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 10.5.2022. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Алексе Новаковића под насловом „Анализа пост-квантних асиметричних криптографских алгоритама“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Алекса Новаковић је рођен 22.10.1998. године у Приштини. Завршио је основну школу „Љуба Ненадовић” у Београду, као носилац Вукове дипломе. Уписао је средњу електротехничку школу „Никола Тесла“ у Београду, коју је завршио са одличним успехом, као носилац Вукове дипломе. Електротехнички факултет у Београду је уписао 2017. године. Дипломирао је на одсеку за рачунарску технику и информатику 2021. године са просечном оценом 8,60. Дипломски рад под називом „Дизајн и имплементација интерактивне апликације за визуелни приказ DDoS напада“ одбранио је у септембру 2021. године са оценом 10. Мастер академске студије на Електротехничком факултету у Београду је уписао октобра 2021. године, на модулу за софтверско инжењерство. Положио је све испите на мастеру са просечном оценом 9,80.

2. Извештај о студијском истраживачком раду

Кандидат Алекса Новаковић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на историју и развој асиметричне криптографије, тренутно стандардне асиметричне алгоритме који се користе за размену кључева, као и пост-квантне алгоритме финалисте треће рунде у оквиру *NIST*-овог процеса стандардизације пост-квантне криптографије из категорије алгоритама за размену кључева. За имплементацију апликације која врши анализу и поређење перформанси и меморијских захтева класичних и пост-квантних алгоритама са различитим сетовима параметара истражио је библиотеке отвореног кода *Crypto++* за класичне алгоритме и *liboqs* за пост-квантне алгоритме. Анализиран је концепт квантних рачунара и *Shor*-овог алгоритма који се користи за разбијање сигурности тренутно стандардних алгоритама за размену кључева. Детаљно је анализиран сваки алгоритам чије је тестирање имплементирано у оквиру апликације.

3. Опис мастер рада

Мастер рад обухвата 63 стране, са укупно 11 слика, 16 табела и 51 референцом. Рад садржи увод, 6 поглавља и закључак (укупно 8 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и прилог.

Прво поглавље представља увод у коме је представљен значај асиметричне криптографије и њена примена у великом броју протокола и система. Наведени су мотиви и циљ мастер рада.

У другом поглављу је описан проблем размене кључева симетричних алгоритама, који представља једну од основних намена асиметричне криптографије.

У трећем поглављу представљене су теоријске основе асиметричне криптографије.

У четвртом поглављу дат је преглед стандардних и тренутно коришћених асиметричних алгоритама (*RSA*, алгоритми размене кључева засновани на *Diffie-Hellman* алгоритму, алгоритми засновани на елиптичним кривама).

У петом поглављу је дат увид у принципе функционисања квантних рачунара и Шоровог алгоритма за факторизацију бројева у полиномијалном времену.

У оквиру шестог поглавља је дата анализа изабраних пост-квантних алгоритама - финалиста треће фазе *NIST*-овог процеса стандардизације пост-квантне криптографије (*Classic McEliece*, *CRYSTALS-Kyber*, *NTRU* и *Saber*).

Седмо поглавље описује апликацију за поређење перформанси између различитих стандардних и пост-квантних асиметричних алгоритама и њихових различитих сетова параметара и приказује добијене резултате.

У оквиру осмог поглавља дат је закључак о развоју пост-квантне криптографије и квантних рачунара и видови унапређења апликације.

У прилогу је дат увод у математику решетки, која представља основу многих алгоритама пост-квантне криптографије.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Алексе Новаковића се бави анализом стандардних и пост-квантних асиметричних алгоритама за размену кључева и поређењем њихових перформанси и меморијских захтева, за већи број различитих сетова параметара. Успешно је реализована апликација која извршава поменута поређења и тестирања алгоритама, у оквиру *C++* програмског језика.

Основни доприноси рада су: 1) анализа пост-квантних асиметричних алгоритама кандидата за стандардизацију и математичких основа њихове сигурности; 2) имплементација апликације за тестирање перформанси и меморијских захтева стандардних и пост-квантних алгоритама са различитим сетовима параметара; 3) анализа и приказ добијених резултата рада апликације; 4) анализа тренутно коришћених стандардних асиметричних алгоритама и њихових слабости на нападе квантних рачунара.

5. Закључак и предлог

Кандидат Алекса Новаковић је у свом мастер раду успешно анализирао пост-квантне алгоритме и поредио њихове брзине рада и меморијске захтеве у односу на тренутно стандардне асиметричне алгоритме. Кандидат је исказао самосталност и систематичност у свом поступку, као и иновативне елементе у решавању проблематике овог рада.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Алексе Новаковића под насловом „Анализа пост-квантних асиметричних криптографских алгоритама“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 08.09.2022. године

Чланови комисије:

_____

др Павле Вулетић, ванредни професор

_____

др Жарко Станисављевић, ванредни професор