КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 29.08.2023. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Анастасие Зеринski, дипл. инж. Електротехнике и рачунарства, под насловом „Минимална хардверска имплементација Kuznyechik алгоритма за шифровање симетричним кључем“. Након прегледа материјала комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Анастасиа Зеринski је рођена 12.08.1997. године у Атини. Завршила је основну школу „Лаза К. Лазаревић” у Шапцу као вуковац. Уписала је Шабачку гимназију у Шапцу, коју је завршила с одличним успехом. Електротехнички факултет уписала је 2016. године. Дипломирала је на смеру за Системско инжењерство одсека за Телекомуникације 2020. године. Дипломски рад одбранила је у новембру 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за информационо комуникационе технологије уписала је у октобру 2021. године. Положила је све испите са просечном оценом 9,40.

2. Извештај о студијском истраживачком раду

Кандидат Анастасиа Зеринski је као припрему за мастер рад проучила релевантну литературу из области криптографије. Након тога се упознала са спецификацијом Kuznyechik алгоритма за шифровање симетричним кључем. Осмислила је дизајн имплементације Kuznyechik алгоритма која троши минималне хардверске ресурсе. Након обављеног студијског истраживачког рада, Анастасиа је приступила изради своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 35 страна, с укупно 10 слика и 8 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), списак коришћене литературе и списак скраћеница.

Предмет рада је хардверска имплементација Kuznyechik алгоритма за шифровање симетричним кључем. Циљ рада је креирање имплементације алгоритма која троши минималне хардверске ресурсе што је постигнуто употребом хардвера рунде алгоритма која се користи за различите итерације рунди. Коришћен је VHDL језик за опис хардвера. Коришћено развојно окружење је Quartus II, као и Eda playground.

У уводном поглављу је прво изложен циљ тезе, а потом је изложен и преглед садржаја остатка тезе по поглављима.

Друго поглавље садржи кратак теоријски осврт на област криптографије. Изложена је улога криптографије, дата је класификација алгоритама за шифровање с кратким објашњењем принципа сваке од класа. Посебан осврт је дат на тзв. Feistel структуре које се користе у многим алгоритмима, између осталог и у Kuznyechik алгоритму који је предмет мастер тезе.

Треће поглавље садржи опис Kuznyechik алгоритма за шифровање симетричним кључем. Објашњене су све појединачне функције алгоритма при чему су наведене и њихове одговарајуће математичке дефиниције.

Четврто поглавље даје кратак преглед VHDL језика и листу популарних симулатора хардверског дизајна.

Пето поглавље садржи опис хардверске имплементације Kuznyechik алгоритма. Описана је архитектура дизајна с објашњењем како је постигнута минимална потрошња ресурса. Описани су и сви саставни делови, односно компоненте реализованог дизајна. При томе су приказани и програмски кодови компоненти.

У шестом поглављу је описана симулација дизајна која је коришћена за верификацију исправности рада урађене имплементације. За проверу су коришћени тест вектори из одговарајуће RFC препоруке. На крају су приказани резултати анализе и синтезе дизајна који потврђују да реализовани дизајн троши веома мале хардверске ресурсе.

Седмо поглавље резимира резултате тезе са датим смерницама потенцијалне даље оптимизације имплементације, а потом су дати списак коришћених референци и списак скраћеница.

4. Анализа рада са кључним резултатима

Мастер рад Анастасие Зеринski, дипл. инж. Електротехнике и рачунарства, се бави реализацијом Kuznyechik алгоритма за шифровање симетричним кључем која троши минималне хардверске ресурсе. Кључни доприноси рада кандидата на тези су следећи:

1) дато детаљно објашњење свих делова Kuznyechik алгоритма;
2) реализована имплементација Kuznyechik алгоритма која троши минималне хардверске ресурсе;
3) реализована имплементација је портабилна тј. може се користити на програмабилним чиповима различитих произвођача.

5. Закључак и предлог

Кандидат Анастасиа Зеринski, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовала Kuznyechik алгоритам за шифровање симетричним кључем. Анастасиа је показала да може брзо да савлада спецификације једног алгоритма за шифровање и да потом реализује имплементацију самог алгоритма. Предложено решење се може користити за потребе шифровања података у уређајима ограничених ресурса. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Анастасие Зеринski, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 12.09.2023. године

Чланови комисије:

др Зоран Чича, ред. професор

др Дејан Драјић, ред. професор