KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena, Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 04.07.2017 godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. inž. Milice Nikolić pod naslovom „Implementacija AES modula u FPGA kolima''. Nakon pregleda materijala Komisija podnosi sledeći

IZVEŠTAJ

1. Biografski podaci kandidata

Milica Nikolić je rođena 12.09.1991. godine u Aranđelovcu. Završila je osnovnu školu "Sveti Sava" u Bukoviku (Aranđelovac) sa odličnim uspehom. Upisala je matematički smer gimnazije "Miloš Savković" u Aranđelovcu koju je završila sa odličnim uspehom. Elektrotehnički fakultet u Beogradu upisala je 2010. godine. Diplomirala je 2014. godine na Modulu za elektroniku sa prosečnom ocenom 7,77. Diplomski rad odbranio je u oktobru 2014. godine sa ocenom 10. Master akademske studije na elektrotehničkom fakultetu u Beogradu, na Modulu za elektroniku, upisala je u oktobru 2014. godine. Položila je sve ispite sa prosečnom ocenom 8,60.

2. Opis master rada

Master rad kandidata napisan je na ukupno 46 stranica. Rad je podeljen u 5 glavnih poglavlja, sadržaj i spisak korišćene literature.

Prvo poglavlje sadrži uvod i opis nastaknka AES -a. (*Advanced Encription Standard*).

Drugo poglavlje sadrži opis hardverske platforme i razvojnog okruženja.

Treće poglavlje sadrži teorijski opis osnovnih pojmova AES algoritma, specifikaciju AES-a. Detaljan postupak enkripcije i dekripcije podataka sa opisom transformacija koje je potrebno izvršiti nad ulaznim podatkom da bi dobili uspšeno kriptovan i dekriptovan podatak. Takođe dat je pregled modova rada AES -a, detaljno je opisan ECB (*Electronic CodeBook*) i CBC (*Cipher Block Chaining*) mod rada.

Četvrto poglavlje safrži opis i način realizacije sistema za implementaciju AES modula. Dat je detaljan opis i blok dijagram svih komponenti sistema, *MicroBlaze* procesora, korišćenih perirerija i AES modula.

Peto poglavlje sadrži prikaz rezultata dobijenih primenom testova koje obezbeđuje CST (*Cryptographic and Security Testing*) labaratorija akreditovana od strane NVLAP (*National Voluntory Laboratory Accreditation Program*).

Šesto poglavlje predstavlja zaključak i elaboraciju pethidno izvućenih zaključaka kao i mogućnost unapređivanja postojećeg sistema.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Milice Nikolić sadrži opis implementacije AES modula u FPGA kolima, i način testiranja implementiranog AES modula .

AES modul ispravno radi enkripciju i dekripciju podataka u dva moda rada, ECB *(Electronic CodeBook)* i CBC (*Cipher Block Chaining*) sa fiksnom dužinom ulanog bloka podataka od 128 bita. Podržava tri duzine ključa od 128 , 192 i 256 bita. Izlaz iz AES modula je enkriptovani/dekriptovani podatak dužine 128 bita. Maksimalna postignuta ućestanos rada AES modula je 60 MHz. Potreno je 19 *clock* ciklusa da bi se na izlazu AES modula pojavio tačan enkriptovani/dekriptovani podatak.

Za realizaciju ovog rada korišćena je AC701 razvojna ploča sa *Xilinx* XC7A200T pogramabilnim sistemom na čipu Atrix - 7 serije . Razvojno okruženje korišćeno tokom izrade projekta je Viavo Design Suite 2017.2 . Za pisanje softvera korišćen je *Xilinx* SDK (*Software Development Kit*).

4. Zaključak i predlog

Kandidat, Milica Nikolić, je u svom master radu uspešno implementirala AES modul za enkripciju i dekripciju podataka na FPGA kolu koje se nalazi u sklopu AC701 razvojne ploće. Rad je koncizan i u potpunosti pokriva datu temu. Kandidat je pokazao temeljno znanje prilikom analize rezultata, kao i u izvedenim zaključcima i predlozima za dalje unapređenje.

Na osnovu gore-navedenog Komisija predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da prihvati rad „Implementacija AES modula u FPGA kolima'' dipl. inž. Milice Nikolić kao master rad i odobri javnu usmenu odbranu.

U Beogradu, 14.09.2017.

dr Lazar Saranovac, vanredni profesor

dr Ivan Popović, docent