KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 28.04.2015. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Milice Mijatović, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Hardverska implementacija JH algoritma za heširanje". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Milica Z. Mijatović je rođena 25.09.1991. godine u Peći, država Srbija. Gimnaziju je završila u Baru, država Crna Gora, sa odličnim uspehom. Elektrotehnički fakultet u Beogradu upisala je 2009. godine, na Odseku za Telekomunikacije i informacione tehnologije. Diplomirala je u septembru 2013. godine sa prosečnom ocenom na ispitima 7.92, na diplomskom 10. Master studije na Elektrotehničkom fakultetu u Beogradu je upisala oktobra 2013. godine - modul Sistemsko inženjerstvo i radio komunikacije. Položila je sve ispite sa prosečnom ocenom 9.0.

2. Opis master rada

Master rad obuhvata 34 strane, sa ukupno 17 slika, 3 tabele i 4 reference. Unutar rada se nalaze i programski kodovi najvažnijih delova realizovane implementacije JH algoritma za heširanje. Rad sadrži uvod, 4 poglavlja, zaključak (ukupno šest poglavlja) i literaturu. Predmet rada je hardverska implementacija JH algoritma za heširanje. Implementacija je realizovana programskim kodom u VHDL jeziku i implementacija podržava sve 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 JH algoritam. Razvoj i verifikacija dizajna je urađena u ISE razvojnom okruženju proizvođača Xilinx. Za simuliranje dizajna i verifikaciju dizajna upotrebljen je ISim simulator koji je integrisan u ISE razvojno okruženje. Verifikacija dizajna je izvršena upotrebom vrednosti test vektora koje su autori JH algoritma priložili u okviru konkursa za SHA-3 algoritam. Kompletan programski kod implementacije JH algoritma, 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 opisana je značaj kriptografije i heš funkcije u telekomunikacijama. Opisan je predmet i cilj teze, i na kraju je ukratko predstavljena struktura ostatka teze po poglavljima.

U drugom poglavlju su definisane heš funkcije, navedene su najznačajnije osobine koje kriptografske heš funkcije moraju da poseduju, pregled primene kriptografskih heš funkcija i dat je kratak pregled napada na kriptografske heš funkcije.

U trećem poglavlju je dat detaljan opis JH algoritma za heširanje, kao i njegovih osnovnih sastavnih funkcija.

U četvrtom poglavlju je dat detaljan opis realizovane implementacije. 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 pojedinih koraka JH algoritma, kao i programski kod koji vrši celokupno heširanje po JH algoritmu. U okviru poglavlja su dati i najbitniji delovi programskog koda.

U petom poglavlju je izložena analiza performansi realizovane implementacije u vidu iskorišćenih resursa čipa, kao i maksimalne radne frekvencije dizajna za sve četiri dužine rezultujućeg

heša. Rezultati performansi su dobijeni kompajliranjem dizajna u ISE razvojnom okruženju. Takođe, prikazana je i verifikacija dizajna kojom je potvrđen pravilan rad realizovane implementacije.

Na kraju teze je izložen zaključak koji sumira rezultate rada, a takođe sadrži i predloge za dalje unapređenje realizovane implementacije JH algoritma. Na kraju rada data je literatura, sa 4 reference, koja je korišćena prilikom izrade master rada.

3. Analiza rada sa ključnim rezultatima

Master rad Milice Mijatović, dipl. inž. Elektrotehnike i računarstva, bavi se hardverskom implementacijom JH algoritma za heširanje. Osnovni doprinosi rada su: 1) hardverska implementacija JH algoritma koja podržava sve 4 dužine sažetka zahtevane SHA-3 standardom; 2) realizovana implementacija je portabilna pa se može bez izmena u kodu implementirati na FPGA čipovima različitih proizvođača (npr. Xilinx, Altera).

4. Zaključak i predlog

Kandidat Milica Mijatović, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovala hardversku implementaciju JH algoritma za heširanje. Milica je pokazala snalažljivost u radu i efikasno i brzo je realizovala hardversku implementaciju JH algoritma. 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 predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata Milice Mijatović, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 01.06.2015. godine

Komisija:

Dr Zoran Čiča, docent

Dr Predrag Ivaniš, vanredni profesor