КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 27.08.2024. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Вање Јанковић, дипл. инж. Електротехнике и рачунарства, под насловом „Хардверска имплементација AES-CMAC алгоритма“. Након прегледа материјала комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Вања Јанковић је рођена 21.06.1998. године. Завршила је Основну школу „Мирослав Антић“ у Београду са Вуковом дипломом. Током основне школе учествовала је на такмичењима из математике и биологије, са успесима на окружним такмичењима. Уписала је ITHS (Information Technology High School) у Београду 2013. године као стопостотни стипендиста, а завршила исту 2017. године такође као вуковац. Електротехнички факултет је уписала 2017. године. Дипломирала је на одсеку за Телекомуникације и информационе технологије 2022. године са просечном оценом 7,48. Дипломски рад је бранила у септембру са оценом 10. Мастер студије је уписала 2022. године и обновила 2023. године (модул Информационо комуникационе технологије). Положила је све испите са оценом 8,40.

2. Извештај о студијском истраживачком раду

Кандидат Вања Јанковић је пре започињања рада на својој мастер тези детаљно проучила релевантну литературу која се бави безбедношћу у телекомуникационим системима са нагласком на решења која се баве аутентификацијом порука. Потом је детаљно проучила алгоритам енкрипције AES као и одговарајућу RFC препоруку која дефинише AES-CMAC алгоритам за аутентификацију порука, а који је имплементиран у тези. Након обављеног студијског истраживачког рада, Вања је започела рад на својој мастер тези.

3. Опис мастер рада

Мастер рад обухвата 36 страна, са укупно 24 слике и 12 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), списак коришћене литературе и списак слика.

Предмет рада представља хардверску реализацију веома популарног AES-CMAC алгоритма аутентификације порука који је описан у RFC 4493. У оквиру тезе је коришћено Xilinx ISE развојно окружење, а за потребе верификације и симулације Isim симулатор који је део наведеног окружења. Коришћен је VHDL језик за писање кода имплементације AES-CMAC алгоритма.

У уводном поглављу је укратко описан значај безбедности комуникације и процеса аутентификације, потом је изложен циљ мастер тезе, а на крају је дат преглед садржаја остатка тезе по поглављима.

Друго поглавље представља основе криптографије. Представљени су принцип симетричних и асиметричних алгоритама енкрипције. Такође је представљен и MAC алгоритам који се често користи као основа за алгоритме аутентификације.

Треће поглавље даје детаљно објашњење AES алгоритма за шифровање симетричним кључем јер је овај алгоритам база за AES-CMAC имплементацију. Потом је објашњен принцип рада самог AES-CMAC алгоритма.

У четвртом поглављу су дати основни подаци о коришћеном VHDL програмском језику.

Пето поглавље представља централно поглавље тезе јер је у њему изложена реализована хардверска имплементација AES-CMAC алгоритма аутентификације порука. Пошто је коришћен принцип коначног аутомата за контролу рада реализованог дизајна, веома је детаљно објашњен реализовани коначни аутомат као и улога свих стања аутомата.

У шестом поглављу је приказана симулација и верификација дизајна којом је потврђена исправност рада релизоване имплементације. Потом су дати процењени хардверски ресурси реализованог дизајна.

Седмо поглавље резимира остварене резултате мастер тезе, а потом је дат списак коришћених референци и списак слика.

4. Анализа рада са кључним резултатима

Мастер рад Вање Јанковић, дипл. инж. Електротехнике и рачунарства, се бави хардверском имплементацијом AES-CMAC алгоритма за аутентификацију порука. Кључни доприноси рада кандидата на тези су следећи:

1) реализован је AES-CMAC алгоритам за аутентификацију порука;
2) реализовано решење је портабилно;
3) извршена је верификација исправности рада реализованог дизајна.

5. Закључак и предлог

Кандидат Вања Јанковић, дипл. инж. Електротехнике и рачунарства, се у свом мастер раду бавила хардверском имплементацијом популарног AES-CMAC алгоритма за аутентификацију порука. Реализовану имплементацију је могуће искористити у телекомуникационим системима за потребе аутентификације размењиваних порука. Вања је детаљно и разумљиво презентовала резултате своје тезе и показала способност да самостално доноси релевантне закључке. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Вање Јанковић, 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