УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 26.05.2015. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Данице Голубичић под насловом „Дигитално потписивање IP пакета коришћењем Блејк алгоритма за хеширање". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Даница Голубичић је рођена 07.10.1988. године у Београду. Завршила је Пету београдску гимназију (природно-математички смер), у Београду, са одличним успехом. Електротехнички факултет у Београду уписала је 2007. године, на одсеку за Телекомуникације и информационе технологије, смер Системско инжењерство. Дипломирала је у септембру 2013. године са просечном оценом 7.80. Мастер студије на Електротехничком факултету у Београду је уписала 2013. на модулу Системско инжењерство и радио комуникације. Положила је све испите са просечном оценом 10.

2. Опис мастер рада

Мастер рад обухвата 34 стране, са укупно 20 слика, 4 табеле и 6 референци. Рад садржи увод, 5 поглавља и закључак (укупно 7 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Такође је представљена и структура остатка рада по поглављима.

У другом поглављу је дат кратак преглед особина хеш функција са детаљним освртом на њихово коришћење у дигиталном потписивању. Основни принципи дигиталног потписа су изложени и објашњени у овом поглављу.

У трећем поглављу је описана структура заглавља IP пакета и детаљно је објашњен процес рачунања контролне суме заглавља при чему је дат и конкретан пример ради бољег разумевања.

Четврто поглавље садржи опис Блејк алгоритма за хеширање. Описан је принцип рада алгоритма и дефинисани су сви улазни и излазни сигнали Блејк алгоритма. Детаљно је описан и принцип допуне поруке.

Пето поглавље садржи главни допринос тезе. Детаљно је описана хардверска реализација дигиталног потписа применом Блејк хеш алгоритма која је намењена имплементацији у FPGA (*Field Programmable Gate Array*) чиповима. Прецизно је описан интерфејс (улазни и излазни портови) реализованог дизајна. Сама унутрашњост реализованог дизајна је веома прецизно и педантно објашњена. При томе је дефинисана позиција реализованог блока у пакетском процесору и његова веза са осталим деловима пакетског процесора. За реализацију дизајна је коришћен VHDL програмски језик.

У шестом поглављу је описан процес верификације дизајна и потврђена је исправност реализације. За процес верификације је коришћена и Matlab симулација рада Блејк алгоритма за хеширање. Поређењем резултата симулације дизајна и резултата добијених Matlab симулацијом потврђена је исправност реализованог дизајна. У другом делу овог поглавља су разматране перформансе дизајна у виду коришћених ресурса FPGA чипа и подржаног протока пакета.

Седмо поглавље је закључак у оквиру кога се резимирају резултати и доприноси тезе.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Данице Голубичић се бави дизајнирањем функције дигиталног потписивања IP пакета у пакетским процесорима рутера. У раду је коришћен Блејк алгоритам за хеширање за реализацију функције потиписивања пакета. Реализовани дизајн је намењен пакетским процесорима имплементираним у FPGA чиповима. При томе, реализована имплементација подржава гигабитске портове, а употребом јачих FPGA чипова могли би да се подрже и 10G портови.

Основни доприноси рада су: 1) имплементација функционалности дигиталног потписивања употребом Блејк алгоритма за хеширање и јасна дефиниција положаја реализованог дизајна у пакетском процесору; 2) верификација исправности реализоване имплементације; 3) анализа перформанси реализоване имплементације која показује да су подржане и гигабитске брзине портова.

4. Закључак и предлог

Кандидат Даница Голубичић је у свом мастер раду успешно имплементирала функцију дигиталног потписивања IP пакета у пакетским процесорима рутера. Реализовано решење има примену у рутерима чији пакетски процесори су реализовани у FPGA чиповима.

Кандидат је показао велику самосталност у анализи и решавању задатог проблема. Само решење је веома педантно и ефикасно урађено при чему су решени многи сложени проблеми попут ефикасног прорачунавања нове контролне суме, различити случајеви који се јављају приликом допуне пакета пре самог процеса хеширања и сл.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Данице Голубичић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 06. 05. 2016. године

Чланови комисије:

Др Зоран Чича, доц.

Др Милан Бјелица, ванр. проф.