIR, arytmetyka rozproszona.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.3.o

**Charakterystyka imas\_u01:**

Pola komutacyjne Pola typu: crossbar, knockout, Banyan, Closa, Sunshine, komutatory współdzielące medium.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.3.o

**Charakterystyka imas\_u01:**

Kryptograficzne układy sprzętowe Obliczenia w ciałach skończonych, potęgowanie Montgomerego. Algorytmy asymetryczne: Dieffiego-Hellmana i RSA. Algorytmy symetryczne AES.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.3.o

**Charakterystyka imas\_u01:**

Tablice routingu Budowa tablic routingu z wykorzystaniem struktur LC-trie.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.3.o

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka imas\_k01:**

Tablice routingu Budowa tablic routingu z wykorzystaniem struktur LC-trie.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Sprzętowe systemy IDS Wyszukiwanie wielu wzorców, algorytmy KMP, Aho-Corasica, algorytm KR, filtry Blooma.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Szybkie i potokowe układy arytmetyczne Technika sum prefiksowych: układy sumujące i odejmujące, komparatory, drzewa Wallace’a, sumator n liczb, układy mnożące, metoda Karaczuby, metoda Newtona, układy dzielące.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Układy sprzętowe realizyjące transformatę FFT oraz filtry Implementacja szybkiej transformaty Fouriera w sprzęcie, zastosowanie twierdzenia o splocie, filtry: implementacja filtrów FIR, IIR, arytmetyka rozproszona.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Kryptograficzne układy sprzętowe Obliczenia w ciałach skończonych, potęgowanie Montgomerego. Algorytmy asymetryczne: Dieffiego-Hellmana i RSA. Algorytmy symetryczne AES.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Kodery i dekodery Kody korygujące błędy. Kody typu: BCH , Reeda-Salomona, oraz Reeda-Mullera.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Kodery i dekodery Kody korygujące błędy. Kody typu: BCH , Reeda-Salomona, oraz Reeda-Mullera.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Szybkie sieci sortujące Zasada 0/1. Sieci bitoniczne, oraz sieci Batchera typu odd-even.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR

**Charakterystyka imas\_k01:**

Pola komutacyjne Pola typu: crossbar, knockout, Banyan, Closa, Sunshine, komutatory współdzielące medium.

Weryfikacja:

egzamin, projekt

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KO, I.P7S\_KK, I.P7S\_KR