KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena, Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 09.06.2015. godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. inž. Miloša Grujića pod naslovom „Implementacija *Hummingbird* kriptografskog algoritma primenom FPGA". Nakon pregleda materijala Komisija podnosi sledeći

IZVEŠTAJ

1. Biografski podaci o kandidatu

Miloš Grujić je rođen 29.07.1991. u Smederevu. Završio je Gimnaziju u Smederevu prosečnom ocenom 5.00, kao nosilac Vukove diplome. Elektrotehnički fakultet u Beogradu upisao je 2010. godine, a diplomirao u oktobru 2014. godine na odseku za Elektroniku, sa prosečnom ocenom na ispitima 9.78, na diplomskom 10. Master studije na Elektrotehničkom fakultetu u Begradu upisao je 2014. godine na odseku za Elektroniku. Položio je sve ispite prosečnom ocenom 9.6.

2. Opis master rada

Master rad kandidata sadrži 76 strana. Rad sadrži šest poglavlja, dva priloga i spisak literature sa 16 referenci.

Prvo poglavlje predstavlja uvod u kome su opisani predmet i cilj rada, kao i značaj kriptografskih algoritama.

U drugom poglavlju je detaljno opisan *lightweight* kriptografski algoritam *Hummingbird*, pri čemu su prikazane faze inicijalizacije, enkripcije i dekripcije, zajedno sa odgovarajućim dijagramima.

Treće poglavlje sadrži opis korišćenih FPGA čipova - *Xilinx*-ov *Spartan-3 XC3S200* i Alterin *Cyclone IV EP4CE22F17C6*, kao i softverskih alata korišćenih za razvoj VHDL koda - *Xilinx ISE Design Suite 14.6* i *Quartus II 13.0*.

U četvrtom poglavlju je opisana implementacija *Hummingbird* kriptografskog algoritma na FPGA čipovima. Na početku su objašnjene prednosti hardverske implementacije kriptografskog algoritma u odnosu na softversku. Opisana je arhitektura projektovane *Hummingbird* komponente, koja se sastoji iz operacione i upravljačke jedinice. Za optimizaciju dizajna blok šifarskog sistema operacione jedinice korišćene su tehnike protočne obrade (*pipelining*) i odmotavanja petlje (*loop unrolling*). Detaljno je opisana projektovana mašina stanja upravljačke jedinice, kao i korišćene strategije u softverskim alatima koje dovode do povećanja maksimalne učestanosti rada projektovane komponente.

Peto poglavlje sadrži rezultate simulacija i testiranja implementirane *Hummingbird* komponente. Dat je pregled postignutih performansi zajedno sa diskusijom rezultata, kao i poređenje sa performansama drugih implementacija *lightweight* kriptografskih algoritama.

U šestom poglavlju je izložen zaključak koji sumira rezultate rada.

Na kraju rada se nalaze i dva priloga: prilog A, koji sadrži VHDL kod FPGA implementacije *Hummingbird* kriptografskog algoritma, i prilog B, koji sadrži softversku implementaciju istog algoritma u jeziku *C*.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Miloša Grujića se bavi FPGA implementacijom *Hummingbird* kriptografskog algoritma na FPGA čipovima malih logičkih resursa, koji se sreću kod RFID transpondera i bežičnih senzorskih mreža. Algoritam je prvo detaljno analiziran uključujući faze inicijalizacije, enkripcije i dekripcije, a zatim opisan u VHDL-u. Za implementaciju su izabrana dva različita FPGA čipa istog cenovnog ranga - *Xilinx Spartan-3* i *Altera Cyclone IV*. Prilikom implementacije su korišćene napredne metode u projektovanju digitalnih sistema, kao i strategije u softverskim alatima koje omogućavaju poboljšanje performansi. Postignute performanse su detaljno analizirane i upoređene sa postojećim implementacijama istog, ali i drugih kriptografskih algoritama. Obe implementacije postižu znantno veće učestanosti rada od prethodno objavljenih implementacija istog algoritma, dok implementacija na *Cyclone*-u *IV* postiže znatno bolje rezultate i po relativnom zauzeću površine i po propusnosti.

Najvažniji doprinosi rada su:

- implementiran je *Hummingbird* kriptografski algoritam pomoću komponenti koje je kandidat samostalno projektovao u *VHDL*-u,

- korišćene su napredne metode za poboljšanje maksimalne učestanosti rada - protočna obrada i odmotavanje petlje,

- korišćene su napredne metode za povećanje propusnosti sistema u vidu sažimanja stanja upravljačke jedinice prilikom enkripcije,

- postignuti rezultati korišćenjem gore navedenih tehnika su bolji u pogledu maksimalne učestanosti rada nego do sada objavljene implementacije istog algoritma.

4. Zaključak i predlog

Kandidat Miloš Grujić je u svom master radu uspešno implementirao *Hummingbird* kriptografski algoritam na dva različita FPGA čipa, pri čemu su postignute znantno veće učestanosti rada od prethodno objavljenih FPGA implementacija istog algoritma zahvaljujući primeni naprednih metoda u projektovanju.

Kandidat je iskazao izuzetnu samostalnost i sistematičnost u svom radu, kao i inovativne elemente u rešavanju problematike rada.

Na osnovu gore navedenog komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da prihvati rad "Implemetacija *Hummingbird* kriptografskog algoritma primenom FPGA" dipl. inž. Miloša Grujića kao master rad i odobri javnu i usmenu odbranu.

U Beogradu, 17.09.2015.

Članovi komisije:

dr Jelena Popović-Božović, doc.

dr Vladimir Rajović, doc.