KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 27.05.2014. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Nine Bijelić, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Hardverska implementacija Fugue algoritma za heširanje". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Osnovnu i srednju školu završila je u Beogradu, nakon čega je upisala Elektrotehnički fakultet, Univerziteta u Beogradu, odsek za Telekomunikacije i informacione tehnologije. Diplomirala je 2012. godine na smeru za Sistemsko inženjerstvo, sa radom na temu "Softverska implementacija Viterbijevog algoritma". Iste godine upisuje master studije na matičnom fakultetu.

2. Opis master rada

Master rad obuhvata 47 strana, sa ukupno 24 slike, 2 tabele i 9 referenci. Rad sadrži uvod, 3 poglavlja, zaključak (ukupno pet poglavlja) i literaturu. Predmet rada je hardverska implementacija Fugue algoritma za heširanje. Implementacija je realizovana programskim kodom u VHDL jeziku i obuhvaćene su četiri dužine heš izlaza (224, 256, 384 i 512 bita) koje su zahtevane u konkursu za izbor SHA-3 kandidata u kome je učestvovao i Fugue algoritam. Za svaku od četiri implementacije izvršeno je kompajliranje dizajna u ISE razvojnom okruženju za razvoj dizajna za FPGA čipove proizvođača Xilinx. Za simuliranje ponašanja dizajna za svaku od četiri dužine heš izlaza upotrebljen je ISim simulator. Izvršena je i verifikacija dizajna korišćenjem vrednosti test vektora koje su autori priložili u okviru konkursa za SHA-3 algoritam. Programski kod svake od četiri implementacije, kao i kod korišćen pri verifikaciji, priloženi su na CD-u zbog obima koda. Na CD-u se nalazi i fajl koji sadrži test vektore i druge podatke relevantne za verifikaciju dizajna.

U uvodnom poglavlju opisan je razlog potrebe za heš algoritmima, predmet i rezultat rada, kao i moguća praktična primena realizovane implementacije.

U drugom poglavlju su predstavljeni definicija i osobine heš algoritama, njihova primena i najpoznatiji predstavnici heš algoritama. Takođe je dat i opis Fugue algoritma.

U trećem poglavlju je dat opis realizovane implementacije na primeru verzije sa 256-bitnom heš vrednošću. Prvo je opisana funkcija dizajna i predstavljeni su i objašnjeni ulazni i izlazni signali dizajna. Potom su detaljno opisane funkcije i procedure napisane za realizaciju koraka Fugue algoritma, kao i programski kod koji vrši celokupno heširanje po Fugue algoritmu. Na kraju poglavlja navedene su razlike u kodu za ostale dužine heš vrednosti.

U četvrtom poglavlju dat je tabelarni pregled performansi za sve dužine izlaza: upotrebljeni resursi na čipu i maksimalna frekvencija na kojoj dizajn može da radi. Rezultati performansi su dobijeni kompajliranjem dizajna u ISE razvojnom okruženju. Takođe, prikazana je i verifikacija dizajna kojom je potvrđen pravilan rad realizovane implementacije.

Zatim sledi zaključak koji sumira rezultate rada, a takođe sadrži i predloge za dalju optimizaciju realizovane implementacije Fugue algoritma. Na kraju rada data je literatura, sa 9 referenci, koja je korišćena prilikom izrade master rada.

3. Analiza rada sa ključnim rezultatima

Master rad Nine Bijelić, dipl. inž. Elektrotehnike i računarstva, bavi se hardverskom implementacijom Fugue algoritma za heširanje. Osnovni doprinosi rada su: 1) hardverska implementacija Fugue algoritma, za četiri dužine heš izlaza (224, 256, 384 i 512 bita) koje se u praksi najčešće i koriste; 2) realizovana implementacija je portabilna tj. može se implementirati na FPGA čipovima različitih proizvođača (npr. Xilinx, Altera).

4. Zaključak i predlog

Kandidat Nina Bijelić, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovala hardversku implementaciju Fugue algoritma za heširanje. Nina je pokazala da može samostalno da koristi relevantnu literaturu i da brzo i kvalitetno rešava probleme na koje je nailazila prilikom izrade teze. Realizovana implementacija može da nađe višestruku primenu u praksi, poput implementacije zaštitnih mehanizama u radu mrežnih čvorova poput Internet rutera. Na osnovu izloženog, Komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta da rad kandidata Nine Bijelić, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 29.08.2014. godine

Komisija:

Dr Zoran Čiča, docent

Dr Predrag Ivaniš, vanredni profesor