3366/14

KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 02.06.2015. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Marković Sanje, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Hardverska implementacija Camellia algoritma za šifrovanje simetričnim ključem". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Sanja Marković je rođena 06.08.1990. godine u Beogradu. Treću beogradsku gimnazijuje završila u Beogradu. Elektrotehnički fakultet u Beogradu upisala je 2009. godine, na Odseku za telekomunikacije i informacione tehnologije. Diplomirala je 2014. godine sa prosečnom ocenom na ispitima 7.43 i ocenom 10 na diplomskom. Master studije na Elektrotehničkom fakultetu u Beogradu je upisala 2014. godine na Modulu za sistemsko inženjerstvo i radio komunikacije.

2. Opis master rada

Master rad obuhvata 31 stranu, sa ukupno 6 slika, 4 tabele i 4 reference. Unutar rada se nalaze i programski kodovi realizovane implementacije Camellia algoritma za šifrovanje simetričnim ključem. Rad sadrži uvod, 4 poglavlja, zaključak (ukupno šest poglavlja) i literaturu. Predmet rada je hardverska implementacija Camellia algoritma za šifrovanje. Implementacija je realizovana u VHDL jeziku. 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 Camellia algoritma objavili na zvaničnom sajtu ovog algoritma. Kompletan programski kod implementacije je priložen na CD-u.

U uvodnom poglavlju opisan je značaj sigurnosti u telekomunikacijama. Opisan je predmet i cilj teze, i na kraju je ukratko predstavljena struktura ostatka teze po poglavljima.

U drugom poglavlju su navedeni osnovni pojmovi kriptografije. Definisana je podela algoritama za šifrovanje na one algoritme koji koriste simetričan ključ i one koji koriste asimetrične ključeve. Pri tome su navedeni i ukratko opisani najpoznatiji predstavnici obe kategorije algoritama.

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

U četvrtom poglavlju je dat detaljan opis realizovane implementacije Camellia algoritma. Detaljno su opisani interfejsi realizovane implementacije i osnovne gradivne komponente. Potom je dizajn opisan koristeći princip "*bottom to top*", tj. objašnjenje je krenulo od hijerarhijski najnižih delova ka hijerahijski najvišim delovima dizajna. Pri objašnjenju su priloženi i delovi programskog koda radi kvalitetnijeg objašnjenja.

U petom poglavlju je izložena analiza performansi realizovane implementacije u vidu iskorišćenih resursa čipa, kao i maksimalne radne frekvencije i maksimalnog podržanog protoka za selektovani FPGA čip. Rezultati performansi su dobijeni kompajliranjem dizajna u ISE razvojnom okruženju. 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 Camellia algoritma u cilju povećanja protoka. Na kraju rada data je literatura, sa 4 reference, koja je korišćena prilikom izrade master rada.

3. Analiza rada sa ključnim rezultatima

Master rad Sanje Marković, dipl. inž. Elektrotehnike i računarstva, realizuje i opisuje hardversku implementaciju Camellia algoritma za šifrovanje simetričnim ključem. Osnovni doprinosi rada su: 1) hardverska implementacija Camellia algoritma; 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 Marković Sanja, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovala hardversku implementaciju Camellia algoritma za šifrovanje. Sanja je pokazala dobro snalaženje u programiranju FPGA čipova i uspešno realizovala Camellia algoritam za heširanje, pri čemu je dala jasne smernice za modifikaciju dizajna ako se želi postići veći protok šifrovanja po cenu nešto povećanih hardverskih resursa. 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 Sanje Marković, 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