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 07.06.2016. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Немање Миљковића под насловом „Имплементација физичког модела протокола квантне дистрибуције кључа у оптичким комуникационим системима". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Немања Миљковић је рођен 23.03.1992. године у Ћуприји. Гимназију је завршио у Параћину са одличним успехом. Електротехнички факултет у Београду уписао је 2011. године, на смеру за Електротехнику и рачунарство. Дипломирао је у септембру 2015. године, на модулу Наноелектроника, оптоелектроника и ласерска техника са просечном оценом на испитима 8,39, на дипломском 10. Мастер студије на Електротехничком факултету у Београду је уписао новембра 2015. на Модулу за Наноелектронику и фотонику. Положио је све испите са просечном оценом 10.

2. Опис мастер рада

Мастер рад обухвата 35 страна, са укупно 12 слика, 1 табелу и 28 референци. Рад садржи увод, 6 поглавља и закључак (укупно 8 поглавља) као и списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљене су основе области и конкретна проблематика којом се рад бави, дат је преглед рада и основна очекивања од истог.

У другом поглављу је дат детаљнији увод у саму област којом се рад бави, о теоријским аспектима ове области као и о тренутном стању саме области у свету. Указано је на проблеме који се јављају у области а чијим се решавањем овај рад бави.

У трећем поглављу представљене су основе функционисања софтверског алата OptiSysetem у коме је извршена симулација модела аутентикационе шеме који је предложен у овом раду.

Четврто поглавље садржи све теоријске аспекте неопходне за разумеванје самог проблема аутентикације Б92 протокола и даје увид и досадашње предлоге физичких модела за реализацију сигурног аутентикационог протокола, који је овде такође објашњен. У овом поглављу је дата и теоријска позадина и преносна карактеристика ДДМЗМ модулатора који је главна компонента предложеног аутентикационог модела.

У оквиру петог поглавља је описана физичка аутентикациона шема и дат је опис на који начин се овим моделом врши аутентикација и синхронизација. У овом поглављу дато је и извођење преносне карактеристике предложеног модела ради лакшег разумевања на који начин се аутентикација врши применом овог модела.

У шестом поглављу дат је опис симулираног модела аутентикационе шеме и опис функције компоненти у моделу. У овом делу је објашњено на који начин се предложена шема симулира као и на који начин постоји аналогија симулационог модела са предложеним моделом. На крају су приказани и дусковани резултати симулације за различите улазне параметре.

Седмо поглавље даје предлоге даљег унапређења предложене шеме са аспекта бољих перформанси и повећања сигурности али и са аспекта веће функционалности.

У осмом поглављу дат је преглед свега што је рад обухватио као и преглед главних закључака када су у питању перформансе предложене шеме, резултати симулације и наредни кораци у развоју модела.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Немање Миљковића се бави проблематиком аутентикације Б92 протокола дистрибуције квантног кључа. Рад даје предлог новог физичког модела, односно нелинеарног оптичког система, који врши аутентикацију Б92 протокола ослањајући се и остајући у базису предложеног сигурног аутентикационог протокола.

Са освртом на досадашње реализације применом синхронизованих хаотичних оптичких система, овај рад даје идејни предлог физичке шеме која додатним улазним параметрима повећава сигурност и интегритет аутентикационог процеса. Са друге стране предложени систем остаје у базису дефинисаног сигурног аутентикационог протокола и самим поступком аутентикације одржава аналогију са истим. Аутентикација се врши у више корака где се, од стране пошиљаоца, прво шаље јавни кључ у облику напона на једном од модулатора и фактора фазног помераја поларизационе компоненте. Након тога се у оба система применом пропратне електронике рачуна напон другог модулатора, са нагласком да излаз остаје у базису аутентикационог протокола, и шаље назад пошиљаоцу, од стране примаоца. У последњем кораку излазни сигнали добијени применом ових улазних параметара се пореде и уколико су аналогни аутентикација се проглашава успешном. Битно је нагласити да је вредност једног од напона унешена од стране пошиљаоца док се фазни фактор генерише произвољно од стране пропратне електронике, што даје систему додатну сигурност.

Основни доприноси рада су: 1) предлог новог физичког модела за аутентикацију Б92 протокола дистрибуције квантног кључа који је у аналогији са предложеним сигурним аутентикационим протоколом; 2) детаљан опис начина аутентикације применом овог система и потврда начина функционисања предложене шеме помоћу OptiSystem симулације; 3) могућност наставка рада на развоју овог модела ради остваривања бољих перформанси и веће функционалности симулацијом модела који обухвата аутентикацију и Б92 и ББ84 протокола дистрибуције квантног кључа.

4. Закључак и предлог

Кандидат Немања Миљковић је у свом мастер раду обрадио једну веома актуелну тему аутентикације приликом диструбуције квантног кључа која омогућава практично потпуну сигурност тј. непробојну енкрипцију преноса података у комуникационим системима. Предложио је нов физички модел кола за његову реализацију и потврдио његову исправност симулацијама.

Кандидат је показао самосталност и привржености раду, а посебно самоиницијативност у формулацији и разради постављених проблема.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Немање Миљковић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 30.08.2016. године

Чланови комисије:

Др Петар Матавуљ, редовни професор

Др Марко Барјактаровић, доцент