KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 26.05.2015. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Jović Strahinje, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Hardverska implementacija Skein algoritma za heširanje". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Jović Strahinja je rođen 13. juna 1990. godine u Smederevu. Pohađao je sa odličnim uspehom srednju tehničku PTT školu na Smeru elektrotehničar telekomunikacija.

Elektrotehnički fakultet Univerziteta u Beogradu upisao je 2009. godine. Studirao je na Odseku Telekomunikacije i informacione tehnologije, smer Radio komunikacije, i diplomirao je septembra 2013. godine sa prosečnom ocenom 8.31 i ocenom 10 na diplomskom radu "Ispitivanje otpornosti sajta Društva Nikole Tesle na napade". Master studije, modul Sistemsko inženjerstvo i radio komunikacije upisao je septembra 2013. godine na Elektrotehničkom fakultetu u Beogradu i položio sve ispite sa prosečnom ocenom 10.00.

2. Opis master rada

Master rad obuhvata 46 strana, sa ukupno 19 slika, 7 tabela i 4 reference. Unutar rada se nalaze i programski kodovi realizovane implementacije Skein algoritma za heširanje. Rad sadrži uvod, 4 poglavlja, zaključak (ukupno šest poglavlja) i literaturu. Predmet rada je hardverska implementacija Skein algoritma za heširanje. Implementacija je realizovana 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 čiji je finalista bio Skein algoritam. Razvoj i verifikacija dizajna je urađena u ISE razvojnom okruženju proizvođača Xilinx. Za simuliranje dizajna i verifikaciju dizajna korišćen je ISim simulator, deo ISE razvojnog okruženja. Verifikacija dizajna je izvršena upotrebom vrednosti test vektora koje su autori Skein algoritma priložili u okviru konkursa za SHA-3 algoritam. Kompletan programski kod implementacije, kao i kod korišćen pri verifikaciji, priloženi su na CD-u. Na CD-u se nalazi i fajl koji sadrži test vektore i druge podatke relevantne za verifikaciju dizajna.

U uvodnom poglavlju opisana je aspekat sigurnosti u telekomunikacijama i uloga heš funkcija u ostvarivanju sigurnosti. Opisan je predmet i cilj teze, i na kraju je ukratko predstavljena struktura ostatka teze po poglavljima.

U drugom poglavlju je data definicija heš funkcija i navedene su osobine koje kriptografske heš funkcije moraju da poseduju. Navedene su najpoznatije heš funkcije koje se trenutno komercijalno koriste.

U trećem poglavlju je dat detaljan opis Skein algoritma za heširanje pri čemu je posebna pažnja posvećena opisu osnovnih delova Skein algoritma.

U četvrtom poglavlju je dat detaljan opis realizovane implementacije. Detaljno je opisan top level entitet i njegovi ulazni i izlazni signali, a potom su detaljno opisani podentiteti koji odgovaraju pojedinim funkcijama Skein algoritma. Objašnjenja su propraćena prikazom programskog koda. Objašnjena je implementacija koja kao rezultat daje sažetak dužine 256b, a na kraju ovog poglavlja su objašnjene razlike koje ostale verzije Skein algoritma imaju u odnosu na opisanu verziju.

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, prikazan je i postupak verifikacije dizajna kojim 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 Skein 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 Jović Strahinje, dipl. inž. Elektrotehnike i računarstva, realizuje i opisuje hardversku implementaciju Skein algoritma za heširanje. Osnovni doprinosi rada su: 1) hardverska implementacija Skein 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 Jović Strahinja, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovao hardversku implementaciju Skein algoritma za heširanje. Strahinja je pokazao dobro poznavanje programiranja FPGA čipova i uspešno realizovao Skein algoritam za heširanje u varijanti koja troši minimalne hardverske resurse. 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 Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata Jović Strahinje, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 14.09.2015. godine

Komisija:

Dr Zoran Čiča, docent

Dr Predrag Ivaniš, vanredni profesor