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 Тијане Пешић, дипл. инж. Електротехнике и рачунарства, под насловом „Пајплајн имплементација Серпент алгоритма за шифровање". Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Тијана Пешић је рођена 23.05.1997. године у Јагодини. Завршила је основну школу „17. октобар" у Јагодини као вуковац. Уписала је гимназију „Светозар Марковић" у Јагодини коју је завршила са одличним успехом. Електротехнички факултет уписала је 2015. године. Дипломирала је на одсеку за Телекомуникације и информационе технологије 2020. године са просечном оценом 7,74. Дипломски рад одбранила је у септембру 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за информационо комуникационе технологије уписала је у октобру 2020. године. Положила је све испите са просечном оценом 8,60.

2. Извештај о студијском истраживачком раду

Кандидат Тијана Пешић је у склопу припреме за израду мастер тезе проучила адекватну литературу из области криптографије и алгоритама шифровања са симетричним кључем. Након тога се упознала са спецификацијом Серпент алгоритма за шифровање симетричним кључем. Осмислила је пајплајн архитектуру Серпент алгоритма која има за циљ остваривање максималног протока шифорвања података. Након обављеног студијског истраживачког рада, Тијана је приступила изради мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 41 страну (12 страна прилога), с укупно 16 слика и 9 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), списак коришћене литературе, списак скраћеница, списак слика и прилог.

Предмет рада је хардверска имплементација Серпент алгоритма за шифровање симетричним кључем. Циљ рада је креирање имплементације алгоритма која остварује максимални проток шифровања што је остварено употребом пајплајн технике. Коришћен је Verilog језик за опис хардвера. Коришћено развојно окружење је ISE компаније Xilinx.

У уводном поглављу је наведен значај сигурности и заштите информација и комуникације, а наведено је и да битну улогу у томе играју алгоритми шифровања. Потом су наведени предмет и циљ тезе, да би на крају био дат преглед остатка рада по поглављима.

Друго поглавље даје основне информације о криптографији. Такође су наведене и објашњене две класе алгоритама за шифровање: симетрични и асиметрични алгоритми.

Треће поглавље садржи опис Серпент алгоритма за шифровање симетричним кључем. Објашњене су све појединачне функције алгоритма, како дела за шифровање података, тако и дела за развој кључева рунди од оригиналног кључа. При томе су приложене илустрације у виду блок-шема за поједине функционалности.

Четврто поглавље даје осврт на пајплајн архитектуру и њена својства, при чему је изложена и пајплајн архитектура за Серпент алгоритам у виду блок шеме са адекватним објашњењима.

Пето поглавље садржи опис хардверске имплементације Серпент алгоритма. Описани су сви реализовани модули у оквиру дизајна. При томе су приказани и делови програмских кодова модула ради бољег објашњења.

У шестом поглављу је описана симулација дизајна која је коришћена за верификацију исправности урађене имплементације. За проверу су коришћени одговарајући тест вектори. На крају је дат преглед потрошње ресурса реализованог дизајна као и прорачун протока шифровања.

Седмо поглавље сумира резултате тезе, а дата је и смерница за потенцијално даље убрзање дизајна. Потом су дати списак коришћених референци, списак скраћеница, списак слика, као и прилог са комплетним програмским кодом и вредностима коришћених тест вектора.

4. Анализа рада са кључним резултатима

Мастер рад Тијане Пешић, дипл. инж. Електротехнике и рачунарства, се бави реализацијом Серпент алгоритма за шифровање симетричним кључем који остварује максимални проток шифровања података. Кључни доприноси рада кандидата на тези су следећи:

1) дато детаљно објашњење свих делова Серпент алгоритма;
2) реализована пајплајн имплементација Серпент алгоритма која остварује веома висок проток шифровања;
3) реализована имплементација је портабилна тј. може се користити на програмабилним чиповима различитих произвођача.

5. Закључак и предлог

Кандидат Тијана Пешић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовала Серпент алгоритам за шифровање симетричним кључем. Тијана је показала способност осмишљавања архитектуре дизајна и потом њене ефикасне реализације при чему су остварени веома високи протоци шифровања. Предложено решење се може користити за потребе шифровања података на великим брзинама у мрежним уређајима. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Тијане Пешић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 13.09.2023. године

Чланови комисије:

др Зоран Чича, ред. професор

др Дејан Драјић, ред. професор