

## **KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU**

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 26.08.2014. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Maje Bijelić, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Hardverska implementacija CubeHash algoritma za heširanje“. Nakon pregleda materijala komisija podnosi sledeći

### **IZVEŠTAJ**

#### **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 "Enigma mašina, princip rada i procedure šifrovanja". Iste godine upisuje master studije na matičnom fakultetu.

#### **2. Opis master rada**

Master rad obuhvata 28 strana, sa ukupno 7 slika, 1 tabelom i 10 referenci. Unutar rada se nalaze i programski kodovi najvažnijih delova realizovane implementacije CubeHash algoritma za heširanje. Rad sadrži uvod, 3 poglavlja, zaključak (ukupno pet poglavlja) i literaturu. Predmet rada je hardverska implementacija CubeHash 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 CubeHash algoritam. Realizovana implementacija je potpuno parametrizovana i jednostavnim promenom parametara se lako postiže željena konfiguracija implementacije. Za nekoliko kombinacija vrednosti parametara implementacije izvršeno je kompajliranje dizajna u ISE razvojnom okruženju za razvoj dizajna za FPGA čipove proizvođača Xilinx. Za simuliranje ponašanja i verifikaciju dizajna upotrebljen je ISim simulator. Verifikacija dizajna je izvršena upotrebom vrednosti test vektora koje su autori CubeHash algoritma priložili u okviru konkursa za SHA-3 algoritam. Kompletan programski kod implementacije CubeHash 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 potreba za heš algoritmima, predmet i rezultat rada, kao i moguća praktična primena realizovane implementacije CubeHash algoritma za heširanje.

U drugom poglavlju su definisane i predstavljene osobine heš algoritama, primena heš algoritama i dat je opis CubeHash algoritma.

U trećem poglavlju je dat opis realizovane parametrizovane 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 CubeHash algoritma, kao i programski kod koji vrši celokupno heširanje po CubeHash algoritmu.

U četvrtom poglavlju dat je tabelarni pregled performansi za nekoliko kombinacija parametara CubeHash algoritma: upotrebljeni resursi na čipu i maksimalna frekvencija na kojoj dizajn može da radi. Rezultati performansi su dobijeni kompajliranjem dizajna u ISE razvojnom okruženju. Analiziran je uticaj parametara na zauzetost resursa čipa i maksimalnu frekvenciju na kojoj dizajn može ispravno da radi. 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 dalju optimizaciju realizovane implementacije CubeHash algoritma. Na kraju rada data je literatura, sa 10 referenci, koja je korišćena prilikom izrade master rada.

### 3. Analiza rada sa ključnim rezultatima

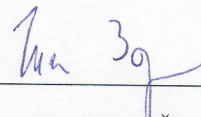
Master rad Maje Bijelić, dipl. inž. Elektrotehnike i računarstva, bavi se hardverskom implementacijom CubeHash algoritma za heširanje. Osnovni doprinosi rada su: 1) hardverska implementacija CubeHash algoritma koja je potpuno parametrizovana; 2) realizovana implementacija je portabilna pa se može bez izmena u kodu implementirati na FPGA čipovima različitih proizvođača (npr. Xilinx, Altera).

### 4. Zaključak i predlog

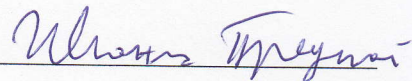
Kandidat Maja Bijelić, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovala hardversku implementaciju CubeHash algoritma za heširanje. Maja je pokazala veliku samostalnost u radu i efikasno je rešavala probleme na koje je nailazila prilikom izrade teze. Realizovana implementacija može da nađe višestruku primenu u praksi, poput implementacije zaštitnih mehanizama u radu mrežnih čvorova poput Internet rutera. Na osnovu izloženog, Komisija predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata Maje Bijelić, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 19.09.2014. godine

Komisija:



Dr Zoran Čiča, docent



Dr Predrag Ivaniš, vanredni profesor