КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 03.09.2024. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Анђелке Вучовић, дипл. инж. Електротехнике и рачунарства, под насловом „Хардверска имплементација Camellia-CMAC алгоритма за аутентификацију порука". Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Анђелка Вучовић је рођена 14.03.1999. године у Параћину. Завршила је основну школу „Стеван Јаковљевић" у Параћину као вуковац и ђак генерације. Уписала је Гимназију у Београду коју је завршила са одличним успехом као вуковац. Током школовања учествовала је на такмичењима из математике, физике и хемије. Из физике и хемије је више пута освајала награде на државним такмичењима. Електротехнички факултет је уписала 2018. године. Дипломирала је на одсеку Телекомуникације и информационе технологије 2022. године са просечном оценом 8,76. Дипломски рад је одбранила у септембру 2022. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Информационо комуникационе технологије уписала је у октобру 2022. године. Положила је све испите са просечном оценом 10.

2. Извештај о студијском истраживачком раду

Кандидат Анђелка Вучовић је у оквиру припреме за рад на својој мастер тези детаљно проучила област која се бави сигурношћу у телекомуникационим системима са посебним освртом на постојећа решења аутентификације. Потом је детаљно проучила релевантне алгоритме којима се бави теза, а то су алгоритми енкрипције AES и Camellia, као и алгоритам AES-CMAC који се користи за аутентификацију порука, а на коме је засновано решење предложено у тези. Након обављеног студијског истраживачког рада, Анђелка је кренула у израду своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 36 страна, са укупно 13 слика, 2 табеле и 13 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Предмет рада представља хардверску реализацију Camellia-CMAC алгоритма аутентификације порука који је креиран по угледу на стандардизован AES-CMAC алгоритам. У оквиру рада је коришћено Xilinx ISE развојно окружење, а за потребе симулације Isim симулатор који је део наведеног окружења. Коришћен је VHDL језик за писање кода имплементације.

У уводном поглављу је укратко описан значај области којој припада теза, потом је изложен циљ мастер тезе, да би на крају био дат преглед садржаја остатка тезе по поглављима.

Друго поглавље даје теоријске основе делова области којој припада теза, а који су релевантни за остатак тезе. У овом поглављу су изложени алгоритми енкрипције са симетричним кључем, као и блок алгоритми који представљају значајну класу алгоритама са симетричним кључем.

Треће поглавље даје детаљно објашњење Camellia алгоритма за шифровање симетричним кључем из разлога што је овај алгоритам основа за Camellia-CMAC имплементацију.

У четвртом поглављу је изложен принцип CMAC аутентификације пошто је овај принцип и имплементиран у оквиру мастер тезе.

Пето поглавље је централно поглавље тезе где је изложена реализована хардверска имплементација Camellia-CMAC алгоритма аутентификације порука. Дата су детаљна објашњења при чему је посебна пажња посвећена коначном аутомату који диктира рад комплетног дизајна.

У шестом поглављу је приказана симулација дизајна да би на крају били дати процењени хардверски ресурси које захтева реализовани дизајн.

Седмо поглавље сумира резултате мастер тезе, а потом је дат списак коришћених референци, списак скраћеница, списак слика и списак табела.

4. Анализа рада са кључним резултатима

Мастер рад Анђелке Вучовић, дипл. инж. Електротехнике и рачунарства, представља реализовану хардверску имплементацију Camellia-CMAC алгоритма за аутентификацију порука. Кључни доприноси рада кандидата на тези су следећи:

1) реализован Camellia-CMAC алгоритма за аутентификацију порука;
2) реализован дизајн је портабилан;
3) извршена је процена неопходних хардверских ресурса.

5. Закључак и предлог

Кандидат Анђелка Вучовић, дипл. инж. Електротехнике и рачунарства, се у свом мастер раду бавила хардверском имплементацијом Camellia-CMAC алгоритма за аутентификацију порука. Реализована имплементација се може користити у телекомуникационим уређајима за потребе аутентификације размењиваних порука. Анђелка је показала способност да на ефикасан начин решава проблеме на које је наилазила током рада на тези, као и да веома квалитетно презентује резултате остварене у оквиру рада на тези. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Анђелке Вучовић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 11.09.2024. године

Чланови комисије:

др Зоран Чича, ред. професор

др Дејан Драјић, ред. професор