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 08.06.2021. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Нађе Милојевић, дипл. инж. Електротехнике и рачунарства, под насловом „Имплементација HMAC-SHA-256 алгоритма за хеширање“. Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Нађа Милојевић је рођена 08.01.1990. године у Београду. Завршила је основну школу "Седам секретара СКОЈ-а" у Београду као вуковац. Уписала је Трећу Београдску гимназију у Београду коју је завршила као вуковац. Електротехнички факултет уписала је 2009. године. Дипломирала је на одсеку за Телекомуникације и информационе технологије 2018. године са просечном оценом 7,39. Дипломски рад одбранила је у септембру 2018. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Системско инжењерство и радио комуникације уписала је 2018. године. Положила је све испите на мастер студијама са просечном оценом 7,40.

2. Опис мастер рада

Мастер рад обухвата 37 страна, са укупно 6 слика, 8 табела и 7 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), и списак коришћене литературе.

Предмет рада представља имплементацију HMAC-SHA-256 алгоритма за хеширање. Имплементација је урађена употребом Verilog језика који спада у групу HDL (*Hardware Description Language*) језика. У изради тезе су коришћени C++ програмски језик за верификацију дизајна, Verilator симулатор, као и јавно доступна библиотека NanGate45 Open Cell.

У уводном поглављу је изложен значај безбедности у модерним комуникацијама, наведен је циљ тезе, као и алати коришћени током израде тезе, а на крају је дат преглед остатка рада по поглављима.

У другом поглављу су обрађене основе хеш функције са посебним освртом на њихову примену у криптографији. Укратко су размотрене најпознатије криптографске хеш функције.

У трећем поглављу је укратко изложен HMAC (*Keyed-Hash Message Authentication Codes*) механизам за проверу интегритета поруке.

Четврто поглавље је посвећено опису имплементације HMAC-SHA-256 алгоритма за хеширање. Детаљно су описани сви делови дизајна, као и принцип комуникације са околином. У поглављу су дати и релевантни делови кода неопходни за боље схватање имплементације.

У петом поглављу је описана верификација дизајна. Урађене су две варијанте тестирања, са унапред познатим улазом и излазом, као и са случајно генерисаним улазним вредностима. Приложен је и релевантан програмски код написан за потребе верификације дизајна у оквиру овог поглавља.

У шестом поглављу су приказани резултати имплементације у виду искоришћених ресурса. Сви подаци су дати табеларно одакле се лако могу видети употребљени ресурси и комплексност имплементације.

У седмом поглављу је дат резиме рада на тези, а потом је наведен списак коришћене литературе.

3. Анализа рада са кључним резултатима

Мастер рад Нађе Милојевић, дипл. инж. Електротехнике и рачунарства, представља имплементацију HMAC-SHA-256 алгоритма за хеширање. Основни доприноси рада су следећи:

1) реализован дизајн за HMAC-SHA-256 функцију хеширања;
2) дизајн остварује комуникацију са околином преко стандардног APB (*Advanced Peripheral Bus*) интерфејса;
3) реализована имплементација је портабилна, тј. може се користити на чиповима различитих произвођача.

4. Закључак и предлог

Кандидат Нађа Милојевић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно имплементирала HMAC-SHA-256 алгоритам за хеширање. Нађа је показала да добро влада дизајном телекомуникационих функција у хардверу употребом HDL језика. Била је веома темељна у припреми реализације дизајна, тако што је добро проучила теоријску позадину самог алгоритма, а потом систематично приступила имплементацији дизајна. Нађа је доказала самосталност у изради тезе и решавању проблема. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Нађе Милојевић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 10.09.2021. године

Чланови комисије:

Др Зоран Чича, ванр. професор

Др Дејан Драјић, ванр. професор