КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 15.07.2014. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Горана Огњановића, дипл. инж. Електротехнике и рачунарства, под насловом „Хардверска имплементација Blake алгоритма за хеширање“. Након прегледа материјала комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци о кандидату

Горан Огњановић је рођен у Београду 30.08.1987 године. Завршио је основну школу „Ужичка република“ у Београду. Године 2006. завршио је Девету београдску гимназију „Михаило Петровић Алас”. Године 2011. завршио је основне академске студије на Електротехничком факултету Универзитета у Београду, на одсеку за Рачунарску техника и информатика, са просечном оценом 7,51. Дипломски рад „Алати и методологије за тестирање веб апликација“ одбрањен је са оценом 10. Од јуна 2012. године ради у фирми „Elsys Eastern Europe“ у Београду као инжењер Дигиталног дизајна и верификације интегрисаних кола.

2. Опис мастер рада

Мастер рад обухвата 30 страна, са укупно 14 слика, 7 табела и 13 референци. Рад садржи увод, 5 поглавља, закључак (укупно седам поглавља) и литературу. Предмет рада је хардверска имплементација Blake алгоритма за хеширање. Имплементација је реализована употребом VHDL језика, као и ISE и Quartus алата намењених чиповима произвођача Xilinx и Altera, респективно. За верификацију дизајна је коришћен ModelSim алат. У оквиру тезе су реализоване три варијанте Blake алгоритма за хеширање које се разликују по ресурсима које заузимају и протоцима хеширања које остварују. Комплетан програмски код имплементације све три варијанте је приложен на CD-у због обима кода.

У уводном поглављу наведен је значај криптографских хеш функција као и предмет и циљ саме тезе.

У другом поглављу су наведене основне карактеристике криптографских хеш алгоритама, описани су најпознатији криптографски хеш алгоритми и набројани су и описани напади на криптографску хеш функцију.

У трећем поглављу је детаљно описан Blake хеш алгоритам и његове фазе.

У четвртом поглављу је описана имплементација Blake-256 хеш алгоритма који генерише 256-битни сажетак (хеш вредност). Описане су три варијанте реализације Blake-256 хеш алгоритма. Прва варијанта подразумева употребу минималних ресурса тако што се једна инстанца рунде користи током комплетног процесирања блока поруке, али по цену споријег протока хеширања. Друга варијанта подразумева

употребу проточне обраде (*pipeline*) и паралелизације, чиме је омогућено истовремено процесирање више порука чиме се постиже веома висок проток хеширања, али по цену већих хардверских захтева. Трећа варијанта подразумева реализацију процесирања једног блока поруке у виду комбинационе логике чиме се постиже процесирање једног блока поруке у једном такту, али цена је веома ниска радна фреквенција оваквог дизајна.

У петом поглављу је објашњен поступак функционалне верификације реализованих имплементација.

У шестом поглављу су анализиране перформансе све три реализоване имплементације и показало се да су они у складу са очекивањима изложеним у четвртом поглављу. Остварени су веома високи протоци хеширања.

На крају тезе је изложен закључак који сумира резултате рада. На крају рада дата је литература, са 13 референци, која је коришћена приликом израде мастер рада.

3. Анализа рада са кључним резултатима

Мастер рад Горана Огњановића, дипл. инж. Електротехнике и рачунарства, бави се хардверском имплементацијом Blake алгоритма за хеширање. Основни доприноси рада су: 1) хардверска имплементација три варијанте Blake алгоритма за хеширање што даје могућност избора у зависности од жељених перформанси и хардверских ресурса на располагању; 2) анализа перформанси све три реализоване варијанте Blake алгоритма за хеширање.

4. Закључак и предлог

Кандидат Горан Огњановић, дипл. инж. електротехнике, је у свом мастер раду успешно имплементирао три варијанте Blake алгоритма за хеширање. Горан је показао добро познавање области VHDL програмирања и функционалне верификације дизајна, као и велику самосталност при изради тезе. Реализоване имплементације се могу вишеструко искористити, на пример, у оквиру мрежних уређаја за постизање већег степена заштите у мрежној комуникацији. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Горана Огњановића, дипл. инж. електротехнике, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 22.09.2014. године

Комисија:

Др Зоран Чича, доцент

Др Захарије Радивојевић, доцент